

Documentación: Proyecto final plataformas I

Lina M. Andrade Gomez

Samuel D. Barona Puente

Kevin S. Nieto Curaca

Ricardo Urbina Ospina

Juan M. Velosa Valencia

Plataformas I

Ing. Nicolas Javier Salazar Echeverry

Universidad Icesi

Facultad Barberi de Ingeniería,

Diseño y Ciencias aplicadas

Cali

2025

Resumen

En el presente documento se expone la arquitectura diseñada para la implementación del sistema propuesto. Se detallan los componentes de red, la disposición física de los equipos, el diseño del sistema de almacenamiento, así como los requerimientos funcionales obtenidos mediante la metodología EARS. Además, se presenta una tabla descriptiva con las especificaciones técnicas de los equipos seleccionados. Este informe tiene como objetivo documentar de forma integral la infraestructura planteada para el desarrollo del proyecto.

Tabla de contenido

Introducción.....	4
Desarrollo del proyecto	5
Diseño sistema de almacenamiento de los servidores principales	5
Diagrama lógico de red	12
Descripción de los equipos utilizados	19
Distribución física de los equipos de rack	20
Análisis de requerimientos (Metodología EARS)	22
Repositorio de archivos de configuración	24
Conclusiones.....	25
Referencias	26

Introducción

El presente proyecto tiene como objetivo presentar el diseño e implementación de una infraestructura de red y servicios, dando respuesta a lo planteado al inicio del curso, donde se estableció la necesidad de implementar un sistema de red basado en GPON, como los utilizados por los ISPs para la prestación de servicios de internet. Integrando los diferentes conocimientos adquiridos y poniendo en práctica los conceptos abordados en clases, se llevó a cabo la virtualización de los entornos y la integración de diversos servicios de red —tales como DNS, DHCP, NTP, servidor de correo electrónico, servidores web, reverse proxy y balanceo de carga— con el fin de simular un entorno controlado que permita analizar el comportamiento, rendimiento y escalabilidad de los sistemas bajo diferentes escenarios de operación.

Para lograrlo, se emplearon dos servidores principales, denominados CJ y Faraday, cada uno con roles y características particulares, lo que permitió aplicar distintas estrategias de almacenamiento, gestión de servicios y configuración de red, adaptadas a los objetivos específicos de la infraestructura.

Desarrollo del proyecto

Diseño sistema de almacenamiento de los servidores principales

Antes de iniciar con el diseño del sistema de almacenamiento, es importante detallar las características de los servidores utilizados dentro de la arquitectura propuesta, los cuales corresponden a los equipos denominados CJ y Faraday.

CJ:

En el caso del servidor CJ, se procedió a validar la configuración actual de almacenamiento mediante el uso de diferentes comandos del sistema:

- Inicialmente, se utilizó el comando *lsblk* para identificar los discos físicos conectados al sistema.

```
cj@admincj:~$ lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0                              7:0      0 50.9M  1 loop /snap/snapd/24505
loop1                              7:1      0 73.9M  1 loop /snap/core22/1963
loop2                              7:2      0  4.4M  1 loop /snap/tree/54
loop3                              7:3      0 73.9M  1 loop /snap/core22/1981
sda                                8:0      0  1.8T  0 disk
├─sda1                             8:1      0    1G  0 part /boot/efi
├─sda2                             8:2      0    2G  0 part /boot
└─sda3                             8:3      0  1.8T  0 part
   └─ubuntu--vg-ubuntu--lv 252:0  0 100G  0 lvm /
```

Fig. 1. Resultado del comando *lsblk* en el servidor CJ.

Posteriormente, se verificó el uso y disponibilidad de espacio en disco a través del comando *df* con la opción *-h*, permitiendo visualizar los tamaños en un formato legible (human-readable).

```
cj@admincj:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           750M  1.9M  749M   1% /run
efivarfs        304K   55K  245K  19% /sys/firmware/efi/efivars
/dev/mapper/ubuntu--vg-ubuntu--lv 98G   62G   32G  66% /
tmpfs           3.7G    0   3.7G   0% /dev/shm
tmpfs           5.0M    0   5.0M   0% /run/lock
/dev/sda2       2.0G  190M  1.6G  11% /boot
/dev/sda1       1.1G   6.2M  1.1G   1% /boot/efi
tmpfs           750M   16K  750M   1% /run/user/1000
```

Fig. 2. Resultado del comando *df* en el servidor CJ.

Finalmente, se revisaron las particiones y la estructura exacta de almacenamiento creada en el sistema de archivos.

```

cj@admincj:~$ sudo parted /dev/sda unit GB print
[sudo] password for cj:
Model: ATA HUS722T2TALA600 (scsi)
Disk /dev/sda: 2000GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start   End     Size    File system  Name  Flags
  1      0.00GB  1.13GB  1.13GB  fat32                boot, esp
  2      1.13GB  3.28GB  2.15GB  ext4
  3      3.28GB  2000GB  1997GB

```

Fig. 3. Resultado del comando parted en el servidor CJ.

Como resultado de este análisis, se identifica que el servidor cuenta con un disco físico de 2 TB, el cual está particionado de la siguiente forma:

- Una partición EFI de aproximadamente 1 GB.
- Una partición de arranque (/boot) de aproximadamente 2 GB.
- El espacio restante se encuentra asignado a una partición principal gestionada mediante LVM (Logical Volume Manager).

Dentro del esquema LVM, se creó un grupo de volúmenes denominado ubuntu-vg, sobre el cual se asignó un volumen lógico (ubuntu-lv) con una capacidad de 100 GB, el cual corresponde al punto de montaje principal del sistema (/).

Cabe resaltar que, aunque el sistema actual cumple con los requerimientos funcionales para el entorno de pruebas, su diseño permite futuras optimizaciones,

tanto en términos de asignación de espacio como de rendimiento, gracias a la flexibilidad que proporciona la gestión mediante LVM.

Entre los aspectos a optimizar se tienen los siguientes:

- Aproximadamente solo el 5.5% del espacio en ubuntu-vg está asignado.
- No hay implementación de algún tipo de RAID, lo que supone un riesgo ante fallos de disco.
- Todos los servicios (DNS, DHCP, SMTP, NTP) comparten el mismo LV (/), lo que puede causar cuellos de botella.

