



**Universidad**  
Zaragoza

# Trabajo Fin de Grado

## Plataformas de enrutamiento alternativas

Autor

Agustín Martín Arranz

Director/es

Director académico: D. Francisco Javier Luzón Marco

Director militar: Cap. D. Alfonso Bravo Ruiz

Centro Universitario de la Defensa-Academia General Militar

Año 2016

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

## **AGRADECIMIENTOS**

*A mi pareja, familia y amigos, por todo el apoyo mostrado durante estos años de duro trabajo.*

*Quiero hacer una especial mención al Teniente de Transmisiones D. Xavier Guerrero Fernández, sin cuyos conocimientos y guía habría sido imposible elaborar este TFG, al Capitán de Transmisiones D. Alfonso Bravo Ruiz, por las facilidades dadas en cuanto al acceso sin límites al material requerido para las pruebas realizadas y, en general, a todo el personal de la Compañía de Centros Nodales del BTI/1 por todo el apoyo y predisposición mostrada. También quiero mostrar mi más sincero agradecimiento al profesor D. Francisco Javier Luzón Marco, por el interés mostrado y el seguimiento y asesoramiento en la elaboración de este trabajo de fin de grado.*



## RESUMEN

El objetivo principal de este trabajo ha sido realizar una comparativa entre los equipos de enrutamiento existentes actualmente en el inventario del Ejército de Tierra y los software de enrutamiento libres Quagga y Vyos.

Los dispositivos usados en la actualidad en el Ejército de Tierra son en su mayoría de la empresa Cisco Systems, ya que tienen unas posibilidades de explotación, seguridad y funcionalidades muy superiores a los de cualquier otra casa. Sin embargo, dichos dispositivos tienen un coste muy elevado, tanto por su adquisición como por la formación necesaria para el personal encargado de su manejo, control y configuración.

Es por ello que es necesario la búsqueda de sistemas alternativos de enrutamiento con el objetivo de reducir costes en este tipo de dispositivos, quizá no para una sustitución total de los equipos Cisco, sino más bien para complementarlos con sistemas más económicos. Para ello, en este proyecto se han analizado los software de enrutamiento Quagga y Vyos, capaces de funcionar en sistemas operativos libres basados en Unix, que pueden ser instalados en dispositivos de enrutamiento de bajo coste, incluidos una amplia gama de routers domésticos, así como en máquinas virtuales.

## ABSTRACT

The main objective of this project has been to carry out a comparative study between the current routing equipment that the Spanish Army has in its inventories and the free routing software packages Quagga and Vyos.

The current devices used by Spanish Army are most of them from Cisco Systems enterprise, that, although they have very superior exploitation possibilities, security and functionalities than devices from other brands, their acquisition has a very high cost, same as the formation required for the personnel in charge of management, control and configuration of the routers.

Because of that it is necessary to find alternative routing systems with the objective of decreasing the cost of this kind of devices, maybe not for a total substitution of the Cisco equipment, but rather to complement them with more economic systems. In order to do that, this project has analyzed the Quagga and Vyos software packages, which are able to work with Unix based operative systems installed on low cost routing devices, included a wide range of home routers, and also in virtual machines.

# PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

## ÍNDICE

AGRADECIMIENTOS .....	iii
RESUMEN .....	v
ÍNDICE .....	vii
ÍNDICE DE FIGURAS .....	viii
ÍNDICE DE TABLAS .....	ix
ABREVIATURAS .....	x
1 Introducción .....	1
1.1 Objetivos del TFG .....	2
1.2 Ámbito de aplicación .....	3
1.3 Estructura de la memoria .....	3
2 Descripción y análisis de los sistemas a comparar .....	5
2.1 Cisco Systems .....	6
2.1.1 Routers Cisco en los CTPC,s .....	6
2.1.2 Entorno de configuración: IOS Cisco .....	7
2.2 Quagga .....	7
2.2.1 Plataforma de pruebas Quagga .....	8
2.2.2 Entorno de configuración de Quagga: vtysh .....	9
2.3 Vynos .....	10
2.3.1 Plataforma de pruebas Vynos .....	10
2.3.2 Entorno de configuración Vynos .....	11
3 Diseño e implementación de pruebas .....	13
3.1 Diseño y topología general de las pruebas .....	13
3.2 Escenarios de pruebas .....	16
3.3 Establecimiento del entorno e implementación de pruebas para el sistema Cisco .....	16
3.4 Establecimiento del entorno e implementación de pruebas para el sistema Quagga .....	18
3.5 Establecimiento del entorno e implementación de pruebas para el sistema Vynos .....	19
4 Resultados de pruebas .....	21
4.1 Resultados Cisco .....	21
4.2 Resultados Quagga .....	22
4.3 Resultados Vynos .....	24
5 Impacto económico y comparativa .....	27
5.1 Análisis económico .....	27
5.2 Comparativa funcional .....	28

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

5.3	Matriz de decisión .....	29
6	Conclusiones .....	31
7	Bibliografía.....	33
	Anexo A: Características Técnicas de los routers Cisco 2821 .....	35
	Anexo B: Características TP-Link modelo TL-WR1043ND .....	37
	Anexo C: Inyector de paquetes Ostinato.....	39
	Anexo D: Tablas de enrutamiento y configuración de interfaces de los router Cisco .....	43
	Anexo E: Comandos introducidos en el entorno de configuración de R1 .....	47
	Anexo F: Documentación gráfica de las pruebas Cisco.....	53
	Anexo G Configuración de interfaces en OpenWrt .....	55
	Anexo H: Herramienta Realtek Ethernet Diagnostic Utility.....	57
	Anexo I: Tablas de enrutamiento de Quagga.....	59
	Anexo J: Configuración de interfaces Vynos.....	61
	Anexo K: Comandos de configuración de los routers Vynos .....	63

## ÍNDICE DE FIGURAS

Figura 1-1:	Logotipos de los sistemas comparados.....	1
Figura 1-2:	Ejemplo de interconexión entre dos CTPC,s de entidad Brigada .....	2
Figura 2-1:	Ejemplo de modelo de capas OSI .....	5
Figura 2-2:	Detalle de los slots de expansión de un Cisco 2821 y tarjeta WIC instalable.....	7
Figura 2-3:	Vista frontal y trasera del Cisco TP-LINK TL-WR1043ND. ....	8
Figura 2-4:	CLI de Quagga mediante conexión Telnet a través de la aplicación PuTTY .....	9
Figura 2-5:	CLI de Vynos mediante conexión Telnet a través de la aplicación PuTTY.....	11
Figura 3-1:	Esquema general de la red de pruebas.....	13
Figura 3-2:	Interfaz de configuración de red de la máquina Lubuntu 3 .....	15
Figura 3-3:	Topología de pruebas Cisco .....	16
Figura 3-4:	Detalle de conexiones virtuales y físicas realizadas.....	17
Figura 3-5:	Esquema de conexiones virtuales y físicas de Quagga.....	19
Figura 3-6:	Topología general de pruebas con Vynos .....	20
Figura 3-7:	Esquema detallado de conexiones físicas y virtuales del Vynos R1.....	20
Figura 4-1:	Traza de ruta desde Lubuntu 1 a Lubuntu 5.....	21
Figura 4-2:	Traza de ruta con el enlace entre R1 y R3 cortado .....	21
Figura 4-3:	Tráfico de red de la interfaz física anfitriona y de la interfaz virtual VOIP.....	22
Figura 4-4:	Tabla de enrutamiento de R1 antes de suprimir el enlace.....	22
Figura 4-5:	Tabla de enrutamiento de R1 después de suprimir el enlace .....	23
Figura 4-6:	Traza de ruta antes del corte .....	23
Figura 4-7:	Traza de ruta después del corte .....	23
Figura 4-8:	Traza de ruta desde Lubuntu 1 a Lubuntu 5 antes de anular el enlace .....	24
Figura 4-9:	Traza de ruta después de suprimir el enlace .....	24
Figura 4-10:	Tráfico de red en la interfaz de Lubuntu 5 saturando el enlace .....	25

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

Figura Anexo C - 1: Vista de la interfaz de inyección de paquetes Ostinato.....	39
Figura Anexo C - 2: Intefaz de configuración de streams .....	40
Figura Anexo C - 3: Interfaz de configuración de Stream en la pestaña de confi .....	40
Figura Anexo D - 1: Tabla de enrutamiento del router R1 .....	43
Figura Anexo D - 2: Configuración de interfaces del router R1.....	43
Figura Anexo D - 3: Tabla de enrutamiento del router R2 .....	44
Figura Anexo D - 4: Configuración de interfaces del router R2.....	45
Figura Anexo D - 4: Configuración de interfaces del router R2.....	45
Figura Anexo D - 5: Tabla de enrutamiento del router 3 .....	45
Figura Anexo D - 6: Configuración de interfaces del router R3.....	46
Figura Anexo E - 1: Vista de la CLI en modo privilegiado a mediante la aplicación Hyperterminal ....	47
Figura Anexo F - 1: Nodo R1 .....	53
Figura Anexo F - 2: Nodos R2 (izquierda) y R3 (derecha).....	53
Figura Anexo F - 3: Detalle de las conexiones Ethernet y serial WIC del router R1 .....	54
Figura Anexo F - 5: Estación satélite 'Asturias' utilizada en las pruebas .....	54
Figura Anexo F - 4: Pareja de antenas Ubiquiti utilizadas para el enlace entre R1 y R3.....	54
Figura Anexo G - 1: Configuración de puertos del router TP-Link mediante interfaz web .....	55
Figura Anexo G - 2: Detalle de configuración de interfaces en OpenWrt mediante interfaz web .....	56
Figura Anexo H - 1: Interfaz de configuración Realtek Ethernet Diagnostics Utility.....	57
Figura Anexo H - 2: Interfaces subinterfaces virtuales de red de la NIC física .....	57
Figura Anexo I - 1: Tabla de enrutamiento del router R1 .....	59
Figura Anexo I - 2: Tabla de enrutamiento del Router R2.....	60
Figura Anexo I - 3: Tabla de enrutamiento del router R3 .....	60
Figura Anexo J - 1: Configuración de interfaces del router R1 .....	61
Figura Anexo J - 2: Configuración de interfaces del router R2 .....	61
Figura Anexo J - 3: Configuración de interfaces del router R3 .....	62

## ÍNDICE DE TABLAS

Tabla 3-1: Direcciones IP de las máquinas virtuales. ....	14
Tabla 5-1: Comparativa Económica de los sistemas .....	27
Tabla 5-2: Comparativa de sistemas .....	28
Tabla 5-3: Matriz de decisión .....	29
Tabla Anexo A - 1: Características Técnicas Cisco modelo 2821.....	35
Tabla Anexo E - 1: Configuración router Cisco R1 .....	47
Tabla Anexo K - 1: Configuración del router Vyos R1.....	63

## ABREVIATURAS

CCNA	Cisco Certified Network Associate
CIS	Communications and Information Systems
CLI	Command Line Interface
CTPC	Centro de Transmisiones de Puesto de Mando
ET	Ejército de Tierra
IOS	Internetworking Operating System
IP	Internet Protocol
LAN	Local Area Network
NIC	Network Interface Card
OSI	Open System Interconnection
QoS	Quality of Service
SIMACET	Sistema de Mando y Control del Ejército de Tierra
SSH	Secure Shell
TCP	Transmission Control Protocol
VLAN	Virtual Local Area Network
VOIP	Voice over Internet Protocol
VTC	Video Teleconferencia
WAN	Wide Area Network
WIC	Wan Interface Card
ZO	Zona de Operaciones

## 1 Introducción

Las empresas civiles utilizan habitualmente la infraestructura de empresas de telecomunicaciones para el envío y recepción de paquetes de datos a través de internet, lo cual es necesario para el uso de servicios tales como correo electrónico, navegación web, videoconferencia, etcétera. Este proceso de transmisión de datos es totalmente transparente para dichas empresas, siendo las operadoras las encargadas de proveerlas de un servicio de conexión a la red rápido, seguro y fiable. Estas empresas son las que gestionan los dispositivos intermedios, denominados routers, que permiten la interconexión entre dispositivos terminales siguiendo habitualmente el modelo *Open System Interconnection* (OSI) correspondiente al estándar ISO/IEC 7498-1. [1]

La evolución de los Sistemas de Información y Comunicaciones (CIS) en las últimas décadas utilizados por el Ejército de Tierra (ET) español ha tenido como principal efecto la aparición de estas mismas necesidades en cuanto al uso de servicios que requieren transferencia de paquetes de datos. No obstante, los distintos CIS con los que trabaja el ET no pueden realizar transmisiones de datos a través de operadoras civiles debido a la naturaleza confidencial de la información transmitida y a la nula disponibilidad de una infraestructura de comunicación civil en una Zona de Operaciones (ZO). Es por esto que el ET gestiona sus propios nodos de enrutamiento, siendo los dispositivos de la empresa Cisco Systems los más utilizados en sus CIS. Estos routers tienen las posibilidades de explotación y configuración superiores a las de cualquier dispositivo de cualquier otro fabricante. No obstante, su coste es muy elevado y su operación requiere de una formación certificada por la propia empresa Cisco, lo que también conlleva un coste.

Con unos presupuestos de defensa cada vez más ajustados, se hace necesaria la búsqueda de posibles alternativas a estos dispositivos para un posible reemplazo de éstos en sistemas que no sean críticos. El paquete de software de enrutamiento Quagga [2] y la distribución basada en Linux "VyOS" [3] pueden dar solución a esta necesidad ya que ambos son gratuitos y basados en código libre. Estos sistemas pueden ser instalados tanto en PC,s convencionales o máquinas virtuales en el caso de VyOS, como en routers domésticos en el caso de Quagga, teniendo ambos productos un coste muy inferior a los de la casa Cisco [4]. Además, los entornos de configuración de Quagga y VyOS son muy similares a la interfaz de línea de comandos (CLI) que usa el sistema operativo IOS de Cisco, con lo que no sería necesaria una formación adicional del personal, salvo unas mínimas nociones en cuanto a las limitaciones que tienen estos software.

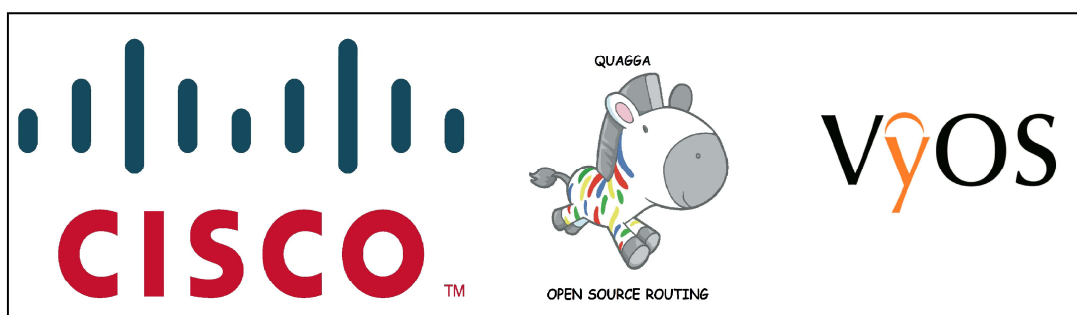


Figura 1-1: Logotipos de los sistemas comparados

## 1.1 Objetivos del TFG

Este TFG tiene como principal objetivo determinar las ventajas e inconvenientes que conllevaría la implementación de los software Quagga y Vyos como plataformas de enrutamiento contrastando sus capacidades y características con las de los routers de la casa Cisco.

Para considerar estos sistemas como una alternativa viable deberían cumplir unas exigencias mínimas de capacidad y rendimiento para dar servicio a un puesto de mando de campaña de entidad brigada o superior. Por lo tanto, atendiendo a estas necesidades, se deberá comprobar que se cumplen los siguientes requisitos mínimos:

- Capacidad mínima de transmisión: 6 Mb/s
- Interfaces de conexión: Ethernet
- Nº mínimo de interfaces: 4
- Compatibilidad con estándar TCP/IP
- Protocolos de acceso remoto: SSH<sup>1</sup>, Telnet<sup>2</sup>
- Protocolos de administración: SNMP
- Gestión de calidad de servicio: QoS
- Protocolos de enrutamiento: RIP v2<sup>3</sup>, OSPF<sup>4</sup>
- Traducción de direcciones mediante NAT
- Protocolo de establecimiento de túneles GRE

En vista a futuras aplicaciones sería también conveniente que soportaran gestión de rutas mediante route-maps y gestión de rutas por defecto mediante protocolo FHRP cuando se implementen varias puertas de enlace (gateways) sobre el mismo router, lo que se conoce como protocolo de redundancia. [4] [5]

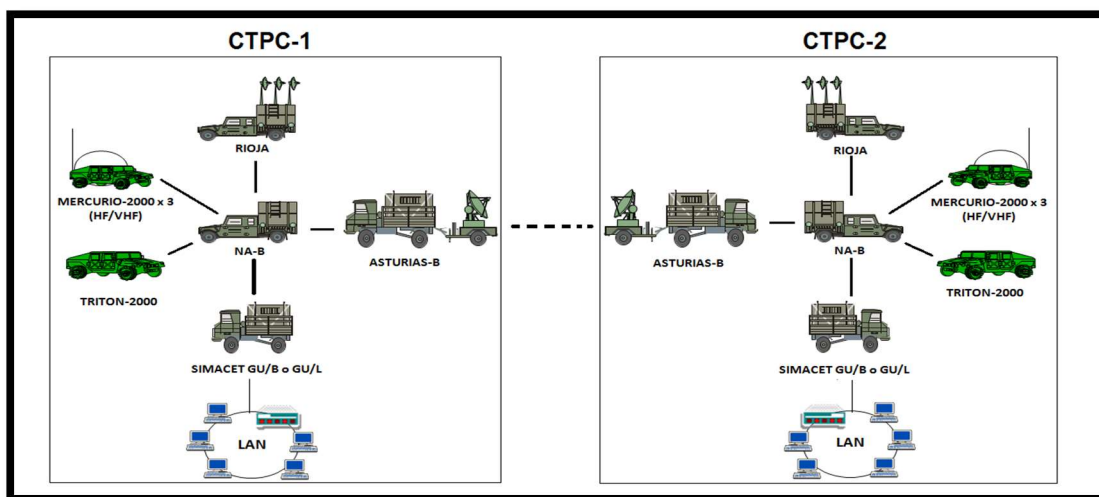


Figura 1-2: Ejemplo de interconexión entre dos CTPC,s de entidad Brigada

1 Ssh: Protocolo de red que permite conexión remota segura a una máquina en red. Puede considerarse como una versión cifrada de Telnet.

2 Telnet: Protocolo de red que permite la conexión remota no segura a una máquina desde otro punto de una red informática.

3 RIP v2: Protocolo de enrutamiento dinámico basado en un algoritmo de vector distancia. Es la segunda versión del protocolo RIP y tiene la particularidad de admitir enrutamiento de redes sin clase

4 OSPF: Protocolo de enrutamiento dinámico por estado de enlace.

Cabe destacar que las especificaciones de velocidad de transmisión vienen dadas por las capacidades del sistema de comunicación más limitado. Para la interconexión entre Centros de Transmisiones de Puestos de Mando (CTPC,s) este sistema es el satélite, cuya estación tiene una capacidad máxima de transmisión de 6 Mb/s. Para la conexión por radioenlaces, mediante la estación de radio VHF "Rioja", la capacidad máxima de transmisión es de 1Mb/s. En la práctica, los routers ya cuentan con una velocidad por interfaz de 100Mb/s, lo que supera con creces los requisitos exigidos. En la figura 1.2 se muestra una topología típica de interconexión entre dos puestos de mando con los tipos de enlace mencionados. [6]

### **1.2   Ámbito de aplicación**

Determinando la idoneidad de Quagga y Vyos y contrastando sus capacidades con las de un equipo Cisco, su uso podría generalizarse en los CIS del ET, como complemento a los actualmente en funcionamiento o incluso reemplazándolos. Esto supondría un ahorro sustancial en la adquisición de nuevos dispositivos y no sería necesaria una formación complementaria para el personal encargado de administrar los routers por su similitud con los routers Cisco actuales.

### **1.3   Estructura de la memoria**

La memoria de este TFG tiene la siguiente estructura. En primer lugar se da una visión general de los sistemas de enrutamiento comparados, tanto de los propios sistemas como de las plataformas (hardware) sobre las que se han ejecutado las pruebas y los entornos de configuración de cada uno de los sistemas. En segundo lugar se describe el diseño y la implementación de los entornos en los que se han realizado las pruebas. Se sigue con los resultados obtenidos de realizar una serie de pruebas de rendimiento y funcionalidad. Se continúa con un análisis del impacto económico de la posible adopción de los nuevos sistemas, una comparativa funcional y una matriz de decisión. Por último se exponen las conclusiones finales en base a los resultados del análisis realizado.

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

## 2 Descripción y análisis de los sistemas a comparar

Antes de empezar a describir los sistemas que se utilizarán en la comparativa, conviene tener unas nociones básicas acerca de las funciones que tiene un router en general.

Un router es un dispositivo intermedio que conecta redes de datos, trabajando en la capa de Red del modelo OSI (ver figura 2-1). [1] [5]

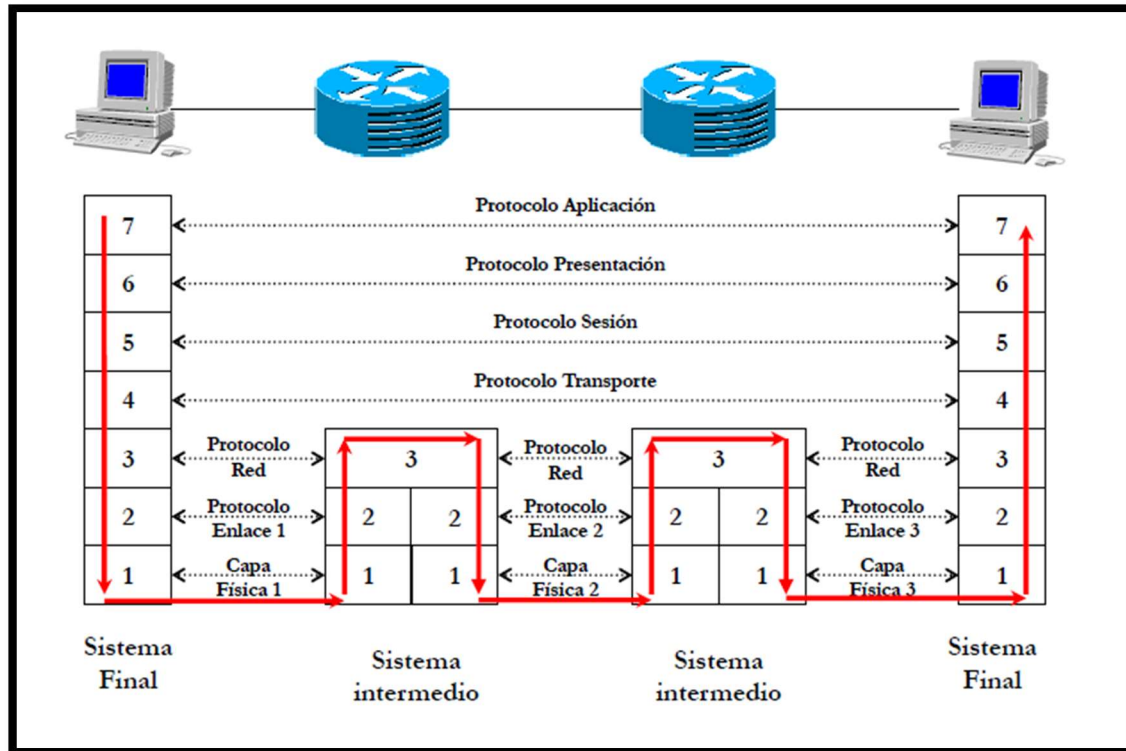


Figura 2-1: Ejemplo de modelo de capas OSI

Su hardware básico lo conforman los siguientes elementos:

- Fuente de alimentación
- Interfaces
- Procesador
- Puertos de administración
- Memorias (volátiles, no volátiles, ROM, etc.)

