Universidad del País Vasco · Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

MÁSTER UNIVERSITARIO EN INGENIERÍA DE TELECOMUNICACIÓN

TRABAJO FIN DE MASTER

DISEÑO, DESPLIEGUE Y ANÁLISIS DEL SISTEMA SATELITAL STARLINK COMO RED DE ACCESO

Estudiante: Bilbao Aguiar, Irati

Director/Directora: Higuero Aperribay, María Victoria

Curso: 2023-2024

Fecha: Bilbao, 6 de junio, 2024

RESUMEN

La necesidad de las redes de telecomunicaciones es indudable en la sociedad actual. En nuestra vida cotidiana, estas redes se han vuelto imprescindibles tanto para el entretenimiento como para el sector industrial. La aparición de ordenadores y redes de telecomunicaciones ha provocado una gran transformación en la industria, facilitando la automatización, monitorización, implementación de robots, control y otras tecnologías avanzadas. Un ejemplo claro de esta transformación es el creciente número de dispositivos conectados a Internet y la variedad de servicios ofrecidos por los proveedores.

Por ello, se hace absolutamente necesario para las empresas actuales tener acceso a Internet. Debido a las mejoras continua de las tecnologías y, por consiguiente, las cada vez más altas velocidades y exigencias de los servicios de Internet, se ha vuelto crítico asegurar que la conectividad a Internet sea continua y confiable. Es necesario que la cobertura y la calidad de servicio de Internet que ofrecen las infraestructuras de Telecomunicaciones sean más ambiciosas, llegando además a los lugares más remotos.

En los últimos años, el acceso a Internet se ha vuelto más accesible gracias a la mejora y mayor asequibilidad de tecnologías como las redes de banda ancha y los dispositivos móviles. Sin embargo, en ciertas áreas rurales y lugares muy remotos la conectividad sigue siendo nula o muy limitada. Esto se debe a que la instalación de líneas de fibra óptica o infraestructuras 4G o 5G en estas zonas es muy costosa y los proveedores no pueden asumir ese gasto.

En este contexto, las comunicaciones vía satélite se han presentado como una solución debido a su amplia cobertura. Sin embargo, los costos asociados con las infraestructuras de estos sistemas han impedido que se conviertan en una solución práctica hasta ahora. Además, las comunicaciones satelitales presentan retrasos y pérdidas significativamente mayores en comparación con los sistemas por cable, lo que imposibilita la provisión de varios servicios en Internet.

Ante este problema, Starlink ofrece una solución innovadora y eficaz. De hecho, el objetivo de esta empresa es crear una constelación de satélites de baja órbita para ofrecer un servicio de conexión a Internet de banda ancha y baja latencia en todo el globo terrestre. Los satélites de baja órbita permiten transmitir señales de mayor potencia, lo que permite obtener mayores velocidades y menores latencias en comparación con otros sistemas satelitales desplegados hasta la fecha.

Este Trabajo de Fin de Máster (TFM) propone la adopción del sistema Starlink por parte de un proveedor de servicios de Internet (ISP), aprovechando sus ventajas, como una solución viable para ofrecer conectividad a Internet a sus clientes en zonas de difícil acceso.

Palabras clave: sistemas de comunicación por satélite, Starlink*, Low Earth Orbit* (LEO), cifrado, autenticación, claves criptográficas, *High Availability* (HA), *Border Gateway protocol* (BGP)

LABURPENA

Telekomunikazio sareen beharra gaur egungo gizartean ukaezina da. Izan ere, gure egunerokotasunean ezinbestekoa bihurtu da, bai aisialdirako zein industriarako. Ordenagailuen eta telekomunikazio sareen agerraldiek eraldaketa handia suposatu dute industrian: automatizazioa, monitorizazioa, robotak, kontrola eta beste hainbat teknologien agerpenei ateak ireki baitzituen. Horren adibide garbia da Internetera konektatutako gailuen eta hornitzaileek eskaintzen dituzten zerbitzuen kopurua.

Hori dela eta, gaur egungo enpresentzako behar-beharrezkoa egiten da Interneterako sarbidea izatea. Gainera, teknologien etengabeko hobekuntzen ondorioz, Interneteko zerbitzuen abiadura eta eskakizunak gero eta handiagoak dira eta, beraz, Interneterako konektibitatea etengabea eta fidagarria izatea ziurtatzea kritikoa bihurtu da. Horregatik, beharrezkoa da telekomunikazio-azpiegiturek eskaintzen duten Interneteko zerbitzuen estaldura eta kalitatea zorrotzagoak izatea, urruneko lekuetara iritsiz.