Para ello, se propone que:

Con el objetivo de mejorar el aislamiento, el rendimiento y la administración de los servicios implementados, se propone crear volúmenes lógicos dedicados para cada uno de los servicios principales. De este modo, cada servicio (DNS, DHCP, NTP, SMTP, ...) dispondría de su propio volumen lógico, reduciendo la posibilidad de interferencias entre ellos en términos de uso de disco.

Inicialmente, a cada volumen lógico se le asignaría una capacidad mínima de 15 GB. No obstante, es importante destacar que, al emplear LVM (Logical Volume Manager), los tamaños de los volúmenes pueden ser ajustados dinámicamente en el futuro utilizando herramientas como *lvextend*, en función de las necesidades operativas que vayan surgiendo.

Cada uno de estos volúmenes sería montado en rutas específicas dentro del sistema de archivos, tales como:

- /mnt/dns
- /mnt/dhcp
- /mnt/ntp
- /mnt/smtp

Posteriormente, se utilizarían enlaces simbólicos (symlinks) para redirigir las rutas originales de los servicios hacia sus correspondientes volúmenes dedicados, facilitando así la compatibilidad con las configuraciones por defecto de cada aplicación y simplificando la administración. Es decir que, se mantendrán las rutas estándar de los servicios, pero se almacenarán los datos reales en los LVs dedicados.

Tolerancia a fallos:

Para dotar al sistema de una mayor tolerancia a fallos y mejorar su rendimiento, se propone la implementación de un esquema de almacenamiento basado en RAID 0+1. Este enfoque combina las ventajas de rendimiento del striping (RAID 0) con la redundancia del mirroring (RAID 1) [1].

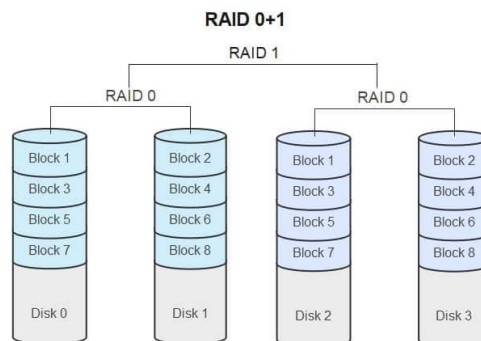


Fig. 4. Implementación de un RAID 0+1.

Para ello, se parte del supuesto en que el servidor CJ cuenta con la posibilidad de alojar al menos cuatro discos físicos. La configuración propuesta sería la siguiente:

- Dos pares de discos trabajando en RAID 0:
 - Primer par: sda + sdb
 - Segundo par: sdc + sdd

Posteriormente, ambos pares serían duplicados entre sí en un RAID 1.

De manera que, sobre esta estructura RAID 0+1 se implementaría LVM, esto proporciona flexibilidad en la asignación, crecimiento y administración de los volúmenes lógicos dedicados.

Es importante recordar que todos los discos deben tener el mismo tamaño.

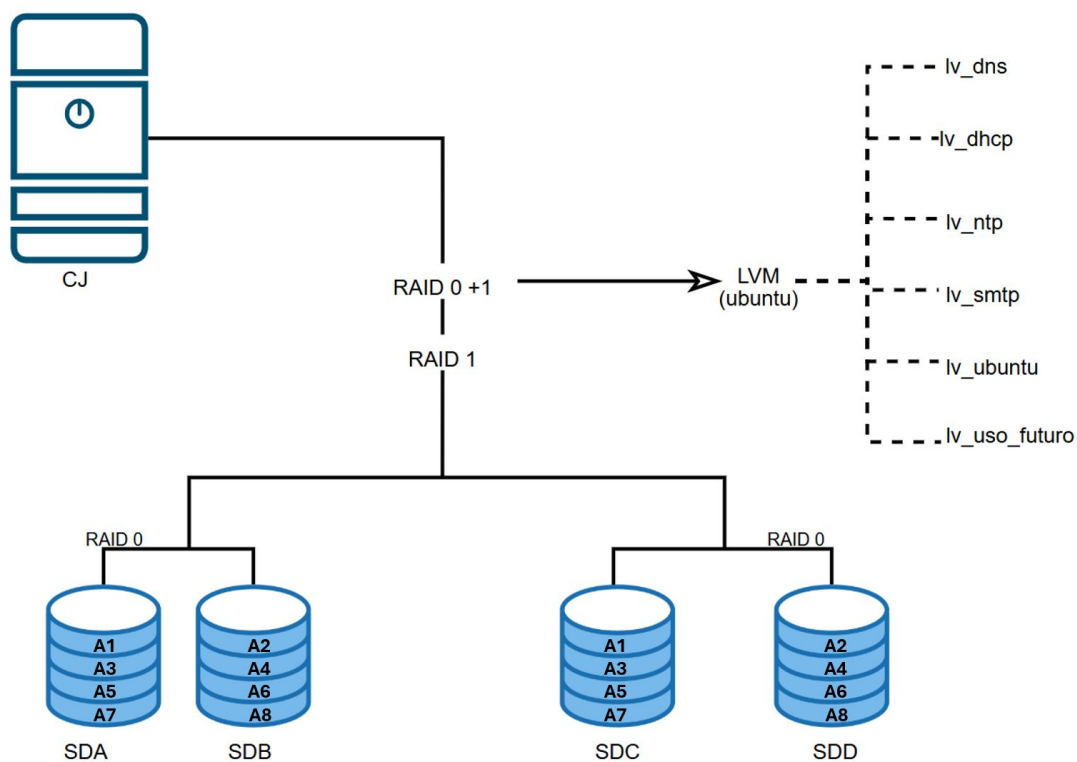


Fig. 5. Diseño de almacenamiento para el servidor CJ.

Con esto, se espera una capacidad usable de al menos 3,6 TB.