En el entorno Cisco, el sistema operativo que se ejecuta en estos dispositivos se denomina *Internetworking Operative System (IOS)*. Este software se encarga entre otras cosas del encaminamiento de paquetes a nivel de red OSI, confección de tablas de encaminamiento o registro de tráfico de paquetes.

Para el acceso a la configuración de este particular tipo de ordenador no se dispone en general ni de teclado ni de un monitor. Es necesario conectar un ordenador de forma directa a uno de los puertos de administración o bien realizar la conexión de forma remota a través de la propia red, siempre y cuando esta función esté permitida por la configuración del router.

En general, para la configuración de un router se tienen que dar los siguientes pasos:

- Establecimiento de medidas de seguridad (contraseñas, usuarios permitidos, modos de acceso, etc.)
- Configuración de interfaces.

- Configuración de rutas estáticas
- Configuración de protocolos de enrutamiento dinámico

El fin último de un router es encaminar paquetes recibidos por la interfaz específica que permita llegar al destino al que se dirige ese paquete, y para ello se tienen que establecer unas rutas de encaminamiento. Estas rutas pueden establecerse de forma manual o automática mediante el uso de protocolos de enrutamiento. En general se puede hablar de rutas estáticas, introducidas manualmente en la configuración del router, y de rutas dinámicas, en las que las rutas a redes remotas son descubiertas de forma automática por los protocolos de enrutamiento. La combinación de estos dos tipos de rutas conforma una tabla de enrutamiento que permite al router enviar los paquetes recibidos al destino requerido. [5]

Las rutas estáticas pueden a su vez subdividirse en dos: predeterminadas y por defecto. Las rutas predeterminadas encaminan directamente los paquetes por una interfaz específica hacia una red específica. En cambio, las rutas por defecto establecen una interfaz de salida por la que se envían paquetes de cuya red de destino se desconoce la localización. Se manda pues por la interfaz determinada hacia otro nodo que puede que sí sepa encaminar ese paquete hacia su destino. En cuanto a los protocolos de enrutamiento dinámico podemos destacar como más usados en las redes militares RIP, OSPF y BGP. No es objeto de este TFG profundizar en las diferencias y el funcionamiento de los distintos protocolos. A continuación se describen los distintos sistemas de enrutamiento a comparar. [5]

### 2.1 Cisco Systems

Cisco es la empresa líder en Tecnologías de Información y Comunicaciones. Desde su fundación en 1984 ha ido evolucionando y ganando prestigio gracias a un proceso constante de innovación e investigación en materia de telecomunicaciones y desarrollo de dispositivos y servicios orientados al establecimiento de redes de datos. Tanto es así, que un gran número de grandes empresas multinacionales e incluso instituciones gubernamentales de muchos países en todo el mundo confían sus servicios de comunicaciones a productos y dispositivos de esta compañía.

La actividad actual de Cisco Systems se centra sobre todo en la fabricación de equipos de enrutamiento y conmutadores de red, telefonía IP y almacenamiento en la "nube". Además desarrolla herramientas de gestión de red y de sistemas, ofrece servicios de mantenimiento y administración de infraestructuras y tiene una línea de programas dedicada a la formación de personal, que se certifica por niveles con unos estándares establecidos por la compañía. Esta formación está orientada a la gestión y administración de equipos Cisco, así como al diseño y desarrollo de infraestructuras de red. Ejemplos de los certificados más comunes son los programas *Cisco Certified Network Associate (CCNA)* y *Cisco Certified Network Professional*. [4]

#### 2.1.1 Routers Cisco en los CTPC,s

Actualmente los CTPC,s de entidad Brigada cuentan con routers del modelo 7200, ubicados en las estaciones SIMACET, las cuales dan múltiples servicios tales como mensajería electrónica, interfaz táctica de presentación de datos o intercambio de ficheros. Como el acceso a estos equipos está limitado por estar habitualmente comprometidos en la actividad diaria de las unidades, para la realización de las pruebas de rendimiento se ha utilizado el modelo 2821, cuyas especificaciones se detallan en el ANEXO A. En la tabla 1 de dicho anexo se muestran las diferencias entre el modelo 7200 utilizado habitualmente por las unidades y el modelo usado en las pruebas.

El hardware de los dispositivos Cisco siguen la arquitectura descrita en la introducción del presente punto, con la particularidad de que además disponen de ranuras o "slots" de expansión en los que se

pueden añadir y cambiar las interfaces de red, de forma que se puede trabajar con varios tipos de interfaces según los requerimientos de la red que se va a conectar al router. Las interfaces más comunes según las redes a conectar son Ethernet para la conexión de redes de área local (LAN) y WIC para las redes de área extensa o *Wide Area Network* (WAN). En la figura 2-2 se aprecia la parte trasera de un router Cisco 2821 con 4 slots de expansión, así como una tarjeta con interfaces WIC.

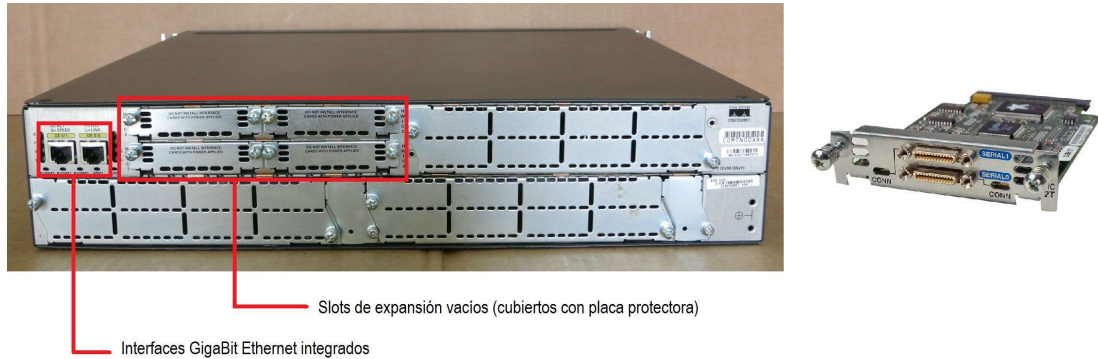


Figura 2-2: Detalle de los slots de expansión de un Cisco 2821 y tarjeta WIC instalable

### 2.1.2 Entorno de configuración: IOS Cisco

Para su configuración y control, el sistema operativo IOS integrado en el router dispone de una CLI, con posibilidad de acceso mediante conexión directa al router, acceso remoto mediante TELNET o SSH e incluso por interfaz Web. Mediante esta interfaz de línea de comandos se configuran entre otras cosas las políticas de seguridad de acceso a la configuración del router, las interfaces físicas de conexión y los protocolos de enrutamiento. También permite la realización de pruebas de conectividad. La versión del IOS del router modelo 2821 que se ha usado en las pruebas ha sido la 12.4.

## 2.2 Quagga

Quagga es un paquete de software de enrutamiento que es capaz de utilizar protocolos de encaminamiento basados en el estándar TCP/IP. Puede ser instalado en cualquier sistema operativo basado en UNIX, lo que le da gran flexibilidad y posibilidades de funcionar sobre múltiples plataformas, desde routers físicos hasta máquinas virtuales. [2]

Dentro de este paquete se incluyen los protocolos de enrutamiento, con la posibilidad de instalar solamente los necesarios acorde a las especificaciones de nuestra red. Estos protocolos funcionan como demonios<sup>5</sup> independientes dentro de Unix, los cuales se pueden dividir en dos tipos:

- Demonio de control de enrutamiento: Zebra
- Demonios de protocolos de enrutamiento: ripd, ripngd, ospf6d, bgpd, etc.

Zebra es el demonio que se encarga de la configuración de las interfaces físicas de la plataforma donde esté instalado Quagga, así como de actualizar las tablas de enrutamiento, establecimiento de bucles de interfaz y distribución de rutas entre diferentes protocolos. Establece pues la configuración base con la que los demonios de los protocolos de enrutamiento tendrán que operar más tarde.

---

<sup>5</sup> Demonio: Proceso ejecutado por el sistema operativo en segundo plano, no interactivo con el usuario.

Aunque los demonios de Quagga se pueden configurar de forma independiente, también se dispone de una herramienta incluida en el paquete que sirve para gestionar el sistema completo, como si se tratase del CLI del IOS Cisco. Esta herramienta se denomina *virtual teletype shell* o *vttysh*. [7]

### 2.2.1 Plataforma de pruebas Quagga

Para la realización de las pruebas se ha usado el router doméstico TP-Link modelo TL-WR1043ND [8]. Las especificaciones y capacidades de este dispositivo se detallan en el ANEXO B. TP-Link es una empresa dedicada al diseño y producción de dispositivos para redes Small Office/Home Office (SOHO). Sus principales productos están orientados a tecnologías de comunicación inalámbrica, ADSL, enrutamiento y conmutación, conversión de medios y adaptadores de red.

Para usar Quagga en un router de estas características se tiene que adaptar este dispositivo de forma que se pueda instalar este paquete. Es necesario por tanto la instalación de un sistema operativo basado en Unix, como si de un ordenador personal se tratase. El sistema más adecuado para este fin es OpenWrt [9], que es una distribución Linux para dispositivos integrados, la cual permite flexibilidad a la hora de instalar y modificar software de todo tipo, en lugar de tener un firmware estático, lo que es habitual en los dispositivos de enrutamiento comerciales. Se puede por tanto personalizar el uso del dispositivo, construyéndose el usuario su propio firmware según las necesidades que se tenga.

El procedimiento a seguir para usar Quagga en el router TP-Link incluirá los siguientes pasos:

- Descarga de la distribución OpenWrt de la página oficial.
- Actualización del firmware base a OpenWrt mediante la interfaz web de configuración incluida en el propio firmware.
- Gestionar las interfaces de red del router mediante la interfaz web de OpenWRT.
- Instalar el paquete de software Quagga.

Tal y como se aprecia en la figura 2-3 derecha, el TP-WR1043 dispone de 5 interfaces Gigabit Ethernet (hasta 1000 Mbits/s), de las cuales el router usa cuatro a priori para switching y una última para la conexión WAN<sup>6</sup>. Para hacer el router más funcional, una vez instalado OpenWrt se pueden separar las interfaces del router dedicadas a switching en VLAN<sup>7</sup>, de forma que se pueda utilizar cada interfaz para enrutamiento de forma independiente en lugar de formar parte todas de la misma LAN privada, tal y como vienen configuradas de fábrica. De esta forma se puede disponer de 5 interfaces configurables.

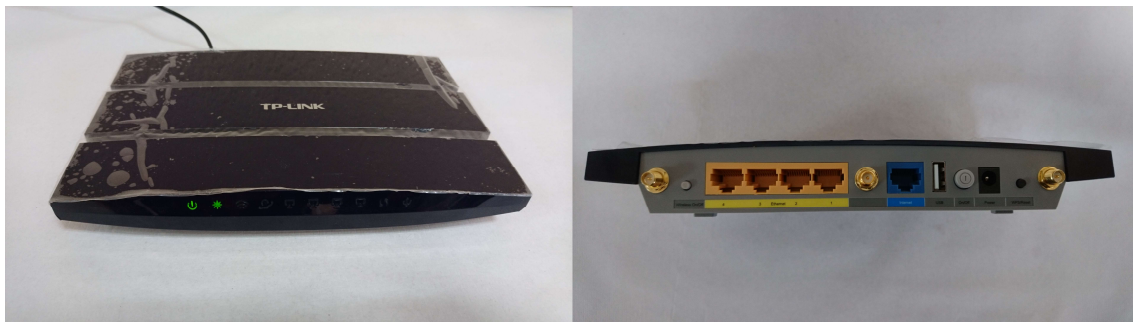


Figura 2-3: Vista frontal y trasera del Cisco TP-LINK TL-WR1043ND.

---

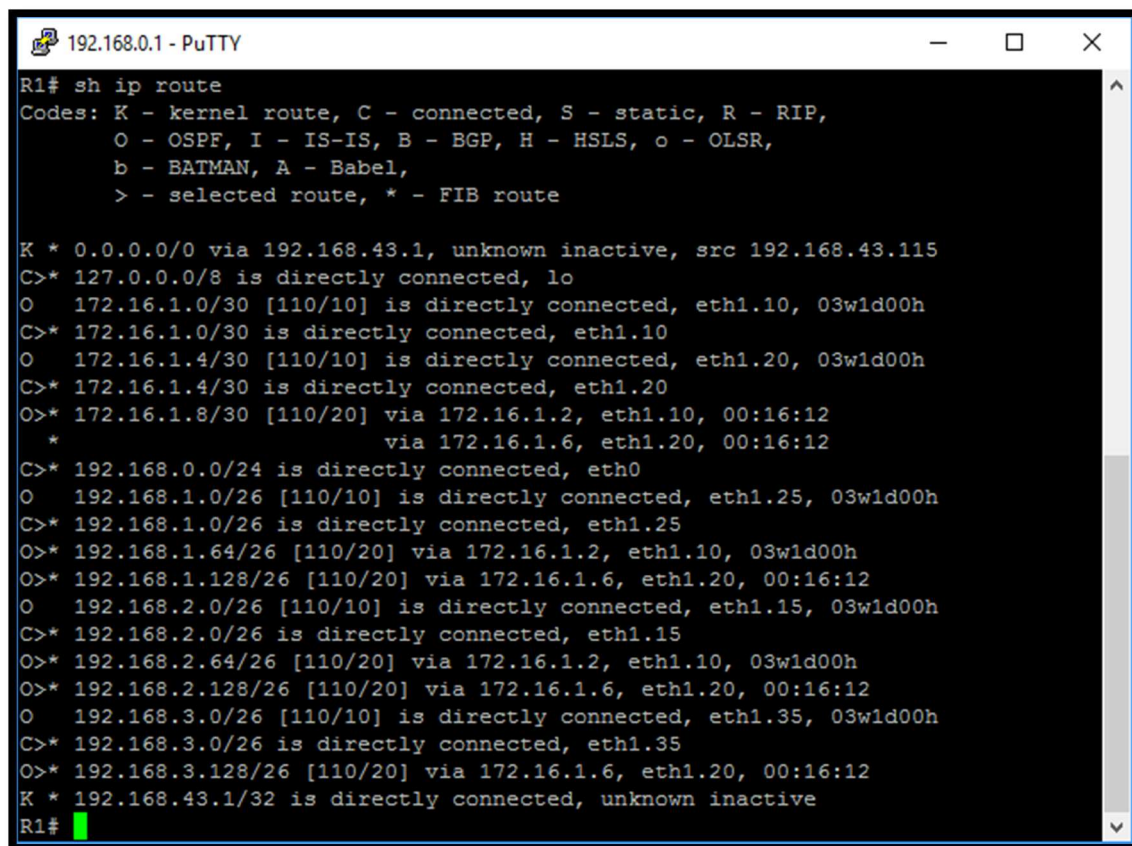
6 Wide Area Network (WAN): Hace referencia a una red que une múltiples redes de área local sin que éstas estén en una misma ubicación física.

7 Virtual Local Area Network (VLAN): Redes de área local que comparten la misma infraestructura de conmutación pero que operan de forma independiente. Son redes lógicas que se crean dentro de una red física.

## 2.2.2 Entorno de configuración de Quagga: vtysh

Una vez configuradas las interfaces mediante la interfaz web de OpenWrt y con Quagga instalado, se puede proceder a configurar el sistema para que realice funciones de enrutamiento, de la misma forma en que se haría en un router Cisco. No obstante no se accede directamente al software Quagga, ya que previamente ha de conectarse vía ssh al entorno de línea de comandos de OpenWrt. Una vez conectados al sistema operativo, simplemente ejecutando el comando *vttysh* se accede a la configuración del software Quagga.

El entorno de configuración (véase figura 2-4) es muy parecido a la CLI del IOS Cisco, con niveles de operación, configuración y comandos similares. Tal y como se indica en el manual de Quagga, dentro de *vttysh* se pueden distinguir 3 modos principales de operación: modo *view*, modo *enable* y modos de configuración. En el modo *view* sólo se pueden realizar operaciones de supervisión del estado actual del router, relacionadas con la situación de las interfaces y de la tabla de enrutamiento. Es el primer nivel, a través del cual se accede al modo *enable*. El modo *enable* permite, además de todas las acciones permitidas en el modo *view*, realizar operaciones de escritura, para poder guardar así la configuración del sistema de enrutamiento. A través de él se puede acceder a los distintos modos de configuración de interfaz y de protocolos contenidos, como ya se ha señalado, en cada demonio de control. [5] [7] [10]



```

192.168.0.1 - PuTTY
R1# sh ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, H - HSLs, o - OLSR,
       b - BATMAN, A - Babel,
       > - selected route, * - FIB route

K * 0.0.0.0/0 via 192.168.43.1, unknown inactive, src 192.168.43.115
C>* 127.0.0.0/8 is directly connected, lo
O  172.16.1.0/30 [110/10] is directly connected, eth1.10, 03w1d00h
C>* 172.16.1.0/30 is directly connected, eth1.10
O  172.16.1.4/30 [110/10] is directly connected, eth1.20, 03w1d00h
C>* 172.16.1.4/30 is directly connected, eth1.20
O>* 172.16.1.8/30 [110/20] via 172.16.1.2, eth1.10, 00:16:12
   * via 172.16.1.6, eth1.20, 00:16:12
C>* 192.168.0.0/24 is directly connected, eth0
O  192.168.1.0/26 [110/10] is directly connected, eth1.25, 03w1d00h
C>* 192.168.1.0/26 is directly connected, eth1.25
O>* 192.168.1.64/26 [110/20] via 172.16.1.2, eth1.10, 03w1d00h
O>* 192.168.1.128/26 [110/20] via 172.16.1.6, eth1.20, 00:16:12
O  192.168.2.0/26 [110/10] is directly connected, eth1.15, 03w1d00h
C>* 192.168.2.0/26 is directly connected, eth1.15
O>* 192.168.2.64/26 [110/20] via 172.16.1.2, eth1.10, 03w1d00h
O>* 192.168.2.128/26 [110/20] via 172.16.1.6, eth1.20, 00:16:12
O  192.168.3.0/26 [110/10] is directly connected, eth1.35, 03w1d00h
C>* 192.168.3.0/26 is directly connected, eth1.35
O>* 192.168.3.128/26 [110/20] via 172.16.1.6, eth1.20, 00:16:12
K * 192.168.43.1/32 is directly connected, unknown inactive
R1#

```

Figura 2-4: CLI de Quagga mediante conexión Telnet a través de la aplicación PuTTY

## 2.3 Vyos

Vyos es un software de enrutamiento libre desarrollado desde 2013 como una variante del sistema Vyatta, creado en 2005 por la empresa del mismo nombre. Vyatta era en origen un sistema operativo de enrutamiento libre, hasta que en 2012 la empresa Vyatta fue comprada por la compañía Brocade. No obstante el núcleo de Vyatta es un software de acceso libre, lo que hizo posible que Vyos fuera desarrollado por la comunidad Linux. Vyos usa un motor de encaminamiento conocido como XORP<sup>8</sup> y en esencia, es una distribución basada en Linux que puede ser usada de múltiples maneras, desde ejecución en modo LiveCD<sup>9</sup> hasta instalada en una máquina física con arquitectura x86, e incluso instalado en una máquina virtual dentro de un servidor.

Si bien Vyos no posee la vasta riqueza funcional de un router Cisco, empresa que invierte cientos de millones de dólares cada año en el desarrollo de sus productos, esto no presenta un problema, ya que Vyos dispone de las funciones y protocolos realmente necesarios para el ET. Además, por ser un software libre, con los conocimientos apropiados se pueden implementar funciones complementarias, como por ejemplo el protocolo CDP<sup>10</sup> de Cisco.

Para usar Vyos el administrador necesita descargar una imagen ISO de la distribución desde la página web oficial. Una vez realizada la descarga y como ya se ha indicado al inicio del punto, se puede usar el método que se desee para trabajar con ella, bien sobre un soporte físico (como LiveCD), instalándola en un PC, o bien en una máquina virtual. El resultado final es la transformación de la máquina, física o virtual, en un sistema de enrutamiento con las mismas funciones disponibles que las que pueda tener cualquier router convencional. [3] [11]

### 2.3.1 Plataforma de pruebas Vyos

Las pruebas del sistema Vyos se han realizado utilizando máquinas virtuales. Las ventajas que aporta la virtualización son muchas en cuanto a la posibilidad de escalar todo lo que se desee nuestro sistema. Esencialmente este sistema tiene 2 elementos:

- Un servidor, que provee de servicios CIS al puesto de mando mediante máquinas virtuales y en el que se configura también una máquina virtual Vyos, que enrutará los paquetes del resto de las máquinas. Este servidor debe tener por lo menos una interfaz física de red.
- Un switch con capacidad de separar sus interfaces en VLAN,s, con los cuales ya se trabaja en el ET.

Mediante un proceso denominado *trunking*<sup>11</sup> se consigue que a través de una única interfaz física del servidor salga toda la información proveniente de las máquinas virtuales, ya encapsulada con su dirección IP y la VLAN a la que pertenece. En el capítulo 3 se detallan las conexiones físicas y virtuales realizadas para las pruebas con Vyos. [3] [5]

---

8 XORP: Software que funciona como motor de enrutamiento que soporta la mayoría de los protocolos enrutamiento existentes hoy en día

9 LiveCD: Modo de funcionamiento de un sistema operativo, que se carga desde un CD/DVD a la memoria RAM de un equipo, sin necesidad de instalarlo en el disco duro de la máquina.

