

Mejora de red y espacio compartido

Solgata S.A.U.



Índice

1. Introducción.....	3
2. Análisis del contexto.....	4
2.1 Identificación y priorización de necesidades.....	4
2.2 Tecnologías existentes.....	6
3. Diseño del proyecto.....	10
3.1 Definición del proyecto.....	10
3.2 Alcance del proyecto.....	11
3.3 Viabilidad Económica.....	12
3.3.1 Análisis DAFO.....	12
3.3.2 Tabla de inversiones, gastos e ingresos.....	16
3.4 Recursos necesarios.....	22
3.4.1 Hardware.....	22
3.4.2 Software.....	23
3.5 Documentación.....	24
3.5.0 Esquema de la red visual.....	24
3.5.1 Esquema de red.....	25
3.5.2 Configuración Básica.....	26
3.5.2.1 Configuración del Router 1 – Holawifi.....	26
3.5.2.2 Configuración del router 2 - LaWifi.....	27
3.5.2.3 Configuración Switch Mikrotik CRS125-24G-1S.....	29
3.5.2.4 Configuración del Mikrotik hAP Lite.....	29
3.5.2.5 Configuración del TPLink Extender.....	30
3.5.2.6 Configuración del AP Huawei.....	30
3.5.3 Configuración Avanzada.....	31
3.5.3.1 Failover en switch Mikrotik.....	31
3.5.3.2 Firewall Avanzado de Mikrotik.....	32
3.5.3.3 Configuración del NAS.....	32
3.5.3.4 Configuración de copias de seguridad con Cobian Reflector.....	33
3.5.3.5 Configuración de redirección de puertos en la red.....	33
4. Puesta en marcha.....	34
4.1 Demostración de funcionamiento.....	34
4.1.1 Prueba de conectividad todos los equipos.....	34
4.1.2 Prueba de FailOver.....	36
4.1.3 Prueba de tráfico malicioso para el Firewall.....	37
4.1.4 Prueba de monitorización del tráfico de la LAN con Torch.....	39
4.1.5 Prueba de transferencia de archivos al NAS.....	40
4.1.5.1 Prueba de transferencia de archivos al NAS mediante SMB.....	40
4.1.5.2 Prueba de transferencia de archivos al NAS mediante SFTP.....	41
4.1.6 Prueba de copias de seguridad de Cobian Reflector.....	43
4.2 Jerarquía de usuarios y grupos y permisos de estos.....	44
4.3 Control de versiones del software.....	46
5. Conclusiones.....	47
6. Bibliografía.....	48

1. Introducción

En el mundo de los negocios de hoy en día, la computación se ha vuelto clave para que las empresas funcionen sin problemas. La necesidad de tener redes sólidas, seguras y flexibles es más grande que nunca, ya que todo depende de la tecnología de la información y las comunicaciones (TIC). Por eso, es crucial que las empresas actualicen sus redes para seguir siendo competitivas y no detenerse por fallos técnicos o ciberataques.

Este trabajo de fin de grado se centra en modificar la red de una empresa. Queremos hacerla más eficiente, agregarle un sistema de respaldo para evitar problemas y fortalecer su seguridad para proteger los datos de la empresa. Estamos en un momento donde todo está digitalizado y los ciberataques son una amenaza constante, así que es vital que las empresas tomen medidas para estar preparadas.

Vamos a hacer varias cosas para mejorar la red: añadir un sistema de respaldo para que si algo falla, no perder el acceso a internet, instalar un servidor de almacenamiento en red (NAS) para tener almacenamiento compartido y reforzar la seguridad para proteger esos datos de posibles robos o daños.

En resumen, este trabajo busca ayudar a las empresas a mantenerse al día con los tiempos digitales y protegerse de posibles problemas técnicos o ataques cibernéticos. Es importante adaptarse y tomar medidas preventivas para que el negocio siga adelante sin problemas..

2. Análisis del contexto

2.1 Identificación y priorización de necesidades

Nos ubicamos en Solgata, una empresa privada del Ayuntamiento de Gata de Gorgos encargada de la gestión de la recogida de contenedores, del alcantarillado, y las inscripciones deportivas de todo el pueblo.

Esta empresa cuenta con alrededor de 20 empleados. También unas oficinas de 2 plantas. Los empleados suelen trabajar en portales web de la Generalitat o a mano con impresiones. Cuentan con servidores de monitorización de los pozos del pueblo, además también tienen servicio de CCTV con unas cámaras montadas alrededor de los puntos importantes para ellos, ya sean pozos, contadores de secciones del pueblo...

Solgata está dispuesta en una red de oficinas en las que tiene la necesidad de una red estructurada en distintas subredes. Los empleados que trabajan en las oficinas, normalmente trabajan en portales WEB, y también tienen un uso elevado de impresoras, por lo que será necesario tener acceso ininterrumpido a internet en toda la oficina y un buen uso de asignación de direcciones IP para todos los dispositivos. Las oficinas constan de un edificio de 2 plantas.

En el momento de iniciar este proyecto el cableado estructurado ya estaba construido, consta de un rack principal y uno secundario. Además, está planteado para que cada empleado tenga dos rosetas, una para VOIP y la otra para futuras expansiones. En el rack principal, encontramos los dos routers, uno para garantizar conexión a internet, y el otro para tener siempre uno de respaldo. También encontramos un switch de telefónica (gestionable solo por el proveedor) que gestiona solo VOIP. Por otro lado en el rack secundario hay otro switch de telefónica para gestionar VOIP de todos los terminales de los empleados dado que solo con uno se quedaban cortos, un patch panel para multiplicar los puertos disponibles, y un switch no gestionable para replicar puertos solo de IP, sin voz.

Adicionalmente, la empresa también utiliza una plataforma de espacio compartido en la nube, para entre ellos poder compartir archivos de forma rápida y eficaz. Este servicio que ellos están utilizando, tiene unos costes excesivos para ellos y necesitan una manera de abaratarlos.

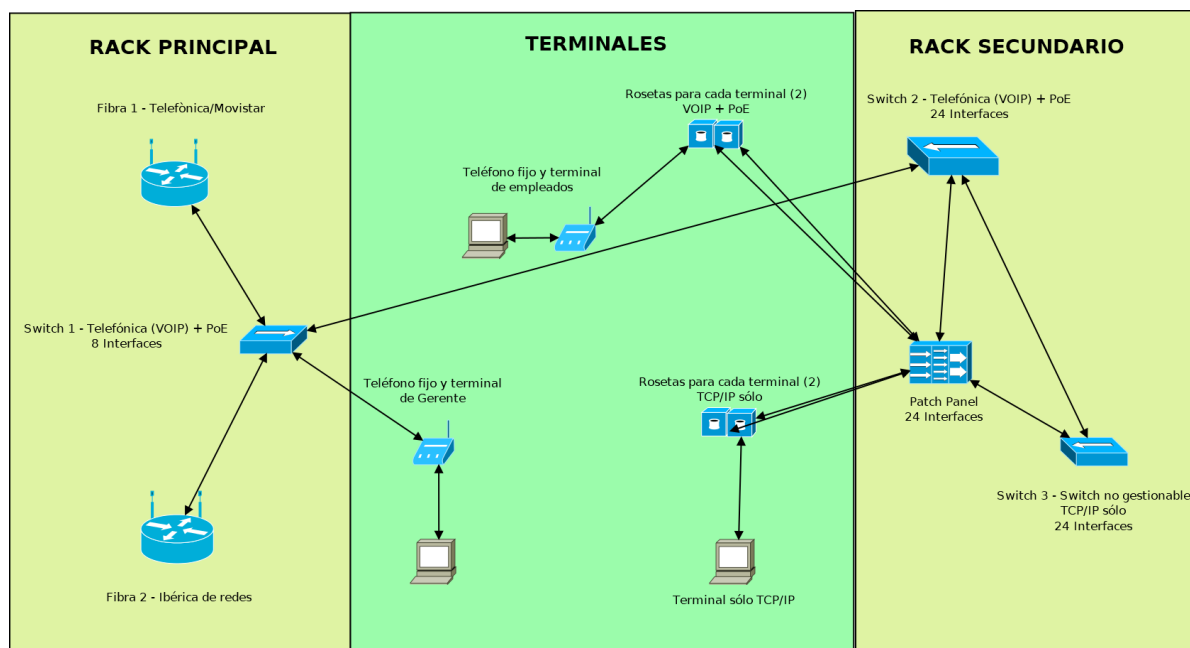


Ilustración 1: Esquema físico de la red de Solgata

Las necesidades principales que priorizaremos serán :

- Brindar conexión a toda el área física de la empresa con diversos acces points repartidos.
- Brindar conexión a todas las rosetas de los empleados.
- Brindar IP fijas a dispositivos fijos como impresoras o servidores en funcionamiento.
- Brindar seguridad a la red con un firewall.
- Brindar conectividad ininterrumpida automática aprovechando las dos líneas de internet.
- Brindar un espacio de almacenamiento compartido en la red.
- Copia de seguridad en el almacenamiento compartido del equipo del gerente.

Estas son las principales líneas sobre las que trabajará el proyecto para dar la conectividad requerida con las mejores prácticas de seguridad.

2.2 Tecnologías existentes

Para cada necesidad, utilizaremos una tecnología o estándar reglado para su funcionamiento, ahora explicaré todas las tecnologías y estándares que estaremos utilizando al proporcionar las necesidades planteadas.

Brindar conexión a toda el área física de la empresa con diversos acces points repartidos.

Para esta necesidad, utilizaremos el estándar WiFi en concreto IEEE 802.11 en concreto el 802.11n. Este estándar se estableció en 2009 y utiliza tanto la frecuencia de 2.4 GHz como la frecuencia de 5 GHz. Este estándar ofrece velocidades de hasta 600 Mbps y es compatible con los dispositivos que utilizan los estándares anteriores de 802.11. Este estándar ha sido muy popular en la industria debido a su alta velocidad y buena compatibilidad.

También utilizaremos el estándar Ethernet en concreto 802.3ab, o también llamados cables de 1000 base-T, cables de cobre con par trenzado sin apantallamiento.



Ilustración 2: Estándar Ethernet



Ilustración 3: Estándar WI-FI

Brindar conexión a todas las rosetas de los empleados.

Para la necesidad comentada, utilizaremos el estándar anteriormente descrito, el 802.3ab, ya que tiene una velocidad de 1Gb de transferencia de datos. También utilizaremos conectores RJ45 con cables de categoría 6 UTP.



Ilustración 4: Cable UTP Categoría 6

Brindar IP fijas a dispositivos fijos como impresoras o servidores en funcionamiento.

En este caso de una buena administración de las cesiones de IP, se hará uso de un servidor DHCP proporcionado por el equipo mikrotik, en concreto el estándar utilizado por DHCP es el definido por el RFC 1541 (reemplazado por el RFC 2131) que le permite a un servidor distribuir dinámicamente la información de configuración y direccionamiento IP a los clientes.

En cuanto al dispositivo mikrotik, estaremos utilizando un switch gestionable l2 y l3, en concreto el Mikrotik Cloud Router Switch CRS125-24G-1S-RM. Que contiene en él un sistema operativo RouterOS V6. Utilizaremos la versión 6 por contra de la 7, debido a que la versión 6 de RouterOS nos confiere una mayor velocidad de rutas. Esto es debido a que el antiguo kernel del Linux (que es el sistema operativo en el que se basa RouterOS) sigue incluyendo una cache de rutas. Mientras que si estuviésemos utilizando la versión 7, no tendríamos esa velocidad. Puntualizar, que la versión 7 de RouterOS está diseñada para tener ventaja utilizando VLAN. Esto es debido a que la v7 otorga una gran velocidad de conmutación en las VLAN sin cargar apenas la CPU. Pero en nuestro caso específico, no tendremos la necesidad de utilizar VLAN por lo que utilizaremos la que más nos conviene, en este caso, la versión 6.



Ilustración 5: Mikrotik Cloud Router Switch CRS125-24G-1S-RM

Brindar seguridad a la red con un firewall.

Para esto, utilizaremos un firewall incluido en el mikrotik, comentada su tecnología y versión anteriormente, en el que definiremos una serie de reglas.

Brindar conectividad ininterrumpida automática aprovechando las dos líneas de internet.

Conseguiremos esto utilizando la tecnología Dual WAN o Failover. Que consiste en resumidas cuentas, a tener dos ISP contratados, y con el switch hacer una conexión con tolerancia a fallos, es decir, tener una línea como predeterminada, y si esta falla o deja de comunicar, cambiar automáticamente a la otra línea de ISP, para así nunca perder conexión a internet. Por eso el switch está constantemente lanzando peticiones al exterior, y cuando tengan un timeout las peticiones, cambiará de puerta de enlace, para así, asegurar la conexión.

Brindar un espacio de almacenamiento compartido en la red

Utilizaremos un sistema NAS, que consiste en un dispositivo de almacenamiento de alta capacidad conectado a una red que permite a los usuarios y clientes autorizados almacenar y recuperar datos en una ubicación centralizada. En este caso, estamos utilizando un ordenador con piezas recicladas y montado específicamente para funcionar como NAS. Este ordenador cuenta con 6 GB de memoria RAM, y 5 discos duros de 500GB cada uno. A estos 5 discos, los hemos agrupado como un array de discos, en este caso nos convenía más un array RAID-5. Sobre estos discos, hemos montado el sistema operativo TrueNAS, que nos convenció por ser uno de los sistemas operativos FreeWare más completo y potentes que puedes encontrar. Contando con plugins instalables, soporte web, servicios de directorio y la capacidad de utilizar el Server Message Block (SMB) para compartir una carpeta en red, que es lo que nos interesa. Este sistema utiliza el protocolo TCP/IP para la transferencia de archivos

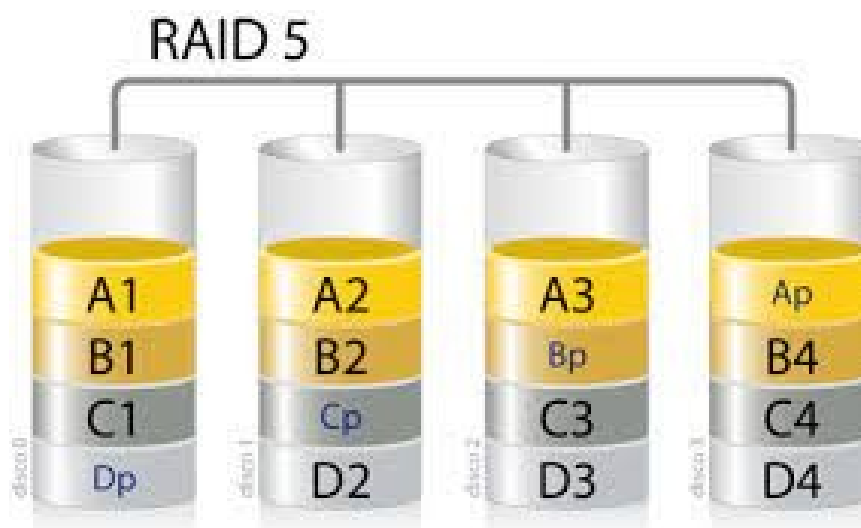


Ilustración 6: Sistema de array RAID-5

Copia de seguridad en el almacenamiento compartido del equipo del gerente.