Azken urteotan, Interneterako sarbidea eskuragarriagoa bihurtu da, banda zabaleko sareak eta gailu mugikorrak bezalako teknologien hobekuntza eta eskuragarritasun handiagoari esker. Hala ere, landa-eremu eta leku oso urrun batzuetan, konektibitatea nulua edo oso mugatua da oraindik. Izan ere, zona horietan zuntz optikoko lineak edo 4G/5G azpiegiturak instalatzea oso garestia da, eta hornitzaileek ezin dute gastu horiekin pairatu.

Arlo horretan, haien kobertura zabalagatik, satelite bidezko komunikazioak irtenbide bezala aurkeztu dira, baina, sistema hauen azpiegiturek suposatzen dituzten kostuengatik ez da soluzio erreala izan orain arte. Gainera, satelite bidezko komunikazioak kable bidezko sistemak baino atzerapen eta galera askoz handiagoak dituzte, Interneteko hainbat zerbitzuen eskaintza ezinezkoa bihurtuz.

Arazo honen aurrean Starlink enpresak soluzio berritzaile eta eraginkor bat eskaintzen du. Izan ere, enpresa honen helburua orbita baxuko sateliteen konstelazio bat sortzea da, Internetera konektatzeko zerbitzu bat eskaintzeko, banda zabalekoa eta latentzia baxukoa lurreko globo osoan. Orbita baxuko sateliteek potentzia handiagoko seinaleak transmititzea ahalbidetzen dute eta, horri esker, abiadura handiagoak eta latentzia txikiagoak lortzen dira orain arteko beste sateliteen bidezko sistemekin konparatuta.

Master Amaierako Lan (MAL) honetan, Starlink sistemak eskaintzen dituen abantailez baliatuz, Interneteko zerbitzuen hornitzaile (ISP) batek Interneterako konektibitatea eskaintzeko soluzio bezala inplementatzea proposatzen da, satelite bidezko komunikazioa sarbide sarea izanik.

Hitz gakoak: satelite bidezko komunikazio sistemak, Starlink*, Low Earth Orbit* (LEO), zifratzea, autentikazioa, gako kriptografikoak, *High Availability* (HA), *Border Gateway protocol* (BGP)

ABSTRACT

The need for telecommunications networks is undeniable in today's society. In our daily lives, these networks have become indispensable for both entertainment and the industrial sector. The appearance of computers and telecommunications networks has led to a significant transformation in the industry, facilitating automation, monitoring, the implementation of robots, control, and other advanced technologies. A clear example of this transformation is the growing number of devices connected to the Internet and the variety of services offered by providers.

Therefore, it is absolutely necessary for modern businesses to have access to the Internet. Due to the continuous improvements in technology and the consequently higher speeds and demands of Internet services, it has become critical to ensure that Internet connectivity is continuous and reliable. The coverage and quality of Internet service offered by telecommunications infrastructures need to be more ambitious, reaching even the most remote areas.

In recent years, Internet access has become more accessible thanks to the improvement and greater affordability of technologies such as broadband networks and mobile devices. However, in certain rural areas and very remote locations, connectivity remains non-existent or very limited. This is because installing fibre optic lines or 4G/5G infrastructures in these areas is very costly, and providers cannot assume that expense.

In this context, satellite communications have emerged as a solution due to their extensive coverage. However, the costs associated with the infrastructures of these systems have prevented them from becoming a practical solution until now. Additionally, satellite communications have significantly higher delays and losses compared to cable systems, making it impossible to provide several Internet services.

Faced with this problem, Starlink offers an innovative and effective solution. In fact, the company's goal is to create a constellation of Low-Earth orbit satellites to provide a broadband, low-latency Internet connection service across the globe. Low-Earth orbit satellites can transmit stronger signals, resulting in higher speeds and lower latencies compared to other satellite systems deployed to date.

This Master's Thesis (TFM) proposes the adoption of the Starlink system by an Internet service provider (ISP), leveraging its advantages as a viable solution to offer Internet connectivity to customers in hard-to-reach areas.