Faraday:

Para Faraday se realiza un análisis similar al desarrollado para CJ.

```
faraday@faradayot2far:~$ lsblk
NAME                                MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
loop0                               7:0      0 104.2M 1 loop /snap/core/17200
loop1                               7:1      0 104.5M 1 loop /snap/core/17210
loop3                               7:3      0  55.4M 1 loop /snap/core18/2855
loop4                               7:4      0  63.8M 1 loop /snap/core20/2571
loop5                               7:5      0  63.8M 1 loop /snap/core20/2582
loop6                               7:6      0  55.5M 1 loop /snap/core18/2887
loop7                               7:7      0  73.9M 1 loop /snap/core22/1963
loop8                               7:8      0  66.8M 1 loop /snap/core24/888
loop9                               7:9      0  66.8M 1 loop /snap/core24/988
loop10                              7:10     0   3.1M 1 loop /snap/mosquitto/941
loop11                              7:11     0   3.1M 1 loop /snap/mosquitto/978
loop12                              7:12     0  44.4M 1 loop /snap/snapd/23771
loop13                              7:13     0  50.9M 1 loop /snap/snapd/24505
loop14                              7:14     0  73.9M 1 loop /snap/core22/1981
sda                                  8:0      0 931.5G 0 disk
├─sda1                              8:1      0    1G 0 part /boot/efi
├─sda2                              8:2      0    2G 0 part /boot
└─sda3                              8:3      0 928.4G 0 part
   └─ubuntu--vg-ubuntu--lv 252:0    0 100G 0 lvm /
```

Fig. 6. Resultado del comando lsblk en el servidor Faraday.

```
faraday@faradayot2far:~$ df -h
Filesystem                Size      Used Avail Use% Mounted on
tmpfs                     1.6G    2.0M    1.6G   1% /run
efivarfs                   494K    245K    245K  51% /sys/firmware/efi/efivars
/dev/mapper/ubuntu--vg-ubuntu--lv 98G     44G     50G  47% /
tmpfs                      7.8G     0      7.8G   0% /dev/shm
tmpfs                      5.0M     0      5.0M   0% /run/lock
tmpfs                      7.8G     0      7.8G   0% /run/qemu
/dev/sda2                  2.0G    508M    1.3G  28% /boot
/dev/sda1                  1.1G     6.1M    1.1G   1% /boot/efi
tmpfs                      1.6G     4.0K    1.6G   1% /run/user/1000
```

Fig. 7. Resultado del comando df en el servidor Faraday.

```

faraday@faradayot2far:~$ sudo parted /dev/sda unit GB print
[sudo] password for faraday:
Model: HPE LOGICAL VOLUME (scsi)
Disk /dev/sda: 1000GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start   End     Size    File system  Name  Flags
  1      0.00GB  1.13GB  1.13GB  fat32                boot, esp
  2      1.13GB  3.28GB  2.15GB  ext4
  3      3.28GB  1000GB  997GB
faraday@faradayot2far:~$ |

```

Fig. 8. Resultado del comando parted en el servidor Faraday.

Se puede observar que tiene una distribución bastante similar a CJ, sin embargo, con una capacidad de almacenamiento menor.

Por ello, en función de priorizar su disponibilidad y tolerancia a fallos se implementará un RAID 5 en este servidor. El uso del RAID 5 proporciona una alta tolerancia a fallos frente a la pérdida de un disco, permitiendo mantener los servicios operativos mientras se reemplaza el disco dañado [2, 3].

Para la configuración de RAID 5 se asume que se usarán 4 físicos de 1 TB cada uno. En esta configuración, la capacidad útil se calcula como el total de discos menos uno (para la paridad), resultando en un total de 3 TB de almacenamiento efectivo.

A diferencia del servidor CJ, en el servidor Faraday no se implementaron volúmenes adicionales mediante LVM, manteniendo una estructura de particiones directa sobre el volumen RAID. El espacio de almacenamiento resultante se organiza de manera lógica, asignando directorios independientes para cada servicio con el fin de aislar su operación y facilitar su gestión, monitoreo y mantenimiento.

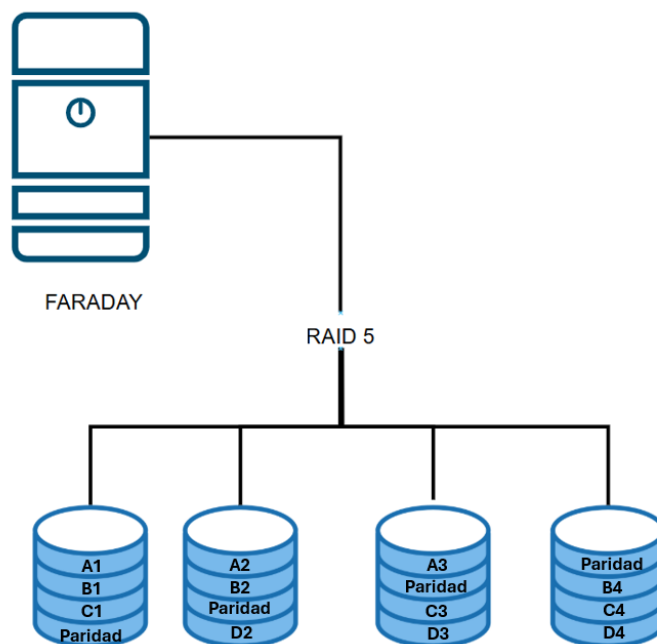


Fig. 9. Diseño de almacenamiento para el servidor Faraday.

Diagrama lógico de red

A continuación, se presenta el diagrama lógico de red, que ilustra la arquitectura de red planteada para el proyecto, detallando los dispositivos de conexión, los segmentos de red, y las relaciones entre los diferentes componentes de la red.

Este diagrama muestra la interconexión de los diferentes dispositivos que componen la infraestructura, incluyendo desde los equipos de borde encargados de gestionar el tráfico hacia y desde Internet:



Fig. 10. Dispositivos de borde.

Así como las ONT, en donde, cada ONT genera su propia subred interna, asignando direcciones privadas a los dispositivos conectados. El direccionamiento IP utilizado en cada segmento se indica dentro del diagrama se indica a continuación:



Fig. 11. Direccionamiento de las diferentes ONTs.