Necesitaremos también como hemos comentado hacer una copia del disco del gerente, cada x tiempo por razones de seguridad de datos. Yo he elegido hacer una copia completa inicial y programarlo automáticamente para que haga copias diferenciales x día a la semana. Y como configuraremos el NAS para que comparta una carpeta en red, haremos que las copias se compriman y se cifren y se envíen a esa carpeta, que tendrá unas ACL para que solo el administrador y el gerente puedan gestionar la carpeta en la cual se enviarán las copias de seguridad. Esto lo haremos con el programa Cobian Reflector, que es uno de los mejores programas FreeWare. Este nos permite hacer todo lo descrito y mucho más, se puede configurar también una conexión SFTP por si tenemos un servidor en remoto.



Ilustración 7: Cobian Software, empresa que ha desarrollado Cobian Reflector

3. Diseño del proyecto

3.1 Definición del proyecto

El proyecto consistirá en un replanteo de toda la red de la empresa con diversos añadidos. En concreto, pasaremos de una red sin control, sin respaldo y sin tolerancia a fallos a una red automatizada, segura y plenamente funcional los 7 días de la semana. El modelo que seguiremos será el de añadir dispositivos de gestión de la red para poder hacer ciertas configuraciones oportunas en estos, estoy hablando de un switch de capa 2 y 3 mikrotik, que será con el que configuremos la mayor parte de los arreglos de la red. En este lo que haremos será gestionar todas las direcciones IP de los terminales, gestionar el firewall y gestionar también el failover o la conexión constante e ininterrumpida a internet.

A parte de esto, también tenemos que tener en cuenta que necesitaremos diversos dispositivos con wireless lan para poder dar puntos de acceso inalámbricos repartidos en toda el área de la empresa, las configuraciones en estos serán normalmente predeterminadas, o en el caso de que reutilicemos algún AP funcional, mostraré la configuración realizada.

Añadir también el NAS que he estado montando para que tengan un espacio de almacenamiento en red local y remoto mediante un dominio que hemos configurado para poder acceder desde fuera y para transferir archivos mediante sftp.

Además añadiremos un software de copias de seguridad freeware, en concreto Cobian reflector en el equipo del gerente para que haga copias de seguridad, en concreto completas y diferenciales, x día de la semana, todas las semanas. Estas copias se cifrarán y se enviarán mediante el protocolo TCP/IP o en el caso de que se encuentre fuera de la red local de la empresa, se harán mediante sftp al dominio creado.

3.2 Alcance del proyecto

Con este proyecto que estoy haciendo me quiero probar a mi mismo, quiero llevar mis conocimientos al extremo, tanto aprendiendo como poniéndolos en prácticas que al fin y al cabo es lo más importante en aprender. Para esto me he propuesto hacer algo relacionado con las redes que tanto me gustan, y sobre eso ir añadiendo cosas, ya que a mi mente le fascina desde algo simple, hacer una cosa muy grande y importante. Aparte de esto, también me encanta ayudar en todo lo que puedo a la empresa, ya que es de mi pueblo y deseo todo lo mejor para ella.

Dejando mis pensamientos al lado, pretendo mejorar la red de muchas maneras distintas. Quiero mejorar la organización que tienen en cuanto a red hablando, ya que hay bastante descontrol y cosas que tienen fuera de su alcance. Primero, quiero que tengan una red bien estructurada, teniendo los dispositivos de gestión (Switch, routers, patch panels, AP...) accesibles y controlados. Sabiendo perfectamente ordenar los cables y los puertos que están conectados, para así si en algún futuro tener que hacer algún cambio, verlo claro a primera vista o tenerlo apuntado.

Mi segunda misión, sería hacer que todos los equipos estén conectados a la red local de la empresa y que estén fuera de peligro de alguna intrusión. También que todos tengan acceso a los recursos necesarios dentro de esta, refiriéndome a impresoras, servidores de trabajo, almacenamiento compartido...

Y como último sería tener tolerancia a fallos, tanto de red como físicos del hardware. Esto lo haremos con el failover y con el servidor NAS que vamos a montar. Así siempre podremos tener una línea de red funcional para trabajar. Y si en algún caso se averiase el ordenador más importante, con más datos sensibles (el terminal del gerente), tener una copia seguridad completa de todos los archivos del disco o una imagen del disco para poder restaurar cualquier cosa en segundos.

Cabe destacar, que en este proyecto no configuraré el switch para tener VOIP, ya que esa configuración ya la están aplicando los switch de telefónica, que solo son gestionables por ellos, y son ellos los que tienen el control de los terminales telefónicos, así que yo me limitaré al protocolo TCP/IP. Agregar que tampoco utilizaré VLANS debido a que no me será necesario ejecutar la configuración para separar tramos de la red, no tengo que organizar ningún grupo destacado dentro de la red, simplemente los que tengan que tener IP estática, la tendrán asignada por MAC desde el DHCP.

Tampoco cambiaré ningún tipo de cableado, el cableado ya está hecho y montado, y nos sirve para los cambios que vamos a hacer. Eso sí, el cableado de dentro de los racks y la organización de los mismos si que cambiará a mejor, añadiendo distintivos a cada cable para tener una organización pulcra y clara.

3.3 Viabilidad Económica

3.3.1 Análisis DAFO

Para el estudio de viabilidad económica sobre el proyecto de reestructuración de red, utilizaremos el análisis DAFO para ver tanto las cosas buenas como malas de el proyecto, ya sea a nivel interno o por componentes externos.



Ilustración 8: Análisis DAFO de la situación del proyecto

Carácter interno

Debilidades:

Hablamos de debilidades cuando pensamos en que le falta a nuestro proyecto, o que aspectos nos están limitando en el desarrollo del proyecto.

-Poco presupuesto :

Me refiero a poco presupuesto al hablar que la empresa si quiere efectuar el proyecto, pero no quiere gastarse mucho dinero, la mayoría del material utilizado, será reutilizado o reciclado. Para así poder aprovechar el máximo de lo que ya tienen.

-No querer organizar las oficinas en VLANs

La definición es, organizar todas las oficinas de la empresa en una VLAN diferente con un rango de IP diferente, para tener una organización pulcra y limpia. Pero al informático de la empresa, mi tutor, no le parece bien o más que eso, no le ve la necesidad de ordenar la empresa en oficina, debido a que la empresa no es muy grande y tampoco son muchos los dispositivos a conectar.

-No añadir un proxy para controlar el tráfico desde dentro de la red:

En cuanto al proxy hablando, estaríamos hablando de un servidor proxy, tipo squid, para poder bloquear cierto tráfico no deseado a una parte de internet. Como por ejemplo, el hecho de que los trabajadores puedan ver cualquier red social al trabajar, o cualquier tipo de distracción de su trabajo. Sin embargo, el tutor, me ha comentado que no es necesario porque creen que el flujo de trabajo es bastante adecuado, por lo tanto no tienen la necesidad de regular el acceso a internet.

-Tener que reestructurar la red entorno a los switch de telefónica:

Con esto, estoy hablando de los switch de telefónica que gestionan la VOIP. Estos switch son gestionables, pero el nuevo plan de seguridad de telefónica no te deja los datos de acceso a ellos, solo pueden ser gestionados mediante la plataforma de telefónica de gestión online, y en cuanto a las opciones son muy limitadas, llegando a ni poder desactivar el DHCP o para poder conectar otro switch a un puerto, tener que llamar al técnico para que habilite el puerto, debido a que por normalidad, cada puerto solo tiene un máximo de 2 direcciones MAC.

Fortalezas:

Las fortalezas son todas aquellas ventajas o puntos a favor que tiene mi proyecto para poder salir a luz o tener una ventaja sobre otros.

-Seguridad en la red:

Añadiremos seguridad a nuestra red añadiendo un firewall totalmente personalizado y hecho para esta red.

-Control del tráfico entrante y saliente:

Esto también lo lograremos con el firewall, además el switch mikrotik principal, nos permite tener un seguimiento de todo el tráfico saliente y entrante.

-Almacenamiento compartido:

Dado a que montaré el NAS para que sea accesible tanto desde la red local como en remoto mediante smb o sftp.

-Disponibilidad de internet 24/7:

Para que los empleados no pierdan conectividad a internet, utilizaré un sistema failover o DualWan, con dos operadores de ISP distintos.

-Tolerancia a fallos físicos:

La tolerancia a fallos físicos se refiere, por ejemplo, si se rompe el disco duro del gerente, o cualquier pieza que haga imposible el uso de su terminal. Poder utilizar para restaurar una copia de seguridad o una imagen de disco que haremos con un programa semanalmente y se enviará al espacio compartido.

-Conectividad completa:

Hablo de conectividad completa cuando me refiero a que cualquier terminal ya sea por cable o inalámbrico tenga acceso a internet y a todos los recursos necesarios para posibilitar su trabajo en la red. Esto lo podemos hacer añadiendo switches y patch panels, y de manera inalámbrica, AP o acces points.

Carácter externo:**Amenazas:**

Son esos factores que pueden impedir la ejecución del proyecto, o pueden restar importancia a este.

-La admisión de la red (débil) actual:

La admisión de la red actual podría ser una amenaza para la realización del proyecto, ya que en muchas empresas si todo les funciona tienden a dejarlo como está aunque suponga un riesgo para la integridad de la empresa.

-El rechazo de las personas hacia las nuevas tecnologías:

Este punto va ligado al anterior, el rechazo a las nuevas tecnologías es muy grande, hay muchas personas que rechazan nuevas tecnologías o otras metodologías de trabajo solo por no haberlas visto nunca o por el simple hecho de no cambiar el que tienen en el momento.

-Los ciclos de trabajo para poder efectuar los cambios en la red:

Los ciclos de trabajo de la empresa son claros, por la mañana trabajan, por la tarde descansan. Por esto, puede ser una gran pega para hacer los cambios. Todos los empleados necesitan internet para trabajar, y por la mañana no se puede tocar ninguna configuración que altere el flujo de internet.

Oportunidades

Las oportunidades son ocasiones o cosas que vemos externas a nosotros que ocasionan que pueda suceder un cambio, en el caso de nuestro proyecto, hay cosas que crean oportunidades para ejecutar lo pensado.

-Errores en la red:

Una buena oportunidad para poder aprovechar sería un error en red. Con esto poder atacar diciendo que con el proyecto actual que estoy desarrollando no pasaría.

-Fallos de conectividad:

Que cualquier equipo se quede sin una IP para poder navegar es un fallo de conectividad, cosa que con mi proyecto no pasaría.

-Pérdida de datos sensibles o importantes:

Las pérdidas de datos sensibles o importantes se pueden solventar haciendo copias de seguridad del dispositivo en cuestión, como se explica en mi proyecto, se hacen copias de seguridad automatizadas a un espacio compartido cifrado.

-Caídas de un ISP:

Si un ISP cae y con él la conexión a internet, los trabajadores no pueden reanudar con su flujo de trabajo. Por esto, mi proyecto solventaría el caso hipotético. Al configurar el failover con dos ISP, nos aseguramos que si uno cae, el otro estará a disposición.

3.3.2 Tabla de inversiones, gastos e ingresos

Cuando hablamos de un proyecto, hablamos de gastos e ingresos. Por esto, vamos a crear una tabla de inversiones, gastos e ingresos, para poder comprobar a que empresas podemos aplicar este proyecto concreto y sobretodo cuanto podríamos ganar por hacer esta labor.

Inversiones

En el punto de inversiones estaré clasificándolas como inversiones materiales para poder ejercer mi trabajo, en este caso, el de montar redes según las personalizaciones que me pidan, pero siempre habrán 3 cosas que no puedan faltar, los switch mikrotik, el cableado y los equipos NAS. Ahora explicaré cada uno con detalle y el gasto que ocasiona. Además añadiré inversiones como un portátil para trabajar o el coste de la creación y mantenimiento de una página web.

Empezaremos hablando del portátil, necesitaré un portátil con lo necesario para desarrollar mi actividad. Necesitaré una tarjeta de red para poder tener conexión cableada y así poder configurar correctamente los equipos. Y también que la tarjeta de red admita conexión wireless, es decir WIFI. Sin olvidar que el portátil tiene que tener potencia para poder funcionar en multitasking y poder estar enviando paquetes a la vez que configurando un terminal. Para esto, he decidido que escogeré el HP Victus 15-fb1002ns, que cuenta con conexión rj-45 y una tarjeta para poder acceder mediante wifi al internet. Este portátil incluye 16 gb de RAM ddr5 4800 y también un procesador ryzen 5 7535HS, para el almacenamiento tendremos 512 GB de SSD. Y con esto conformamos nuestro portátil para ejecutar las pruebas. Este tiene un coste de **599,99€**.



Ilustración 9: Portátil escogido

El siguiente artículo del que hablaré serán los switch mikrotik, en concreto utilizaremos un modelo bastante asequible y que a su modo es muy funcional. Tiene 24 puertos GigabitEthernet2 y además dos puertos adicionales sfp para poder interconectarse con otros routers o switches. Cuenta con un puerto de consola por si quieres conectarte vía putty. Este modelo es el Cloud Router Switch CRS326-24G-2S+RM que tiene un precio base de **166,67€**



Ilustración 10: Equipo Mikrotik Elegido

Para el cableado, dispondremos de packs de cableado, es decir, dos packs de cableado serán necesarios para interconectar todas las secciones del router con los patch pannels y así habilitar todos los puertos. Cada pack de cableado traerá 14 cables Ethernet categoría 6 utp de 1.5 metros de longitud, cada uno de estos costará 1 euro. También incluirá 1 SFP para interconectar los switch mediante el puerto SFP, cada cable de estos cuesta 38,16 euros. por lo que el pack costará **52,16 euros**.