Keywords: satellite communication systems, Starlink*, Low Earth Orbit* (LEO), encryption, authentication, cryptographic keys, *High Availability* (HA), *Border Gateway protocol* (BGP)

Tabla de contenido

Índice de imágenes

Índice de tablas

1 INTRODUCCIÓN

Actualmente, las redes de telecomunicaciones resultan imprescindibles tanto en el ámbito profesional como social. Claro ejemplo de ello es el creciente número de dispositivos conectados a Internet y de los servicios ofrecidos por los proveedores.

El sector de las telecomunicaciones tiene, por ello, una constante demanda de innovación y mejora continua de las tecnologías, dónde las tecnologías obsoletas son rápidamente reemplazadas por nuevas soluciones que permiten abordar nuevas y más exigentes demandas. Es así que, las redes de telecomunicaciones han evolucionado desde las conexiones por cable a tecnologías de fibra óptica hasta el 5G. Cada generación de tecnología de red ofrece mayores velocidades, menor latencia y mayor capacidad, permitiendo nuevos usos como el Internet de las Cosas (IoT) o servicios de live streaming.

Además, con el crecimiento en los últimos años del teletrabajo y la educación a distancia, se ha vuelto crítico asegurar que la conectividad sea continua y confiable. Por consiguiente, es necesario que la cobertura y la calidad de servicio que ofrecen las infraestructuras de conexión a Internet sean más ambiciosas, llegando además a los lugares más remotos.

En los últimos años, el acceso a Internet se ha vuelto más accesible, gracias a la mejora y la mayor asequibilidad de la tecnología, como las redes de banda ancha y los dispositivos móviles. Aun así, todavía sigue existiendo la llamada “brecha digital”, donde la conectividad en ciertas áreas rurales y lugares muy remotos la accesibilidad a Internet es nula o muy escasa. Esto se debe a que la instalación de líneas de fibra óptica o de infraestructura de 4G o 5G en estos lugares es muy costoso y los proveedores no pueden lidiar con ello.

Ante este problema, la solución más recurrida han sido los sistemas de comunicación por satélite. Desde los inicios, estos sistemas se han presentado como alternativa a los cables utilizados para telefonía y, ahora, para acceso a Internet. Existen 3 principales órbitas terrestres: GEO (*Geo-synchronous Earth Orbit*), MEO (*Medium Earth Orbit*), LEO (*Low Earth Orbit*). Cada una de ellas tiene sus características propias y son más adecuadas para ciertas aplicaciones. Por ejemplo, en la órbita MEO se encuentran los satélites necesarios para el sistema de geolocalización GPS, puesto que en esta órbita tan solo se necesitan de siete a diez satélites para cubrir la mayor parte del globo. No obstante, la latencia que se obtiene en la transmisión de datos en esta órbita es alta, haciendo incluso imposible ofrecer servicios como video streaming. En cambio, la latencia en la órbita LEO mejora considerablemente, puesto que, al encontrarse los satélites más cerca de la capa terrestre el recorrido que deben hacer las señales es menor. Sin embargo, se necesitan más satélites para poder cubrir el globo y ofrecer una cobertura amplia y, además, los satélites LEO tienen una vida útil notablemente menor. En resumen, si se quiere ofrecer un servicio de gran velocidad y baja latencia se debe hacer frente al gran coste de mantener satélites en una órbita baja entre otras desventajas.

Starlink ha apostado por ofrecer una cobertura global a Internet afrontando las dificultades que supone y ofreciendo soluciones novedosas. Starlink es una empresa filial de SpaceX cuyo objetivo

es el de crear una constelación de satélites para ofrecer un servicio de conectividad a Internet, de banda ancha y baja latencia en todo el globo terrestre. Los satélites Starlink se encuentran en órbitas mucho más bajas que los satélites de los sistemas de comunicación tradicionales, concretamente, en la mencionada órbita LEO. Junto con la red satelital, antenas terminales mejoradas y una infraestructura terrestre óptima, Starlink ofrece a sus clientes todo tipo de servicios con una cobertura mucho mayor hasta lo ahora conocido.

Starlink ofrece su servicio para diversas aplicaciones, desde proveer conectividad a Internet en domicilios, hasta conectar empresas, flotas de barco o de aviones o, incluso, para servicios de emergencia.

Está claro que todo esto supone un gran cambio con respecto a las tecnologías desplegadas hasta ahora. Es por ello que este Trabajo de Fin de Máster se basa en diseñar, implementar y analizar el servicio Starlink como red de acceso entre un cliente final y un proveedor de servicios de Internet (ISP).