Diagrama inicial

El diagrama de partida inicial se muestra a continuación:

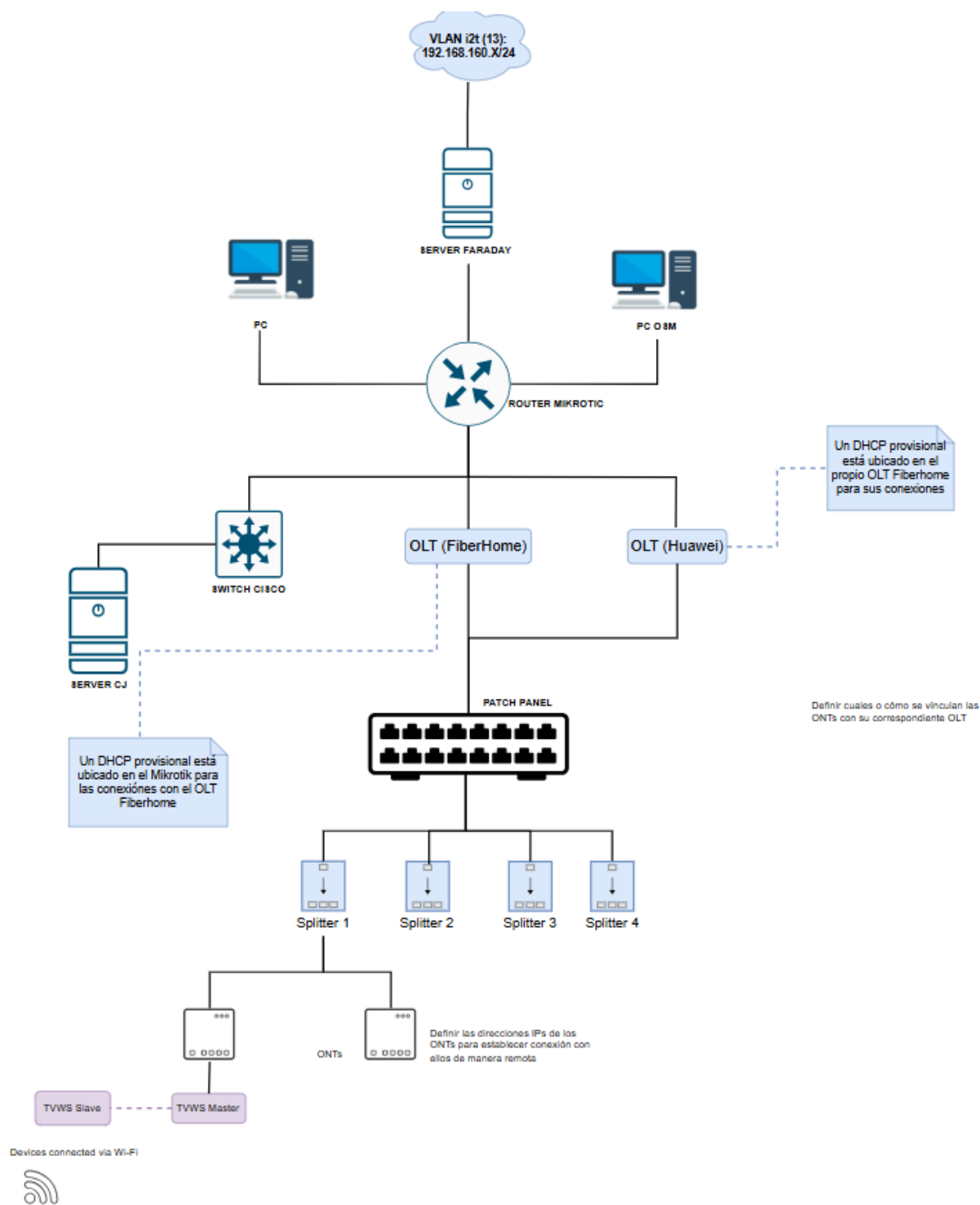


Fig. 12. Diagrama lógico inicial.

El diagrama anterior fue la base principal para el desarrollo del proyecto, sin embargo, a medida que el proyecto iba escalando, fueron necesarias ciertas modificaciones, obteniendo como resultado final, el siguiente diagrama lógico:

Nota: El diagrama lógico se presenta de forma segmentada con el fin de facilitar su visualización y comprensión. En caso de requerir una mejor visualización, los diagramas completos se encuentran disponibles en el siguiente enlace complementario al proyecto: [Diagramas](#)

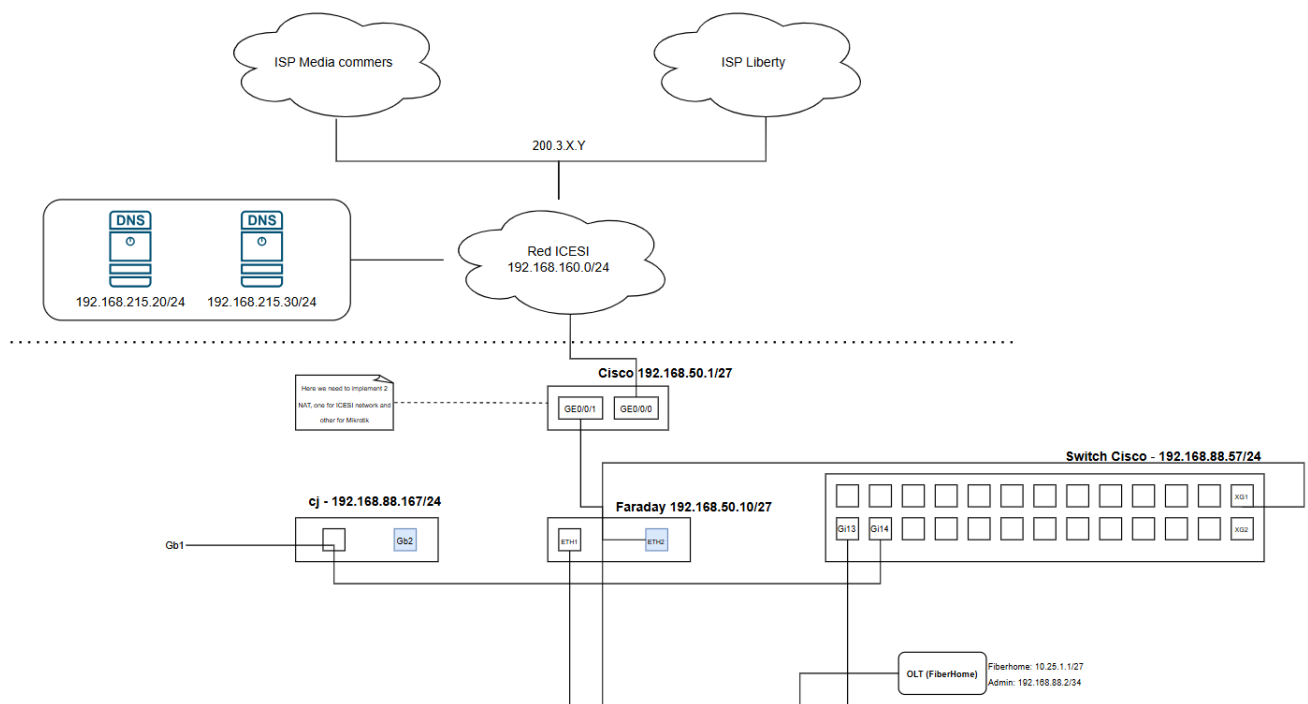


Fig. 13. Diagrama lógico implementado.