Ilustración 11: Cable SFP que utilizaremos

Y sigo con los equipo NAS, que son equipos con prestaciones de potencia ligeramente medianas, pero con una capacidad de almacenamiento y poder de fuente de alimentación bastante elevado. Estamos hablando de que necesitaremos un equipo con 5 discos, 1 disco para el sistema operativo truenas de alrededor de 256 GB, y luego 4 discos de 1TB SSD para hacer el array de discos RAID-5. El equipo constará de los siguientes componentes:

- Procesador :Intel Core i5 12400 2.5 GHZ – 166,99€
- Placa base : MSI PRO B760-P WIFI DDR4 – 137,99€
- Memoria RAM : Kingston Fury Beast DDR4 3200 16 GB 2x8GB – 39,99€
- Caja : Tempest Umbra ATX – 64,99€
- Refrigeración CPU: Tempest Cooler 4 pipes – 32,98€
- Fuente de alimentación: Nox Urano 750W plus bronze – 58€
- Disco duro del S.O.: Gigabyte SSD M.2 256 GB – 42,99€
- Discos Duro array : Samsung 870 EVO SSD 1 TB x 4 - 387,92€

Sería un total de **931,85€** cada equipo NAS que vayamos a montar.

MI configuración [Reiniciar] [Compartir] [Guardar]

Componentes base
Los componentes base son los imprescindibles para que se pueda realizar un montaje funcional.

PROCESADOR *
Intel Core i5-12400 2.5 GHz 166,99€

PLACA BASE *
MSI PRO B760-P WIFI DDR4 137,99€

MEMORIA RAM *
Kingston FURY Beast DDR4 3200 MHz 16GB 2x8GB CL16 39,99€

CAJA/TORRE *
Tempest Umbra RGB Torre ATX Negra 64,99€

REFRIGERACIÓN LÍQUIDA
No se puede añadir una refrigeración líquida porque ya has añadido una refrigeración CPU.

REFRIGERACIÓN CPU
Tempest Cooler 4Pipes 120mm Ventilador CPU Negro 32,98€

FUENTE DE ALIMENTACIÓN
Nox Urano VX 750W 80+ Bronze 140MM PWM 58€

Gráfica
Las tarjetas gráficas son un componente indispensable si vas a jugar a videojuegos o buscas un mejor rendimiento en diseño, edición de imagen y vídeo.

TARJETA GRÁFICA

Almacenamiento
Añadir un disco duro a tu configuración es esencial para poder almacenar todo el contenido posible en tu ordenador: fotos, vídeos, videojuegos...

DISCO DURO
Gigabyte SSD M.2 2280 256GB PCIe 3.0 x4 NVMe 42,99€

DISCO DURO 2
Samsung 870 EVO SSD 2.5" 1TB SATA3 Negro 387,92€
Precio por unidad: 96,98€

Información
Unidades: 1 TOTAL: 931,85€
Añadir al carrito
La fecha estimada de entrega será proporcionada al finalizar el proceso de compra, antes de realizar el pago.
Todos nuestros montajes cuentan con **garantía de 3 años** para todos los componentes.

Ilustración 12: Configuración equipo NAS

Añadir que encargaremos a un programador web, para que nos diseñe una página web atractiva para promocionar y dar información de nuestro producto. En esta ofreceremos consulta personalizada, contacto y precio de nuestros servicios. El programador nos comentó que el diseño personalizado y la creación base de la página cuesta **700€**.

Gastos

En el segundo punto de la tabla se encuentra el punto de gastos, en este punto quiero especificar que a gastos me refiero a salidas de dinero por algún tipo de servicio que nos puedan ofrecer, ya sea luz, agua ... Los gastos mas normales y que voy a enumerar, serán: Luz, alquiler, nóminas, internet, gestor y publicidad. Como los servicios que ofreceré, no tienen que ver con una sede fija, nos quitaremos de encima los gastos de luz y alquiler.

Voy a empezar hablando de las nóminas, en el supuesto de la empresa, veremos que es pequeña porque aún estaré empezando, por lo tanto en un principio no voy a necesitar ayudantes. Pero en los meses de verano, como vemos en el aumento de compra de dispositivos, tendremos un repunte de peticiones de crear redes, por lo que los meses de julio y agosto, necesitaré contratar a gente. Les estaré pagando **2500 €** al mes. Por lo que en el mes de julio solo necesitaré a una persona, mientras que en agosto, ascenderán bastante las peticiones por lo que necesitaré otra persona más.

También voy a comentar el caso del internet, porque por ejemplo, nosotros no tenemos sede fija y por lo tanto no tenemos gastos de internet, pero les ofrecemos a los clientes que si ellos no tienen una tarifa buena de internet, nosotros dentro de nuestros servicios poder crearles el failover con las dos líneas de ISP que nosotros consideremos. En nuestro caso, siempre que la empresa o sitio que tengamos que instalar el servicio esté dentro de casco urbano con conectividad a internet, una tarifa de movistar y de vodafone, con un coste de 29,99€ a 300 MB de velocidad fija cada uno. Por lo que el precio del internet nos costará **59,98€** al mes.

Seguiré con el punto de inversiones comentando los gestores. El gestor, es muy importante en todos los aspectos de la empresa, ya que al tener muchos gastos e inversiones, es quien tiene el saber de que cosas puede deducir la empresa y que cosas no, para poder ahorrar dinero en la declaración o poder acceder a ayudas para pymes. En este caso contrataremos un servicio de asesoría gestora mensual, que nos llevará la contabilidad y también los contratos y gestión de pagos a empleados. Este servicio nos costará **194€** al mes.

El siguiente servicio que contrataremos será un servicio de publicidad, ya que queremos lo mejor para nuestra empresa, sobretodo por la zona, así que necesitaremos una empresa SEO en google adds, para que nos pueda brindar posicionamiento web y publicidad en distintas plataformas. Esta empresa al ver que no íbamos muy bien en cuanto a servicios prestados, nos comentó que le gustaría implementar un plan de 6 meses con nosotros a un precio fijo de **150€** al mes.

Y por último, el gasto de mantenimiento de la página web, que incluye, hosting, protección a tiempo real y monitorización de la misma. El precio nos cuesta **30€** al mes para que la página siga activa.

Ingresos:

Y ya como tercer y último punto, añadiremos el punto de ingresos. Este punto se compone de todos los ingresos esperados que estimamos que llegarán en los meses del próximo año.

Nuestros ingresos se basarán en los 3 servicios que ofrecemos y su mantenimiento respectivo.

Servicio Completo, este servicio se basa en todo lo que nosotros ofrecemos, dispone de un arreglo de la red arreglando los tramos de la red LAN con cables , segmentando los trozos de la red con distintivos y con el switch mikrotik que nos permite añadir un firewall para una mejor defensa de la red. Además incluimos el Failover, añadiendo nosotros las líneas de los ISP que creamos correspondientes evaluando las condiciones del entorno. Y por último, montaremos un NAS de última generación con un espacio de 2,5 TB de espacio para el almacenamiento de nuestros clientes. Este servicio, tiene un coste de entrada de **3062,84€**, con esto, pagaremos todos los componentes con los que trabajamos y pondremos un precio de mano de obra de 60€/h. Y también tenemos el servicio de mantenimiento y garantía que es obligatorio durante el primer año de contrato, que tiene un precio de **100€ al mes** por el servicio completo.

Servicio de red, este servicio es la opción más económica. Ya que este lo que haremos será como hemos explicado antes con el servicio completo, arreglar la red según las necesidades de cada empresa, segmentar las áreas de trabajo según necesidad y añadir defensa a la red, todo esto lo conseguiremos con el mikrotik. Además este servicio incluye el Failover, que también incluye el estudio de ISP acorde con las condiciones del entorno físico de la empresa. El servicio descrito tiene un coste de entrada de **1230,99€**, como hemos explicado anteriormente, este servicio cubre todos los costes de los equipos y componentes utilizados, añadiendo también el precio estándar de 60€/h. El precio de mantenimiento del servicio y la garantía de este durante el primer año tiene un precio de **50€ al mes** por el servicio de red.

Servicio de espacio, este servicio es la opción intermedia entre el servicio completo y el de red. Cubrirá las necesidades de red como hemos explicado en los otros dos servicios, pero la única cosa que no incluye es el failover y el estudio de ISP. Incluye el NAS con 2,5 TB de almacenamiento. Este servicio tiene un coste de entrada de **2402,84€**, este precio cubrirá todos los componentes utilizados, añadiendo que el coste de mano de obra se mantiene en 60€/h. El precio de mantenimiento del servicio y garantía durante el primer año tiene un precio de **75€ al mes** por el servicio de espacio.

TABLA DE INVERSIONES, GASTOS E INGRESOS													
Inversiones	Enero	febrero	marzo	abril	mayo	junio	julio	agosto	septiembre	octubre	noviembre	diciembre	Cantidad TOTAL
Accesori	589,99 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	589,99 €
Equipos Mikrotik	833,35 €	166,67 €	0,00 €	233,34 €	0,00 €	233,34 €	1.000,00 €	1.666,70 €	233,34 €	0,00 €	166,67 €	233,34 €	5.186,77 €
Cableado	521,69 €	104,32 €	0,00 €	208,64 €	521,69 €	0,00 €	312,86 €	1.043,20 €	208,64 €	0,00 €	104,32 €	208,64 €	3.233,52 €
Equipos NAS	2.795,35 €	331,85 €	1.063,70 €	0,00 €	1.383,70 €	0,00 €	3.772,40 €	3.313,50 €	331,85 €	0,00 €	0,00 €	1.063,70 €	23.286,25 €
Página Web	700,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	700,00 €
Capacidad de portal	1	0	0	0	0	0	0	0	0	0	0	0	1
Capacidad de Productos Mikrotik	5	1	0	2	0	2	6	10	2	0	1	2	31
Capacidad de Productos de Cableado	10	2	0	4	10	0	6	20	4	0	2	4	62
Capacidad de Productos NAS	2	1	2	0	2	0	4	10	1	0	0	2	25
Capacidad de Páginas Web	1	0	0	0	0	0	0	0	0	0	0	0	1
Capacidad de Productos TOTAL	20	4	2	6	12	2	16	40	7	0	3	6	120
Recuo TOTAL INVERSIONES	5.436,49 €	1.202,84 €	1.863,70 €	541,98 €	2.385,39 €	333,34 €	5.040,38 €	12.036,40 €	1.475,83 €	0,00 €	270,99 €	2.405,68 €	32.996,93 €
Gastos	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €
Alquiler	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €
Mantenimiento	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	2.500,00 €	5.000,00 €	0,00 €	0,00 €	0,00 €	0,00 €	7.500,00 €
Internet	59,98 €	59,98 €	0,00 €	0,00 €	59,98 €	119,96 €	119,96 €	239,90 €	0,00 €	0,00 €	0,00 €	119,96 €	839,72 €
Electricidad	154,00 €	154,00 €	154,00 €	154,00 €	154,00 €	154,00 €	154,00 €	154,00 €	154,00 €	154,00 €	154,00 €	154,00 €	2.308,00 €
Publicidad	0,00 €	0,00 €	0,00 €	150,00 €	150,00 €	150,00 €	150,00 €	150,00 €	150,00 €	0,00 €	0,00 €	0,00 €	900,00 €
Mantenimiento Página Web	30,00 €	30,00 €	30,00 €	30,00 €	30,00 €	30,00 €	30,00 €	30,00 €	30,00 €	30,00 €	30,00 €	30,00 €	360,00 €
Capacidad de pagos por Luz	0	0	0	0	0	0	0	0	0	0	0	0	0
Capacidad de pagos por Alquiler	0	0	0	0	0	0	0	0	0	0	0	0	0
Capacidad de pagos por Mantenimiento	0	0	0	0	0	0	1	2	0	0	0	0	3
Capacidad de pagos por Internet	1	1	0	0	1	2	2	5	0	0	0	2	14
Capacidad de pagos por Gestor	1	1	1	1	1	1	1	1	1	1	1	1	12
Capacidad de pagos por Publicidad	0	0	0	1	1	1	1	1	1	1	0	0	6
Capacidad de pagos por mantenimiento Pag Web	1	1	1	1	1	1	1	1	1	1	1	1	12
Capacidad de pagos TOTALES	3	3	2	3	4	5	10	13	5	2	2	4	47
Recuo TOTAL GASTOS	283,98 €	283,98 €	224,00 €	374,00 €	493,96 €	493,96 €	2.895,96 €	5.675,90 €	374,00 €	224,00 €	224,00 €	543,96 €	47
Ingresos	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €
Servicio Completo (Red, Firewall, NAS)	3.062,84 €	3.062,84 €	3.062,84 €	0,00 €	3.062,84 €	6.125,68 €	6.125,68 €	0,00 €	3.062,84 €	0,00 €	0,00 €	6.125,68 €	33.681,24 €
Servicio de Red (Red y Firewall)	0,00 €	1.230,99 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1.230,99 €	0,00 €	0,00 €	0,00 €	0,00 €	7.285,94 €
Servicio de Espacio (Red y NAS)	4.805,68 €	0,00 €	0,00 €	0,00 €	0,00 €	2.402,84 €	4.805,68 €	4.805,68 €	0,00 €	0,00 €	0,00 €	4.805,68 €	33.638,76 €
Mantenimiento Servicio Completo	0,00 €	100,00 €	200,00 €	300,00 €	300,00 €	400,00 €	600,00 €	800,00 €	800,00 €	900,00 €	900,00 €	900,00 €	6.200,00 €
Mantenimiento Servicio Red	0,00 €	0,00 €	50,00 €	50,00 €	50,00 €	50,00 €	50,00 €	50,00 €	200,00 €	200,00 €	200,00 €	200,00 €	1.500,00 €
Mantenimiento Servicio Espacio	0,00 €	150,00 €	150,00 €	150,00 €	150,00 €	150,00 €	225,00 €	375,00 €	900,00 €	900,00 €	900,00 €	900,00 €	4.950,00 €
Capacidad de ingresos por Servicio Completo	1	1	1	0	1	2	2	0	1	0	0	2	11
Capacidad de ingresos por Servicio de Red	0	1	0	0	0	0	0	0	0	0	0	0	6
Capacidad de ingresos por Servicio de Espacio	2	0	0	0	0	1	2	7	0	0	0	2	14
Mantenimiento Servicio Completo	0	1	2	3	3	4	6	8	8	9	9	9	62
Mantenimiento Servicio Red	0	0	1	1	1	1	1	6	6	6	6	6	30
Mantenimiento Servicio Espacio	0	2	2	2	2	2	3	5	12	12	12	12	66
Capacidad de ingresos TOTALES	3	3	6	6	7	10	14	26	27	27	21	21	189
Ingresos TOTALES	7.886,52 €	4.543,83 €	3.462,84 €	500,00 €	3.562,84 €	9.128,52 €	11.806,36 €	24.199,83 €	5.062,84 €	2.100,00 €	2.100,00 €	13.021,36 €	87.386,94 €
TOTAL A PERCIBIR	2.134,05 €	1.057,01 €	1.375,14 €	-415,98 €	125,36 €	3.301,22 €	2.772,02 €	6.467,53 €	2.215,01 €	1.976,00 €	1.876,01 €	10.281,75 €	32.542,29 €

Inversiones + Gastos	
Enero	5.436,49 €
febrero	1.202,84 €
marzo	1.863,70 €
abril	541,98 €
mayo	2.385,39 €
junio	333,34 €
julio	5.040,38 €
agosto	12.036,40 €
septiembre	1.475,83 €
octubre	0,00 €
noviembre	270,99 €
diciembre	2.405,68 €
Total Anual	32.996,93 €

Ingresos	
Enero	7.886,52 €
febrero	4.543,83 €
marzo	3.462,84 €
abril	500,00 €
mayo	3.562,84 €
junio	9.128,52 €
julio	11.806,36 €
agosto	24.199,83 €
septiembre	5.062,84 €
octubre	2.100,00 €
noviembre	2.100,00 €
diciembre	13.021,36 €
Total Anual	87.386,94 €

Entrada - Salida	
Enero	2.134,05 €
febrero	1.057,01 €
marzo	1.375,14 €
abril	-415,98 €
mayo	125,36 €
junio	3.301,22 €
julio	2.772,02 €
agosto	6.467,53 €
septiembre	2.215,01 €
octubre	1.976,00 €
noviembre	1.876,01 €
diciembre	10.281,72 €
Total Anual	42.442,29 €

Ilustración 13: Tabla de inversiones, gastos e ingresos.