Para llevar a cabo este proyecto, primero, se ha procedido con el diseño general del sistema que se pretende implementar. Posteriormente, se han analizado, diseñado e implementado cada componente del mismo. Finalmente, se ha realizado un análisis del rendimiento del sistema en diferentes situaciones y una breve evaluación sobre sus limitaciones.

Todo ello se hará desde el punto de vista del proveedor de servicios de Internet y se explicará cómo se podría implantar Starlink entre sus servicios ofrecidos a sus clientes. Debido a esto, en este proyecto se han tenido en cuenta desde el principio algunos aspectos esenciales para cualquier proveedor, como lo es la seguridad.

Es evidente que la seguridad es un aspecto que se encuentra en auge en los últimos años. A medida que más usuarios se conectan a Internet, las infraestructuras de telecomunicaciones se vuelven más vulnerables. Esta vulnerabilidad puede llegar a plantear riesgos significativos para la privacidad individual y la seguridad de datos. Por ello es importante proteger la infraestructura crítica y los datos sensibles. En este trabajo se han analizado también, teniendo en cuenta las necesidades del ISP, dos diferentes tecnologías de VPN para, después, implementarlas sobre Starlink.

Este TFM ha sido desarrollado en la empresa Sarenet, un Proveedor de Servicios de Internet para empresas ubicada en el parque tecnológico de Zamudio, Bizkaia. El objetivo de Sarenet es proveer a otras empresas de conectividad a Internet, ofreciendo servicios de datos y voz. Sarenet es un Proveedor de Servicios de Internet (ISP) opera su propia red mediante un Sistema Autónomo (AS).

2 CONTEXTO TECNOLÓGICO

En este apartado se explica el contexto tecnológico del proyecto, resaltando los aspectos más importantes de las tecnologías relacionadas con este TFM. Puesto que el proyecto trata de la implementación y análisis del servicio satelital Starlink, primero se explican los rasgos generales de cualquier sistema de comunicación por satélite. Después, se detalla el sistema satelital Starlink y sus componentes. Por último, como se podrá ver después, en este TFM se implementan protocolos de VPN por lo que en este apartado también se mencionan los aspectos generales de los protocolos de redes virtuales (VPN), ya que, constituye un aspecto importante en relación al rendimiento del sistema a desarrollar al añadir estas tecnologías.

2.1 Sistemas de comunicación por satélite

La comunicación por satélite es aquella que tiene lugar entre dos estaciones terrestres pasando a través de un satélite. En este tipo de comunicaciones se utilizan ondas electromagnéticas como señales portadoras para transmitir los mensajes desde el emisor hasta el receptor.

Un satélite es todo cuerpo, artificial o natural, que gira alrededor de otro mayor, atrapado por su atracción gravitatoria y siguiendo una trayectoria determinada. Esta trayectoria es denominada órbita. Un satélite de comunicaciones no es más que un satélite artificial que orbita alrededor de la Tierra y que se comporta como una estación repetidora de microondas en el espacio. Más concretamente, amplifica y cambia la banda de frecuencia de la señal transmitida con respecto a la recibida, con lo que se puede decir que se comporta como un transpondedor [1].

Los principales componentes de un satélite son: el sistema de comunicaciones, que incluye las antenas y transpondedores que reciben y retransmiten las señales, el sistema de energía, que incluye los paneles solares que proporcionan energía, y el sistema de propulsión, que incluye los cohetes que impulsan el satélite. Un satélite necesita su propio sistema de propulsión para situarse en la posición orbital correcta y así poder corregir su trayectoria [2].

La vida útil de un satélite viene determinada por la cantidad de combustible que tiene para alimentar estos propulsores. Una vez que se agota el combustible, el satélite se desplaza hacia el espacio y deja de funcionar, convirtiéndose en basura espacial.

Además del combustible para los propulsores, cualquier satélite necesita energía interna para hacer funcionar sus sistemas electrónicos. La fuente principal de energía de estos satélites es la luz solar, que es obtenida mediante paneles solares integrados en el propio satélite. Cuando el satélite se encuentra en el lado opuesto al Sol no recibe rayos de este, por lo que también necesita baterías para suministrar energía cuando el Sol está tapado por la Tierra. Las baterías se recargan con el exceso de corriente generada por los paneles solares cuando reciben luz solar [2].