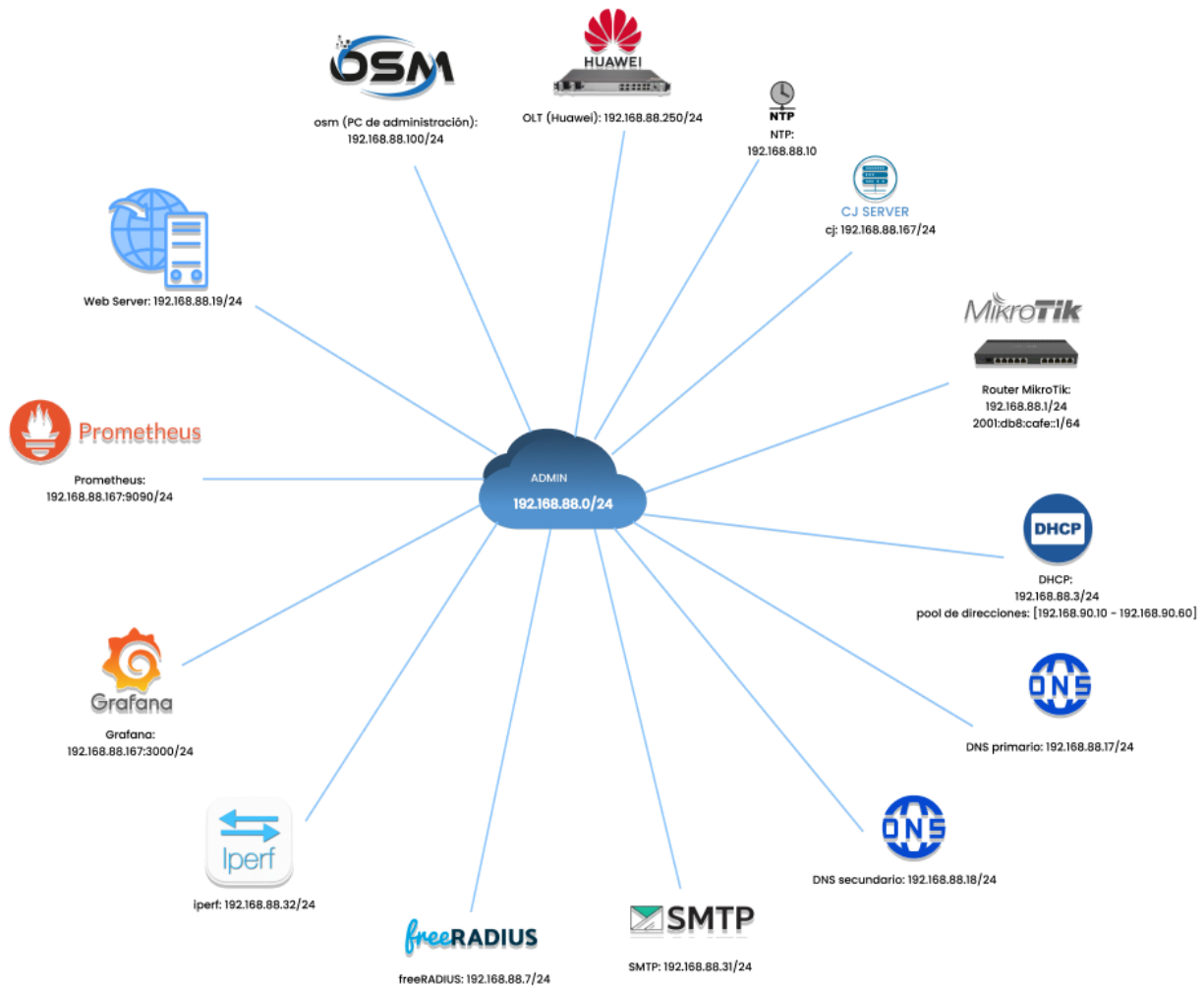


Fig. 16. Distribución de equipos y servicios en el segmento de red 192.168.88.0.

Por otro lado, en un segmento de red distinto se implementaron servidores web y un reverse proxy, con el objetivo de evaluar la distribución de carga y analizar el comportamiento del sistema bajo diferentes escenarios de tráfico. Para este fin, se configuraron servidores web Nginx con soporte para HTTP/2, así como un servidor proxy Nginx que actúa como balanceador de carga, implementando soporte para HTTP/3 (QUIC). El propósito principal de esta configuración es demostrar y facilitar la implementación de HTTP/3 en un entorno de pruebas local.

Para obtener más información al respecto, consulte [4].