Anexo : El documento completo para verlo de manera detallada y con buena resolución se encuentra en [Tabla de inversiones, gastos e ingresos.odt](#)

3.4 Recursos necesarios

Todo sistema informático consiste de dos partes esenciales en su creación, del hardware y del software, en este punto estaremos explicando los dos puntos por separado y los componentes que corresponden a cada punto.

3.4.1 Hardware

Al hardware nos referimos a cualquier elemento físico o material que constituyen un sistema informático o una máquina. En nuestro caso voy a ir enumerando todos los dispositivos hardware que utilizaremos en el servicio completo para Solgata.

- Switch Mikrotik CRS125-24G-1S-RM
- Cable Ethernet Categoría 6 UTP 1,5 M
- Equipo NAS
- Router TPLINK (ISP1)
- Router Mitrastar (ISP2)
- Switch Huawei 24 Gigabit Ethernet (Gestión del ISP)
- Patch panel
- x24 Rosetas rj45
- Switch GTLAN 12 Gigabit Ethernet (Gestión ISP)
- 1 Extender TPLink
- 1 Mikrotik hAP Lite
- 1 Huawei AP

3.4.2 Software

El software es todo aquello no físico y intangible que compone una máquina o sistema informático, en este punto hablaré de todos los programas que he utilizado tanto como mecanismos de seguridad como servicios utilizados.

Aplicaciones/Nivel de aplicación

- Winbox
- MikrotikNetinstall
- Zenmap
- TheDude
- AdvanceIPScanner
- CobianReflector
- Filezilla
- DUC

Servicios

- NETBIOS
- SMB
- HTTP
- HTTPS
- SSH/SFTP
- ICMP
- TCP/UDP
- RDP
- Winbox
- DNS
- NTP

3.5 Documentación

3.5.0 Esquema de la red visual

En este esquema, mostramos todos los dispositivos que estamos conectando a la red y marcaremos actualmente los que yo he configurado, ya que algunos ya estaban preconfigurados en la empresa.

Este esquema muestra toda la configuración de la red física, todos los dispositivos que existen en la empresa, junto con el espacio que comparten y como están conectados.

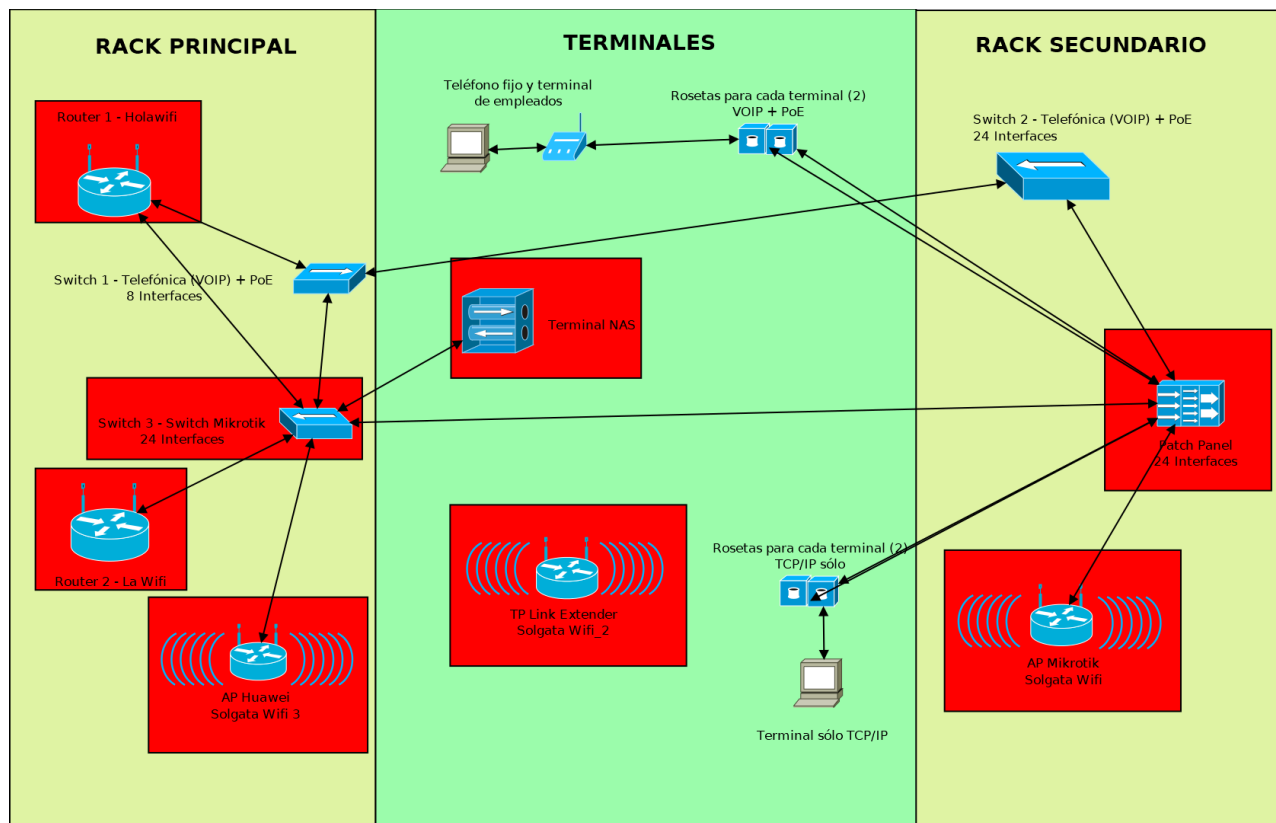


Ilustración 14: Esquema físico visual de la red

Como vemos, los dispositivos sin el cuadro rojo son los switch gestionados por el ISP a los que no tenemos acceso, estos gestionan los dispositivos vía VOIP con una configuración de VLANs que solo ellos saben.

3.5.1 Esquema de red

En el esquema de la red, veremos exactamente con un diagrama todos los equipos (imprescindibles para nosotros) en la red con sus respectivas IP y las subredes con su respectiva información. Esto lo haremos omitiendo los switches de telefónica. Solo plantearemos el aspecto de red.

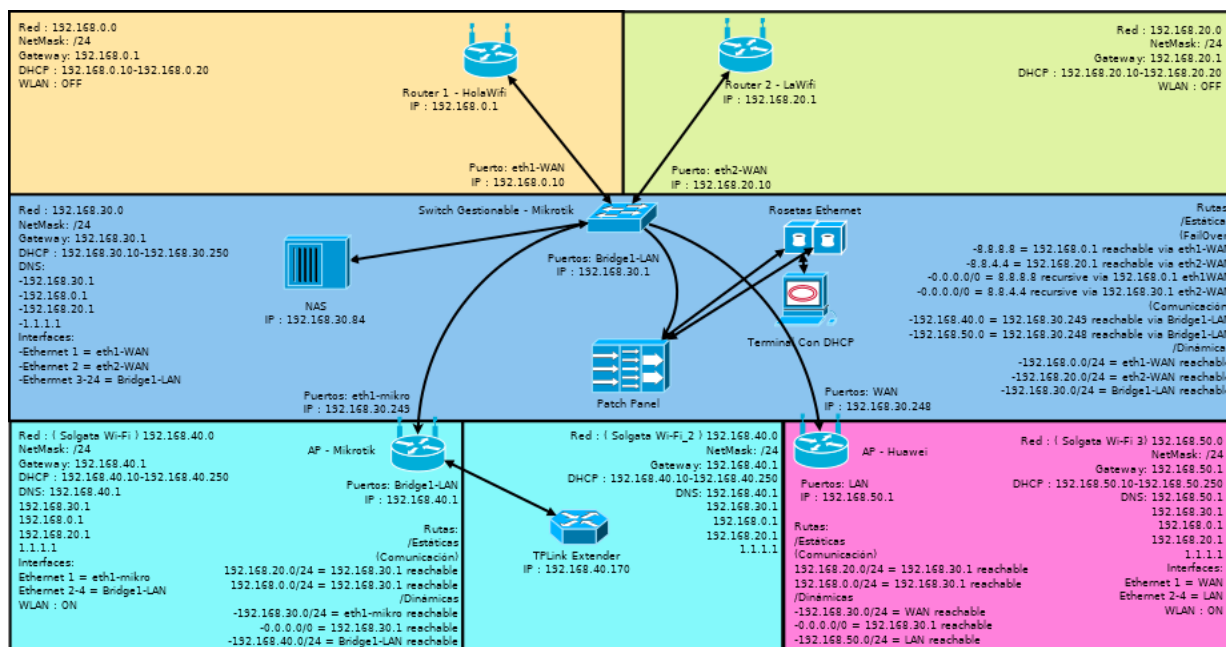


Ilustración 15: Esquema de la red

Podemos ver en el esquema que tenemos 2 routers lo cual nos permitirá hacer el failover. Luego también tenemos el switch con su respectivo patch panel y las rosetas para ofrecer el servicio de ethernet distribuido por toda la empresa. Ahora que ya tenemos todas las conexiones cableadas terminadas, nos pondremos con las inalámbricas.

Tenemos dos AP con dos subredes distintas, y un entendedor de señal para uno de estos dos AP. Por lo que tendremos 2 AP que emitirán Wi-Fi en dos subredes distintas, y también un extender que nos permitirá alargar el área de conexión inalámbrica de uno de estos dos AP sin crear una subred.

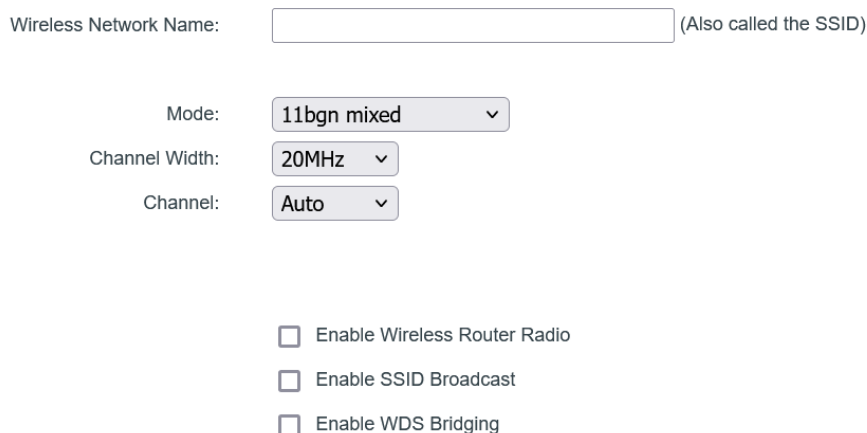
3.5.2 Configuración Básica

3.5.2.1 Configuración del Router 1 – Holawifi

En el router 1, accederemos a su plataforma de configuración mediante el navegador con la ip del router.

Acto seguido, introduciremos los credenciales de acceso a la administración del router. El primer paso que haremos será desactivar el Wireless debido a que no lo necesitaremos.

Wireless Settings



Wireless Network Name: (Also called the SSID)

Mode:

Channel Width:

Channel:

☐ Enable Wireless Router Radio

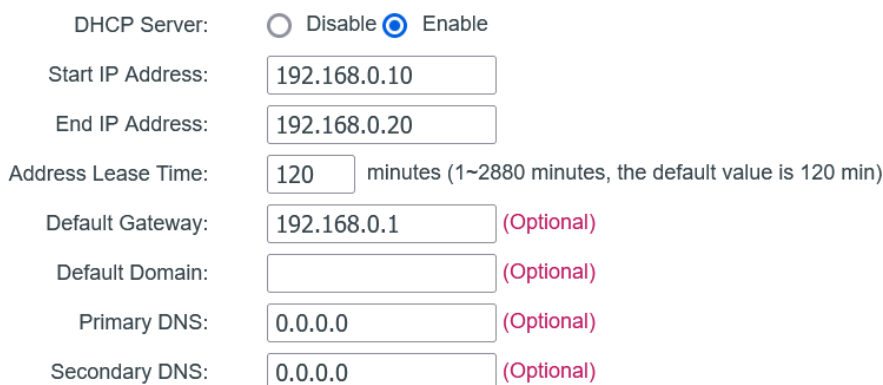
☐ Enable SSID Broadcast

☐ Enable WDS Bridging

Ilustración 16: Desactivar la transmisión de Wi-Fi del router 1

El segundo será modificar el DHCP para que tenga un rango solo de 10 direcciones asignables, ya que no utilizaremos su conexión LAN, sino la del Switch. Y dejaremos 10 para posibles configuraciones o según necesidades futuras

DHCP Settings



DHCP Server: ☐ Disable ☒ Enable

Start IP Address:

End IP Address:

Address Lease Time: minutes (1~2880 minutes, the default value is 120 min)

Default Gateway: (Optional)

Default Domain: (Optional)

Primary DNS: (Optional)

Secondary DNS: (Optional)

Ilustración 17: Desactivar el DHCP del router 1

Ahora, haremos que el router reserve la ip 192.168.0.10 por MAC, que es la que le asigna al switch mikrotik para que siempre sea la misma.

Address Reservation


ID	MAC Address	Reserved IP Address	Status	Modify
1		192.168.0.10	Enabled	Modify Delete

Ilustración 18: Reservar dirección del switch mikrotik en el router 1

3.5.2.2 Configuración del router 2 - LaWifi

En el router 2, accederemos a su plataforma de configuración mediante el navegador con la ip del router.