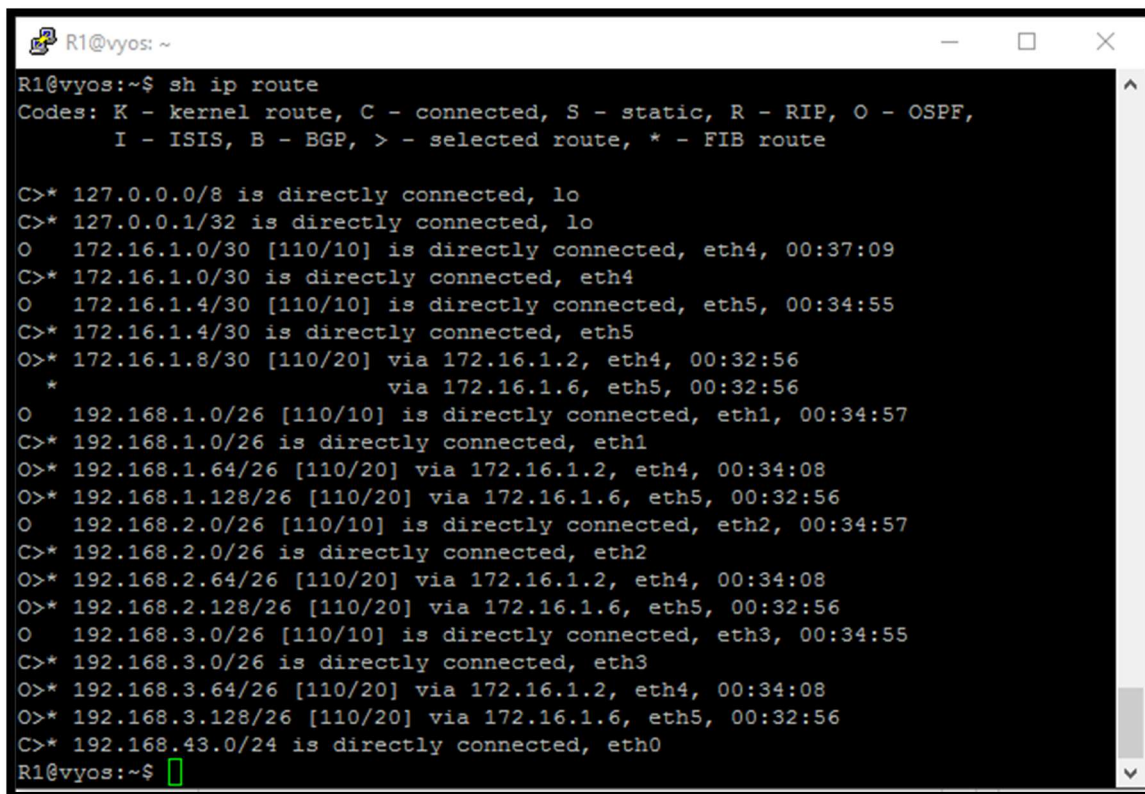
10 CDP: Cisco Discovery Protocol. Es un protocolo propietario de Cisco que permite a un router anunciar a sus router vecinos, es decir, los conectados directamente a él. Funciona a nivel de capa 2 del modelo OSI.

11 Trunking: Por un enlace "trunk" viajan paquetes IP encapsulados con el número de VLAN a la que pertenecen. Este encapsulado se denomina *dot1q*.

### 2.3.2 Entorno de configuración Vyos

La CLI de Vyos se denomina xorpsh, no muy diferente de la del IOS Cisco y que, además ofrece una potente interfaz de configuración web. Para acceso remoto a la plataforma de enrutamiento se puede usar indistintamente *ssh* o *telnet*.

Se dispone de 2 modos de trabajo dentro de la CLI de Vyos: modo de operación y modo de configuración. En el modo de operación solamente se pueden visualizar estadísticas y estado actual de la configuración del router. A través del modo de operación se accede al modo de configuración, donde se puede configurar todos los parámetros del router, desde las interfaces hasta los protocolos de enrutamiento. En la figura 2-5 se muestra una captura de la CLI de Vyos. [3]



```
R1@vyos:~$ sh ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

C>* 127.0.0.0/8 is directly connected, lo
C>* 127.0.0.1/32 is directly connected, lo
O  172.16.1.0/30 [110/10] is directly connected, eth4, 00:37:09
C>* 172.16.1.0/30 is directly connected, eth4
O  172.16.1.4/30 [110/10] is directly connected, eth5, 00:34:55
C>* 172.16.1.4/30 is directly connected, eth5
O>* 172.16.1.8/30 [110/20] via 172.16.1.2, eth4, 00:32:56
   *                               via 172.16.1.6, eth5, 00:32:56
O  192.168.1.0/26 [110/10] is directly connected, eth1, 00:34:57
C>* 192.168.1.0/26 is directly connected, eth1
O>* 192.168.1.64/26 [110/20] via 172.16.1.2, eth4, 00:34:08
O>* 192.168.1.128/26 [110/20] via 172.16.1.6, eth5, 00:32:56
O  192.168.2.0/26 [110/10] is directly connected, eth2, 00:34:57
C>* 192.168.2.0/26 is directly connected, eth2
O>* 192.168.2.64/26 [110/20] via 172.16.1.2, eth4, 00:34:08
O>* 192.168.2.128/26 [110/20] via 172.16.1.6, eth5, 00:32:56
O  192.168.3.0/26 [110/10] is directly connected, eth3, 00:34:55
C>* 192.168.3.0/26 is directly connected, eth3
O>* 192.168.3.64/26 [110/20] via 172.16.1.2, eth4, 00:34:08
O>* 192.168.3.128/26 [110/20] via 172.16.1.6, eth5, 00:32:56
C>* 192.168.43.0/24 is directly connected, eth0
R1@vyos:~$
```

Figura 2-5: CLI de Vyos mediante conexión Telnet a través de la aplicación PuTTY

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

### 3 Diseño e implementación de pruebas

#### 3.1 Diseño y topología general de las pruebas

Los servicios de VOIP<sup>12</sup> y VTC son relativamente recientes en cuanto a su uso por parte de las unidades de transmisiones del ET, de forma que no se muestran en la figura 1-2. Estos servicios son los que actualmente consumen la mayor parte del ancho de banda disponible en cada enlace, de ahí que estas pruebas se han diseñado en torno a estos dos servicios.

Las pruebas se han diseñado para comprobar si se cumplen los requisitos establecidos en la introducción, adaptados a los medios disponibles en la unidad. Para el desarrollo de estas pruebas se ha utilizado la topología mostrada en la figura 3-1, cuya base son tres routers (R1, R2 y R3) conectados entre sí. Este esquema ha sido utilizado para probar los tres sistemas con el objeto de establecer un escenario común para todos, siendo además una topología típica de interconexión entre tres puestos de mando, utilizado comúnmente por las unidades de transmisiones en sus despliegues.

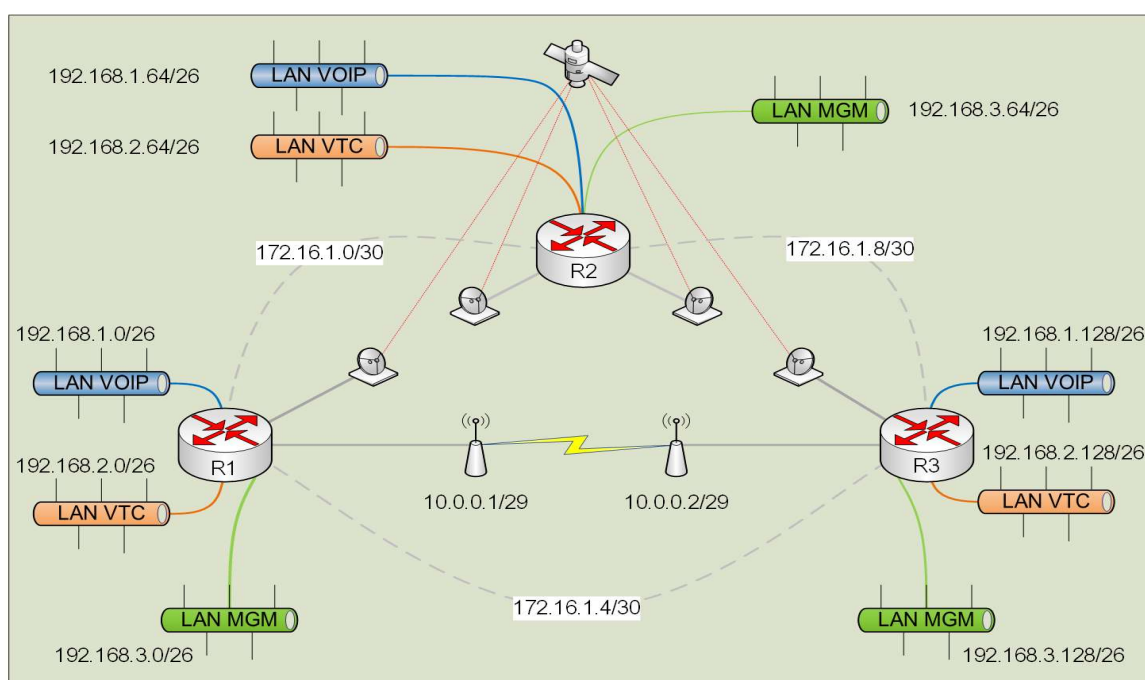


Figura 3-1: Esquema general de la red de pruebas

Como se acaba de mencionar, los servicios CIS más exigentes actualmente en los CTPC,s en cuanto a demanda de ancho de banda son los de voz sobre IP (VOIP) y video teleconferencia (VTC), teniendo el resto de servicios una demanda despreciable. Teniendo en cuenta lo anterior, se han establecido los siguientes parámetros de calidad de servicio (QoS), que deberá cumplir cada sistema en las pruebas:

- 4 llamadas simultáneas de VOIP. Cada llamada requiere, usando el códec G.711, 64 Kbits. Luego cada router debe reservar 256 Kbit/s de ancho de banda para VOIP.

<sup>12</sup> Voice over Internet Protocol. Es un sistema de telefonía que usa el tecnología IP para la realización de llamadas, diferenciándose de la telefonía en que no funcionan por conmutación de circuitos, si no por transmisión de los paquetes de datos a través de las redes de datos de las operadoras.

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

- Ancho de banda mínimo de 128 Kbit/s para VTC por corresponsal que participe en la videoconferencia. Por la topología establecida se necesitará ancho de banda para 3 corresponsales simultáneos. Esto requeriría 384 Kbit/s por router, no obstante, para garantizar una mejor calidad de servicio, se suele fijar un mínimo de 512 Kbit/s.
- Los enlaces punto a punto entre todos los routers estarán limitados a 1 Mbit/s, que es el máximo que admite un enlace punto a punto convencional mediante radioenlace IP.

Cabe destacar que el enlace entre R1 y R3 se realiza físicamente mediante antenas Ubiquiti de tecnología WiFi, con una capacidad de transmisión de 150 Mbit/s. No obstante las interfaces que conectan R1 y R3 con las antenas forman parte de la misma subred, de forma que virtualmente están conectadas como si formaran un enlace punto a punto físico. Las antenas Ubiquiti funcionan a estos efectos como un puente de red, totalmente transparente a la configuración de la red. Así mismo la conexión entre R2 y los routers R1 y R3 se realiza mediante enlace satélite, también transparente a nivel de capa 3 como en el caso anterior. Estos dos elementos son los enlaces más frecuentes entre unidades de transmisión, por lo que su introducción en la topología de las pruebas le confiere a ésta realismo, estableciendo unos límites de velocidad de red, que, con una conexión directa entre routers no se tendría, ya que la capacidad de las interfaces de red es de hasta 1 Gbit/s.

Esta topología se ha adaptado en las pruebas a cada sistema, puesto que cada uno tiene unos requisitos de hardware distintos, como se detallarán en las subsecciones correspondientes a cada sistema. Para la simulación de las redes VOIP y VTC se han utilizado máquinas virtuales creadas con la plataforma VMware, de forma que cada una de las máquinas está asociada a una red IP distinta: VOIP, VTC y MGM (Management)<sup>13</sup>. Esta configuración es común para los tres sistemas comparados y la subred a la que pertenece cada servicio está detallada en la Figura 3-1.

En las máquinas virtuales se ha instalado el sistema operativo Ubuntu, basado en la distribución Linux Ubuntu. Esta distribución tiene la particularidad de que consume muy pocos recursos de memoria y de procesamiento, conservando todas las funcionalidades necesarias para la realización de las pruebas. [12]

El direccionamiento IP de las máquinas y el direccionamiento genérico común de las interfaces usadas como puertas de enlace de los routers de los tres sistemas, así como el de las interfaces punto a punto que conectan los routers, viene descrito en la tabla 3-1. Además, en la figura 3-2 puede verse la interfaz gráfica de configuración de conexiones de red de una máquina virtual con sistema operativo Ubuntu, dentro del entorno de VMware. [12] [13]

Tabla 3-1: Direcciones IP de las máquinas virtuales.

Máquina (Red de pertenencia)	Dirección IP / Máscara	Máquina	Dirección IP / Máscara
Lubuntu 1 (LAN VOIP)	192.168.1.2/26	Puerta de enlace VTC R2	192.168.2.65/26
Lubuntu 2 (LAN VTC)	192.168.2.2/26	Puerta de enlace VTC R3	192.168.2.129/26
Lubuntu MGM 1 (LAN MGM)	192.168.3.2/26	Puerta de enlace MGM R1	192.168.3.1/26
Lubuntu 3 (LAN VOIP)	192.168.1.66/26	Puerta de enlace MGM R2	192.168.3.65/26
Lubuntu 4 (LAN VTC)	192.168.2.66/26	Puerta de enlace MGM R3	192.168.1.129/26

<sup>13</sup> La red de gestión (management) se ha utilizado tanto para el control y supervisión remoto de los routers así como para introducir tráfico de saturación para la realización de las pruebas de rendimiento.

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

Lubuntu 5 (LAN VOIP)	192.168.1.130/26	Interfaz R1-R2 (de R1)	172.16.1.1/30
Lubuntu 6 (LAN VTC)	192.168.2.130/26	Interfaz R1-R3 (de R1)	172.16.1.5/30
Lubuntu MGM 2 (LAN VOIP)	192.168.3.130/26	Interfaz R1-R2 (de R2)	172.16.1.2/30
Puerta de enlace VOIP R1	192.168.1.1/26	Interfaz R2-R3 (de R2)	172.16.1.9/30
Puerta de enlace VOIP R2	192.168.1.65/26	Interfaz R1-R3 (de R3)	172.16.1.6/30
Puerta de enlace VOIP R3	192.168.1.129/26	Interfaz R2-R3 (de R3)	172.16.1.10/30
Puerta de enlace VTC R1	192.168.2.1/26		

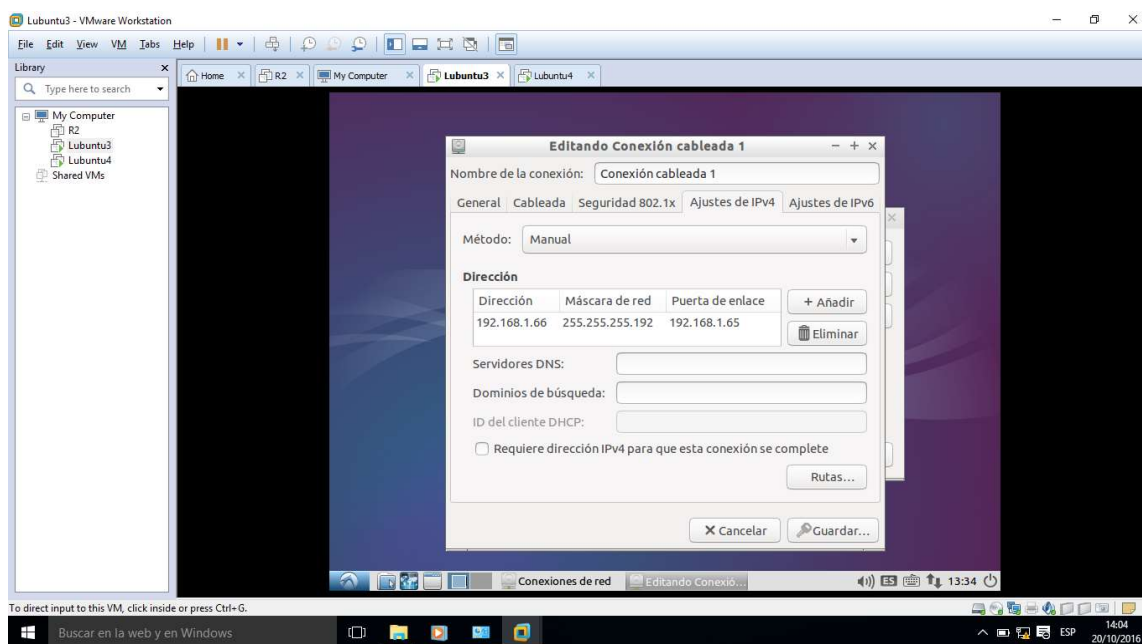


Figura 3-2: Interfaz de configuración de red de la máquina Lubuntu 3

Las máquinas portátiles físicas que hacen de anfitrión para las virtuales cuentan con un sistema operativo Windows 10, un procesador Intel Dual Core de 1.8 GHz de velocidad y una memoria RAM de 4 GB.

Se han realizado 2 pruebas para cada sistema:

- Pruebas de enrutamiento: El protocolo de enrutamiento utilizado en las pruebas ha sido OSPF. Se ha comprobado el correcto funcionamiento del protocolo realizando trazas de ruta desde las máquinas virtuales, primero con la topología mostrada conectada completamente y después cortando la conexión entre R1 y R3.
- Pruebas de rendimiento: Con la conexión entre R1 y R3 anulada, se ha comprobado el correcto envío y recepción de paquetes entre las máquinas virtuales situadas en los extremos de la red, de forma que mediante la aplicación Ostinato, se ha inyectado tráfico de paquetes ICMP desde cada máquina virtual de cada LAN hasta llegar a saturar la red, de forma que se ha comprobado el mantenimiento de los niveles de transmisión mínimos para las redes VOIP y VTC determinados previamente como requisito. Para comprobar el volumen de tráfico de las máquinas de destino se ha utilizado el programa de análisis de tráfico de red Wireshark, así como el monitor de tráfico de red incluido en el sistema operativo Lubuntu, que facilita

visión gráfica del tráfico entrante y saliente de la interfaz de la máquina. En el ANEXO C se muestra la interfaz de configuración de la aplicación Ostinato, instalada en una máquina virtual, y se detalla la configuración de la misma. La saturación de la red se ha llevado a cabo a través de la red MGM. [14]

### 3.2 Escenarios de pruebas

Los escenarios de pruebas han sido principalmente dos. Se ha realizado una primera fase de pruebas en un entorno de laboratorio dentro de la Base Militar Cid Campeador (Castrillo del Val, Burgos), en el cual, los tres routers en cada caso se localizaban en la misma habitación, por comodidad a la hora de configurarlos. Se ha utilizado en estas pruebas la topología de la figura 3-1

En la segunda fase de pruebas, se han probado estos sistemas en el ejercicio Tiwar 2016, que tuvo lugar en el campo de maniobras de Matagrande (Burgos) entre los días 26 y 30 de Septiembre de 2016, utilizando la misma topología que en el entorno de laboratorio, con la diferencia de que en este caso cada router se localizaba en Puestos de Mando distintos. Estas pruebas se realizaron para introducir los nuevos sistemas en un entorno de operación real, pudiendo comprobarse que su comportamiento fue similar al observado en las pruebas realizadas en el entorno de la base.

### 3.3 Establecimiento del entorno e implementación de pruebas para el sistema Cisco

La topología adaptada a los dispositivos Cisco 2821 se detalla en la figura 3-3.

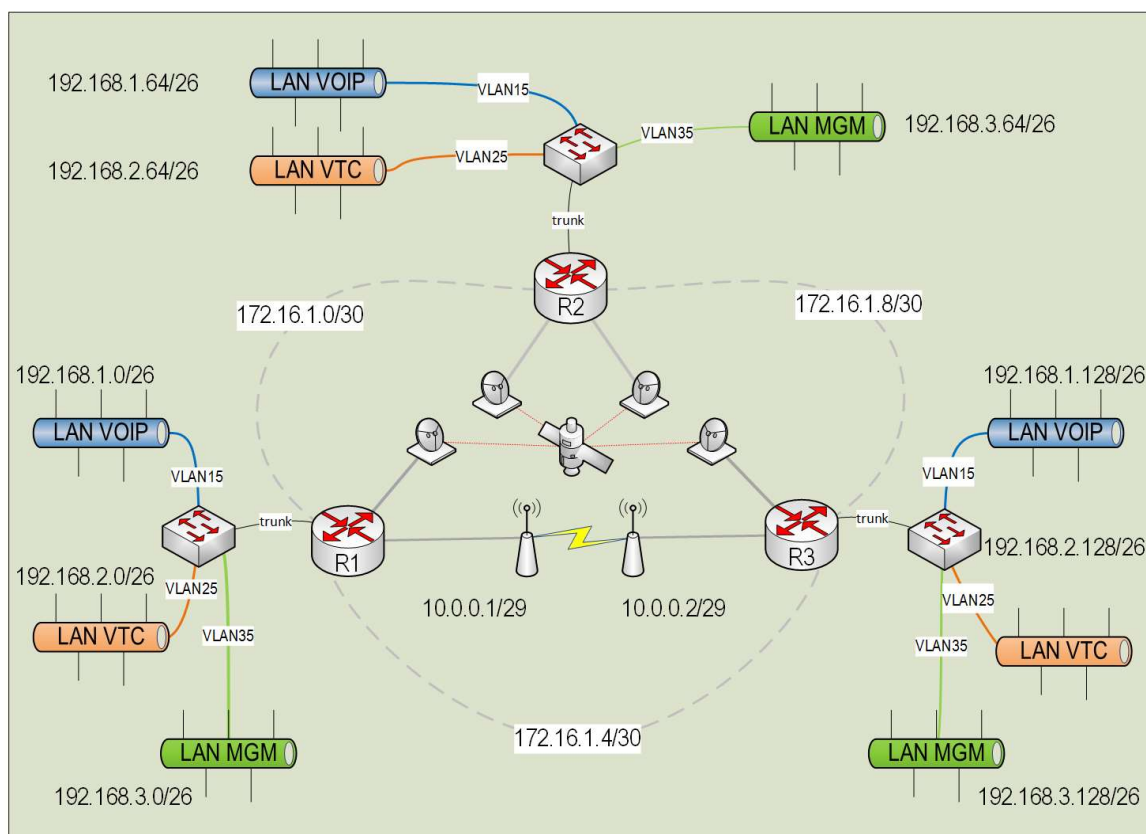


Figura 3-3: Topología de pruebas Cisco

Se han utilizado los siguientes elementos en la configuración de estas pruebas:

- 2 Switch no configurables DLINK DGS 10160 (no incluido en figura 3-3)

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

- 1 Switch no configurable 3COM 3C16470 (no incluido en figura 3-3)
- 3 Switch configurables Cisco Catalyst 2960
- 3 Router Cisco 2821

Como se muestra en la Figura 3-3 se han separado los distintos servicios en tres VLAN,s, numeradas como 15, 25 y 35 y correspondientes a los servicios de VOIP, VTC y MGM respectivamente. Destacar que un switch no configurable no tiene la posibilidad de configurar sus interfaces de modo que se puedan separar, creando de esta forma VLAN,s que pueden operar distintas subredes sin que exista conmutación de paquetes entre ellas. A nivel de red actúan como un puente transparente<sup>14</sup>. Se han usado estos switches debido a que sólo se dispone de una interfaz de red cableada Ethernet en la máquina anfitrión<sup>15</sup>, que da salida a las interfaces virtuales de las máquinas alojadas en ella. No obstante en este proceso no se efectúa el marcado de los paquetes IP con el número de la VLAN a la que pertenece cada máquina, y es por eso que al switch no programable se conectan 3 enlaces correspondientes a las 3 VLAN,s configuradas en el Catalyst 2960. El router va conectado al switch Catalyst mediante un enlace trunk<sup>16</sup>. En el esquema de la figura 3-4 se muestra con más claridad las conexiones realizadas para el router R1, extrapolable a los otros 2 nodos de la red.