El proceso de comunicación por satélite comienza en una estación terrestre. Esta estación deberá estar diseñada para transmitir y recibir señales de un satélite en órbita alrededor de la Tierra. Las estaciones terrestres envían la información a los satélites en forma de señales en una determinada

frecuencia, normalmente de escala de GHz. Los satélites reciben y retransmiten las señales de vuelta a la Tierra, donde son recibidas por otras estaciones terrestres en la zona de cobertura del satélite [1]. A la zona de cobertura del satélite se le denomina footprint [2].

La frecuencia con la que se envían al espacio las señales se denomina frecuencia de enlace ascendente o Uplink frequency. Del mismo modo, la frecuencia con la que el transpondedor envía la señal tanto a la estación terrestre como a la antena terminal, se denomina frecuencia de enlace descendente o Downlink frequency. Es decir, la frecuencia de enlace ascendente es la frecuencia con la que el emisor terrestre se comunica con el satélite. El transpondedor del satélite convierte esta señal en otra frecuencia (frecuencia de enlace descendente) y la envía a una segunda estación terrestre [1].

Los servicios por satélite pueden darse en una sola dirección o bidireccional. Esto es, en el caso de una sola dirección la información es transmitida desde una estación terrestre a una o más estaciones terrestres a través de satélites. Sin embargo, en los sistemas bidireccionales la información puede intercambiarse entre dos estaciones terrenas cualesquiera a través de un satélite.

Los sistemas de una sola dirección proporcionan tanto conectividad punto a punto como conectividad punto a multipunto mientras que los sistemas bidireccionales sólo proporcionan conectividad punto a punto [2].

2.1.1 Órbitas terrestres

Como se ha mencionado anteriormente, la trayectoria que sigue un satélite alrededor de la Tierra se llama órbita. Por la altura respecto a la superficie de la Tierra y por las diferentes características de cada una de ellas, se definen 3 tipos de órbitas terrestres: *Geo-synchronous Earth Orbit* (GEO), *Medium Earth Orbit* (MEO), *Low Earth Orbit* (LEO) [1].

GEO

La órbita geosíncrona o GEO es aquella que se sitúa a 35.786 km de la superficie terrestre. Esta altitud permite que los satélites cubran grandes porciones de la Tierra y, de hecho, sólo tres satélites podrían cubrir la mayor parte del globo. Este tipo de órbita tiene la particularidad de que su periodo de traslación es igual al periodo de rotación de la Tierra, esto es, el satélite tarda 24 horas en dar una vuelta a la Tierra. Si la órbita que describe el satélite es circular se denomina órbita Geoestacionaria. A los satélites presentes en estas órbitas se les considera estacionarios ya que tienen la misma velocidad angular que la Tierra por lo que están sincronizados con la rotación terrestre. La principal ventaja de la órbita geoestacionaria es que no es necesario rastrear las antenas para encontrar la posición de los satélites, puesto que cubren una posición fija en el suelo. Toda órbita geoestacionaria es una órbita geosíncrona, pero lo contrario no siempre se cumple [2].

MEO

Los satélites MEO orbitan a distancias de entre 5.000 y 12.000 km de la superficie terrestre. Esta distancia es suficiente para que una constelación de siete a diez satélites pueda cubrir la mayor parte del globo. Las señales que se envían en este caso recorren una distancia más corta que en el caso de los satélites GEO. Gracias a ello, la intensidad de la señal mejora respecto a los satélites de tipo GEO y esto permite utilizar terminales receptores más pequeños y ligeros. La aplicación más conocida de esta órbita son los sistemas de navegación global como el GPS [3].

LEO

Por último, en la órbita terrestre baja (LEO), los satélites suelen ser más pequeños y menos complejos que los más grandes de las órbitas superiores. Estos orbitan a una distancia de entre unos 500 y 2.000 km sobre la superficie terrestre, y con un periodo de traslación de unos 90 minutos. Llevar los satélites a esta órbita es más sencillo que alcanzar las más altas y, a menudo, un solo lanzamiento de cohete transporta varios LEO. Estos satélites tienen un campo de visión más pequeño que los satélites de los tipos anteriormente descritos, por lo que se necesitan más satélites para poder cubrir el globo. La gran ventaja de estos satélites es que permiten transmitir señales más potentes y a mayor velocidad con una baja latencia. Sin embargo, esto tiene un coste: los satélites LEO tienen una vida útil de aproximadamente cinco a siete años, en comparación con los satélites GEO, que pueden durar más de 15 años en órbita [2].