Acto seguido, introduciremos los credenciales de acceso a la administración del router. El primer paso que haremos será desactivar el Wireless debido a que no lo necesitaremos.

Configuración Inalámbrica Básica

Red Inalámbrica

Radio Encendido/Apagado

Radio Apagado


Wireless Connection Mode

AP

Modo de Red

11b/g/n modo mixto

Multiple SSID

 Habilitar ☒ Esconder ☐ Aislado ☐ Cliente Máximo 16

Multiple SSID1

Habilitar ☒ Esconder ☐ Aislado ☐ Cliente Máximo 16

Multiple SSID2

Habilitar ☒ Esconder ☐ Aislado ☐ Cliente Máximo 16

Multiple SSID3

Habilitar ☒ Esconder ☐ Aislado ☐ Cliente Máximo 16

transmitir(SSID)

☒ Habilitar ☐ Deshabilitar


Aislamiento AP

☐ Habilitar ☒ Deshabilitar

MBSSID Aislamiento AP

☐ Habilitar ☒ Deshabilitar

BSSID



Frecuencia (Canal)

Auto

HT Modo Físico

☒ Modo Mixto ☐ Campo Verde

Modo de Operación

☐ 20 ☒ 20/40

Ancho de Banda del Canal

Ilustración 19: Apagar Wireless en el router 2

El segundo será modificar la red del router, por defecto viene con la 192.168.0.0/24, pero nosotros al tener que hacer un failover, no podemos poner la misma red en dos interfaces diferentes, ya que lo que hará es que al intentar buscar el camino a internet, no diferenciará entre cual ip es la de cada router, por lo tanto, cambiaremos la dirección de red a 192.168.20.0/24. El DHCP también lo modificaremos para que tenga un rango solo de 10 direcciones asignables, ya que no utilizaremos su conexión LAN, sino la del Switch. Y dejaremos 10 para posibles configuraciones o según necesidades futuras

Puertos de PC(LAN)

Dirección IP Local	192.168.20.1
Máscara de Red Local	255.255.255.0
Servidor DHCP Local	Habilitar ▼
Dirección de Inicio del DHCP	192.168.20.10
Dirección de Término del DHCP	192.168.20.20
Modo de DNS	Auto ▼
DNS Primario	192.168.20.1
DNS Secundario	1.1.1.1
Tiempo de Arriendo del Cliente(0-86400s)	86400
Lista de Clientes DHCP	

Ilustración 20: Configuración DHCP del router 2

Ahora, haremos que el router reserve la ip 192.168.20.10 por MAC, que es la que le asigna al switch mikrotik para que siempre sea la misma.

Asignación Estática de DHCP

NO.	MAC	IP Dirección
1	<input type="text"/>	192.168.20.10
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>

DNS Proxy [Habilitar ▼](#)

Ilustración 21: Configuración de IP estática para el switch mikrotik en el router 2

3.5.2.3 Configuración Switch Mikrotik CRS125-24G-1S

La configuración básica de un switch Mikrotik CRS125-24G-1S-RM es crucial para su integración y funcionamiento en una red empresarial. Este dispositivo ofrece capacidades avanzadas de conmutación y enrutamiento, esenciales para una gestión eficiente de la red.

Los pasos fundamentales incluyen la asignación de direcciones IP para permitir la gestión remota, la configuración de un servidor DHCP para la asignación automática de direcciones IP a los dispositivos conectados, y la personalización del nombre del switch para facilitar su identificación y monitoreo. Esta configuración inicial asegura que el switch esté preparado para gestionar el tráfico de red de manera efectiva y optimiza su rendimiento en el entorno empresarial.

Toda la configuración del switch y las explicaciones las encontraremos en un anexo llamado [AnexoSWMikrotik.pdf](#) que se encuentra en la carpeta anexos.

3.5.2.4 Configuración del Mikrotik hAP Lite

La configuración de un hAP Mikrotik como punto de acceso inalámbrico es crucial para mejorar la cobertura y la conectividad de red en entornos empresariales o domésticos. Este dispositivo versátil permite una gestión eficiente de la red Wi-Fi, ofreciendo capacidades avanzadas de enrutamiento y conmutación.

Los pasos básicos incluyen la asignación de direcciones IP, la configuración del servidor DHCP, y la creación de la red inalámbrica con sus credenciales de seguridad. Además, se establecerá un nombre para el dispositivo para facilitar su gestión.

Esta configuración inicial asegura un funcionamiento óptimo del hAP Mikrotik como punto de acceso inalámbrico, proporcionando una conexión estable y segura para todos los dispositivos en la red.

Toda la configuración del hAP Lite Mikrotik se encuentra en el anexo [AnexoAPMikrotik.pdf](#) que se encuentra en la carpeta anexos.

3.5.2.5 Configuración del TPLink Extender

Un TPLink Extender es una herramienta inalámbrica de aumento de rango Wi-Fi, es decir, es un dispositivo que se conecta a la señal de cualquier Wi-Fi para aumentar el rango de dispersión de este y también para hacer correcciones en la señal.

La configuración es sencillísima, lo único que se tiene que hacer es acceder al portal web del dispositivo, y seleccionar la red que queremos amplificar y ya tienes tu red wifi amplificada.

Nosotros hemos configurado el extender para que tenga la dirección IP 192.168.40.170, es decir el extender sirve de DHCP relay del Wi-Fi Solgata principal y asigna a todos los clientes que se conecten a él, el DHCP del servidor del AP Mikrotik.

3.5.2.6 Configuración del AP Huawei

La configuración de este dispositivo no tiene mucha complejidad, simplemente, entraremos en el portal web del flybox (AP Huawei), iremos al apartado de WLAN>DHCP y ahí cambiaremos la IP del equipo a 192.168.50.1, y el rango de cesión de su DHCP haremos que sea la subred 192.168.50.0, su rango será 50.10-50.250



Ilustración 22: Configuración de IP y cesión de IP del AP Huawei

Y posteriormente para terminar con la configuración del AP, iremos al apartado Seguridad>Estado del Firewall. Y desactivaremos el firewall que implementa este AP, principalmente lo desactivaremos porque no podemos cambiar las reglas que nos aplica, y estas no nos interesan, porque bloquean todo tráfico entrante desde la interfaz WAN, y además bloquea la detección de equipos cosa que no nos interesa por el NAS.

Estado del Firewall

Habilita o deshabilita las funciones de filtro de cortafuegos. Las funciones de filtro de direcciones IP, ping a puerto WAN y filtro de nombres de dominio solo están disponibles cuando está habilitado el cortafuegos.

- ☐ Activar cortafuegos (interruptor principal del cortafuegos)
- ☐ Activar filtro de direcciones IP
- ☒ Desactivar ping del puerto WAN
- ☐ Habilitar filtro de nombres de dominio
- ☐ Habilitar filtrado de MAC

Ilustración 23: Configuración de seguridad del AP Huawei

3.5.3 Configuración Avanzada

En esta configuración avanzada vamos a desglosar los aspectos mas importantes que hemos configurado.

Explicaremos como he logrado hacer un failover con los dos ISP, como he conseguido hacer un firewall con el software que nos ofrece mikrotik avanzado, también la configuración del sistema operativo truenas con el protocolo smb y por último que ajustes he hecho redireccionando puertos y software utilizado para tener el NAS accesible mediante un dominio web.

3.5.3.1 Failover en switch Mikrotik

El Balanceo de carga o Failover consiste en distribuir paquetes IP entre diferentes enlaces.

Una de las potencialidades con que cuentan los Router Mikrotik es la opción Multi-WAN, lo que significa que podemos conectarnos a más de una conexión WAN, incluso con proveedores de servicio diferentes, con lo que logramos:

- Asegurar que la conectividad de red se mantenga mediante el uso de múltiples enlaces a Internet o WAN.
- Puede configurarse para gestionar varios tipos de conexiones (por ejemplo, DSL, fibra óptica, LTE).
- Reducir el riesgo de interrupciones prolongadas de servicio.

Estuvimos contemplando la opción de implementar el protocolo VRRP, que a resumidas cuentas es lo mismo. Lo que nos hizo no acceder a esta opción, es que el protocolo VRRP se configura en los dos enrutadores, y los routers que estábamos utilizando no tenían accesibilidad a ese protocolo, en cambio el Failover se configura en un dispositivo de red que en nuestro caso es el switch mikrotik y por lo tanto si podemos configurar la redundancia de red.

Mas información de la configuración de nuestro Failover en este anexo → [AnexoFailover](#) que se encuentra en la carpeta anexos.

3.5.3.2 Firewall Avanzado de Mikrotik

Un firewall es una barrera de seguridad que controla el tráfico entrante y saliente de una red, basándose en un conjunto de reglas predefinidas. En una red empresarial, un firewall actúa como la primera línea de defensa contra amenazas externas, como ataques cibernéticos, malware y accesos no autorizados.

MikroTik, reconocido por sus soluciones de enrutamiento y gestión de redes, ofrece capacidades avanzadas de firewall en sus dispositivos. Estos firewall son configurables y pueden adaptarse a las necesidades específicas de la red, proporcionando un control granular sobre el tráfico y las políticas de seguridad. Configurando un firewall en mikrotik conseguiremos :

- Proporcionar una protección robusta contra amenazas externas, protegiendo los activos de la red.
- Permitir una gestión detallada del tráfico de red, asegurando que solo el tráfico autorizado pueda acceder a los recursos internos.
- Poder adaptarlo a diversas configuraciones de red, desde pequeñas empresas hasta grandes corporaciones.

Nosotros hemos configurado diversas reglas en el firewall de Mikrotik, con el que hemos añadido seguridad al entorno de la empresa y accesibilidad protegida a esta. Todos los detalles de como se ha hecho y las reglas explicadas al detalle se encuentran en el anexo de [AnexoFirewall.pdf](#) que se encuentra en la carpeta anexos.

3.5.3.3 Configuración del NAS

Un Network Attached Storage (NAS) montado con el sistema operativo TrueNAS ofrece una solución robusta y personalizable para el almacenamiento y gestión de datos en entornos domésticos y empresariales. TrueNAS, basado en FreeBSD, proporciona una plataforma confiable y escalable para centralizar el almacenamiento de archivos y servicios en red.

Al utilizar TrueNAS, los usuarios pueden aprovechar las funciones avanzadas de gestión de datos, como la replicación remota, el cifrado de datos y la integración con servicios en la nube. Además, TrueNAS ofrece una interfaz intuitiva que facilita la configuración y administración del NAS, incluso para aquellos con poca experiencia técnica.

Nosotros hemos configurado el NAS con 5 discos conformando un array (agrupación de discos) y utilizando SMB para compartir un repositorio en red, para que sea accesible por todos los usuarios de la red, además hemos añadido varios servicios para poder acceder a él.

Lo explico todo en el anexo [AnexoNAS.pdf](#) que se encuentra en la carpeta anexos.

3.5.3.4 Configuración de copias de seguridad con Cobian Reflector

Cobian Reflector es un programa freeware de copias de seguridad. Este programa tiene muchas características configurables, como parametrizar el copiado de seguridad, que copia elegir a la hora de hacerla, donde guardarlas...

Por eso, vamos a configurar el Cobian Reflector en el equipo del gerente para poder hacer copias de seguridad de su equipo, parametrizandolas a nuestro gusto y antojo.

Además, haremos que si el ordenador se encuentra tanto dentro de la red de la empresa como fuera de esta se envíen mediante SFTP al NAS para almacenarlas.

Lo explico todo en el [AnexoCobianReflector.pdf](#) que se encuentra en la carpeta anexos.

3.5.3.5 Configuración de redirección de puertos en la red

La redirección de puertos es un concepto muy importante en el área de red y sobretodo en salida a internet. Con esto quiero decir que al tenes muchas subredes y varios equipos con los que necesitamos acceder al internet público es imprescindible hacer redirección de puertos.

En el caso de la empresa, necesitamos tener 3 puertos activos en los dos routers, uno para el despliegue web del NAS, uno para el SSH del NAS también, y el último para el RDP (Conexión a escritorio remoto) de el pc informático.

Todo el proceso de configuración desde los routers hasta el NAS lo encontraremos en el anexo [AnexoRedPuertos.pdf](#) que se encuentra en la carpeta Anexos.

4. Puesta en marcha

4.1 Demostración de funcionamiento

Para las demostraciones de funcionamiento vamos a hacer varias pruebas, tanto redactadas y con imágenes como en el caso de las mas importantes videos demostrativos y explicativos de el funcionamiento del sistema.

4.1.1 Prueba de conectividad todos los equipos

Empezaremos haciendo una prueba sencilla para garantizar el interconectado de todos los dispositivos de una red. Lo que haremos será colocar equipos en diferentes subredes y hacer pings para garantizar poder responder a las peticiones.

30.0 → 40.0

Para esta prueba de conexión, nos situaremos conectados vía ethernet al switch y nos asignará la dirección IP 192.168.30.243. Haremos ping a un dispositivo móvil conectado a la red Wi-Fi que su dirección IP es 192.168.40.211.

```
C:\Users\Josep>ping 192.168.40.211

Haciendo ping a 192.168.40.211 con 32 bytes de datos:
Respuesta desde 192.168.40.211: bytes=32 tiempo=46ms TTL=63
Respuesta desde 192.168.40.211: bytes=32 tiempo=34ms TTL=63
Respuesta desde 192.168.40.211: bytes=32 tiempo=172ms TTL=63
Respuesta desde 192.168.40.211: bytes=32 tiempo=76ms TTL=63

Estadísticas de ping para 192.168.40.211:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 34ms, Máximo = 172ms, Media = 82ms
```

Ilustración 24: Ping de la subred 30.0 a la 40.0

30.0 → 50.0

Para esta prueba de conexión, nos situaremos conectados vía ethernet al switch y nos asignará la dirección IP 192.168.30.243. Haremos ping a un dispositivo móvil conectado a la red Wi-Fi que su dirección IP es 192.168.50.10. Nos saldrá como que no podremos hacer ping, pero esto se debe a que el modelo concreto Flybox, tiene en su firmware una opción que bloquea el tráfico ICMP proveniente del puerto WAN, es decir de toda subred ajena a él. Sin embargo, solo bloquea este protocolo, se pueden montar recursos compartidos y también hacer peticiones ssh ...