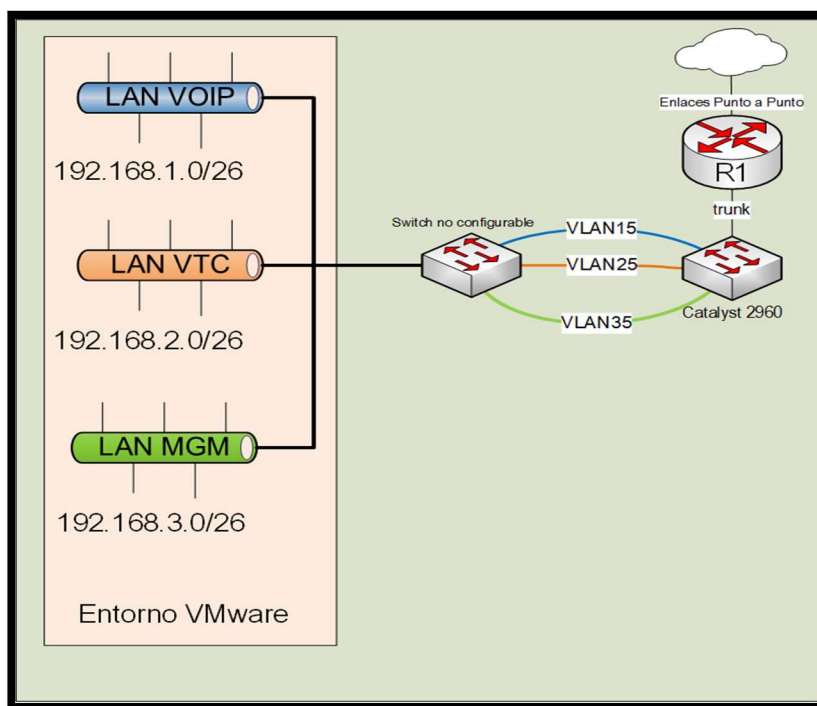


Figura 3-4: Detalle de conexiones virtuales y físicas realizadas.

En la configuración de los routers se han introducido políticas de calidad de servicio que garantizan la independencia de las subredes, así como la tasa mínima de transmisión y recepción requeridas. También se han configurados sus interfaces Ethernet de forma que se han creado sub-interfaces, cada una de las

<sup>14</sup> Puente transparente: Es un dispositivo que conecta en red físicamente dos o más ordenadores, pero que no realiza ninguna función a nivel de capa de red.

<sup>15</sup> Máquina anfitrión: Es la máquina física que aloja las máquinas virtuales. Para el desarrollo de este TFG se han utilizado a este fin ordenadores personales portátiles.

<sup>16</sup> Conexión trunk: Conecta el router con el switch Catalyst, de forma que la interfaz física del router está dividida en sub-interfaces lógicas que al contrario que la interfaz del PC anfitrión, sí que encapsula los paquetes IP con el número de VLAN a la que corresponde, gracias a lo cual el switch determina por qué VLAN encaminar esos paquetes marcados.

cuales sirve de puerta de enlace a las VLAN,s correspondientes a cada servicio. Así mismo se ha configurado el protocolo de enrutamiento OSPF para establecer las rutas. En el ANEXO D se muestran las tablas de enrutamiento de cada router antes de anular el enlace entre R1 y R3.

Los comandos de configuración introducidos para el router R1 Cisco vienen detallados en el ANEXO E, así como una breve explicación del efecto de cada uno. Se ha omitido los de R2 y R3 por ser análogos.

En el ANEXO F se pueden ver una serie de ilustraciones del montaje físico de los tres nodos de enrutamiento.

### 3.4 Establecimiento del entorno e implementación de pruebas para el sistema Quagga

Como se ha indicado en el capítulo 2 de esta memoria, el software de enrutamiento Quagga puede instalarse en cualquier sistema basado en UNIX. En este caso se ha optado por la instalación sobre el sistema operativo OpenWrt, instalado previamente en la memoria flash de los router TP-LINK que son los únicos utilizados. Para dicha instalación basta con actualizar el firmware de fábrica del router con una imagen descargada de OpenWrt. Estas acciones se realizan mediante la interfaz web de configuración de los router. Tras la actualización, el firmware de fábrica desaparece y la interfaz de configuración web pasa a ser la de OpenWrt. [8]

Una vez instalado OpenWrt en el router, se descargan e instalan los paquetes de Quagga necesarios para nuestros requisitos, que incluyen los demonios de control y de protocolos de enrutamiento. Cabe destacar que Quagga no dispone de ningún paquete que implemente políticas de calidad de servicio. Esta carencia puede suplirse mediante el paquete *sqm-scripts* para OpenWrt, no obstante, esto se escapa al análisis de Quagga como sistema de enrutamiento. [9]

Una vez terminada la instalación de los paquetes de Quagga, el siguiente paso es la configuración de las interfaces de red, implementando el direccionamiento descrito en la tabla 3-1. Esto se hace mediante la interfaz de configuración web de OpenWrt. En el ANEXO G se detalla este proceso de configuración. También se podría optar por configurar el direccionamiento de las interfaces mediante la interfaz *vttysh* de Quagga como si de un router Cisco se tratase, pero la interfaz de OpenWrt es mucho más sencilla de utilizar y más rápida. Destacar que el puerto Ethernet 1 del router se ha dividido en sub-interfaces, de forma que este puerto será el que conecte con la interfaz física de la máquina anfitrión, que da salida a las máquinas virtuales. Además, para que el tráfico de las máquinas virtuales salga con el etiquetado de la VLAN a la que pertenece, se ha usado la aplicación Realtek Ethernet Diagnostic Utility, que permite crear interfaces (o NIC,s<sup>17</sup>) de red virtuales a las que conectar las máquinas de VMware (ver ANEXO H). De esta forma se consigue emular un enlace *trunk* entre el router y la máquina física, sin necesidad de utilizar un switch Cisco intermedio, con lo que se ahorra un dispositivo más en la red. En la figura 3-5 se da una visión esquemática de las conexiones virtuales y físicas realizadas para estas pruebas, así como de la topología de pruebas adaptada al sistema Quagga. La topología usada se ajusta a la figura 3-1, sin necesidad de añadir ningún elemento más. [7] [10]

Una vez configuradas las interfaces, se configura con *vttysh* el protocolo OSPF, publicando las redes que se vayan enrutar a través de este protocolo. Los comandos de configuración en Quagga para OSPF son idénticos a los utilizados para Cisco.

---

17 NIC: Acrónimo de Network Interface Card.

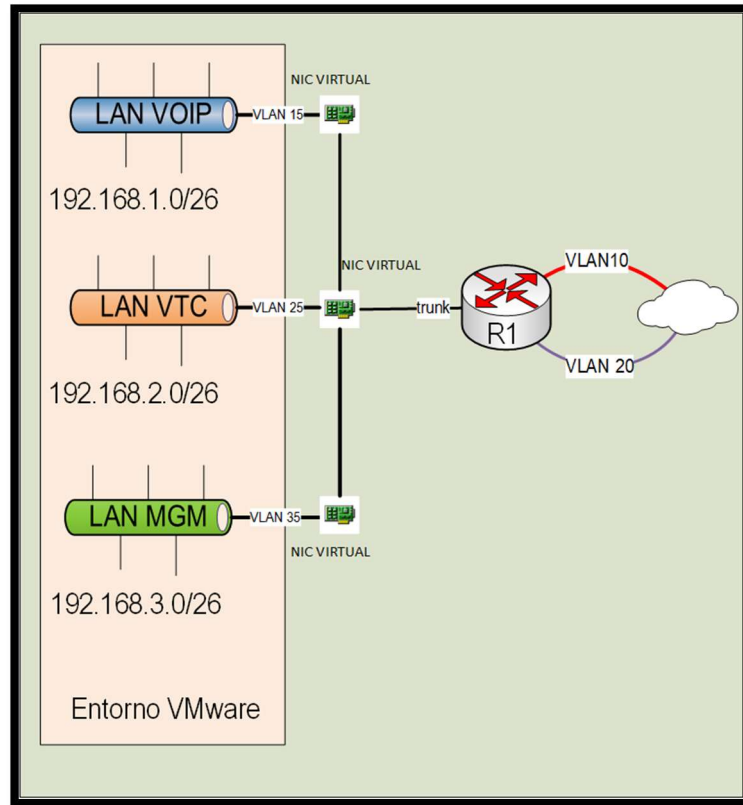


Figura 3-5: Esquema de conexiones virtuales y físicas de Quagga

### 3.5 Establecimiento del entorno e implementación de pruebas para el sistema Vynos

Para las pruebas realizadas con el sistema Vynos se ha utilizado la topología adaptada de la figura 3-6 utilizando únicamente, además de los portátiles que sirven como anfitrión a las máquinas virtuales, switches Catalyst 2960.

Vynos ha sido instalado en máquinas virtuales creadas en el entorno de VMware en cada máquina física. Las interfaces de red virtuales de los clientes de VOIP, VTC y MGM se conectan ahora de forma interna a redes de área local virtuales. Estas redes de área local tienen como puertas de enlace las interfaces de la máquina Vynos, que, como no existe límite, se pueden crear tantas como se quiera. De esta forma evitamos tener que crear sub-interfaces dentro de la máquina Vynos, aunque sí que existe la posibilidad. Las conexiones punto a punto entre routers virtuales se realizan conectando las interfaces de Vynos determinadas para salida al exterior en la configuración de VMware. Tal y como se detalla en la figura 3-7, estas interfaces virtuales de VMware se conectan a interfaces virtuales creadas en la máquina anfitrión con la herramienta Realtek Ethernet Diagnostic Utility, que, al igual que con las pruebas realizadas con Quagga, nos permite sacar el tráfico de esas VLAN,s etiquetado por la interfaz física de la máquina física. El esquema 3-7 es extrapolable a los otros 2 routers de la topología. [3]

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

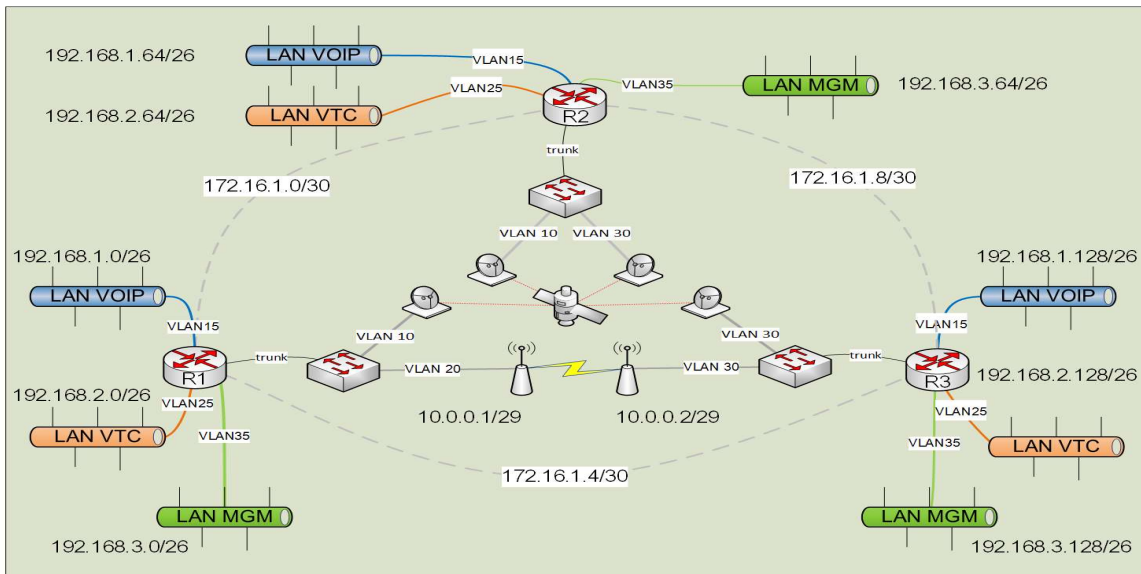


Figura 3-6: Topología general de pruebas con Vyos

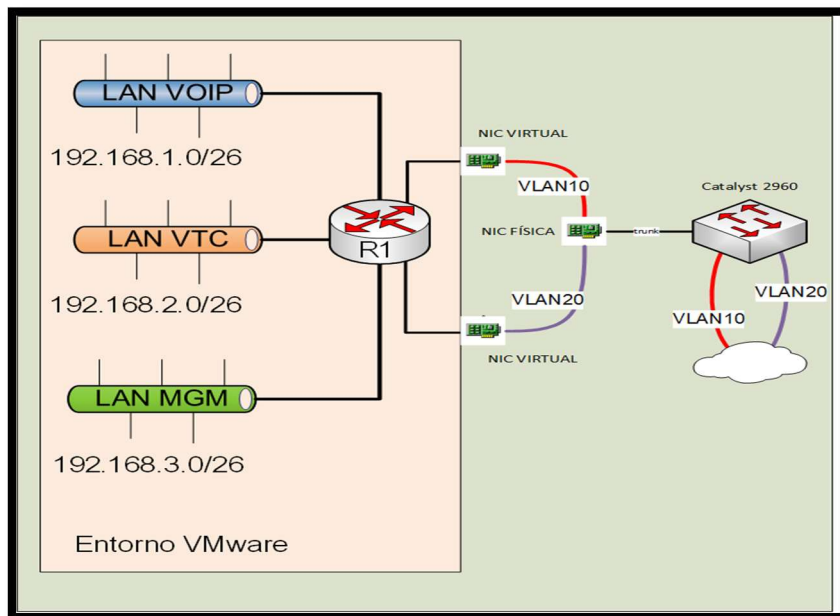


Figura 3-7: Esquema detallado de conexiones físicas y virtuales del Vyos R1

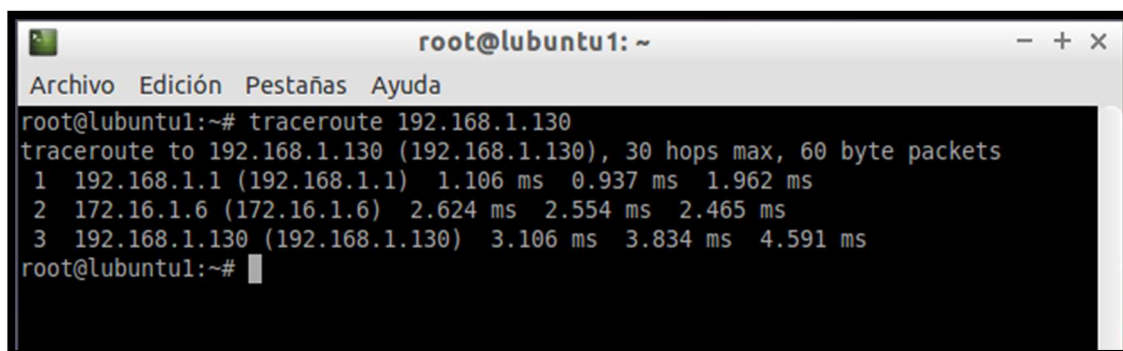
La conexión al exterior entre máquinas se realiza a través de los Catalyst 2960, que conectan las máquinas anfitriones con las estaciones satélite y las antenas Ubiquiti respectivamente, configurando las interfaces del switch para separar las VLAN,s que enlazan cada router Vyos. Estas VLAN,s han sido etiquetadas como 10, 20 y 30 para los enlaces R1-R2, R1-R3 y R2-R3 respectivamente. La conexión entre la máquina física y el Catalyst funciona como enlace *trunk*. En el ANEXO J se muestra cómo quedan configuradas las interfaces de red del router R1. Una vez comprobada la conectividad entre interfaces, se configura el protocolo de enrutamiento OSPF y se introducen las políticas QoS requeridas, al igual que se hizo con los router Cisco. En el ANEXO K vienen detallados los comandos de configuración utilizados para configurar la máquina Vyos, así como una explicación de la propia configuración.

## 4 Resultados de pruebas

### 4.1 Resultados Cisco

Como cabía esperar, los resultados de las pruebas con los enrutadores Cisco muestran que cumplen a la perfección con los requisitos establecidos en este TFG, lo que es obvio puesto que los dispositivos Cisco son los que actualmente están en el inventario de las Unidades de Transmisiones.

En la figura 4-1 se muestra una traza de ruta desde las máquina de VOIP del router R1 a su homóloga en el router R3. Al anular el enlace entre R1 y R3, el protocolo de enrutamiento OSPF reencamina los paquetes a través de R2. Tal y como se detalla en la figura 4-2, la dirección IP del segundo salto que da el paquete corresponde a la interfaz serial del router R2 que conecta con R1, cuando antes de suprimir en enlace correspondía a la dirección de interfaz Ethernet del router R3.

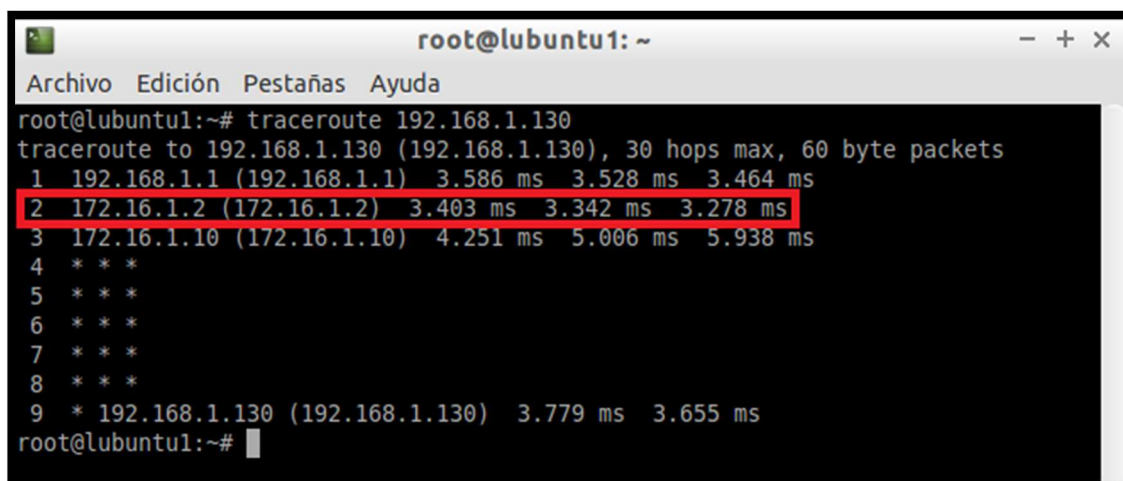


```

root@lubuntu1: ~
Archivo Edición Pestañas Ayuda
root@lubuntu1:~# traceroute 192.168.1.130
traceroute to 192.168.1.130 (192.168.1.130), 30 hops max, 60 byte packets
 1 192.168.1.1 (192.168.1.1)  1.106 ms  0.937 ms  1.962 ms
 2 172.16.1.6 (172.16.1.6)  2.624 ms  2.554 ms  2.465 ms
 3 192.168.1.130 (192.168.1.130)  3.106 ms  3.834 ms  4.591 ms
root@lubuntu1:~#

```

Figura 4-1: Traza de ruta desde Lubuntu 1 a Lubuntu 5



```

root@lubuntu1: ~
Archivo Edición Pestañas Ayuda
root@lubuntu1:~# traceroute 192.168.1.130
traceroute to 192.168.1.130 (192.168.1.130), 30 hops max, 60 byte packets
 1 192.168.1.1 (192.168.1.1)  3.586 ms  3.528 ms  3.464 ms
 2 172.16.1.2 (172.16.1.2)  3.403 ms  3.342 ms  3.278 ms
 3 172.16.1.10 (172.16.1.10)  4.251 ms  5.006 ms  5.938 ms
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * 192.168.1.130 (192.168.1.130)  3.779 ms  3.655 ms
root@lubuntu1:~#

```

Figura 4-2: Traza de ruta con el enlace entre R1 y R3 cortado

En cuanto a las pruebas de rendimiento, al realizar una inyección de tráfico desde cada máquina de R1 a sus homólogas en R3, se comprueba que las políticas de calidad de servicio introducidas funcionan perfectamente, ya que se garantizan los parámetros mínimos de servicio requeridos, es decir, 256 kbit para VOIP y 512 kbit para VTC. En la figura 4-3 se muestra, en la ventana superior derecha, el tráfico de red que atraviesa la interfaz física de red de la máquina anfitriona y, en la parte inferior, el tráfico que atraviesa la interfaz virtual de la máquina virtual Lubuntu 5, que pertenece al servicio de VOIP de R3. Se puede

comprobar que el nivel de transmisión máximo es de alrededor de 2 MB/s y el nivel de recepción y transmisión de Lubuntu 5 es de alrededor de 32 kB/s, es decir 256 Kbit/s.