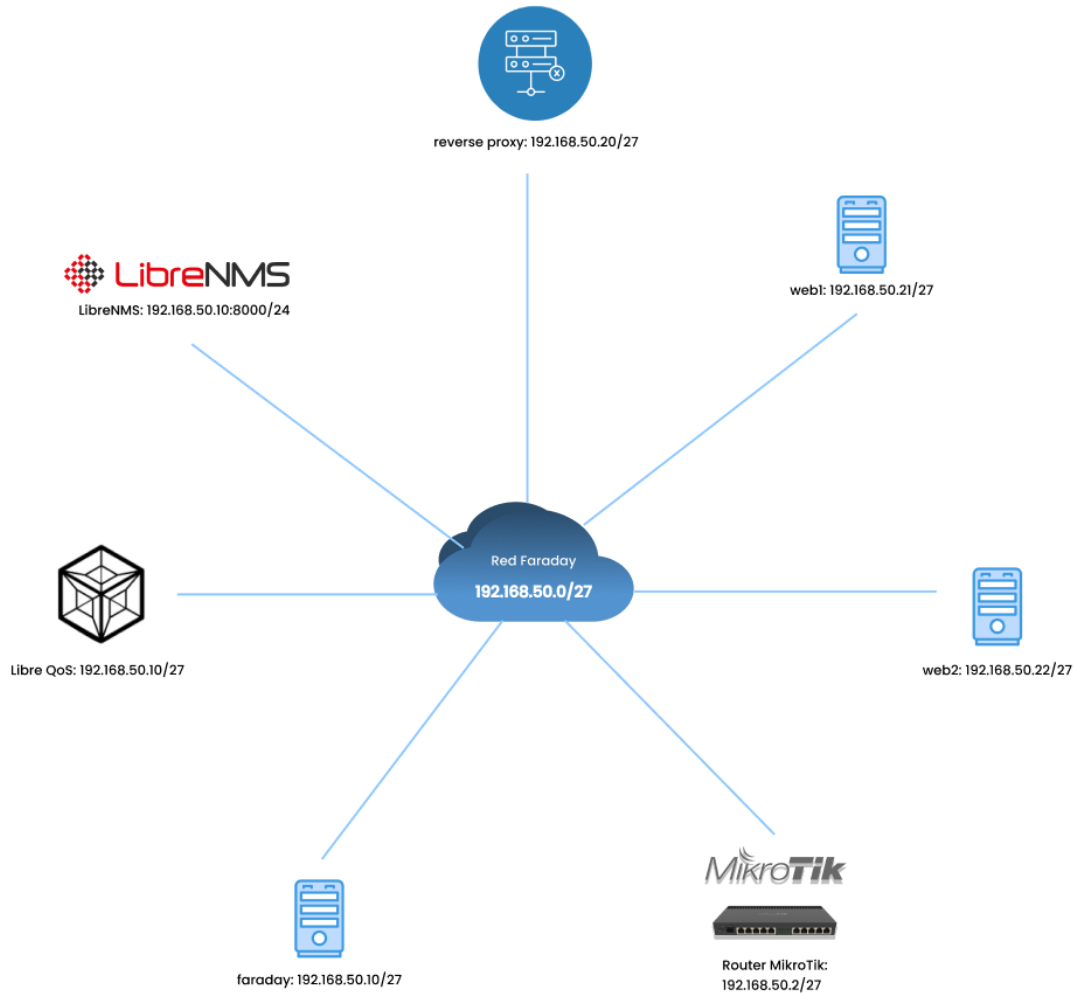


Fig. 16. Distribución de equipos y servicios en el segmento de red 192.168.50.0.

Si bien, no se implementó DHCP versión 6, se usó la alternativa SLAAC (Stateless Address Autoconfiguration). SLAAC, o Autoconfiguración de Direcciones sin Estado, es un método para que los dispositivos IPv6 obtengan sus direcciones IP automáticamente, sin necesidad de un servidor DHCP. El router, utilizando un demonio de anuncio de enrutador como *radvd*, envía mensajes de anuncio (*Router Advertisement* o RA) que contienen información de la red, como el prefijo y la dirección *gateway*, a los dispositivos en la red. Estos dispositivos, a su vez, utilizan esta información para crear sus propias direcciones IPv6, generalmente utilizando el estándar EUI-64 o de manera aleatoria, según el sistema operativo.

Para más información sobre el proceso de configuración relacionada a ipv6 y a SLAAC consulte [5, 6].

Descripción de los equipos utilizados

A continuación, se presenta una descripción breve de los dispositivos físicos utilizados para llevar a cabo el despliegue de la infraestructura. La tabla presentada a continuación detalla la información correspondiente al modelo, fabricante y versión del sistema operativo de cada uno de los dispositivos que componen el entorno.

Nombre del Dispositivo	Modelo	Fabricante	Sistema Operativo	Versión del SO
Servidor Faraday	ProLiant DL20 Gen10	HPE (Hewlett Packard Enterprise).	Ubuntu	22.04.5 LTS
Servidor CJ	PowerEdge R440	Dell Inc.	Ubuntu	22.04.2 LTS
PC OSM	ASUS TUF Gaming F15 FX506LI_FX506LI	Asus.	Ubuntu	22.04.5 LTS
Switch Cisco	SG350X-24	Cisco.	Cisco IOS	2.4.5.71
Router Cisco	ISR4321/K9	Cisco.	Cisco IOS	3.16.04b.S
Router Mikrotik	RB3011UiAS	Mikrotik.	RouterOS	7.18.2
OLT	EA5800V	Huawei.	Huawei OS	V100R021C10

Tabla 1. Descripción de los equipos físicos utilizados.

Distribución física de los equipos de rack

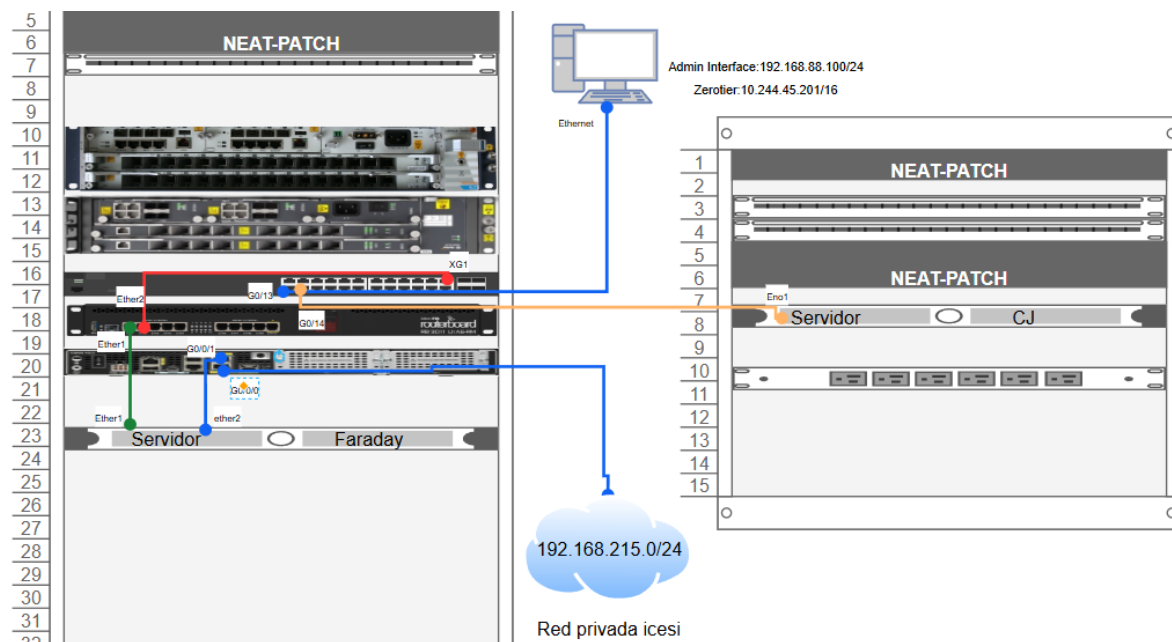


Fig. 17. Diagrama con la distribución física de los equipos en el rack.