40.0 → 30.0

Para esta prueba de conexión, nos situaremos conectados vía Wi-Fi al AP y nos asignará la dirección IP 192.168.40.148. Haremos ping a el dispositivo NAS conectado a la red ethernet del switch que su dirección IP es 192.168.30.84.

```
C:\Users\Josep>ping 192.168.30.84

Haciendo ping a 192.168.30.84 con 32 bytes de datos:
Respuesta desde 192.168.30.84: bytes=32 tiempo=97ms TTL=63
Respuesta desde 192.168.30.84: bytes=32 tiempo=1ms TTL=63
Respuesta desde 192.168.30.84: bytes=32 tiempo=2ms TTL=63
Respuesta desde 192.168.30.84: bytes=32 tiempo=5ms TTL=63

Estadísticas de ping para 192.168.30.84:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 1ms, Máximo = 97ms, Media = 26ms
```

Ilustración 25: Ping de la subred 40.0 a la 30.0

40.0 → 50.0

Para esta prueba de conexión, nos situaremos conectados vía Wi-Fi al AP y nos asignará la dirección IP 192.168.40.148. Haremos ping a un dispositivo móvil conectado a la red Wi-Fi que su dirección IP es 192.168.50.10. Nos saldrá como que no podremos hacer ping, pero esto se debe a que el modelo concreto Flybox, tiene en su firmware una opción que bloquea el tráfico ICMP proveniente del puerto WAN, es decir de toda subred ajena a él. Sin embargo, solo bloquea este protocolo, se pueden montar recursos compartidos y también hacer peticiones ssh ...

50.0 → 30.0

Para esta prueba de conexión, nos situaremos conectados vía Wi-Fi al AP y nos asignará la dirección IP 192.168.50.11. Haremos ping a el dispositivo NAS conectado a la red ethernet del switch que su dirección IP es 192.168.30.84. En este caso si nos dejará hacer ping a esta dirección, ya que como habíamos descrito antes, la regla que viene implementada a nivel de firmware es solo para el tráfico ICMP proveniente del puerto wan, no saliente de el. Por lo que tendremos conectividad.

```
C:\Users\Josep>ping 192.168.30.84

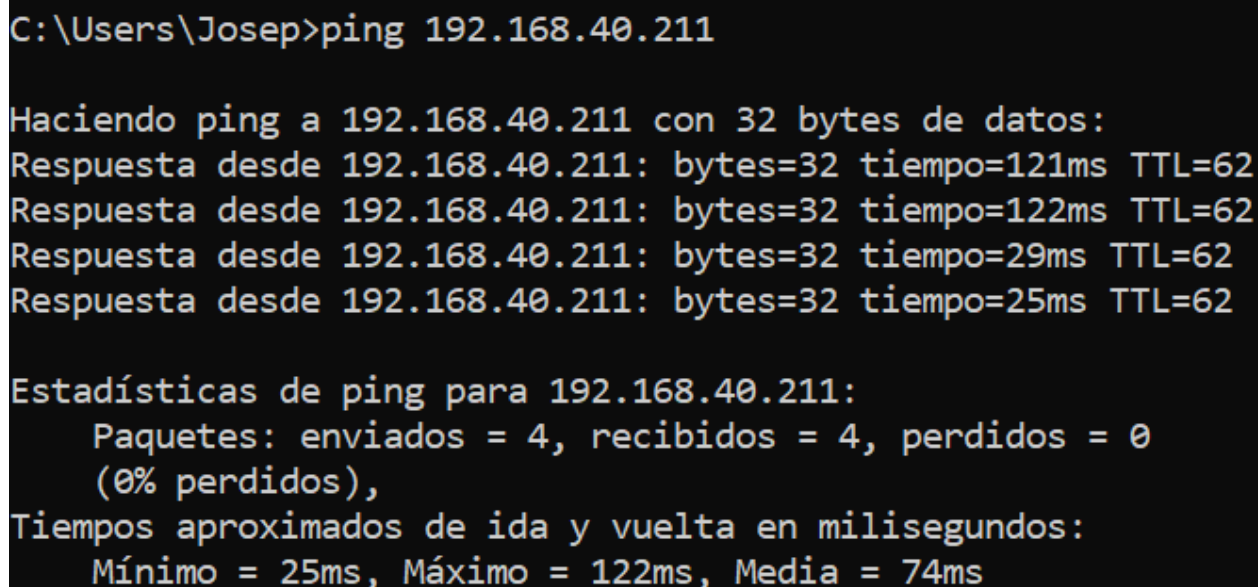
Haciendo ping a 192.168.30.84 con 32 bytes de datos:
Respuesta desde 192.168.30.84: bytes=32 tiempo=7ms TTL=63
Respuesta desde 192.168.30.84: bytes=32 tiempo=3ms TTL=63
Respuesta desde 192.168.30.84: bytes=32 tiempo=2ms TTL=63
Respuesta desde 192.168.30.84: bytes=32 tiempo=2ms TTL=63

Estadísticas de ping para 192.168.30.84:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 2ms, Máximo = 7ms, Media = 3ms
```

Ilustración 26: Ping de la subred 50.0 a la 30.0

50.0 → 40.0

Para esta prueba de conexión, nos situaremos conectados vía Wi-Fi al AP y nos asignará la dirección IP 192.168.50.11. Haremos ping a un dispositivo móvil conectado a la red Wi-Fi del AP que su dirección IP es 192.168.40.211. En este caso si nos dejará hacer ping a esta dirección, ya que como habíamos descrito antes, la regla que viene implementada a nivel de firmware es solo para el tráfico ICMP proveniente del puerto wan, no saliente de el. Por lo que tendremos conectividad.



```
C:\Users\Josep>ping 192.168.40.211

Haciendo ping a 192.168.40.211 con 32 bytes de datos:
Respuesta desde 192.168.40.211: bytes=32 tiempo=121ms TTL=62
Respuesta desde 192.168.40.211: bytes=32 tiempo=122ms TTL=62
Respuesta desde 192.168.40.211: bytes=32 tiempo=29ms TTL=62
Respuesta desde 192.168.40.211: bytes=32 tiempo=25ms TTL=62

Estadísticas de ping para 192.168.40.211:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 25ms, Máximo = 122ms, Media = 74ms
```

Ilustración 27: ping de la subred 50.0 a la 40.0

4.1.2 Prueba de FailOver

Para la prueba de funcionamiento del failover, he grabado un breve video explicativo donde explico brevemente las rutas utilizadas para formar el failover y una prueba de funcionamiento donde se ve claramente la funcionalidad de este.

El video en cuestión es [FailOverPrueba.wmv](#) que se encuentra en la carpeta Pruebas de funcionalidad.

4.1.3 Prueba de tráfico malicioso para el Firewall

Haremos una prueba de tráfico malicioso para comprobar la potencia del firewall. Esto lo haremos desde un equipo conectado a el DHCP del router 1, ya que el tráfico tiene que provenir desde la WAN. En esta prueba, no podemos comprobar todas las reglas del firewall porque son muchas, usaremos los más importantes.

En este caso haremos escaneo de puertos con NMAP para observar como descarta todos los paquetes y además añade la IP del equipo que lanza el ataque a una lista de bloqueo durante 2 semanas.

Y por último, la segunda comprobación será utilizando el programa the dude, que lo que hace es escuchar en el puerto winbox para ver como lo pone en la lista winbox y bloquea las peticiones.

En la primera prueba haremos en nmap un intense scan y todos los puertos, sin hacer ping.

Target: 192.168.30.0

Command: nmap -p 1-65535 -T4 -A -v -Pn 192.168.30.0

Ilustración 28: Escáner de puertos en ZenMap para la red 30.0

Ahora le daremos a scan, y automáticamente nos iremos al firewall y veremos como ha empezado a bloquear paquetes y ha puesto la IP en las listas de bloqueo. En este caso, nmap conseguirá descubrir los puertos, pero ya se le habrá bloqueado el acceso, por lo que no podrá hacer nada mas.

-- Bloqueig de TELNET WAN1											
3	add	input	6 (tcp)	23.2323	WAN1				bloqueo_telnet	176 B	4
4	drop	input								5.6 MB	132 061
-- Bloqueig de SSH WAN1											
5	add	input	6 (tcp)	22	WAN1				bloqueo_ssh	0 B	0
6	drop	input								0 B	0
-- Filtrar trafico de Scanners Botnet (Scanners afectan al port 8291 en busca de equipos mikrotik)											
7	add	input	6 (tcp)	8291	WAN1				winbox-1	0 B	0
-- Bloqueig de 4 mins a scanners botnet											
8	add	input	6 (tcp)	8291	WAN1				winbox-1	0 B	0
-- Bloqueig de 4 mins a scanners botnet											
9	add	input	6 (tcp)	8291	WAN1				winbox-2	0 B	0
-- Bloqueig de 14 dias a scanners botnet											
10	add	input	6 (tcp)	8291	WAN1				winbox-3	0 B	0
11	drop	input	6 (tcp)	8291	WAN1				winbox-4	0 B	0
-- Bloqueig de peticions dns externas											
12	drop	input	17 (udp)	53	WAN1					0 B	0
-- Bloqueig de proxys web externos											
13	drop	input	6 (tcp)	80	WAN1					80 B	2
-- Bloqueig Spamware del port 25											
14	add	forward	6 (tcp)	25	WAN1				clientes_spamware	0 B	0
-- Bloqueig spammers port 25											
15	drop	forward	6 (tcp)	25	WAN1				clientes_spamw...	0 B	0
-- Bloqueig de 14 dias a scanners de ports											
16	add	input	6 (tcp)		WAN1				port scanners	308 B	7
-- NMAP FIN Stealth scan											
17	add	input	6 (tcp)		WAN1			fin, isyn, rst, psh, ack, urg	port scanners	0 B	0
-- SYN/FIN scan											
18	add	input	6 (tcp)		WAN1			fin, syn	port scanners	0 B	0
-- SYN/RST scan											
19	add	input	6 (tcp)		WAN1			syn, rst	port scanners	0 B	0
-- FIN/PSH/URG scan											
20	add	input	6 (tcp)		WAN1			fin, isyn, rst, psh, ack, urg	port scanners	0 B	0
-- ALL/ALL scan											
21	add	input	6 (tcp)		WAN1			fin, syn, rst, psh, ack, urg	port scanners	0 B	0
-- NMAP NULL scan											
22	add	input	6 (tcp)		WAN1			!fin, isyn, rst, psh, ack, urg	port scanners	0 B	0
-- Bloqueig total a scanners de ports											
23	drop	input	6 (tcp)		WAN1			port scanners		308 B	7

Ilustración 29: Firewall de mikrotik con los paquetes bloqueados por cada regla

	Name	Address	Timeout	Creation Time
D	bloqueo_telnet	192.168.0.12	13d 23:58:17	Jun/04/2024 12:32:08
D	port scanners	192.168.0.12	13d 23:57:38	Jun/04/2024 12:32:07

Ilustración 30: Listas de bloqueo creadas por el firewall

Ahora, iremos directamente a la prueba de la lista de bloqueo winbox, para equipos que estén intentando buscar este equipo para conectarse a él desde la WAN, en concreto al puerto 8291.

Iniciaremos el the dude, y pondremos la dirección IP de el switch con el puerto del winbox para escuchar. Le daremos a connect y veremos como automáticamente se añade a la lista y se descartan los paquetes de esta IP.

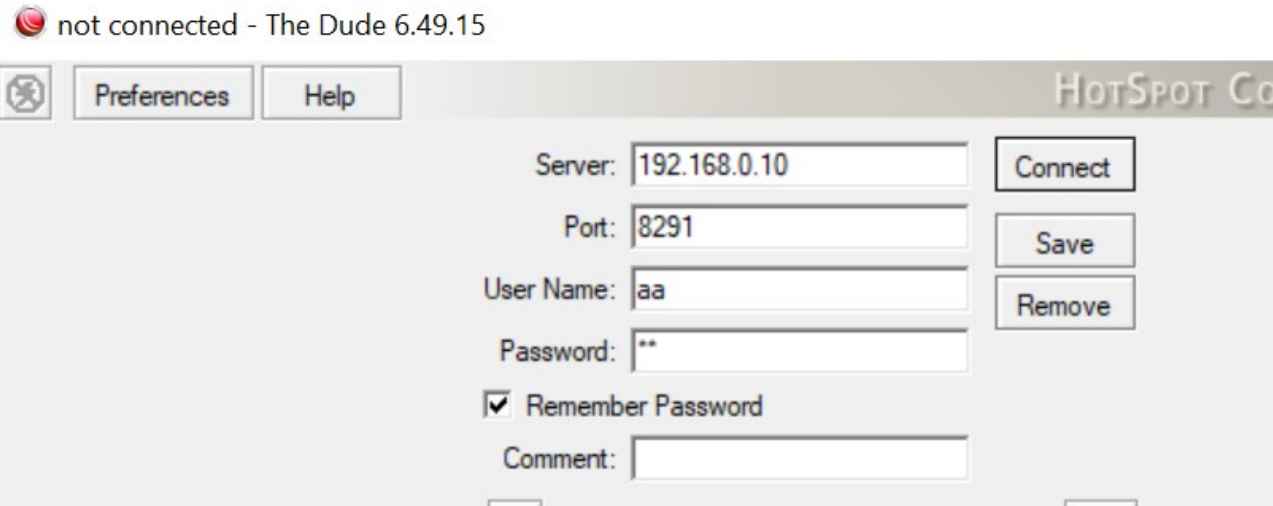


Ilustración 31: the dude, escuchar puerto 8291 winbox

Filtrar tráfico de Scanners Botnet (Scanners afectan al port 8291 en busca de equipos mikrotik)											
7	add	input	6 (tcp)	8291		WAN1				winbox-1	104 B 2
Bloqueo de 4 mins a scanners botnet											
8	add	input	6 (tcp)	8291		WAN1	winbox-1			winbox-2	104 B 2
Bloqueo de 4 mins a scanners botnet											
9	add	input	6 (tcp)	8291		WAN1	winbox-2			winbox-3	104 B 2
Bloqueo de 14 dias a scanners botnet											
10	add	input	6 (tcp)	8291		WAN1	winbox-3			winbox-4	104 B 2
11	drop	input	6 (tcp)	8291		WAN1	winbox-4			winbox-4	104 B 2

Ilustración 32: Reglas del firewall con sus respectivos paquetes bloqueados

D	winbox-1	192.168.0.12	00:03:07	Jun/04/2024 12:45:58
D	winbox-2	192.168.0.12	00:03:07	Jun/04/2024 12:45:58
D	winbox-3	192.168.0.12	00:03:07	Jun/04/2024 12:45:58
D	winbox-4	192.168.0.12	13d 23:59:07	Jun/04/2024 12:45:58

Ilustración 33: Listas de bloqueo winbox para la dirección IP atacante

Hay un video haciendo la prueba en directo del firewall. Se encuentra en [FirewallPrueba.wmv](#) es un video que se encuentra en la carpeta Pruebas de funcionalidad.