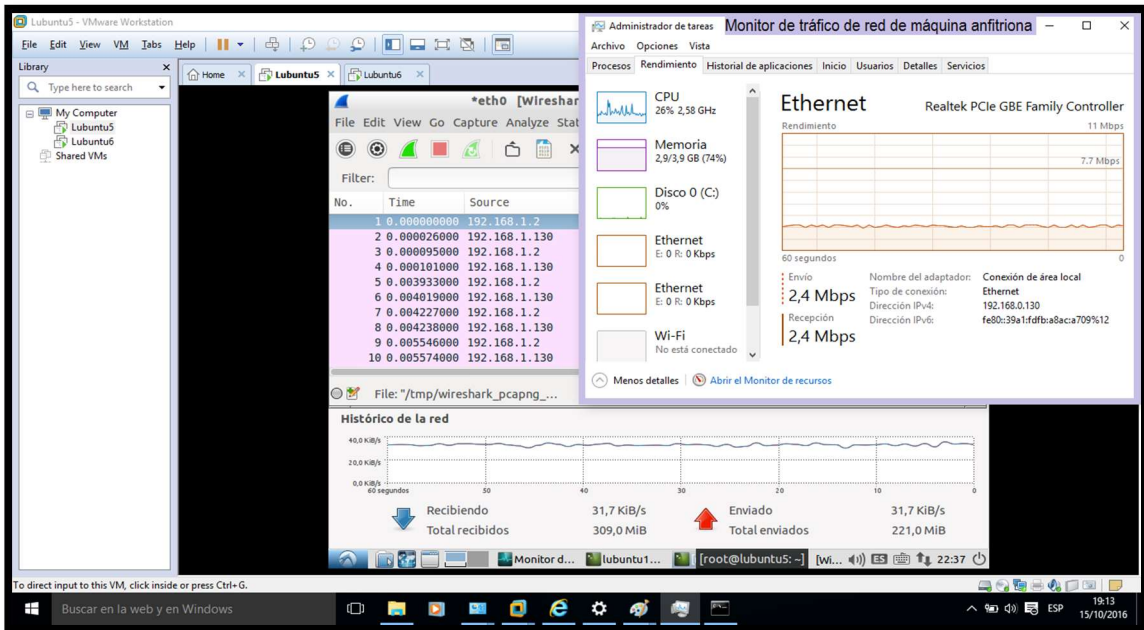


Figura 4-3: Tráfico de red de la interfaz física anfitriona y de la interfaz virtual VOIP

## 4.2 Resultados Quagga

Las pruebas de enrutamiento con Quagga fueron satisfactorias. Al suprimir el enlace entre R1 y R3, la ruta entre estos routers se reencaminó a través de R2. En las figuras 4-4 y 4-5 se muestran las tablas de enrutamiento de R1 antes y después del corte.

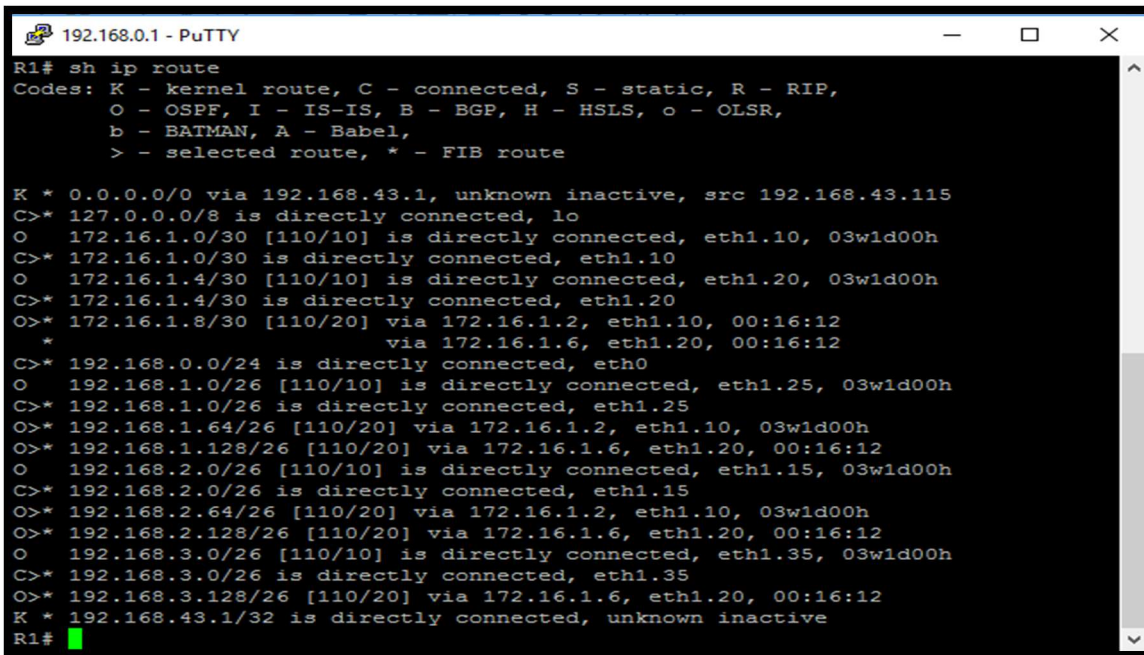


Figura 4-4: Tabla de enrutamiento de R1 antes de suprimir el enlace

```

192.168.0.1 - PuTTY
R1# sh ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, H - HSLs, o - OLSR,
       b - BATMAN, A - Babel,
       > - selected route, * - FIB route

K * 0.0.0.0/0 via 192.168.43.1, unknown inactive, src 192.168.43.115
C>* 127.0.0.0/8 is directly connected, lo
O  172.16.1.0/30 [110/10] is directly connected, eth1.10, 03w1d00h
C>* 172.16.1.0/30 is directly connected, eth1.10
O  172.16.1.4/30 [110/10] is directly connected, eth1.20, 00:00:09
C>* 172.16.1.4/30 is directly connected, eth1.20
O>* 172.16.1.8/30 [110/20] via 172.16.1.2, eth1.10, 00:00:13
C>* 192.168.0.0/24 is directly connected, eth0
O  192.168.1.0/26 [110/10] is directly connected, eth1.25, 03w1d00h
C>* 192.168.1.0/26 is directly connected, eth1.25
O>* 192.168.1.64/26 [110/20] via 172.16.1.2, eth1.10, 03w1d00h
O>* 192.168.1.128/26 [110/30] via 172.16.1.2, eth1.10, 00:00:13
O  192.168.2.0/26 [110/10] is directly connected, eth1.15, 03w1d00h
C>* 192.168.2.0/26 is directly connected, eth1.15
O>* 192.168.2.64/26 [110/20] via 172.16.1.2, eth1.10, 03w1d00h
O>* 192.168.2.128/26 [110/30] via 172.16.1.2, eth1.10, 00:00:13
O  192.168.3.0/26 [110/10] is directly connected, eth1.35, 03w1d00h
C>* 192.168.3.0/26 is directly connected, eth1.35
O>* 192.168.3.128/26 [110/30] via 172.16.1.2, eth1.10, 00:00:13
K * 192.168.43.1/32 is directly connected, unknown inactive
R1#
    
```

Figura 4-5: Tabla de enrutamiento de R1 después de suprimir el enlace

Como puede observarse, para llegar a las redes conectadas y publicadas por R3 es necesario ir a través de la interfaz de R2. Se comprueba también que la traza de ruta entre la máquina VOIP de R1 y R3 cambia, como se muestra en las figuras 4-6 y 4-7. En el ANEXO I se muestran las tablas de enrutamiento de los tres routers.

```

root@ubuntu1: ~
Archivo Edición Pestañas Ayuda
root@ubuntu1:~# traceroute 192.168.1.130
traceroute to 192.168.1.130 (192.168.1.130), 30 hops max, 60 byte packets
 1 192.168.1.1 (192.168.1.1)  0.526 ms  0.251 ms  0.351 ms
 2 172.16.1.6 (172.16.1.6)  2.537 ms  2.457 ms  2.571 ms
 3 192.168.1.130 (192.168.1.130)  3.465 ms  4.460 ms  4.396 ms
root@ubuntu1:~#
    
```

Figura 4-6: Traza de ruta antes del corte

```

root@ubuntu1: ~
Archivo Edición Pestañas Ayuda
root@ubuntu1:~# traceroute 192.168.1.130
traceroute to 192.168.1.130 (192.168.1.130), 30 hops max, 60 byte packets
 1 192.168.1.1 (192.168.1.1)  1.112 ms  0.857 ms  0.329 ms
 2 172.16.1.2 (172.16.1.2)  1.167 ms  1.077 ms  0.975 ms
 3 172.16.1.10 (172.16.1.10)  0.899 ms  0.824 ms  3.554 ms
 4 192.168.1.130 (192.168.1.130)  3.494 ms  3.420 ms  5.518 ms
root@ubuntu1:~#
    
```

Figura 4-7: Traza de ruta después del corte

Debido a que Quagga no dispone de herramientas para aplicar políticas de calidad de servicio, no se puede realizar un estudio similar al realizado con Cisco y con Vyos. No obstante como las interfaces Ethernet del router TP-Link son de clase Gigabit, cabe pensar que el tráfico que se introduzca en la red se verá estrangulado por los medios por los que se conecten los enlaces punto a punto entre routers, que como se ha indicado en el capítulo 1 de esta memoria, los medios más restrictivos a estos efectos son los enlaces mediante satélite, que limitan la velocidad de transmisión a 2 Mbit/s. Contando con que el tráfico generado por los sistemas CIS de un Puesto de Mando distintos de VOIP y VTC (mensajería, replicación SIMACET, etc.) es despreciable, se puede decir que sería difícil que se diera una saturación de la red tal que se impidiese la facilitación de esos servicios.

### 4.3 Resultados Vyos

Tanto las pruebas de enrutamiento como las de rendimiento de las políticas QoS han tenido un resultado positivo.

En las pruebas de enrutamiento al realizar el corte entre R1 y R3 se ha observado como el protocolo OSPF reencamina el tráfico entre estos routers a través de R2. En las figuras 4-8 y 4-9 se muestran las trazas de ruta efectuadas entre las máquinas de R1 y R3, donde puede comprobarse que al realizar el corte, la traza muestra un salto más, a través de la interfaz de R2, con lo que se llega a la conclusión de que el protocolo OSPF funciona correctamente.

```

lubuntu1@lubuntu1: ~
Archivo Edición Pestañas Ayuda
lubuntu1@lubuntu1:~$ traceroute 192.168.1.130
traceroute to 192.168.1.130 (192.168.1.130), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  0.781 ms  0.437 ms  0.513 ms
 2  172.16.1.6 (172.16.1.6)  5.854 ms  8.250 ms  8.210 ms
 3  192.168.1.130 (192.168.1.130)  8.193 ms  9.634 ms  10.375 ms
lubuntu1@lubuntu1:~$
    
```

Figura 4-8: Traza de ruta desde Lubuntu 1 a Lubuntu 5 antes de anular el enlace

```

lubuntu1@lubuntu1: ~
Archivo Edición Pestañas Ayuda
lubuntu1@lubuntu1:~$ traceroute 192.168.1.130
traceroute to 192.168.1.130 (192.168.1.130), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  0.450 ms  0.260 ms  0.217 ms
 2  172.16.1.2 (172.16.1.2)  2.971 ms  3.971 ms  4.016 ms
 3  172.16.1.10 (172.16.1.10)  6.829 ms  7.792 ms  7.963 ms
 4  192.168.1.130 (192.168.1.130)  7.916 ms  7.894 ms  8.796 ms
lubuntu1@lubuntu1:~$
    
```

Figura 4-9: Traza de ruta después de suprimir el enlace

En cuanto los resultados de las pruebas de rendimiento, se puede decir que se garantizan los niveles mínimos de transmisión definidos en los requisitos establecidos en el capítulo 1. No obstante, tal y como se observa en la figura 4-10, en el monitor de red de Lubuntu 5 se observan algunas fluctuaciones que no se observaban con Cisco, debidos al consumo de recursos de las máquinas virtuales en cuanto a procesamiento y memoria RAM. Esta limitación de hardware no se tendría si se usaran los clústeres de virtualización utilizados por las unidades de transmisiones, que disponen de múltiples procesadores así como una memoria RAM de más de 8 GB, con lo que cabe pensar que, de alojarse los routers Vyos en

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

estos clústeres, tales fluctuaciones no se producirían, puesto que cada máquina virtual contaría con unos recursos muy superiores a los disponibles en las máquinas de estas pruebas.

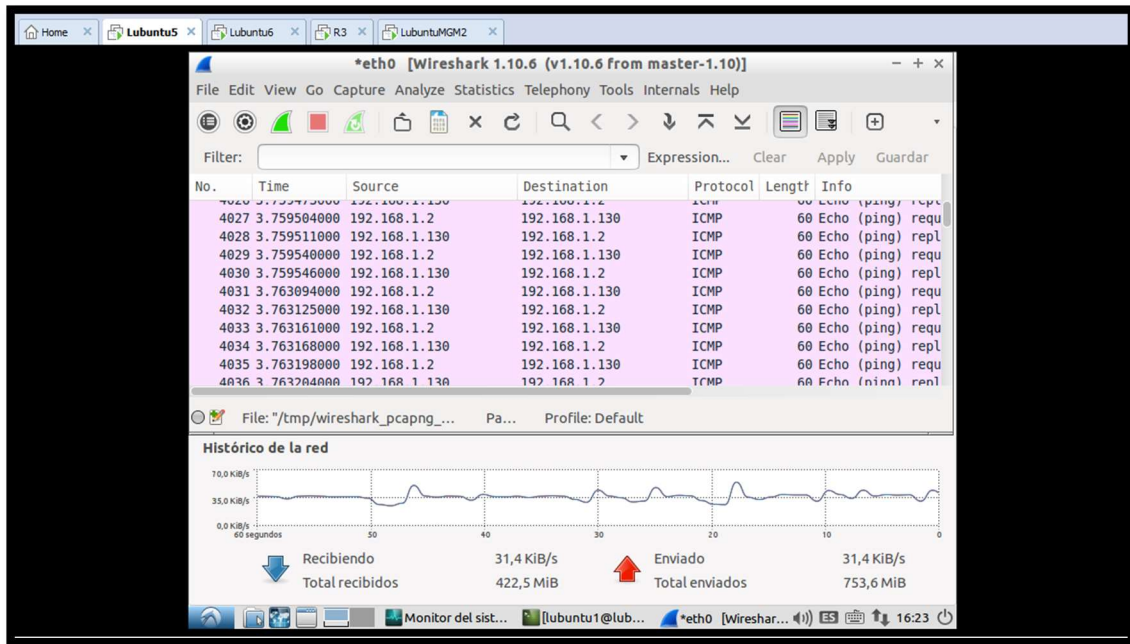


Figura 4-10: Tráfico de red en la interfaz de Lubuntu 5 saturando el enlace



## 5 Impacto económico y comparativa

### 5.1 Análisis económico

Para realizar una comparativa económica se han considerado los costes de los elementos implicados en cada nodo por separado. En la tabla 5-1 se detallan los costes asociados a cada nodo de pruebas considerando todos los elementos necesarios para hacerlos funcionar, obviando los de los enlaces punto a punto entre routers, es decir, los enlaces satélites y las antenas Ubiquiti. También se ha obviado el coste de los ordenadores portátiles usados como máquinas anfitrión, no obstante se ha considerado el coste de la licencia de software de VMware, necesario para el uso de Vynos. [4] [15]

Tabla 5-1: Comparativa Económica de los sistemas

Elementos	Cisco	Quagga	Vynos
Router Cisco 2821	1000€	-	-
Switch Cisco Catalyst 2930	1350€	-	1350€
Switch no configurable D-Link DGS 1016d	90€	-	-
Switch no configurable 3COM 16470	80€	-	-
Licencia de uso VMware Workstation 12	-	-	250€
Router TP-LINK TL-WR1043ND	-	60€	-
Licencias de uso OpenWrt/Quagga	-	0€ (software libre)	-
Licencia de uso Vynos	-	-	0€ (software libre)
<b>Total</b>	<b>2520€</b>	<b>60€</b>	<b>1600€</b>

Puede apreciarse que el sistema más económico es Quagga, instalado sobre el router TP-LINK TL1043ND, ya que no requiere de más elementos que el mencionado router. Por el contrario, el sistema más caro se ha demostrado que es el que usa routers Cisco. Cabe destacar que se ha considerado los routers 2821 para este análisis económico, pero los utilizados en realidad por las unidades son los routers Cisco 7200, cuyo precio medio oscila los 3000€, con lo que, en realidad, esa misma topología con los Cisco 7200 sería incluso más costosa.

## 5.2 Comparativa funcional

En la tabla 5-2 se muestra una comparativa de los tres sistemas, en base a los requerimientos establecidos en el capítulo 1.

Tabla 5-2: Comparativa de sistemas

	Cisco	Quagga	Vyos
Sistema Operativo	IOS	Linux	Linux
Código libre	NO	SI	SI
Instalable	NO	SI	SI
Compatibilidad TCP/IP	SI	SI	SI
Rutas Estáticas	SI	SI	SI
RIP v2	SI	SI	SI
OSPF	SI	SI	SI
NAT	SI	SI	SI
Acceso remoto SSH	SI	SI	SI
Acceso remoto Telnet	SI	SI	SI
QoS	SI	NO	SI
SNMP	SI	SI	SI
Túneles GRE	SI	NO	SI
FHRP	SI	NO	SI
Route-maps	SI	NO	SI

Como puede observarse en la tabla 5-2, tanto Cisco como Vyos cumplen con todas las especificaciones declaradas en el capítulo 1. Por el contrario, Quagga no cumple con algunos aspectos avanzados de los requisitos de enrutamiento exigidos, tales como implementación de QoS. No obstante estas carencias pueden subsanarse mediante la instalación paquetes adicionales en la distribución Linux sobre la que se esté ejecutando Quagga. Para el caso concreto de QoS podría instalarse el paquete `qsm-scripts`, que permite la regulación de tráfico de datos por las interfaces de red configuradas. No obstante no es objeto de este TFG profundizar en este tipo de soluciones. [9]

### 5.3 Matriz de decisión

Para determinar el sistema de enrutamiento idóneo se ha confeccionado una matriz de decisión en la que se han definido los siguientes criterios:

- Coste de plataforma
- Funcionalidad
- Dificultad de operación
- Instrucción de personal
- Portabilidad del sistema
- Soporte de empresa externa

En la tabla 5.3 se muestra estos criterios, su ponderación y la evaluación ponderada de los tres sistemas.

Tabla 5-3: Matriz de decisión

	Ponderación (%)	Cisco	Quagga	Vyos
Coste de plataforma Evaluación (sobre 100 puntos)	25	40	95	80
Funcionalidad Evaluación (sobre 100 puntos)	25	100	60	100
Dificultad de operación Evaluación (sobre 100 puntos)	15	90	75	90
Instrucción del personal Evaluación (sobre 100 puntos)	10	100	90	80
Portabilidad del sistema Evaluación (sobre 100 puntos)	10	0	75	100
Soporte de empresa externa Evaluación (sobre 100 puntos)	15	100	0	0
Total	100	450	395	445
Media ponderada (sobre 100)		73.5	66.5	76.5
Ranking		2	3	1

Se han considerado los costes y la funcionalidad como los dos parámetros de más peso para evaluar los sistemas, ya que se ha determinado que son los más importantes de cara a una evaluación y adquisición por parte de las unidades de transmisiones del ET. Hay que tener en cuenta que esta evaluación se hace en base a las pruebas realizadas, considerando no solo los sistemas de enrutamiento

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

comparados sino también los sistemas y aplicaciones asociadas a cada uno para la realización de las pruebas.

## 6 Conclusiones

Este TFG ha supuesto un reto en cuanto a la investigación realizada para la operación de los tres sistemas, así como el diseño del entorno de pruebas, que se ha basado en las topologías y configuraciones que son empleadas de forma común en las unidades de transmisiones del ET en sus ejercicios de despliegue, así como en zona de operaciones. Aunque se ha creado una topología común a los tres sistemas, ésta ha tenido que ser adaptada a cada sistema por las características de operación e instalación particulares de cada uno, por ejemplo, usando tecnologías de virtualización. No obstante las pruebas realizadas han sido comunes a los tres, pudiéndose así establecer una evaluación imparcial.

Atendiendo a la matriz de decisión expuesta en la tabla 5-3 se puede concluir que, a la vista de los resultados obtenidos, el sistema de enrutamiento Vynos se muestra como un candidato ideal para sustituir a los actuales routers de la casa Cisco. Su funcionalidad es comparable a la de los sistemas Cisco, y el ser un sistema libre lo hace claramente mucho más económico, pese al pago de licencias por el entorno de virtualización utilizado para las pruebas. A ello hay que sumarle también la portabilidad del propio sistema, ya que la posibilidad de poderse instalar en entornos virtuales permite clonar tantas copias de la máquina virtual como sean necesarias. Hay que destacar que el uso de sistemas virtualizados en el entorno VMware ya está implantado en las unidades de transmisiones del ET, con lo que el personal ya tiene la formación necesaria para poder instalar el sistema de enrutamiento Vynos sobre una máquina virtual. Como último apunte, cabe decir que el uso de los switches Catalyst 2960 de Cisco sería opcional, puesto que añadiendo interfaces de red físicas a nuestro sistema anfitrión se pueden separar las interfaces de salida de Vynos, lo que elimina la necesidad de establecer un enlace *trunk* entre la máquina anfitrión y el switch. Esta posibilidad se puede llevar a cabo con tarjetas de red Ethernet por USB, mucho más económicas que los switches Cisco.

Quagga por contra no se muestra tan eficiente como Vynos, ya que no dispone de funcionalidades de uso general como implementación de políticas QoS. Podría ser usado como un sistema de enrutamiento puro en nodos intermedios de la red, ya que es capaz de ejecutar los protocolos de enrutamiento con la misma eficiencia que Cisco o Vynos, pero no como puerta de enlace en nodos extremos, donde sí que se requiere implementar políticas de calidad de servicio y route-maps. En cuanto a facilidad de operación, el entorno de configuración de Quagga es similar a la CLI de los routers Cisco, teniendo los mismos comandos de configuración básicos para interfaces y protocolos de enrutamiento. No obstante hay que tener en cuenta que hay que dominar mínimamente el entorno Linux, así como la interfaz gráfica de configuración web de OpenWrt, lo cual no supone mayor reto. En el plano económico se puede considerar como el sistema más barato de los tres. Por ser un paquete software de Linux, también podría instalarse en una máquina virtual con un sistema operativo Linux instalado, con lo que se llegaría a tener una portabilidad similar a la de Vynos.