En este diagrama podemos ver la topología física de una red estructurada en dos racks, donde se interconectan varios dispositivos simulando una ISP. De arriba hacia abajo, el primer equipo es una OLT Huawei, encargada de gestionar la distribución de servicios a través de fibra óptica, debajo se encuentra una OLT Fiberhome, que cumple funciones similares, proporcionando redundancia o expansión de cobertura dentro de la red.

Más abajo, se encuentra un switch Cisco, el cual está conectado directamente al Router MikroTik. Este switch facilita la conexión entre las OLT y el MikroTik, además de organizar el flujo de datos entre los distintos equipos del rack. El MikroTik actúa como un nodo central de enrutamiento y es responsable de la gestión de tráfico dentro de la infraestructura, seguidamente está el router cisco que es el equipo de borde con el que salimos a la red privada de la universidad y a internet.

también se cuenta con el servidor Faraday, en el cual están configurados varios servicios, tales como, los servidores web, el reverse proxy, librenms.

Finalmente, se tiene en el rack auxiliar, el servidor CJ donde están ubicados la mayoría de los servicios descritos en este documento.

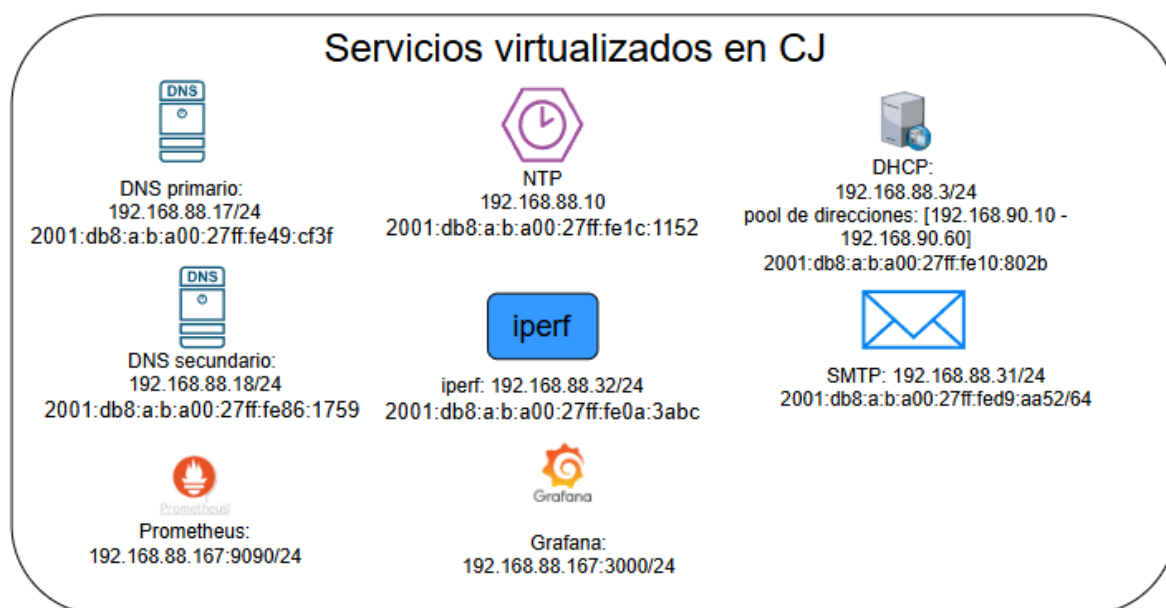


Fig. 18. Distribución de servicios virtualizados en el servidor CJ.

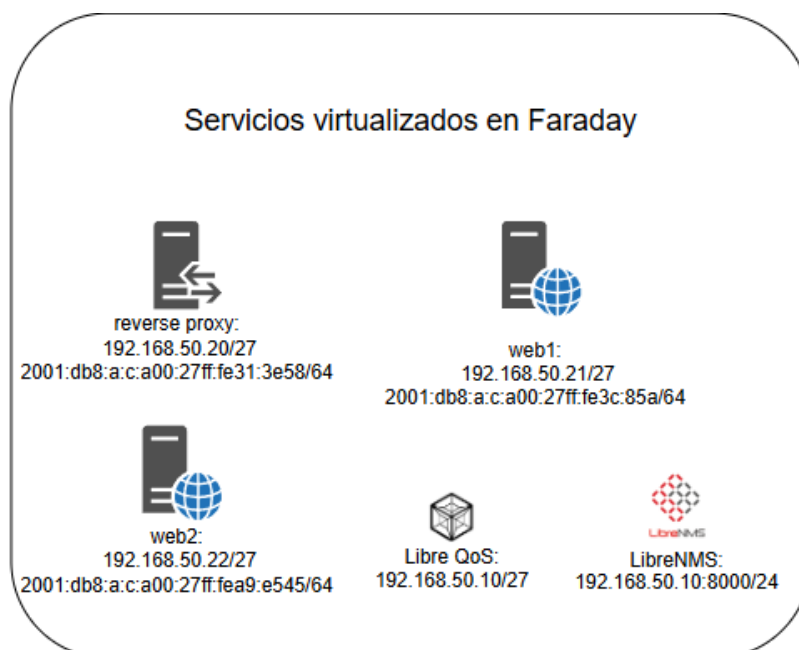


Fig. 19. Distribución de servicios virtualizados en el servidor Faraday.