4.1.4 Prueba de monitorización del tráfico de la LAN con Torch

Haremos una prueba de monitorización del tráfico de la LAN con Torch y el tráfico de la interfaz LAN, esto nos apoyará para ver todo el tráfico que ocurre, tanto los paquetes enviados como los recibidos, de que IP origen a que IP destino, y también el consumo que tiene esta interfaz.

Lo que haremos será irnos a interfaces y ahí clicar la bridge1-LAN, que es la que conforma toda la red privada de solgata. Nos iremos a traffic y veremos solo los paquetes enviados y recibidos, no tendremos mucha mas información. Pero ahora es donde viene la monitorización con Torch para obtener los detalles deseados.

En nuestro caso desearíamos saber la IP origen y destino, además de el puerto que está siendo utilizado.

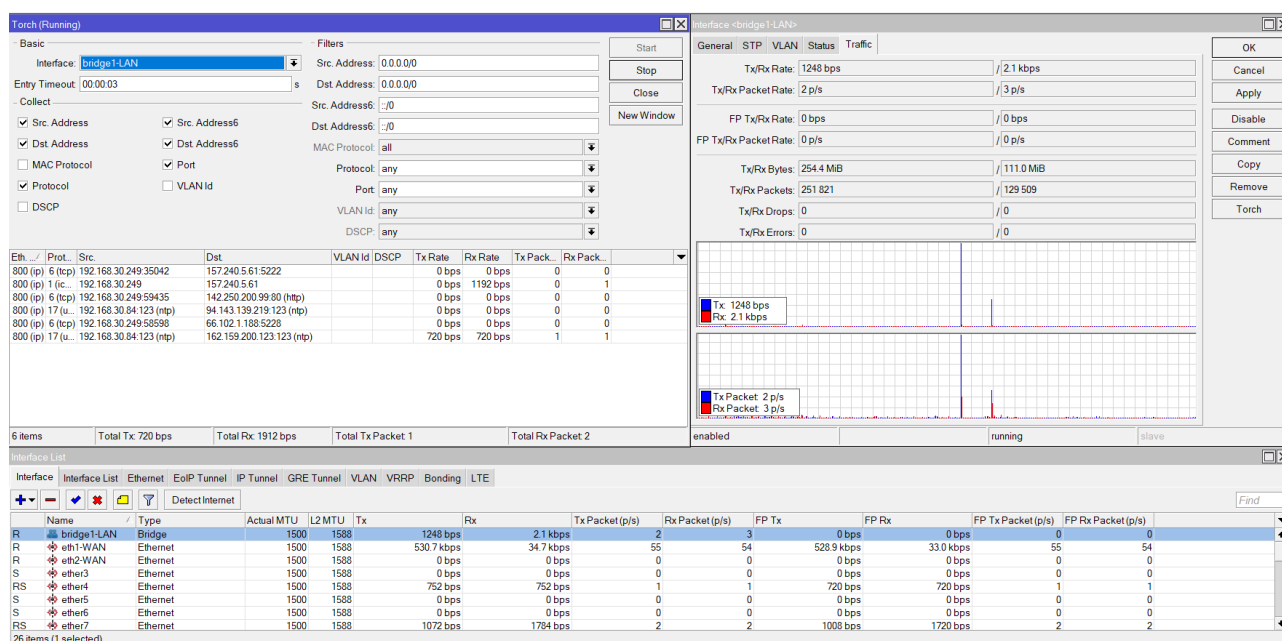


Ilustración 34: Monitorización del tráfico LAN con torch y traffic

Como vemos, tenemos la ip 192.168.30.249, que equivale al AP mikrotik con la SSID de Wi-Fi “Solgata Wi-Fi”, está haciendo peticiones a varias IP públicas que serán páginas WEB.

Luego tenemos la ip del NAS la 192.168.30.84 que está sincronizando su reloj con un servidor de tiempo mediante el puerto ntp.

Nuestra idea era monitorizar el tráfico de la red con la aplicación the dude conectada al mikrotik, pero el procesador de nuestro switch tiene arquitectura mipsbe, y por desgracia no existe el paquete de servidor dude para esta arquitectura de procesador y por lo tanto no podemos incluirlo dentro de los servicios ofrecidos por el propio mikrotik.

4.1.5 Prueba de transferencia de archivos al NAS

4.1.5.1 Prueba de transferencia de archivos al NAS mediante SMB

Para la transferencia de archivos, lo vamos a hacer de manera muy sencilla y visual, lo que haremos será irnos a la ubicación de red y buscar la dirección IP del servidor NAS que está en la 192.168.30.84 y nos pedirá autenticación.

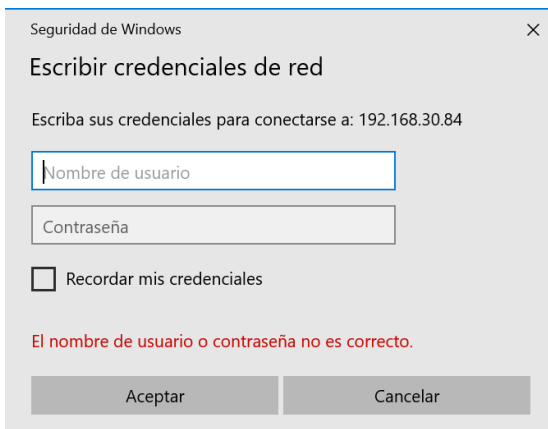


Ilustración 35: Credenciales de acceso al NAS

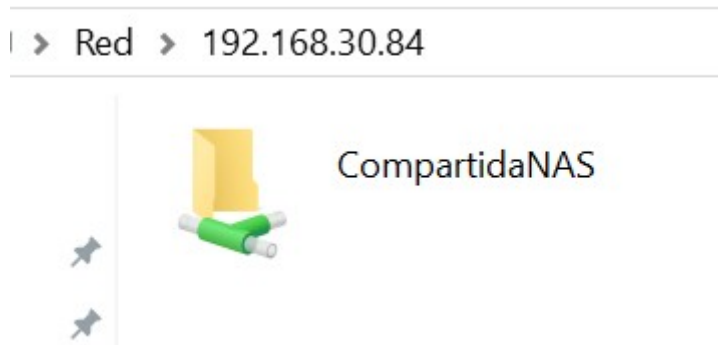


Ilustración 36: Carpeta compartida por el NAS mediante SMB

Una vez ya logueado, entraremos a la carpeta compartida por el NAS mediante SMB y probaremos la compartición de archivos arrastrando. Y veremos que se hace de manera perfecta siempre que tengas los permisos adecuados en función del usuario.

4.1.5.2 Prueba de transferencia de archivos al NAS mediante SFTP

Una de las últimas pruebas de funcionamiento es la transferencia de archivos mediante el protocolo SFTP al NAS. Estaremos utilizando el programa Filezilla para transferencia de archivos a la carpeta compartida por el SMB.

Empezaremos entrando al Filezilla y gestor de sitios, y añadiremos dos sitios para transferencia de archivos, un sitio para local y uno para cuando estemos fuera de la red privada LAN de la empresa. Utilizaremos para el local la dirección IP del NAS, la 192.168.30.84 y el puerto será el que hayamos configurado en el NAS para conexiones ssh, el puerto 48180. Y además añadiremos el usuario con el que nos loguearemos. En el caso de en remoto, pondremos la IP pública o podemos poner el dominio que tenemos asociado. También con el mismo puerto.

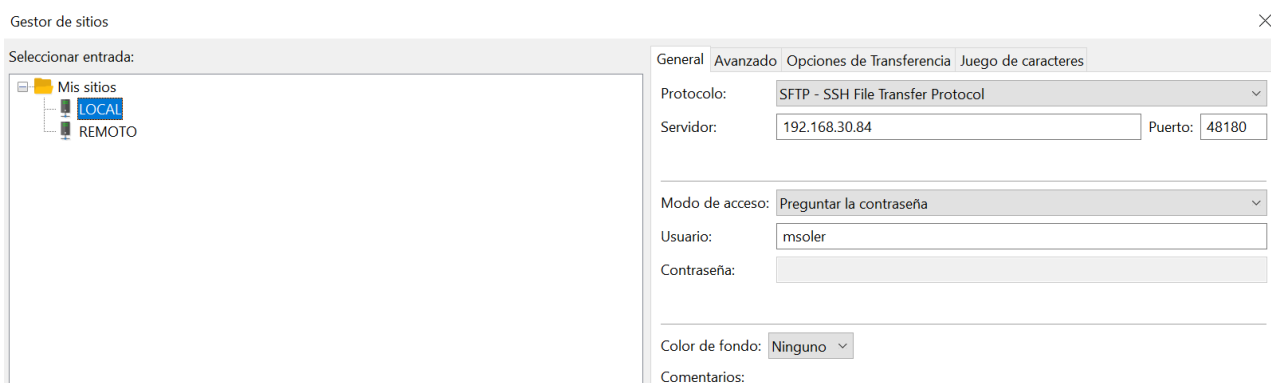


Ilustración 37: Sitio en local

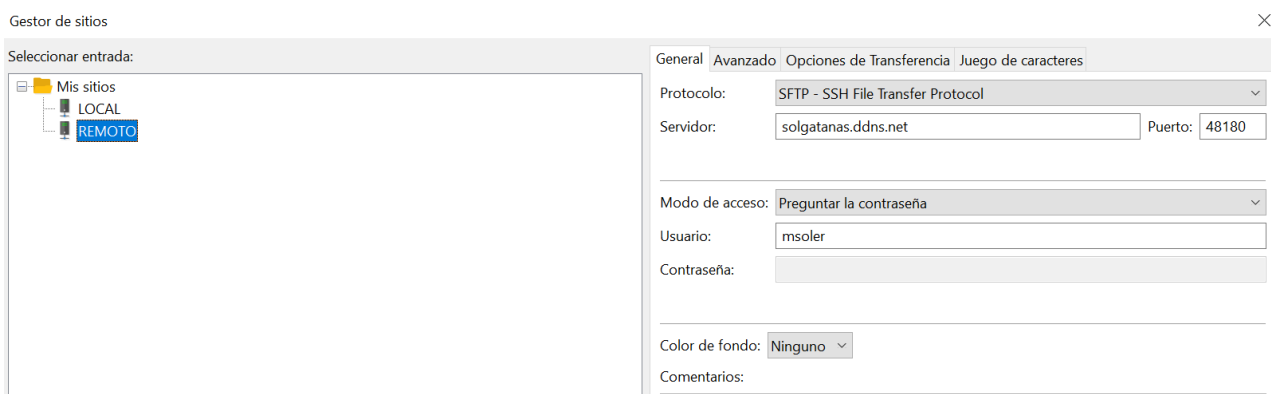


Ilustración 38: Sitio en Remoto

Como nos encontramos en local, haremos la prueba de transferencia de archivos con el sitio en Local. Ahora veremos el resultado. En la prueba trasladaremos el The Dude hasta la carpeta personal de Miguel-Pruebas.

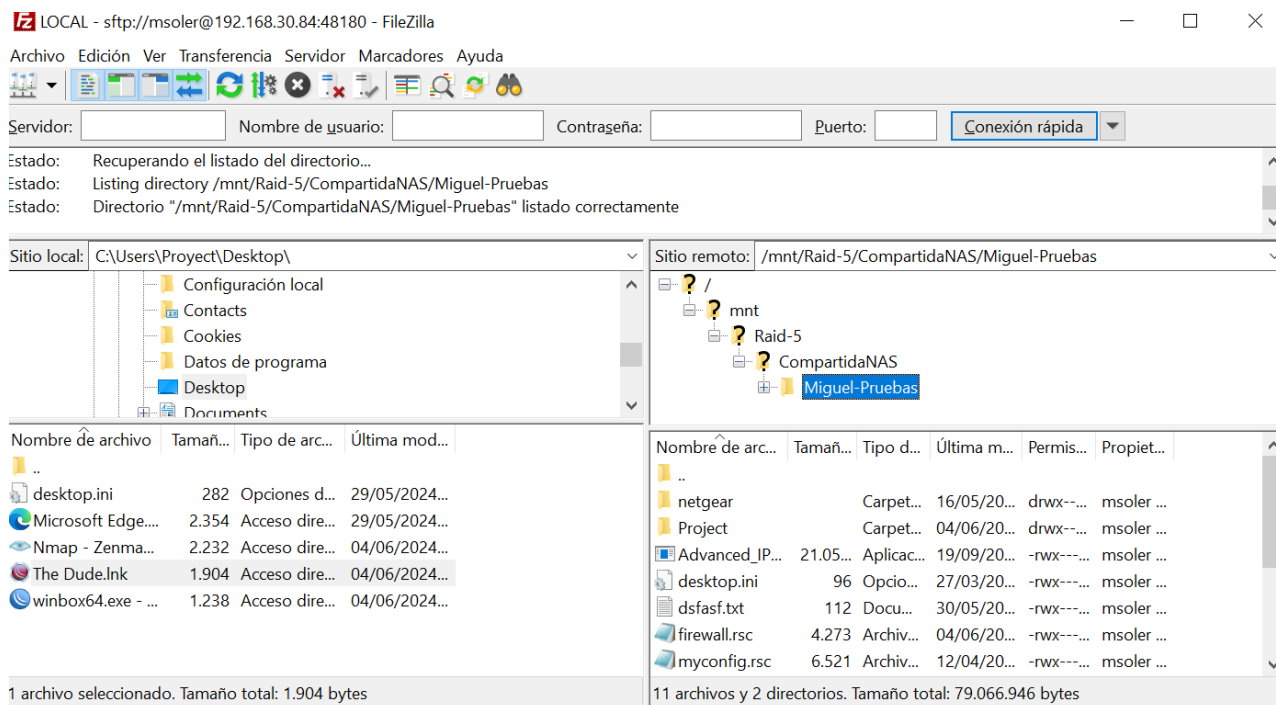


Ilustración 39: Traslado de archivos en local mediante sftp con filezilla

Le daremos botón derecho al The dude en el sitio local, y le daremos en subir. Como podremos ver se habrá subido exitosamente el archivo y si entramos a la carpeta compartida de SMB, dentro del sitio elegido, estará el archivo.