En cuanto a Cisco, era de esperar que superara con éxito las pruebas realizadas, puesto que es el sistema actualmente en uso ya en las unidades de transmisiones del ET. No obstante su coste sigue siendo muy superior al de los sistemas alternativos evaluados, no sólo por el precio de adquisición de los routers, sino también por el coste de las tarjetas de expansión a instalar en ellos y de los switches necesarios para completar las topologías.

Como última reflexión se puede decir que, a la vista de los resultados de este trabajo, es factible e incluso necesaria la exploración de sistemas alternativos de enrutamiento, en la búsqueda de opciones mucho más económicas e igual de eficientes que los sistemas Cisco actualmente implantados en las unidades de transmisiones del Ejército de Tierra español.

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

## 7 Bibliografía

- [1] A. S. TANENBAUM, Redes de Ordenadores, Prentice Hall, 2003.
- [2] Web <http://www.nongnu.org/quagga/> (Consultada en 2016).
- [3] Web [http://wiki.vyos.net/wiki/User\\_Guide](http://wiki.vyos.net/wiki/User_Guide) (Consultada en 2016).
- [4] Web <http://www.cisco.com>, Consultada en 2016.
- [5] AGM, Redes de Ordenadores, Zaragoza: Academia General Militar, 2015.
- [6] AGM, Sistemas de Transmisiones, Zaragoza: Academia General Militar, 2015.
- [7] K. ISHIGURO, Quagga, 2005.
- [8] Web <http://www.tp-link.es>, Consultada en 2016.
- [9] Web <https://openwrt.org/>, Consultada en 2016.
- [10] Web <https://openmaniak.com/quagga.php>.
- [11] Web <https://en.wikipedia.org/wiki/Vyatta> (Consultada en 2016).
- [12] Web <http://lubuntu.net/> (Consultada en 2016).
- [13] M. H. RYAN TROY, VMware Cookbook: A Real-World Guide to Effective VMware Use, O'reilly, 2012.
- [14] Web <http://ostinato.org/> (Consultada en 2016).
- [15] Web <https://www.pccomponentes.com> (Consultada en 2016).
- [16] E. Duarte, Implementación De Enrutamiento Dinámico En Linux, artículo web, 2014.

[Página intencionadamente en blanco]

## Anexo A: Características Técnicas de los routers Cisco 2821

Tabla Anexo A - 1: Características Técnicas Cisco modelo 2821

Cisco 2800 Series	Cisco 2821
Product Architecture	
DRAM	<ul style="list-style-type: none"> <li>• Default: 256 MB</li> <li>• Maximum: 1 GB</li> </ul>
Onboard LAN Ports	2-10/100/1000
Network-Module Slot	1 slot, supports NM, NME and NME-X type modules
Extension Voice Module Slot	1
PVDM (DSP) Slots on Motherboard	3
Wall Mounting	No
Power Requirements	
AC Input Current	3A (110V) 2A (230V)
AC-IP Maximum In-Line Power Distribution	240W
AC-IP Input Current	8A (110V) 4A (230V)
DC Input Current	<ul style="list-style-type: none"> <li>• 12A (24V)</li> <li>• 5A (60V)</li> <li>• Startup current 50A&lt;10 ms</li> </ul>
Typical Power Dissipation (No Modules)	54W (184 BTU/hr)
Power Dissipation-AC without IP Phone Support	280W (955 BTU/hr)
Power Dissipation-AC with IP Phone Support-System Only	310W (1058 BTU/hr)
Power Dissipation-AC with IP Phone Support-IP Phones	240W (819 BTU/hr)

PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

Power Dissipation-DC	300W (1024 BTU/hr)
Environmental Especification	
Dimensions (H x W x D)	<ul style="list-style-type: none"> <li>• 3.5 x 17.25 x 16.4 in.</li> <li>• (88.9 x 438.2 x 416.6 mm)</li> </ul>
Rack Height	2RU
Weight (Fully Configured)	25 lb (11.4 kg)
Noise Level (Min/Max)	<ul style="list-style-type: none"> <li>• 44 dBA for normal operating temperature (&lt;90°F/32.2°C)</li> <li>• 53 dBA (@ maximum fan speed)</li> </ul>
Regulatory Compliance	
NEBS	Yes

Fuente: [www.cisco.com](http://www.cisco.com)

## Anexo B: Características TP-Link modelo TL-WR1043ND

A continuación se describen las características técnicas del router TP-Link modelo TL-WR1043ND. [8]

### CARACTERÍSTICAS DE HARDWARE

- Interfaz 4 puertos LAN 10/100/1000Mbps
- 1 puerto WAN 10/100/1000Mbps
- 1 puerto USB 2.0
- Botones: Botón WPS/Reset
- Botón de encendido
- Botón Wi-Fi
- Antenas: 3 antenas omnidireccionales de 5dBi (RP-SMA)
- Fuente de Alimentación Externa 12VDC / 1.5A
- Estándares Inalámbricos IEEE 802.11n, IEEE 802.11g, IEEE 802.11b
- Dimensiones: 8.9 x 5.6 x 1.2 pulgadas. (225 x 141 x 30mm)

### CARACTERÍSTICAS INALÁMBRICAS

- Frecuencia 2.4-2.4835GHz
- Tasa de Señal
  - 11n: Hasta 450Mbps(dynamic)
  - 11g: Hasta 54Mbps(dynamic)
  - 11b: Hasta 11Mbps(dynamic)
- Sensibilidad de Recepción
  - 270M: -68dBm@10% PER
  - 130M: -68dBm@10% PER
  - 108M: -68dBm@10% PER
  - 54M: -68dBm@10% PER
  - 11M: -85dBm@8% PER
  - 6M: -88dBm@10% PER
  - 1M: -90dBm@8% PER
- Potencia de Transmisión
  - CE: <20dBm(2.4GHz)
  - FCC: <30dBm
- Funciones Inalámbricas Activación/desactivación señal inalámbrica, bridge WDS, WMM, estadísticas conexión inalámbrica
- Seguridad Inalámbrica 64/128/152-bit WEP / WPA / WPA2,WPA-PSK / WPA2-PSK

### Características de Software

- Calidad de Servicio: WMM, gestión de ancho de banda
- Tipo de WAN: IP dinámico / IP estático / PPPoE /PPTP (acceso dual)/L2TP (acceso dual)/servidor BigPond
- Gestión Control de acceso
  - Manejo Local
  - Manejo remoto
- DHCP Cliente, lista de clientes DHCP, reserva de direcciones

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

- Reenvío de Puertos: servidor virtual, activación de puertos, UPnP, DMZ
- DNS Dinámico: DynDns, Comexe, NO-IP
- VPN Pass-Through: PPTP, L2TP, IPSec (Cabecera ESP)
- Control de Acceso: Control parental, control de gestión local, lista de hosts, programación de acceso, gestión de reglas
- Seguridad Firewall
  - DoS, cortafuegos SPI
  - Filtrado de direcciones IP/filtrado de direcciones MAC/filtrado de dominios
  - Vinculación de direcciones IP y MAC
- Protocolos: Support IPv4 and IPv6
- Red de Invitados: 2.4GHz Guest Network×1
- Factores Ambientales
  - Temperatura de funcionamiento: 0°C ~ 40°C (32°F ~ 104°F)
  - Temperatura de almacenamiento: -40°C ~ 70°C (-40°F ~ 158°F)
  - Humedad de funcionamiento: 10% ~ 90% sin condensación
  - Humedad de almacenamiento: 5% ~ 90% sin condensación

## Anexo C: Inyector de paquetes Ostinato

Ostinato es un software de inyección de paquetes que ha permitido realizar las simulaciones de tráfico a través de la red en las pruebas de rendimiento. [14]

En este anexo se muestran las ventanas de configuración del software de inyección de paquetes Ostinato, software libre instalada en la máquina Linux Lubuntu 2, perteneciente a la LAN VTC de pruebas.

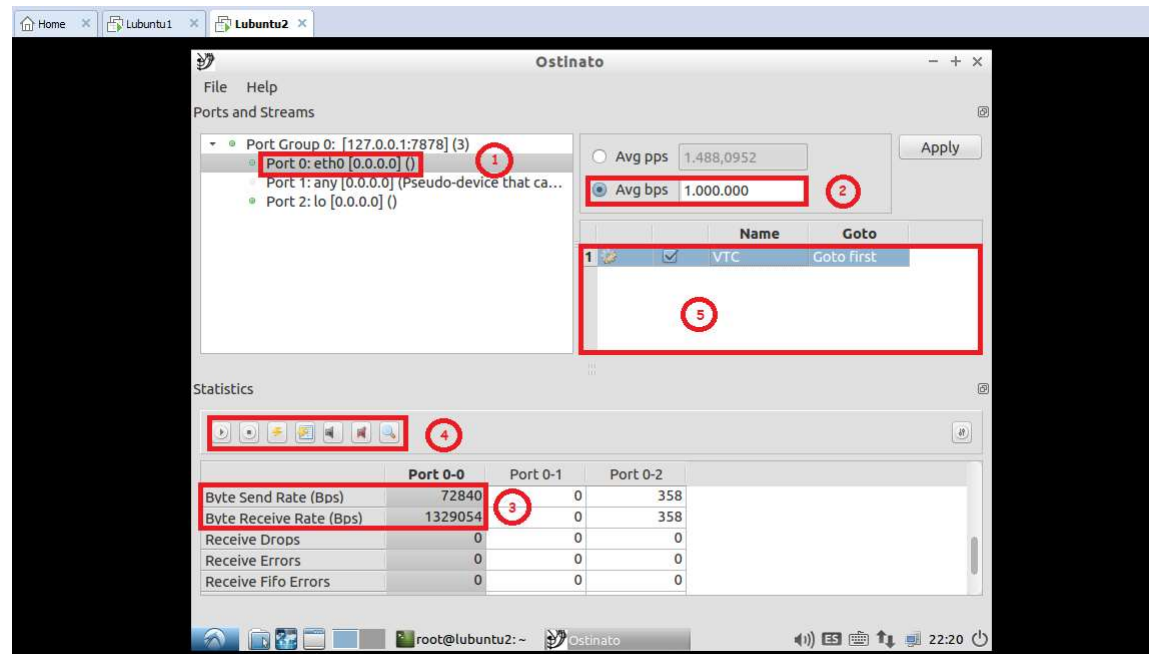


Figura Anexo C - 1: Vista de la interfaz de inyección de paquetes Ostinato

En la figura 1 del presente anexo se pueden distinguir los siguientes elementos:

1. Interfaz de salida de tráfico: esta es la interfaz de red de la máquina virtual
2. Ratio de inyección de paquetes: selecciona la velocidad de inyección de paquetes en bits/s
3. Cuadro de información de tráfico: facilita, entre otras cosas, información acerca de la velocidad de transmisión y recepción de tráfico en Bytes/s
4. Botones de operación: sirven para iniciar y parar la inyección, eliminar los datos estadísticos, e iniciar y parar la escucha de tráfico entrante a través de la interfaz.
5. Cuadro de *streams* en uso: las *streams* se configuran para regular el tráfico de inyección de paquetes así como para determinar el origen y destino de los mismos. Se pueden configurar varias *streams* de forma que se pueden usar de forma secuencial

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

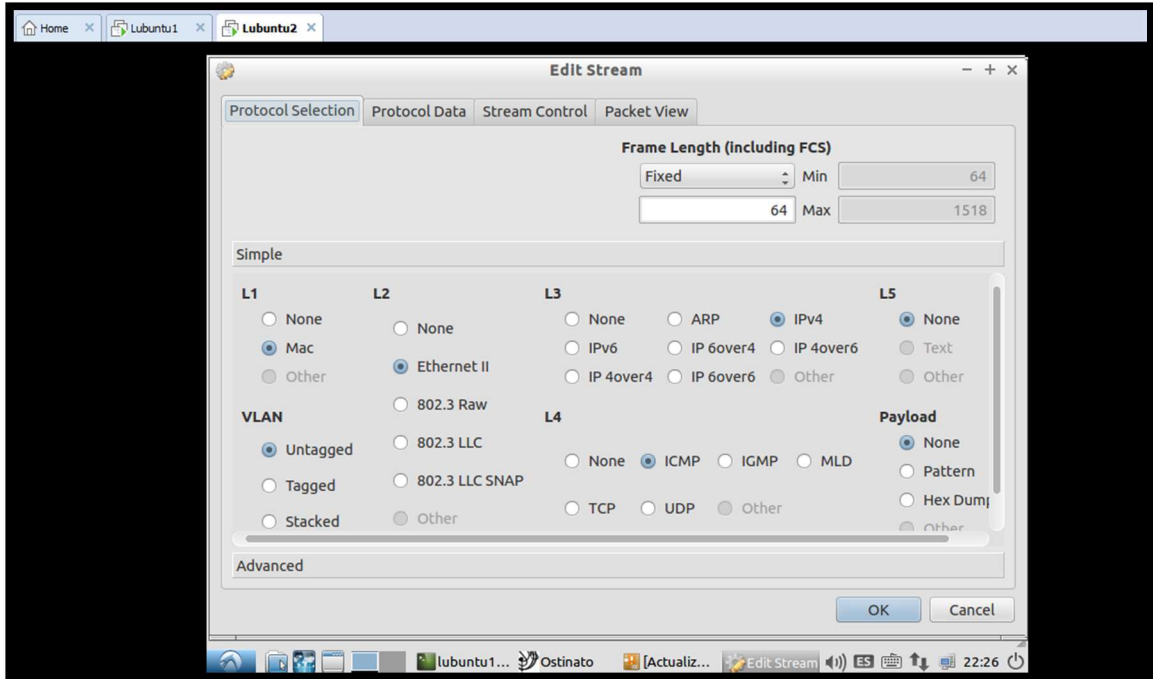


Figura Anexo C - 2: Interfaz de configuración de streams

En la figura C-2 se muestra la interfaz de configuración de *streams* de la aplicación Ostinato, con sus distintas pestañas de selección de protocolos, configuración de protocolos, control de tráfico del *stream* y la visión de los paquetes generados.

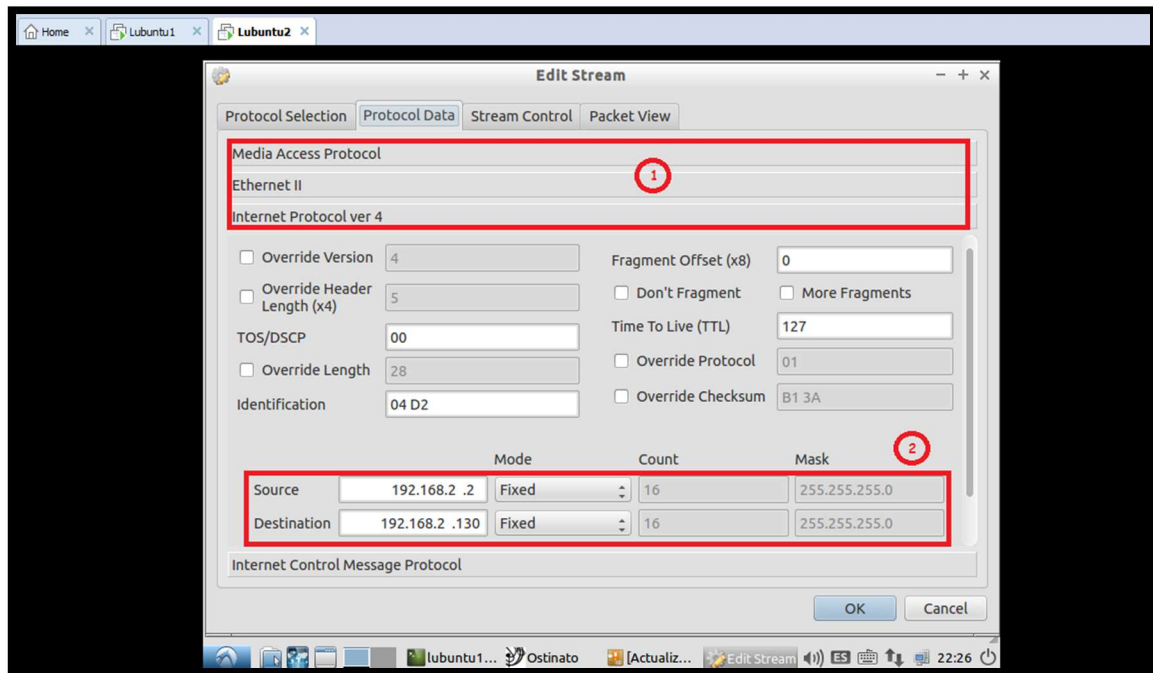


Figura Anexo C - 3: Interfaz de configuración de Stream en la pestaña de configuración de protocolo

En la figura C-3 se muestra la interfaz de configuración de protocolos: con los siguientes elementos resaltados:

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

1. Pestañas de acceso a configuración de las distintas capas OSI del tráfico a inyectar en el *stream*: en estas pestañas se pueden configurar toda la información necesaria para la confección de un *stream*, relativas a origen y destino de tráfico a nivel de capa 2 y capa 3 y contenido de los paquetes
2. Vista en detalle de la pestaña de configuración IP de los paquetes, con la dirección IP de origen y destino de los paquetes inyectados.

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

## Anexo D: Tablas de enrutamiento y configuración de interfaces de los router Cisco

```

R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/30 is subnetted, 2 subnets
O   172.16.1.8 [110/100] via 172.16.1.2, 02:06:39, Serial0/1/0
C   172.16.1.0 is directly connected, Serial0/1/0
192.168.3.0/26 is subnetted, 2 subnets
C   192.168.3.0 is directly connected, GigabitEthernet0/1.35
O   192.168.3.128 [110/101] via 172.16.1.2, 01:34:28, Serial0/1/0
192.168.1.0/26 is subnetted, 3 subnets
O   192.168.1.64 [110/51] via 172.16.1.2, 00:01:34, Serial0/1/0
C   192.168.1.0 is directly connected, GigabitEthernet0/1.25
O   192.168.1.128 [110/101] via 172.16.1.2, 02:06:40, Serial0/1/0
192.168.2.0/26 is subnetted, 3 subnets
O   192.168.2.64 [110/51] via 172.16.1.2, 00:01:35, Serial0/1/0
C   192.168.2.0 is directly connected, GigabitEthernet0/1.15
O   192.168.2.128 [110/101] via 172.16.1.2, 02:06:44, Serial0/1/0
192.168.0.0/32 is subnetted, 1 subnets
C   192.168.0.1 is directly connected, Loopback0
R1#_
    
```

Figura Anexo D - 1: Tabla de enrutamiento del router R1

En la figura D-1 se puede observar como el router como para llegar a las redes conectadas a los router R2 y R3 se usa el protocolo de enrutamiento OSPF, estando estas redes marcadas como una 'O' en el margen izquierdo de la tabla. Esto ocurre de manera análoga en los router R2 y R3.

```

R1#sh ip int br
Interface                IP-Address      OK? Method Status    Prot
ocol
GigabitEthernet0/0      172.16.1.5     YES manual  up        down
GigabitEthernet0/1      unassigned      YES manual  up         up
GigabitEthernet0/1.35   192.168.3.1    YES manual  up         up
GigabitEthernet0/1.15   192.168.2.1    YES manual  up         up
GigabitEthernet0/1.25   192.168.1.1    YES manual  up         up
Serial0/1/0              172.16.1.1     YES SLARP   up         up
Loopback0                192.168.0.1    YES manual  up         up
R1#_
    
```

Figura Anexo D - 2: Configuración de interfaces del router R1

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

En la figura D-2 se la configuración de las interfaces de red del router R1 asignadas de la siguiente manera:

- GigabitEthernet0/0: Interfaz de enlace R1-R3
- GigabitEthernet0/1.15: Sub-interfaz puerta de enlace para la LAN VTC
- GigabitEthernet0/1.25: Sub-interfaz puerta de enlace para la LAN VOIP
- GigabitEthernet0/1.35: Sub-interfaz puerta de enlace para la LAN MGM
- Serial0/1/0: Interfaz de enlace R1-R2
- Loopback0: La dirección de esta interfaz identifica al router cuando el protocolo OSPF publica sus rutas.

```
R2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/30 is subnetted, 2 subnets
C    172.16.1.8 is directly connected, Serial0/0/1
C    172.16.1.0 is directly connected, Serial0/0/0
192.168.3.0/26 is subnetted, 3 subnets
C    192.168.3.64 is directly connected, GigabitEthernet0/1.35
O    192.168.3.0 [110/51] via 172.16.1.1, 01:35:58, Serial0/0/0
O    192.168.3.128 [110/51] via 172.16.1.10, 01:35:21, Serial0/0/1
192.168.1.0/26 is subnetted, 3 subnets
C    192.168.1.64 is directly connected, GigabitEthernet0/1.25
O    192.168.1.0 [110/51] via 172.16.1.1, 02:07:23, Serial0/0/0
O    192.168.1.128 [110/51] via 172.16.1.10, 02:15:04, Serial0/0/1
192.168.2.0/26 is subnetted, 3 subnets
C    192.168.2.64 is directly connected, GigabitEthernet0/1.15
O    192.168.2.0 [110/51] via 172.16.1.1, 02:07:24, Serial0/0/0
O    192.168.2.128 [110/51] via 172.16.1.10, 02:15:06, Serial0/0/1
192.168.3.0/32 is subnetted, 1 subnets
C    192.168.0.2 is directly connected, Loopback0
R2#
```

Figura Anexo D - 3: Tabla de enrutamiento del router R2

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

```
R2#sh ip int br
Interface                               IP-Address      OK? Method Status      Prot
ocol
GigabitEthernet0/0                      unassigned      YES NVRAM   administratively down down
GigabitEthernet0/1                      unassigned      YES NVRAM   up          up
GigabitEthernet0/1.35                   192.168.3.65   YES manual  up          up
GigabitEthernet0/1.15                   192.168.2.65   YES NVRAM   up          up
GigabitEthernet0/1.19                   unassigned      YES unset   up          up
GigabitEthernet0/1.25                   192.168.1.65   YES NVRAM   up          up
Serial0/0/0                              172.16.1.2     YES NVRAM   up          up
Serial0/0/1                              172.16.1.9     YES NVRAM   up          up
Loopback0                                192.168.0.2    YES NVRAM   up          up
R2#_
```

Figura Anexo D - 4: Configuración de interfaces del router R2

En la figura D-4 se la configuración de las interfaces de red del router R1 asignadas de la siguiente manera:

- Serial0/0/0: Interfaz de enlace R1-R2: Interfaz de enlace R1-R3
- GigaBitEthernet0/1.15: Sub-interfaz puerta de enlace para la LAN VTC
- GigaBitEthernet0/1.25: Sub-interfaz puerta de enlace para la LAN VOIP
- GigaBitEthernet0/1.35: Sub-interfaz puerta de enlace para la LAN MGM
- Serial0/1/0: Interfaz de enlace R1-R2
- Loopback0: La dirección de esta interfaz identifica al router cuando el protocolo OSPF publica sus rutas.

```
R3#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/30 is subnetted, 2 subnets
C       172.16.1.8 is directly connected, Serial0/0/1
O       172.16.1.0 [110/100] via 172.16.1.9, 02:13:34, Serial0/0/1
192.168.5.0/32 is subnetted, 1 subnets
C       192.168.5.1 is directly connected, Loopback0
192.168.0.0/26 is subnetted, 2 subnets
O       192.168.0.0 [110/101] via 172.16.1.9, 01:37:26, Serial0/0/1
C       192.168.0.128 is directly connected, GigabitEthernet0/1.10
192.168.1.0/26 is subnetted, 3 subnets
O       192.168.1.64 [110/51] via 172.16.1.9, 00:03:56, Serial0/0/1
O       192.168.1.0 [110/101] via 172.16.1.9, 02:08:50, Serial0/0/1
C       192.168.1.128 is directly connected, GigabitEthernet0/1.25
192.168.2.0/26 is subnetted, 3 subnets
O       192.168.2.64 [110/51] via 172.16.1.9, 00:03:58, Serial0/0/1
O       192.168.2.0 [110/101] via 172.16.1.9, 02:08:53, Serial0/0/1
C       192.168.2.128 is directly connected, GigabitEthernet0/1.15
R3#_
```

Figura Anexo D - 6: Tabla de enrutamiento del router 3

```

R3#sh ip int br
Interface                               IP-Address   OK? Method Status        Prot
ocol
GigabitEthernet0/0                     unassigned   YES unset   administratively down down
GigabitEthernet0/1                     unassigned   YES manual up              up
GigabitEthernet0/1.35                   192.168.3.129 YES manual up              up
GigabitEthernet0/1.15                   192.168.2.129 YES manual up              up
GigabitEthernet0/1.25                   192.168.1.129 YES manual up              up
Serial0/0/0                             172.16.1.6   YES manual down            down
Serial0/0/1                             172.16.1.10  YES SLARP up              up
Loopback0                               192.168.0.3  YES manual up              up
R3#_

```

En la figura D-4 se la configuración de las interfaces de red del router R1 asignadas de la siguiente manera:

**Figura Anexo D - 7: Configuración de interfaces del router R3**

- Serial0/0/0: Interfaz de enlace R1-R2: Interfaz de enlace R1-R3
- GigaBitEthernet0/1.15: Sub-interfaz puerta de enlace para la LAN VTC
- GigaBitEthernet0/1.25: Sub-interfaz puerta de enlace para la LAN VOIP
- GigaBitEthernet0/1.35: Sub-interfaz puerta de enlace para la LAN MGM
- Serial0/1/0: Interfaz de enlace R1-R2

Loopback0: La dirección de esta interfaz identifica al router cuando el protocolo OSPF publica sus rutas.