Los satélites de órbita baja se clasifican en tres categorías: LEO pequeños, LEO grandes y los Mega-LEO. Los LEO pequeños operan en la banda de 800 MHz (0,8 GHz), los LEO grandes en la gama de 2 GHz o más, y los Mega-LEO en la de 20-30 GHz [2].

2.1.2 Bandas de frecuencias

En los sistemas de comunicación satelitales, como en muchos otros, se utilizan ondas electromagnéticas como señales portadoras para transmitir los mensajes. Las ondas electromagnéticas cubren una amplia gama de frecuencias o de longitudes de ondas y pueden clasificarse según su principal fuente de producción dentro de en un espectro electromagnético. Las frecuencias utilizadas para las comunicaciones satelitales se encuentran, concretamente, entre 1 GHz y 40 GHz. Dentro de este intervalo se definen diferentes bandas de frecuencia: L, S, C, X, Ku, K, Ka y V.

Las señales de la gama baja (bandas L, S y C) del espectro de frecuencias de los satélites se transmiten con poca potencia, por lo que se necesitan antenas más grandes para recibirlas. Las señales de la gama alta (bandas X, Ku, Ka y V) tienen más potencia, por lo que pueden recibirse con antenas más pequeñas que en el caso de las señales de gama baja. En el caso la recepción de las señales de gama alta las antenas son de unos 45 cm de diámetro [4].

A continuación, se describen de forma breve las características más relevantes de cada una de estas bandas de frecuencia:

Banda L

Las frecuencias de banda L operan en el rango de 1-2 GHz del espectro electromagnético y se utilizan para radares y servicios GPS. Con un ancho de banda reducido y un rango de frecuencias bajo, la banda L no es adecuada para aplicaciones de streaming como vídeo, voz y conectividad de banda ancha de alta velocidad, pero es perfecta para aplicaciones como gestión de flotas, seguimiento de activos, Internet de las Cosas (IoT) y servicios de seguridad marítima y aeronáutica.

Banda S

Las frecuencias de la banda S operan entre 2 y 4 GHz y se utilizan para la comunicación por satélite y el radar. La banda S tiene una importancia clave para las industrias naval, aeronáutica y espacial. Se utiliza mayormente para radares meteorológicos, radares de buques de superficie y algunos satélites de comunicaciones.

Banda C

La banda C opera en el rango de 4-8 GHz del espectro electromagnético. Con antenas de entre 1,8 y 2,4 metros de largo, los satélites de banda C transmiten una señal directa de extremo a extremo, que se utiliza principalmente para comunicaciones por satélite, redes de televisión por satélite y transmisiones en bruto por satélite, útiles en zonas de difícil acceso afectadas por lluvias torrenciales o condiciones climáticas extremas.

Bandas Ku y Ka

La banda Ku suele definirse entre 12 GHz y 18 GHz y la banda Ka se encuentra entre 27 y 40 GHz. Ambas se utilizan principalmente para ofrecer conectividad a Internet por satélite, que requiere gran volumen de transferencias de datos.

Estas frecuencias de mayor potencia admiten aplicaciones que necesitan un mayor ancho de banda, como videoconferencias, retransmisiones en directo, Internet de alta velocidad para servicios como Wi-Fi a bordo de aviones y aplicaciones multimedia. Esta frecuencia también facilita la oferta de Internet por satélite en regiones residenciales y remotas del planeta [4].

2.1.3 Tipos de servicios satelitales

Los servicios comerciales de comunicaciones por satélite se agrupan en tres categorías [5]:

- Servicios Fijos por Satélite (*Fixed Satellite Services*-FSS): utiliza equipos terrestres en ubicaciones fijas para recibir y transmitir señales de satélite.
- Servicios Móviles por Satélite (*Mobile Satellite Services*-MSS): utiliza diversos equipos transportables de recepción y transmisión para prestar servicios de comunicación a clientes œtelefonía móvil terrestre, marítima y aeronáutica.
- Servicios de Radiodifusión por Satélite (*Broadcast Satellite Services*-BSS): ofrece una alta potencia de transmisión permitiendo así utilizar equipos terrestres muy pequeños para la recepción.

2.1.4 Ventajas y desventajas de los sistemas de comunicaciones satelitates

Teniendo en cuenta las características de los sistemas satelitales descritos anteriormente, se pueden concluir ciertas ventajas y desventajas de estos sistemas frente a los sistemas terrestres.