Análisis de requerimientos (Metodología EARS)

Ubiquitous:

*El sistema de red **debe** soportar conectividad Dual Stack (IPv4 e IPv6) en los dispositivos de la infraestructura.*

*El servidor DHCPv4 **debe** asignar direcciones IPv4 dentro del rango definido.*

*El servidor DNS primario **debe** implementar DNSSEC para validación de firmas digitales.*

*El servidor DNS primario **debe** incluir todos los registros necesarios para la resolución básica de nombres (A, AAAA, MX, NS, SOA, PTR).*

*El servidor de correo **debe** soportar los protocolos SMTP, IMAP y POP3.*

*Todos los servidores **deben** sincronizar su hora bien sea con un servidor NTP del pool global o con el servidor NTP local.*

Event-driven:

***Cuando** un cliente se conecte a la red GPON, el sistema **debe** asignarle una dirección IPv4 y, opcionalmente una Ipv6.*

***Cuando** se asigne el servidor DNS autoritativo, el servidor **debe** replicar las zonas DNS desde el primario dentro de un plazo máximo de 48 horas.*

***Cuando** un cliente IPv6 se conecta a la red, el router **debe** enviar anuncios RA (Router Advertisement) para permitir SLAAC.*

***Cuando** un cliente inicie sesión para enviar correo, el servidor **debe** verificar credenciales mediante autenticación básica (usuario/contraseña).*

State driven:

Mientras el cliente final no tenga una IP asignada, el servidor DHCPv4 debe proporcionar una dirección IPv4, máscara de red, gateway y servidores DNS.

Mientras el servidor DNS primario esté activo, el servidor secundario **debe** sincronizar las zonas DNS cada 24 horas.

Mientras el servidor NTP local esté disponible, los servidores internos **deben** priorizarlo sobre servidores externos

Unwanted behaviour:

Si el servidor DNS primario falla, **entonces** el servidor secundario **debe** asumir las consultas autoritativas.

Si la sincronización NTP falla por más de 5 minutos, **entonces** el sistema **debe** notificar al administrador.

Si el servidor NTP no responde, **entonces** el sistema **debe** sincronizarse con un servidor del pool global.

Si un correo no puede ser entregado después de 3 intentos, **entonces** el servidor **debe** moverlo a la carpeta 'postmaster' y notificar al remitente.

Optional:

Donde un cliente soporte IPv6, el router **debe** permitir la autoconfiguración de direcciones mediante SLAAC.

Donde se requiera seguridad adicional, el servidor SMTP **debe** implementar STARTTLS para encriptación opcional, pero no será obligatorio.

Es importante mencionar que identificaron los requerimientos funcionales y no funcionales del sistema, tomando como referencia la estructura planteada por EARS [7].

Repositorio de archivos de configuración

Todos los archivos de configuración, scripts y documentación complementaria utilizados durante el desarrollo de este proyecto se encuentran disponibles en el siguiente repositorio:

<https://github.com/internetServiceProvider>

Especialmente, lo relacionado con la asignatura de plataformas I se encuentra en:

<https://github.com/internetServiceProvider/platforms>

DHCP : <https://github.com/internetServiceProvider/platforms/tree/main/src/dhcp>

DNS: <https://github.com/internetServiceProvider/platforms/tree/main/src/dns>

NTP: <https://github.com/internetServiceProvider/platforms/tree/main/src/ntp>

FIREWALL:

<https://github.com/internetServiceProvider/platforms/tree/main/docs/firewall>

Conclusiones

El desarrollo de este proyecto permitió la implementación de una infraestructura de red robusta y escalable, basada en tecnologías GPON y virtualización de servicios críticos, simulando de manera realista la operación de un ISP. La integración de servicios como DHCP, DNS con DNSSEC y TSIG, NTP, servidores web con soporte HTTP/3 (QUIC), y correo electrónico, demuestra una arquitectura bien estructurada, capaz de soportar diversos escenarios de operación y crecimiento.

El diseño del sistema de almacenamiento, con la aplicación de esquemas RAID 0+1 y RAID 5, proporciona redundancia, tolerancia a fallos y mejora en el rendimiento de los servidores, garantizando alta disponibilidad de los servicios. La implementación de volúmenes lógicos dedicados optimiza la administración y facilita futuras ampliaciones.

El uso de dual stack (IPv4 e IPv6), junto con mecanismos como SLAAC para la autoconfiguración, posiciona la red dentro de los estándares actuales y permite una transición natural hacia entornos completamente IPv6. Además, la correcta distribución física y lógica de los equipos asegura un flujo eficiente de datos y una administración centralizada, con capacidad de monitoreo y respuesta ante fallos.

De manera general, es posible afirmar que, el proyecto cumplió satisfactoriamente con los objetivos propuestos, permitiendo no solo la construcción de una red funcional, sino también la adquisición de conocimientos prácticos avanzados en diseño, configuración y gestión de plataformas de telecomunicaciones.

Referencias

[1] A. Cervera. "RAID 0 vs. RAID 1 | Diferencia y comparación". Accedido el 12 de junio de 2025. [En línea]. Disponible: <https://recoverit.wondershare.es/windows-tips/raid-0-vs-raid-1.html>

[2] Recoverit. "Qué es el RAID 5 - Explicación del RAID 5". [Oficial] Recoverit - Lo último en soluciones de recuperación de datos para Windows/Mac. Accedido el 12 de junio de 2025. [En línea]. Disponible: <https://recoverit.wondershare.es/windows-tips/what-is-raid-5.html>

[3] Equipo editorial de IONOS. "RAID 5: toda la información importante sobre este nivel RAID". IONOS Digital Guide. Accedido el 12 de junio de 2025. [En línea]. Disponible: <https://www.ionos.com/es-us/digitalguide/servidores/seguridad/raid-5/>

[4] R. Urbina. "GitHub - internetServiceProvider/LoadbalancerQuic: Webservers and reverse proxy config for ISP webpage using QUIC/http3". GitHub. Accedido el 12 de junio de 2025. [En línea]. Disponible: <https://github.com/internetServiceProvider/LoadbalancerQuic>

[5] K. Nieto. "Ipv6 Network Setup in Our Lab". Accedido el 12 de junio de 2025. [En línea]. Disponible: <https://github.com/internetServiceProvider/platforms/tree/main/docs/ipv6>

[6] "IPv6 Neighbor Discovery - RouterOS - MikroTik Documentation". MikroTik Routers and Wireless - Support. Accedido el 8 de junio de 2025. [En línea]. Disponible: <https://help.mikrotik.com/docs/spaces/ROS/pages/40992815/IPv6+Neighbor+Discovery>

[7] S.Barona. "ISP Platforms Deployment". Accedido el 12 de junio de 2025. [En línea]. Disponible : <https://github.com/internetServiceProvider/platforms.git>

[8] "Alistair Mavin EARS - Alistair Mavin". Alistair Mavin. Accedido el 12 de junio de 2025. [En línea]. Disponible: <https://alistairmavin.com/ears/>