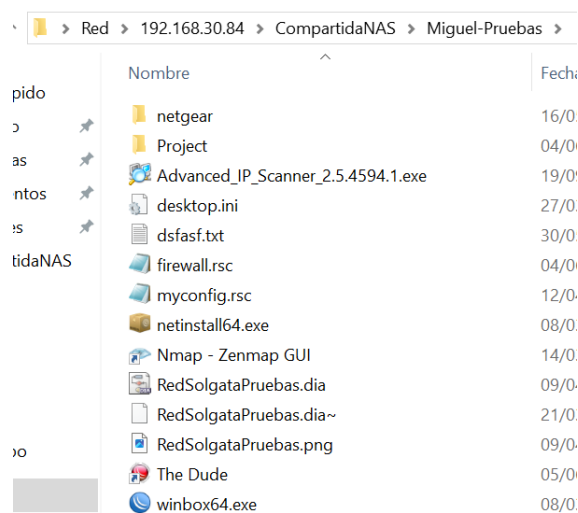


Ilustración 40: Carpeta compartida por SMB

4.1.6 Prueba de copias de seguridad de Cobian Reflector

Para las pruebas, elegiremos la tarea que hemos creado en el [AnexoCobianReflector.pdf](#) en concreto la tarea Copia de seguridad del gerente. Y para la prueba pondré una hora próxima para poder enseñar el suceso.

2024-06-06 11:20:49 El respaldo ha terminado. Hay errores. Consulte el fichero de registro de actividades.

2024-06-06 11:21:00 Comprobando la disponibilidad de actualizaciones...

2024-06-06 11:21:02 El programa está al día.

Ilustración 41: Copia terminada

Como vemos, la copia ha terminado, ahora veremos el rar en la carpeta del NAS que se transfirió vía SFTP y observaremos como pide contraseña para extraer.

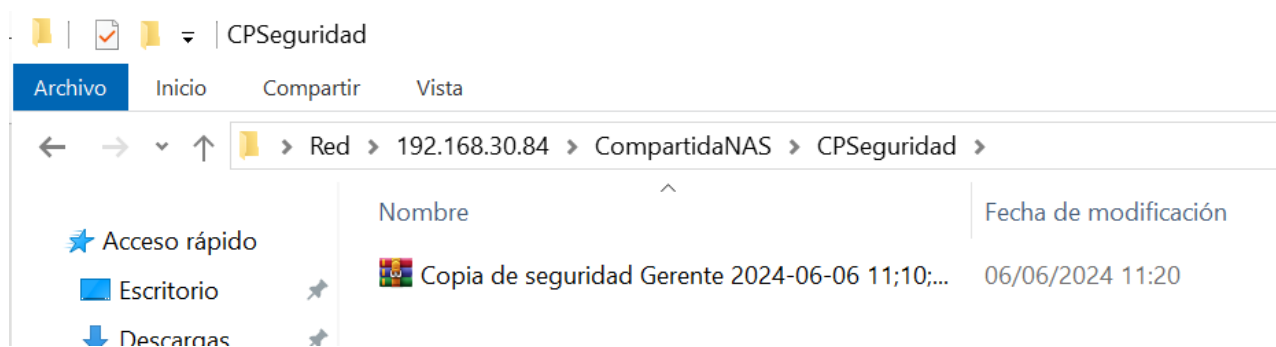


Ilustración 42: Carpeta copias de seguridad

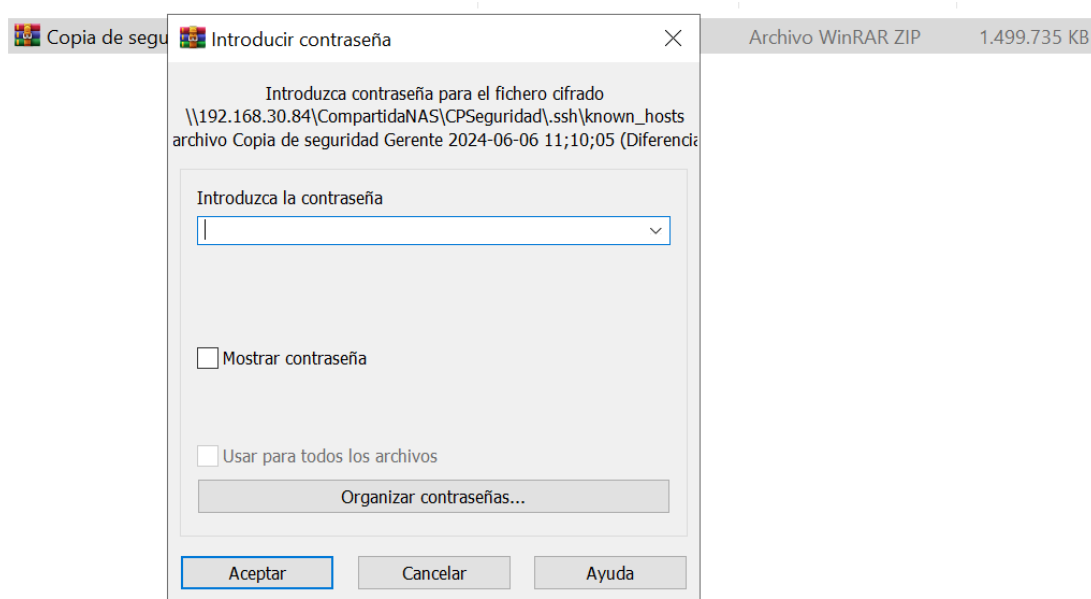


Ilustración 43: Cifrado del archivo de copia de seguridad

4.2 Jerarquía de usuarios y grupos y permisos de estos

En el proyecto, hemos trabajado con varios servicios los cuales necesitan una serie de usuarios grupos y permisos. En este aspecto hablaremos sobre los distintos usuarios y grupos que se encuentran en el NAS. Hablaremos solo del NAS, porque en este es donde se gestionan las ACL de el SSH, SFTP y SMB. Por lo tanto miraremos los permisos que se le conceden a cada usuario o grupo dentro de los servicios esmentados.

Empezaremos por los grupos, habrán 4 grupos. Estos se dividirán en : informáticos, administradores, contratación y userssolgata.

Cada usuario tendrá un usuario y contraseñas, en este caso, el grupo informáticos, tendrán acceso a todo. Los administradores solo podrán ver las carpetas de contrataciones y contratos, y las personales de cada usuario. Los de contratación serán los que pueden ver las carpetas de contrataciones y contratos. Y por último los userssolgata, que es el nivel mas bajo en la escala, todo el mundo que este contratado en la empresa será userssolgata con su respectiva carpeta personal que solo podrá ser accedida por el mismo, por un administrativo o por el informático.



Grupos		Q Filter Grupos	COLUMNAS	AÑADIR	
Grupo	GID	Builtin	Permit Sudo		
Administracion	1002	no	no		>
Contratacion	1003	no	no		>
Informaticos	1001	no	sí		>
userssolgata	1000	no	no		>

Ilustración 45: Grupos en el NAS

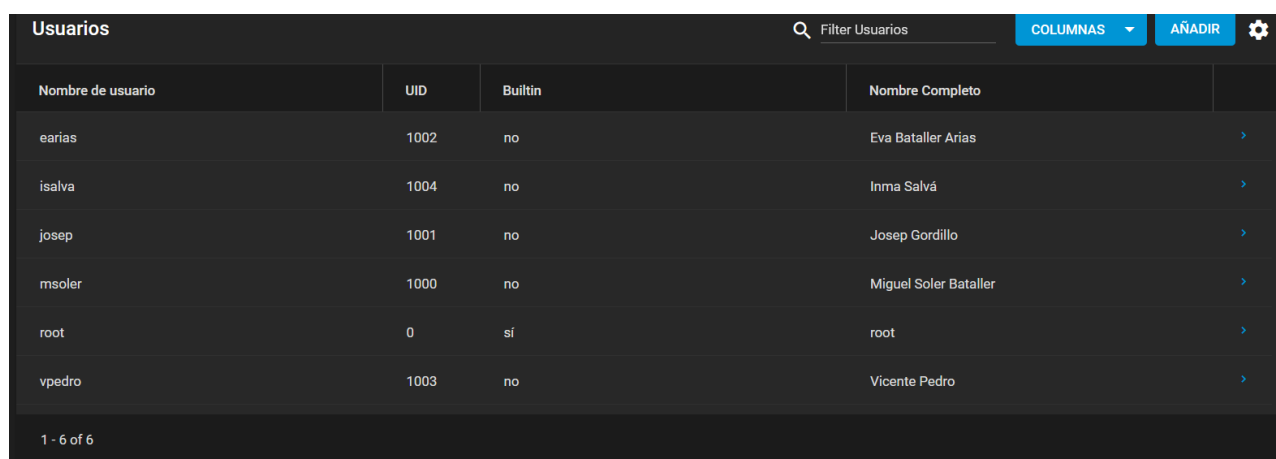
Y si vamos con los usuarios, tendremos 6 usuarios. El usuario 1 y mas importante es el root, este usuario solo se utiliza para entrar a la plataforma de configuración de truenas ya que es el único que puede entrar a esta, además este usuario no puede autenticarse en SMB por lo que tendrás que tener un usuario creado para tu persona para utilizar la carpeta compartida.

Los siguientes usuarios serán josep y msoler. Estos dos usuarios son los dos únicos informáticos, es decir tienen acceso a todo y potestad para cambiar lo que sea dentro de la carpeta compartida SMB.

Nos vamos al rango de Administración, este rango se le ha asignado al usuario earias, es la única administrativa que pertenece a este rango, tiene permisos para ver las carpetas personales de todos pero no modificarlas.

Siguiendo con la cadena ahora está el grupo de Contratación, al que pertenece el usuario isalva. Esta tiene permiso solo para ver el contenido de su carpeta personal y de la carpeta de contrataciones.

Y como último está el grupo de userssolgata, al que forman parte todos. Si solo tienes este grupo asignado como es el caso del último usuario vpedro, solo tienes acceso para ver tu carpeta personal.



The screenshot shows the 'Usuarios' (Users) management interface in Truenas. It features a table with columns for 'Nombre de usuario', 'UID', 'Builtin', and 'Nombre Completo'. There are also buttons for 'Filter Usuarios', 'COLUMNAS', 'AÑADIR', and a settings icon. The table lists six users: earias, isalva, josep, msoler, root, and vpedro, each with their respective UID, Builtin status, and full name. A pagination bar at the bottom indicates '1 - 6 of 6'.

Nombre de usuario	UID	Builtin	Nombre Completo
earias	1002	no	Eva Bataller Arias
isalva	1004	no	Inma Salvà
josep	1001	no	Josep Gordillo
msoler	1000	no	Miguel Soler Bataller
root	0	sí	root
vpedro	1003	no	Vicente Pedro

Ilustración 46: Usuarios de NAS y SMB

4.3 Control de versiones del software

Sistemas operativos:

- Windows 10
- RouterOS 6.49.15
- RouterOS 7.14.1
- TrueNAS 13.0 Stable
- Ubuntu 22.04

Programas:

- Winbox 3.40
- MikrotikNetinstall 7.14.1
- Zenmap 7.95
- TheDude 6.49.15
- AdvanceIPScanner 2.5.4594.1
- CobianReflector 2.7.10
- Filezilla 3.67.0
- DUC 4.1.1

Servicios Puerto Común/Puerto utilizado:

- NETBIOS 137/138/139
- SMB 445
- HTTP 80 – 8080
- HTTPS 443
- SSH/SFTP 22 - 48180
- ICMP 1
- TCP/UDP 6/17
- RDP 3389 - 48188
- Winbox 8291
- DNS 53
- NTP 123

5. Conclusiones

El proyecto se centra en mejorar la red de la empresa Solgata, que se encarga de la gestión de contenedores, alcantarillado e inscripciones deportivas en Gata de Gorgos. Se identificaron necesidades como brindar conexión a toda el área física con acces points, conectar todas las rosetas de los empleados, asignar IP fijas a dispositivos como impresoras, implementar un firewall, garantizar conectividad ininterrumpida con dos líneas de internet, ofrecer un espacio de almacenamiento compartido y realizar copias de seguridad. Se mencionan elementos de hardware necesarios como switches, cables Ethernet, equipos NAS, routers, patch panels, rosetas RJ45, entre otros.

Se ha priorizado brindar conectividad y seguridad a la red de Solgata.

Se implementarán medidas como la asignación de IP fijas, firewall y almacenamiento compartido.

La red contará con acces points para cobertura total y conectividad ininterrumpida.

Se realizarán copias de seguridad en el equipo del gerente para proteger la información.

Se ha considerado la viabilidad económica del proyecto para mejorar la red y el espacio compartido de la empresa.

Este proyecto ha costado mucho de hacer debido a que tenías que tener en cuentas muchas variables que podían poner en jaque toda la red. Por esto nos hemos volcado al 100% con este proyecto y lo hemos hecho con todo el esfuerzo y actitud del mundo. Siendo crítico, tendría varias mejoras a implementar como pudiese ser implementación de IDS y IPS, un analizador de tráfico potente como zabbix y incluso mejorar el NAS con discos SSD o una versión de pago de truenas. Pero con lo que tenían y el tiempo que teníamos, hemos hecho todo lo posible para la mejora de red que ellos buscaban

6. Bibliografía

- Para conocer los distintos estándares de red wifi, visité [Estándares Wifi](#)
- Para conocer un poco de la historia de Mikrotik, su página de wikipedia [Mikrotik](#)
- Para conocer los distintos estándares ethernet, visité [Estándares Ethernet](#)
- Para las características de los cables ethernet, está [Características Ethernet](#)
- Para saber el estándar que usan los cables con sus características, encontré [Cables](#)
- Características de DHCP en Windows [DHCP](#)
- Hilo de reddit donde se debate que versión de RouterOS elegir [RouterOS](#)
- Configuración de FailOver [Failover](#)
- Información de un NAS y sus características [NAS](#)
- Tipos de copias de seguridad [Copias de seguridad](#)
- Información acerca de VOIP [VOIP](#)
- Información de Spanning Tree [SPT](#)
- Tipos de topologías de red [Topologías](#)
- Como hacer un análisis DAFO [DAFO](#)
- Switch Mikrotik que se utiliza [Switch Mikrotik](#)
- Configuración de pc del NAS [Configuración PC NAS](#)
- Cables SFP Mikrotik [SFP Mikrotik](#)
- Que es el hardware [Hardware](#)
- Rutas recursivas en failover [RecursivasFailover](#)
- Configurar SFTP en el TrueNAS [SFTP en NAS](#)
- Jails en NAS para SFTP [Jail](#)
- Descargar cobian reflector [Cobian Reflector](#)
- Configuración remote desktop [RDP](#)
- Descarga paquetes mikrotik para routerOS [Paquetes Mikrotik](#)
- Descarga herramienta port scanner [NMAP](#)
- Descarga detección de IP en la red [AdvancedIPScanner](#)
- Descarga filezilla [Filezilla](#)
- NO-IP servicio DDNS [NOIP](#)
- Página de TruenasCORE [TrueNAS Core](#)