La ventaja más clara es el amplio alcance que ofrecen estos sistemas. El área de cobertura es mayor que la de los sistemas terrestres, llegando a zonas inaccesibles y de difícil acceso. Esto la convierte en una solución perfecta para la comunicación en regiones en las que los sistemas de comunicaciones terrestres no son viables o su instalación no es rentable. Dependiendo de la órbita en la que operen los satélites, es posible cubrir la mayoría de la superficie terrestre con una determinada cantidad de satélites, y en distancias largas puede ser más barato que desplegar todo un sistema terrestre.

Además, se puede decir que ofrecen facilidades en cuanto a movilidad y adaptabilidad. Las aplicaciones de comunicación inalámbrica y móvil pueden establecerse fácilmente mediante comunicación por satélite independientemente de la ubicación y pueden impulsarse satélites adicionales para ampliar su capacidad y alcance. Esto permite una comunicación adaptable y rentable que puede ajustarse a las necesidades cambiantes.

Por último, los servicios por satélite no se ven influidos por las condiciones climáticas ni las catástrofes naturales. Esto la convierte en una opción predominante para las aplicaciones básicas como los servicios de emergencia.

Respecto a las desventajas, uno de los principales inconvenientes técnicos de los satélites, sobre todo de los situados en órbita geoestacionaria, es el retraso inherente a la transmisión de datos. El retardo de propagación de los sistemas por satélite es mayor que el de los sistemas terrestres convencionales, puesto que la distancia que deben recorrer las señales transmitidas es mayor. Esto puede hacer que la comunicación en tiempo real sea problemática, ya que puede haber un retraso excesivo en la transmisión de información de voz o vídeo. Aun así, como se va a explicar más adelante, en algunos escenarios se pueden desarrollar soluciones que consiguen reducir significativamente el retardo en la transmisión de los datos.

Por otro lado, el lanzamiento y la puesta en órbita de satélites es un proceso costoso. Esto lo hace menos accesible para las pequeñas empresas. Además, en caso de alguna avería en un sistema de satélites es difícil ofrecer actividades de reparación; el mantenimiento de los satélites es complejo y costoso. Por tanto, el desarrollo, la inversión y el mantenimiento de los satélites requieren un coste más elevado que cualquier otro sistema de comunicación terrestre [6].

2.1.5 Aplicaciones

Una vez explicadas las ventajas y desventajas de los sistemas de comunicación satelitales, existen ciertas aplicaciones claras en las que este tipo de comunicaciones son especialmente adecuadas. En la siguiente lista se mencionan las aplicaciones más comunes de los sistemas de comunicación satelital:

- Predicción meteorológica: los satélites meteorológicos monitorizan continuamente el clima y las condiciones meteorológicas.
- Navegación: una de las aplicaciones más comunes es para determinar la ubicación geográfica de aviones, barcos, coches, trenes o cualquier otro objeto. El GPS (Sistema de Posicionamiento Global) es un ejemplo de sistema de navegación.
- Astronomía: los satélites se pueden utilizar también para estudiar u observar las estrellas, galaxias, planetas, etc. Se utilizan principalmente para encontrar nuevas estrellas, galaxias y planetas. El telescopio espacial Hubble es un ejemplo de satélite astronómico. Capta imágenes de alta resolución de estrellas lejanas, galaxias, planetas, etc.
- Telefonía satelital: la telefonía satelital es un tipo de telefonía móvil que utiliza satélites en lugar de torres de telefonía móvil para transmitir la señal o la información a larga distancia. Generalmente, este tipo de telefonía se usa para ofrecer conectividad a flotas de barco o en situaciones de desastres naturales. Los teléfonos por satélite utilizan satélites geoestacionarios y satélites de órbita terrestre baja (LEO) para transmitir la información.
- Televisión satelital: La televisión por satélite es un sistema inalámbrico que utiliza satélites de comunicaciones para hacer llegar señales de televisión a los usuarios o telespectadores.
- Satélites militares: Los satélites militares son utilizados por las fuerzas armadas para comunicarse entre sí. Estos satélites también se utilizan para determinar la ubicación exacta de un objeto.
- Internet satelital: Internet por satélite es un sistema inalámbrico que utiliza satélites para hacer llegar las señales de Internet a los usuarios. Internet por satélite no utiliza sistemas de cable, sino satélites para transmitir la información o la señal.
- Radiodifusión por satélite: La radio por satélite es un servicio de transmisión inalámbrica que utiliza satélites en órbita para hacer llegar la información o las señales de radio a los consumidores.
- Comunicación en situaciones de desastres naturales: la tecnología de comunicaciones por satélite se utiliza a menudo en catástrofes naturales y emergencias, cuando los servicios de comunicación terrestres no funcionan. Los equipos móviles por satélite pueden desplegarse de forma rápida y efectiva en las zonas siniestradas para prestar servicios de comunicaciones de emergencia.
- Conexiones para zonas remotas o en desarrollo: Debido a su situación geográfica, muchos lugares del mundo carecen de conexión directa a la red telefónica o a Internet. Los satélites ofrecen en estos escenarios una conectividad rápida y sencilla a las redes mundiales.