## Anexo E: Comandos introducidos en el entorno de configuración de R1

La CLI está estructurada por niveles. En cada nivel el usuario tiene una serie de privilegios y acceso a distintas configuraciones. A continuación se detallan estos niveles. En general se puede hablar de 6 modos de configuración:

- Usuario: visualización de configuración del router.
- Privilegiado: mismas atribuciones que el modo usuario, permitiendo además salvar la configuración y reiniciar el dispositivo. Proporciona acceso al modo de configuración global.
- Configuración global: Configuración básica (hostname, mensaje del día, contraseñas de acceso a la configuración, etc.)
- Sub-modos de configuración: Interfaces, protocolos de enrutamiento, políticas QoS.

Existen además otros dos modos de operación: modo Rommon, que ejecuta una versión reducida del IOS y permite entre otras cosas una carga manual del IOS cuando este no se produce por algún fallo de forma automática, y el modo Setup, que permite una configuración interactiva cuando no existe un fichero de configuración previo que cargar al inicio. En la tabla E-1 se muestran los comandos introducidos en el router Cisco R1. [5]

```

cisco - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
User Access Verification
Password:
R1>en
Password:
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/30 is subnetted, 2 subnets
O   172.16.1.8 [110/100] via 172.16.1.2, 02:06:39, Serial0/1/0
C   172.16.1.0 is directly connected, Serial0/1/0
C   192.168.0.0/26 is subnetted, 2 subnets
O   192.168.0.0 is directly connected, GigabitEthernet0/1.10
O   192.168.0.128 [110/101] via 172.16.1.2, 01:34:28, Serial0/1/0
C   192.168.1.0/26 is subnetted, 3 subnets
O   192.168.1.64 [110/51] via 172.16.1.2, 00:01:34, Serial0/1/0
C   192.168.1.0 is directly connected, GigabitEthernet0/1.25
O   192.168.1.128 [110/101] via 172.16.1.2, 02:06:40, Serial0/1/0
C   192.168.2.0/26 is subnetted, 3 subnets
O   192.168.2.64 [110/51] via 172.16.1.2, 00:01:35, Serial0/1/0
O   192.168.2.0 is directly connected, GigabitEthernet0/1.15
C   192.168.2.128 [110/101] via 172.16.1.2, 02:06:44, Serial0/1/0
O   192.168.3.0/32 is subnetted, 1 subnets
C   192.168.3.1 is directly connected, Loopback0
R1#_
    
```

Figura Anexo E - 1: Vista de la CLI en modo privilegiado a mediante la aplicación Hyperterminal

Tabla Anexo E - 1: Configuración router Cisco R1

APARTADOS DE CONFIGURACIÓN	COMANDOS INTRODUCIDOS
HOSTNAME	hostname R1
PASSWORDS	enable secret cisco

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

<b>BANNER</b>	banner motd #El uso de este dispositivo esta restringido a los usuarios expresamente autorizados. Todos los usuarios estaran monitorizados constantemente y podran ser perseguidos en el caso de un uso fraudulento de este dispositivo. #
<b>SSH</b>	ip ssh version 2
	ip ssh source-interface loopback0
	crypto key zeroize rsa
	crypto key generate rsa general-keys modulus 1024
<b>SNMP</b>	snmp-server community Pruebas ro
	snmp-server enable traps
<b>CONF. GLOBAL</b>	service password-encryption
	no ip domain lookup
	ip http server
	ip http secure-server
<b>LINE VTY 0 4</b>	line vty 0 4
	password manabo
	transport input ssh
	login
<b>LINE CONSOLE</b>	line console 0
	password manabo
	login
<b>ACCESS LIST</b>	access-list 111 permit ip 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255
	access-list 112 permit ip 192.168.2.0 0.0.0.255 192.168.2.0 0.0.0.255
	access-list 113 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

	access-list 114 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
<b>QoS</b>	class-map match-any VOIP
	match access-group 111
	match access-group 113
	class-map match-any VTC
	match access-group 112
	match access-group 114
	policy-map marcado
	class VOIP
	set dscp ef
	class VTC
	set dscp af41
	policy-map prioridad
	class VOIP
	priority percent 25
	class VTC
	priority percent 50
<b>INTERFACES WAN</b>	<b>interface Serial0/1/0</b>
	description RED R1-R2
	clockrate 56000
	bandwidth 2000
	service-policy input marcado
	service-policy input prioridad

PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

	ip address 172.16.1.1 255.255.255.252
	no shutdown
	<b>interface GigabitEthernet0/0</b>
	description RED R1-R3
	bandwidth 150000
	service-policy input marcado
	service-policy input prioridad
	ip address 172.16.1.5 255.255.255.252
	no shutdown
<b>INTERFACES LAN</b>	<b>interface GigabitEthernet0/1</b>
	no ip address
	no shutdown
	<b>interface GigabitEthernet0/1.35</b>
	description RED GESTION
	encapsulation dot1q 35
	ip address 192.168.3.1 255.255.255.0
	no shutdown
	<b>interface GigabitEthernet0/1.15</b>
	description RED VTC
	encapsulation dot1q 15
	ip address 192.168.2.1 255.255.255.192
	no shutdown
	<b>interface GigabitEthernet0/1.25</b>

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

	description RED VOIP
	encapsulation dot1q 25
	ip address 192.168.1.1 255.255.255.192
	no shutdown
	<b>interface Loopback0</b>
	ip address 192.168.0.1 255.255.255.255
<b>OSPF</b>	<b>router ospf 1</b>
	network 172.16.1.0 0.0.0.3 area 0
	network 172.16.1.4 0.0.0.3 area 0
	network 192.168.2.0 0.0.0.63 area 0
	network 192.168.1.0 0.0.0.63 area 0
	network 192.168.3.0 0.0.0.63 area 0

### Explicación de apartados de configuración:

- Hostname: Se establece el nombre del router
- Passwords: Se establece el password de acceso al router
- Banner: Se establecen un mensaje de bienvenida al ingresar en el router
- Access-list: En este apartado se introducen comandos que permiten o deniegan el acceso de unas redes a otras
- QoS: En este apartado se introducen los comandos que sirven para establecer las políticas de servicio a aplicar posteriormente en las interfaces, tales como permisos de acceso y ancho de banda mínimo de servicio
- Interfaces WAN: Se configuran las interfaces serial para los enlaces punto a punto y se aplican las políticas de calidad de servicio y enrutamiento que se precisen.
- Interfaces LAN: Se configuran las interfaces para las redes LAN. También se configuran las sub-interfaces, que necesitan un encapsulado denominado 'dot1q' para trabajar con VLAN,s. Tener en cuenta que se trabaja con enlaces *trunk*, a través de los cuales, por una interfaz física entra y sale toda la información de las LAN,s.
- OSPF: Se configuran las redes que van a publicarse mediante el protocolo OSPF. Hay que tener en cuenta que hay que configurar una dirección IP en una interfaz Loopback del router para que sirva como identificador.



## Anexo F: Documentación gráfica de las pruebas Cisco



Figura Anexo F - 1: Nodo R1

En la figura F-1 se puede observar las conexiones del nodo R1. Los tres dispositivos del margen izquierdo de fotografía son, de abajo arriba, el router Cisco 2821, el switch Catalyst 2960 y el switch no configurable 3COM. Se observa también el ordenador portátil que sirve de anfitrión a las máquinas virtuales utilizadas en las pruebas.



Figura Anexo F - 2: Nodos R2 (izquierda) y R3 (derecha)

En la figura F-2 se puede observar la misma configuración de dispositivos que en el nodo R1, para los nodos R2 y R3 respectivamente, sustituyendo el switch 3COM por dos D-LINK.

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS



Figura Anexo F - 3: Detalle de las conexiones Ethernet y serial WIC del router R1



Figura Anexo F - 5: Pareja de antenas Ubiquiti utilizadas para el enlace entre R1 y R3



Figura Anexo F - 4: Estación satélite 'Asturias' utilizada en las pruebas

## Anexo G Configuración de interfaces en OpenWrt

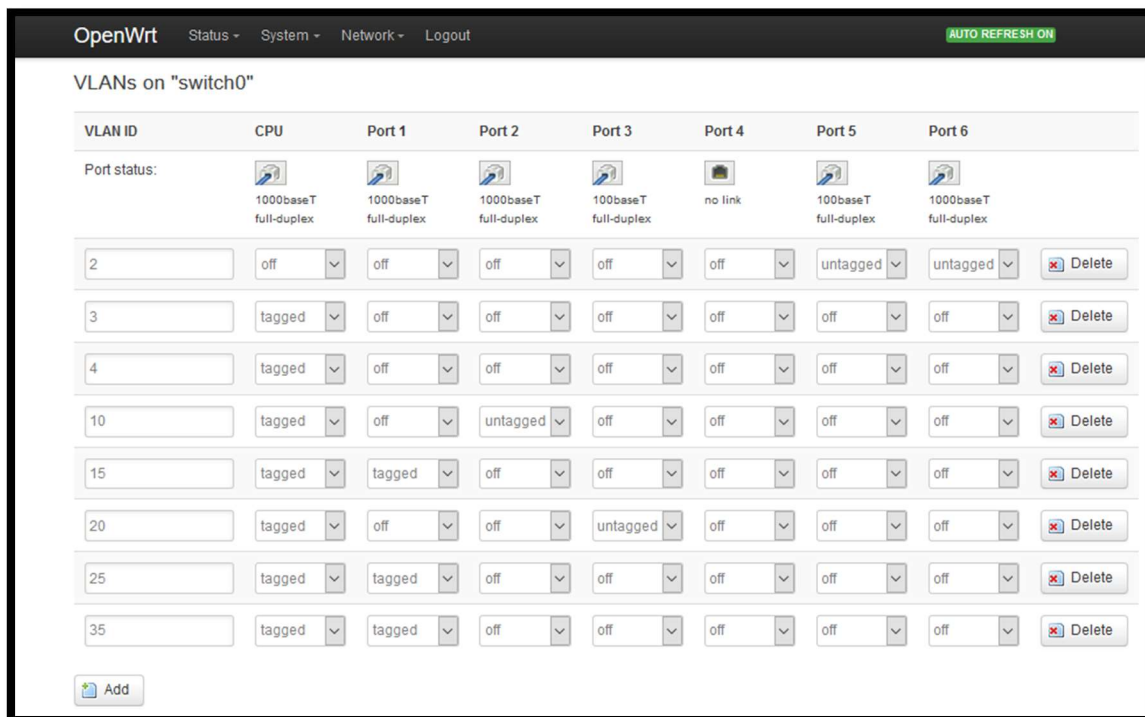


Figura Anexo G - 1: Configuración de puertos del router TP-Link mediante interfaz web

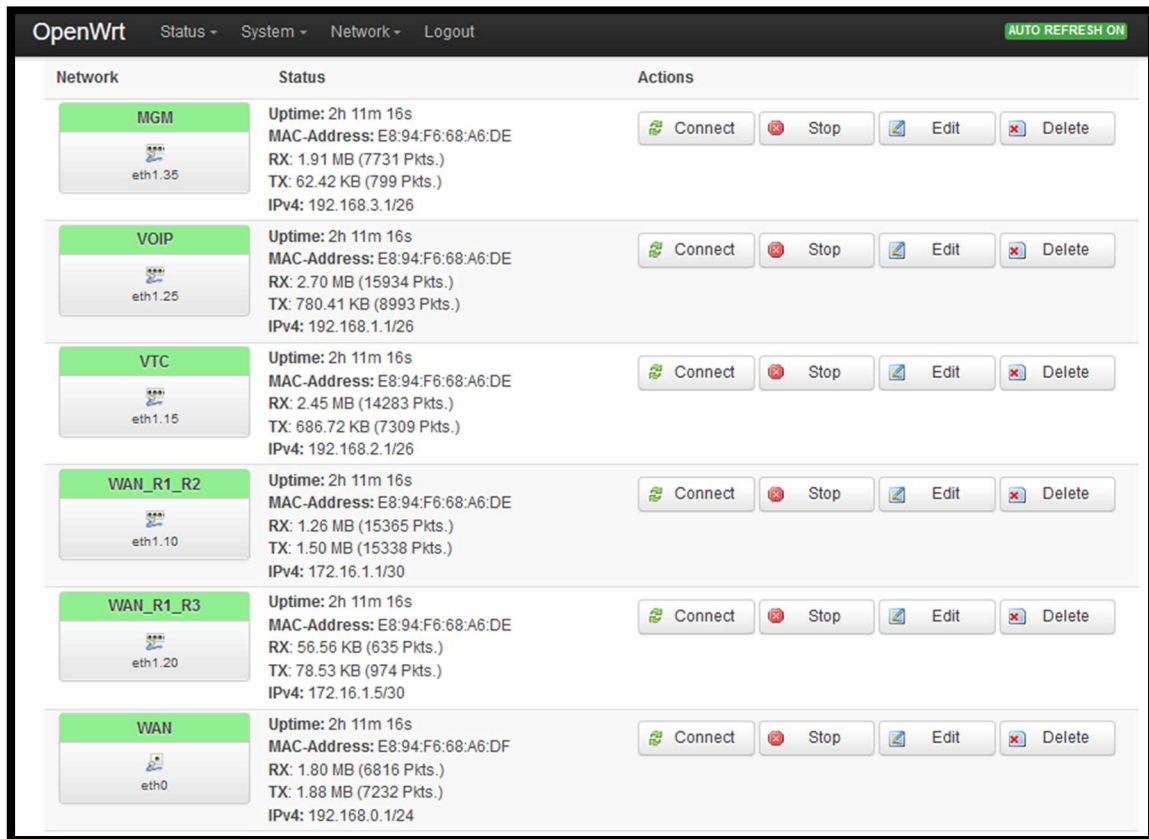
En este anexo se detalla la configuración de OpenWrt para separar sus interfaces en VLAN,s.

Según se puede ver en la figura G-1, en la columna izquierda se van añadiendo VLAN,s de forma que cada una va numerada tal y como se ha especificado para las pruebas. Los puertos 1-6 corresponden con los puertos físicos de salida, siendo el 5 y el 6 correspondientes al mismo puerto pero con velocidades de transmisión distintas de 100 Mbit/s y 1000Mbit/s respectivamente. Las VLAN 3 y 4 son auxiliares y están desactivadas. La VLAN 2 tiene correspondencia con el puerto 5/6 que es el puerto WAN de configuración.

Las etiquetas *tagged/untagged* significan que en el caso de estar seleccionado en *tagged*, los paquetes saldrán encapsulados por el puerto determinado número de VLAN que se le ha asignado. En caso de seleccionar *untagged*, no se efectuará dicho encapsulado

Una vez configurados los puertos físicos se configuran, también mediante interfaz web las interfaces y sub-interfaces dedicadas a cada VLAN, estableciendo los parámetros de dirección IP y máscara de red.

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS



The screenshot displays the OpenWrt web interface for network management. At the top, there are navigation menus for 'Status', 'System', 'Network', and 'Logout', along with an 'AUTO REFRESH ON' indicator. The main content is a table with three columns: 'Network', 'Status', and 'Actions'. Each row represents a network interface with its name, icon, and associated statistics and actions.

Network	Status	Actions
MGM eth1.35	Uptime: 2h 11m 16s MAC-Address: E8:94:F6:68:A6:DE RX: 1.91 MB (7731 Pkts.) TX: 62.42 KB (799 Pkts.) IPv4: 192.168.3.1/26	Connect Stop Edit Delete
VOIP eth1.25	Uptime: 2h 11m 16s MAC-Address: E8:94:F6:68:A6:DE RX: 2.70 MB (15934 Pkts.) TX: 780.41 KB (8993 Pkts.) IPv4: 192.168.1.1/26	Connect Stop Edit Delete
VTC eth1.15	Uptime: 2h 11m 16s MAC-Address: E8:94:F6:68:A6:DE RX: 2.45 MB (14283 Pkts.) TX: 686.72 KB (7309 Pkts.) IPv4: 192.168.2.1/26	Connect Stop Edit Delete
WAN_R1_R2 eth1.10	Uptime: 2h 11m 16s MAC-Address: E8:94:F6:68:A6:DE RX: 1.26 MB (15365 Pkts.) TX: 1.50 MB (15338 Pkts.) IPv4: 172.16.1.1/30	Connect Stop Edit Delete
WAN_R1_R3 eth1.20	Uptime: 2h 11m 16s MAC-Address: E8:94:F6:68:A6:DE RX: 56.56 KB (635 Pkts.) TX: 78.53 KB (974 Pkts.) IPv4: 172.16.1.5/30	Connect Stop Edit Delete
WAN eth0	Uptime: 2h 11m 16s MAC-Address: E8:94:F6:68:A6:DF RX: 1.80 MB (6816 Pkts.) TX: 1.88 MB (7232 Pkts.) IPv4: 192.168.0.1/24	Connect Stop Edit Delete

Figura Anexo G - 2: Detalle de configuración de interfaces en OpenWrt mediante interfaz web

En la figura G-2 se puede comprobar cómo quedan configuradas las interfaces de red una vez establecidos todos los parámetros. A cada interfaz se le puede asignar un nombre. El caso de la figura corresponde al router R1.

## Anexo H: Herramienta Realtek Ethernet Diagnostic Utility

En este anexo se muestra la configuración de sub-interfaces de red con la herramienta Realtek Ethernet Diagnostic Utility, la cual permite crear VLAN,s. En las pruebas con Quagga, las interfaces de red de las máquinas virtuales se han conectado a estas VLAN,s para darles salida al exterior, tal y como se muestra en la figura 3-8.

En la figura H-1 se puede ver la creación de las sub-interfaces de la NIC física de uno de los ordenadores que han hecho de máquina anfitrión, las cuales se puede ver su correspondencia con las interfaces Ethernet 3, 4 y 5 de los adaptadores de red de la figura H-2.

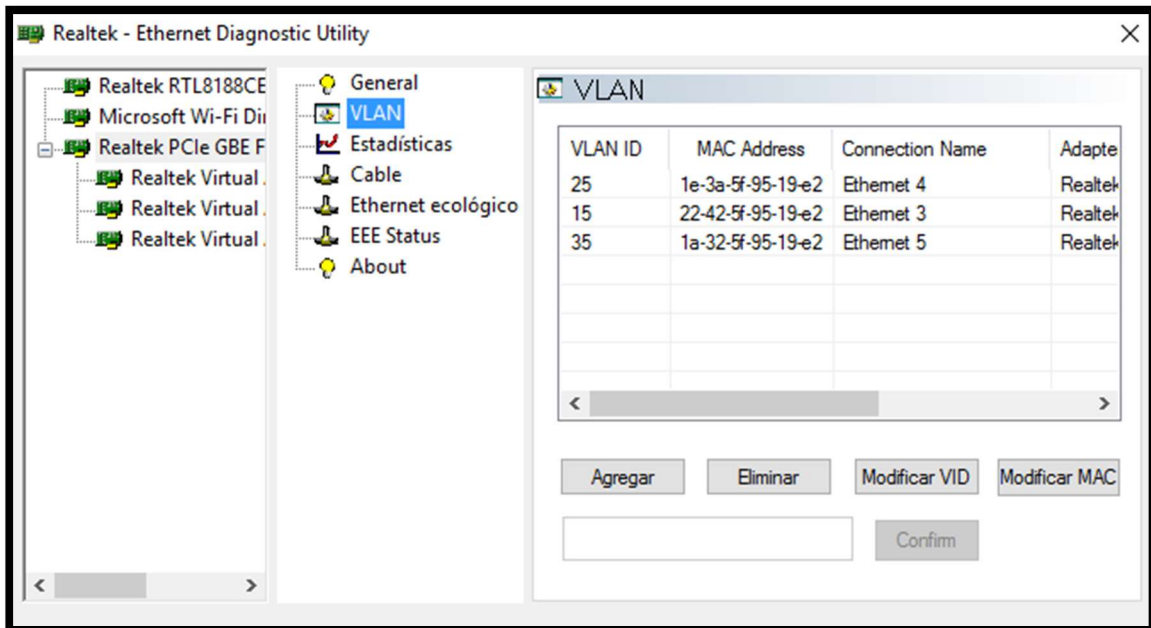


Figura Anexo H - 1: Interfaz de configuración Realtek Ethernet Diagnostic Utility

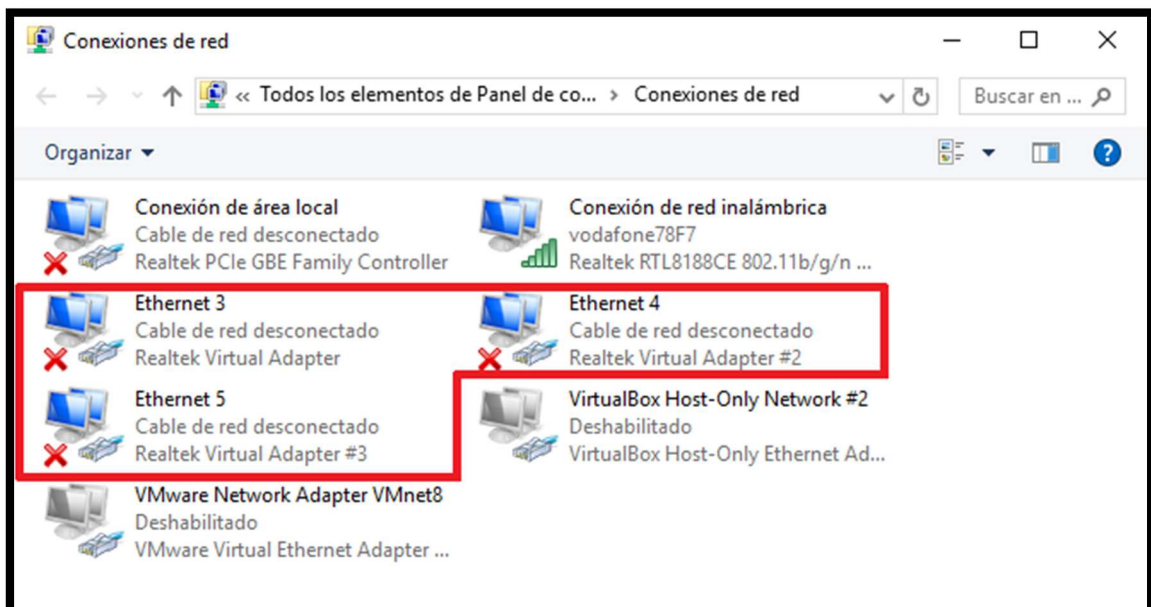


Figura Anexo H - 2: Interfaces sub-interfaces virtuales de red de la NIC física



## Anexo I: Tablas de enrutamiento de Quagga

En este anexo se muestran las tablas de enrutamiento de los tres routers configurados en las pruebas, como evidencia del funcionamiento del protocolo de enrutamiento OSPF. Como puede comprobarse, es una tabla similar a las confeccionadas por el IOS de Cisco, tal y como se muestra en las figuras I-1, I-2 e I-3.

```

R1# sh ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, H - HSL, o - OLSR,
       b - BATMAN, A - Babel,
       > - selected route, * - FIB route

K * 0.0.0.0/0 via 192.168.43.1, unknown inactive, src 192.168.43.115
C>* 127.0.0.0/8 is directly connected, lo
O  172.16.1.0/30 [110/10] is directly connected, eth1.10, 03w1d00h
C>* 172.16.1.0/30 is directly connected, eth1.10
O  172.16.1.4/30 [110/10] is directly connected, eth1.20, 03w1d00h
C>* 172.16.1.4/30 is directly connected, eth1.20
O>* 172.16.1.8/30 [110/20] via 172.16.1.2, eth1.10, 00:16:12
   *
   *      via 172.16.1.6, eth1.20, 00:16:12
C>* 192.168.0.0/24 is directly connected, eth0
O  192.168.1.0/26 [110/10] is directly connected, eth1.25, 03w1d00h
C>* 192.168.1.0/26 is directly connected, eth1.25
O>* 192.168.1.64/26 [110/20] via 172.16.1.2, eth1.10, 03w1d00h
O>* 192.168.1.128/26 [110/20] via 172.16.1.6, eth1.20, 00:16:12
O  192.168.2.0/26 [110/10] is directly connected, eth1.15, 03w1d00h
C>* 192.168.2.0/26 is directly connected, eth1.15
O>* 192.168.2.64/26 [110/20] via 172.16.1.2, eth1.10, 03w1d00h
O>* 192.168.2.128/26 [110/20] via 172.16.1.6, eth1.20, 00:16:12
O  192.168.3.0/26 [110/10] is directly connected, eth1.35, 03w1d00h
C>* 192.168.3.0/26 is directly connected, eth1.35
O>* 192.168.3.128/26 [110/20] via 172.16.1.6, eth1.20, 00:16:12
K * 192.168.43.1/32 is directly connected, unknown inactive
R1#

```

Figura Anexo I - 1: Tabla de enrutamiento del router R1

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

```
192.168.0.1 - PuTTY
R2(config)# exit
R2# sh ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, H - HSLs, o - OLSR,
       b - BATMAN, A - Babel,
       > - selected route, * - FIB route

C>* 127.0.0.0/8 is directly connected, lo
C>* 127.0.0.2/32 is directly connected, lo
O 172.16.1.0/30 [110/10] is directly connected, eth1.10, 03:08:49
C>* 172.16.1.0/30 is directly connected, eth1.10
O>* 172.16.1.4/30 [110/20] via 172.16.1.1, eth1.10, 00:20:39
   *                               via 172.16.1.10, eth1.30, 00:20:39
O 172.16.1.8/30 [110/10] is directly connected, eth1.30, 03:08:49
C>* 172.16.1.8/30 is directly connected, eth1.30
C>* 192.168.0.0/30 is directly connected, eth0
O>* 192.168.1.0/26 [110/20] via 172.16.1.1, eth1.10, 02:12:34
O 192.168.1.64/26 [110/10] is directly connected, eth1.25, 03:08:49
C>* 192.168.1.64/26 is directly connected, eth1.25
O>* 192.168.1.128/26 [110/20] via 172.16.1.10, eth1.30, 00:22:39
O>* 192.168.2.0/26 [110/20] via 172.16.1.1, eth1.10, 02:12:34
O 192.168.2.64/26 [110/10] is directly connected, eth1.15, 03:08:49
C>* 192.168.2.64/26 is directly connected, eth1.15
O>* 192.168.2.128/26 [110/20] via 172.16.1.10, eth1.30, 00:22:39
O>* 192.168.3.0/26 [110/20] via 172.16.1.1, eth1.10, 02:12:34
O>* 192.168.3.128/26 [110/20] via 172.16.1.10, eth1.30, 00:22:39
R2#
```

Figura Anexo I - 2: Tabla de enrutamiento del Router R2

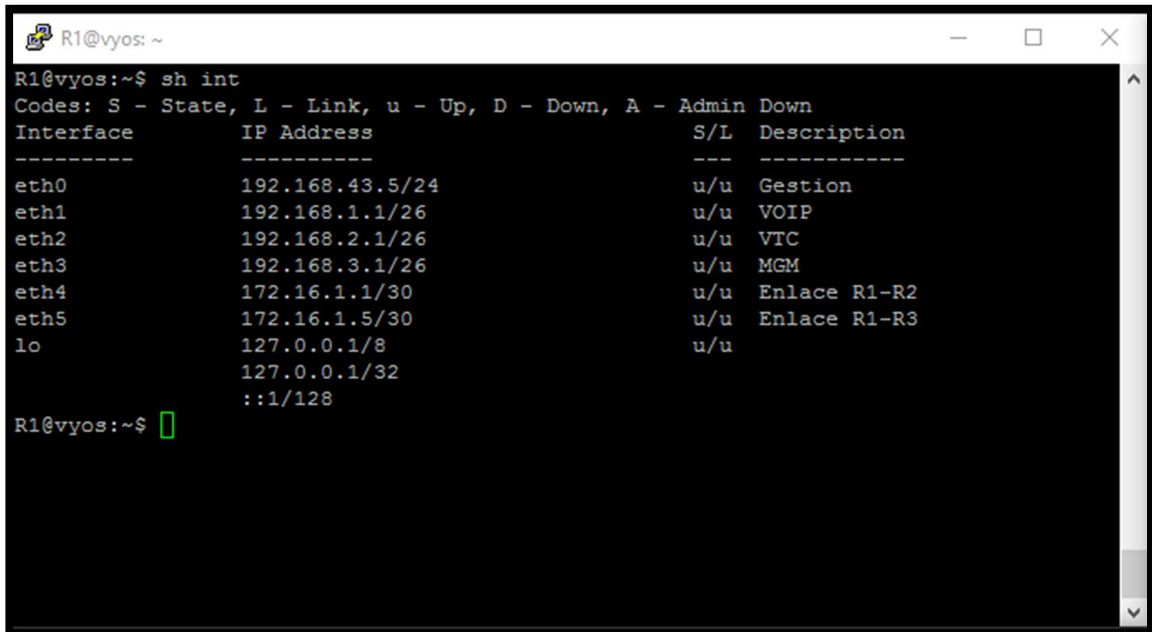
```
192.168.0.1 - PuTTY
R3# sh ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, H - HSLs, o - OLSR,
       b - BATMAN, A - Babel,
       > - selected route, * - FIB route

C>* 127.0.0.0/8 is directly connected, lo
C>* 127.0.0.3/32 is directly connected, lo
O>* 172.16.1.0/30 [110/20] via 172.16.1.5, eth1.20, 00:22:39
   *                               via 172.16.1.9, eth1.30, 00:22:39
O 172.16.1.4/30 [110/10] is directly connected, eth1.20, 00:31:11
C>* 172.16.1.4/30 is directly connected, eth1.20
O 172.16.1.8/30 [110/10] is directly connected, eth1.30, 00:31:11
C>* 172.16.1.8/30 is directly connected, eth1.30
C>* 192.168.0.0/24 is directly connected, eth0
O>* 192.168.1.0/26 [110/20] via 172.16.1.5, eth1.20, 00:22:39
O>* 192.168.1.64/26 [110/20] via 172.16.1.9, eth1.30, 00:24:40
O 192.168.1.128/26 [110/10] is directly connected, eth1.25, 00:31:11
C>* 192.168.1.128/26 is directly connected, eth1.25
O>* 192.168.2.0/26 [110/20] via 172.16.1.5, eth1.20, 00:22:39
O>* 192.168.2.64/26 [110/20] via 172.16.1.9, eth1.30, 00:24:40
O 192.168.2.128/26 [110/10] is directly connected, eth1.15, 00:31:11
C>* 192.168.2.128/26 is directly connected, eth1.15
O>* 192.168.3.0/26 [110/20] via 172.16.1.5, eth1.20, 00:22:39
O 192.168.3.128/26 [110/10] is directly connected, eth1.35, 00:31:11
C>* 192.168.3.128/26 is directly connected, eth1.35
R3#
```

Figura Anexo I - 3: Tabla de enrutamiento del router R3

## Anexo J: Configuración de interfaces Vyos

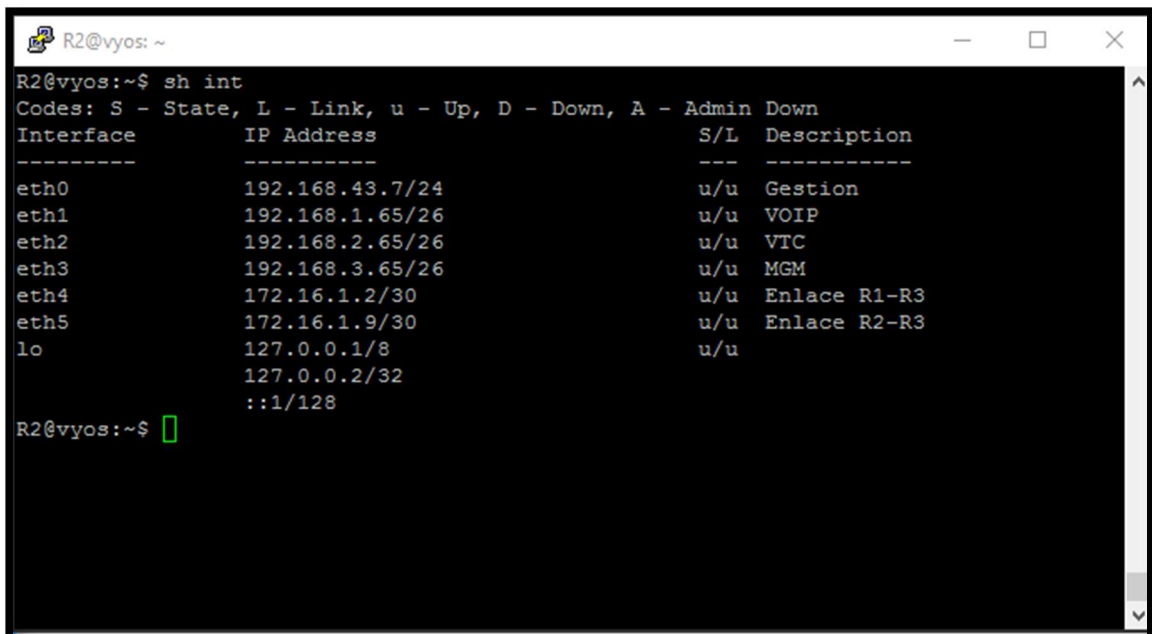
A continuación, en las figuras J-1, J-2 y J-3 se muestran las configuraciones de las interfaces de los router Vyos, mostrados mediante CLI abierta con la herramienta de conexiones remotas PuTTY.



```

R1@vyos:~$ sh int
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface      IP Address      S/L  Description
-----
eth0           192.168.43.5/24 u/u   Gestion
eth1           192.168.1.1/26  u/u   VOIP
eth2           192.168.2.1/26  u/u   VTC
eth3           192.168.3.1/26  u/u   MGM
eth4           172.16.1.1/30   u/u   Enlace R1-R2
eth5           172.16.1.5/30   u/u   Enlace R1-R3
lo             127.0.0.1/8     u/u
              127.0.0.1/32
              ::1/128
R1@vyos:~$
    
```

Figura Anexo J - 1: Configuración de interfaces del router R1

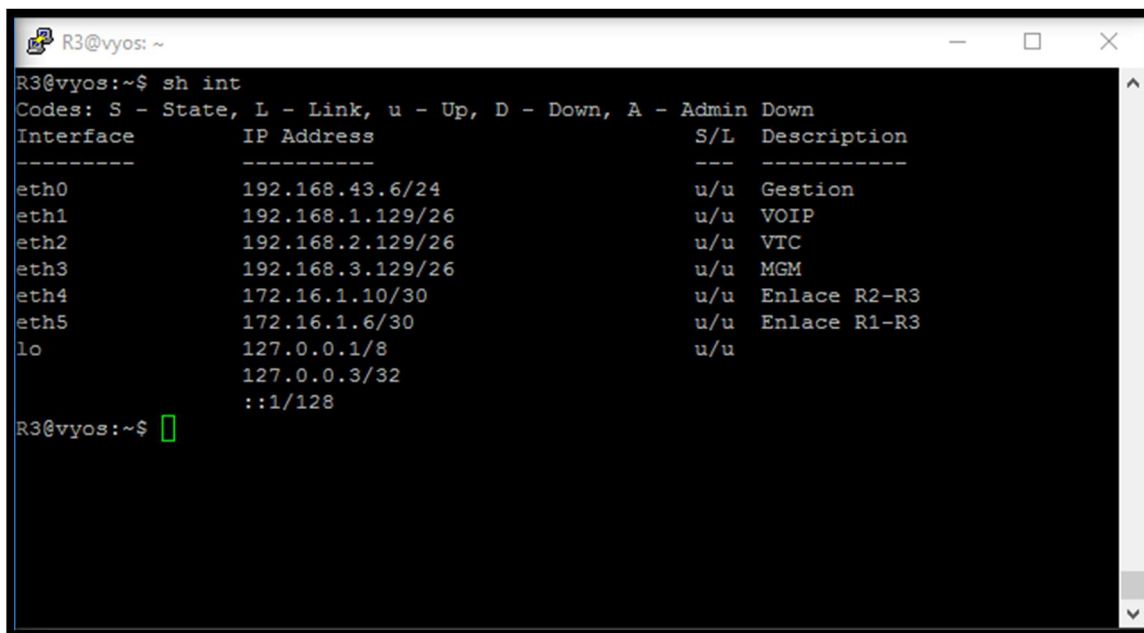


```

R2@vyos:~$ sh int
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface      IP Address      S/L  Description
-----
eth0           192.168.43.7/24 u/u   Gestion
eth1           192.168.1.65/26 u/u   VOIP
eth2           192.168.2.65/26 u/u   VTC
eth3           192.168.3.65/26 u/u   MGM
eth4           172.16.1.2/30   u/u   Enlace R1-R3
eth5           172.16.1.9/30   u/u   Enlace R2-R3
lo             127.0.0.1/8     u/u
              127.0.0.2/32
              ::1/128
R2@vyos:~$
    
```

Figura Anexo J - 2: Configuración de interfaces del router R2

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS



```
R3@vyos: ~  
R3@vyos:~$ sh int  
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down  
Interface      IP Address      S/L  Description  
-----  
eth0           192.168.43.6/24 u/u   Gestion  
eth1           192.168.1.129/26 u/u   VOIP  
eth2           192.168.2.129/26 u/u   VTC  
eth3           192.168.3.129/26 u/u   MGM  
eth4           172.16.1.10/30  u/u   Enlace R2-R3  
eth5           172.16.1.6/30   u/u   Enlace R1-R3  
lo             127.0.0.1/8     u/u  
              127.0.0.3/32  
              ::1/128  
R3@vyos:~$
```

Figura Anexo J - 3: Configuración de interfaces del router R3

## Anexo K: Comandos de configuración de los routers Vynos

En este anexo se detallan los comandos utilizados para la configuración del router Vynos R1. Por tener una configuración análoga, se han omitido las configuraciones de los routers R2 y R3.

Tabla Anexo K - 1: Configuración del router Vynos R1

APARTADOS DE CONFIGURACIÓN	COMANDOS INTRODUCIDOS
<b>HOSTNAME</b>	set system login user R1 full-name R1
<b>PASSWORDS</b>	set system login user R1 authentication plaintext-password vyos
	set system login user R1 level admin
<b>SSH</b>	set service ssh port '22'
<b>QoS</b>	set traffic-policy shaper VOIP bandwidth 256kbit
	set traffic-policy shaper VTC bandwidth 512kbit
	set traffic-policy limiter WAN_SATELITE 2000kbit
	set policy access-list 101 rule 10 action permit
	set policy access-list 101 rule 10 destination network 192.168.1.0
	set policy access list 101 rule 10 source network 192.168.1.0
	set policy access list 101 rule 10 inverse-mask 0.0.0.255
	set policy route-map VOIP rule 10 action permit
	set policy route-map VOIP
	set policy route-map VOIP rule 10 match ip address access-list 101
	set policy access-list 102 rule 10 action permit
	set policy access-list 102 rule 10 destination network 192.168.2.0
	set policy access list 102 rule 10 source network 192.168.2.0

## PLATAFORMAS DE ENRUTAMIENTO ALTERNATIVAS

	set policy access list 102 rule 10 inverse-mask 0.0.0.255
	set policy route-map VTC rule 10 action permit
	set policy route-map VTC
	set policy route-map VTC rule 10 match ip address access-list 101
<b>INTERFACES WAN</b>	set interfaces Ethernet eth4 description 'Enlace R1-R2'
	set interfaces Ethernet eth4 address '172.16.1.1/30'
	set interfaces Ethernet eth4 traffic-policy WAN_SATELITE
	set interfaces Ethernet eth5 description 'Enlace R1-R3'
	set interfaces Ethernet eth5 address '172.16.1.5/30'
<b>INTERFACES LAN</b>	set interfaces Ethernet eth1 address '192.168.1.1/26'
	set interfaces Ethernet eth1 description 'VOIP'
	set interfaces Ethernet eth1 traffic-policy VOIP
	set interfaces Ethernet eth2 address '192.168.2.1/26'
	set interfaces Ethernet eth2 description 'VTC'
	set interfaces Ethernet eth1 traffic-policy VTC
	set interfaces Ethernet eth3 address '192.168.3.1/26'
	set interfaces Ethernet eth3 description 'MGM'
<b>OSPF</b>	set interfaces loopback lo address 127.0.0.1/32
	set protocols ospf area 0 network 192.168.1.0/26
	set protocols ospf area 0 network 192.168.2.0/26
	set protocols ospf area 0 network 192.168.3.0/26
	set protocols ospf area 0 network 172.16.1.0/30
	set protocols ospf area 0 network 172.16.1.4/30

Explicación de apartados de configuración:

- **Hostname:** Se establece el nombre del router
- **Passwords:** Se establece el password de acceso al router
- **Access-list:** En este apartado se introducen comandos que permiten o deniegan el acceso de unas redes a otras
- **QoS:** En este apartado se introducen los comandos que sirven para establecer las políticas de servicio a aplicar posteriormente en las interfaces, tales como permisos de acceso y ancho de banda mínimo de servicio. También se configuran las access-list que permiten después la transición de tráfico sólo entre las redes permitidas.
- **Interfaces WAN:** Se configuran las interfaces serial para los enlaces punto a punto y se aplican las políticas de calidad de servicio y enrutamiento que se precisen.
- **Interfaces LAN:** Se configuran las interfaces para las redes LAN. También se configuran las sub-interfaces, que necesitan un encapsulado denominado 'dot1q' para trabajar con VLAN,s. Tener en cuenta que se trabaja con enlaces *trunk*, a través de los cuales, por una interfaz física entra y sale toda la información de las LAN,s. Se aplican también las políticas de calidad de servicio y enrutamiento que se precisen.
  - **OSPF:** Se configuran las redes que van a publicarse mediante el protocolo OSPF. Hay que tener en cuenta que hay que configurar una dirección IP en una interfaz Loopback del router para que sirva como identificador.