2.2 Starlink

Existen varias empresas o instituciones gubernamentales que operan, y/o comercializan sistemas de comunicación por satélite para distintas aplicaciones o servicios. Entre las instituciones gubernamentales las más conocidas pueden ser Intelsat (EEUU), Inmarsat (británica), Eutelsat (Francia), Hispasat (España) o AsiaSat (China). Pero también hay empresas privadas que comercializan estos servicios satelitales, como pueden ser Iridium, Globalstar, OneWeb, Project Kuiper (Amazon) o Starlink.

En este apartado se explica cómo la empresa Starlink ofrece una cobertura de Internet satelital a nivel mundial, puesto que es la tecnología escogida para la realización de este proyecto. Gracias a que sus satélites se encuentran en la órbita LEO se obtene mayor velocidad de señal y baja latencia, lo cual es esencial para ofrecer una conexión a Internet de calidad.

2.2.1 Red satelital Starlink

Starlink es una empresa filial de SpaceX cuyo objetivo es el de crear una constelación de satélites para ofrecer un servicio de conectividad a Internet, de banda ancha y baja latencia en todo el globo terrestre. SpaceX comenzó a lanzar satélites Starlink en 2019 y a 2024 ya dispone de más o menos 5000 satélites operativos en órbita.

Los satélites Starlink se encuentran en órbitas mucho más bajas que los satélites de los sistemas de comunicación tradicionales. Orbitan a sólo unos 550 kilómetros por encima de la superficie terrestre; esto es, se encuentran en la órbita LEO. Los satélites en esta órbita viajan a una velocidad de unos 7,8 km por segundo y a esta velocidad, un satélite tarda aproximadamente 90 minutos en dar la vuelta a la Tierra [7].

Además de la red de satélites, el servicio de Starlink se basa también en un sistema de estaciones terrestres llamadas *gateways*. Estas estaciones están repartidas por todo el mundo e intercambian señales con los satélites Starlink, conectándolos a una infraestructura de fibra óptica existente en tierra. La antena doméstica de un usuario se conecta a un satélite Starlink cuando éste pasa por encima de él, que a su vez lo conecta con el *gateway* más cercano. En un principio, los usuarios necesitan una estación terrestre a menos de 800 km de su ubicación para recibir el servicio, lo cual podría suponer un problema para ofrecer una cobertura mundial.

Para solventar este problema las últimas generaciones de satélites Starlink disponen de láseres para comunicarse entre ellos. Estos satélites están equipados con terminales de comunicación láser que les permiten transmitir datos a velocidades superiores a las de las radiofrecuencias tradicionales. Esta tecnología, que se conoce como óptica de espacio libre (FSO), utiliza un haz de luz visible para transmitir datos a distancias de hasta 10 kilómetros.

Los datos transmitidos desde tierra se envían de satélite en satélite hasta llegar a su destino. Este proceso se conoce como saltos o *hops* y cada salto requiere aproximadamente 10 milisegundos para completarse. Este proceso se repite hasta que los datos llegan a su destino. En lugar de

conectar a los usuarios con una estación terrestre cercana, los láseres permiten a los satélites hablar entre sí directamente a la velocidad de la luz.

Para transmitir datos entre los satélites, SpaceX utiliza una combinación de frecuencias de microondas en las bandas Ka y Ku. La banda Ka, que opera entre 26,5 y 40 GHz, se utiliza para transmitir datos desde tierra a los satélites. La banda Ku, de 11,7 a 14,5 GHz, se utiliza para transmitir datos desde los satélites a tierra [8].

Por último, los satélites también tienen radios definidas por software que les permiten ajustar sus frecuencias en función del entorno. Esto permite al sistema adaptarse a las condiciones cambiantes y mantener una conexión fiable.

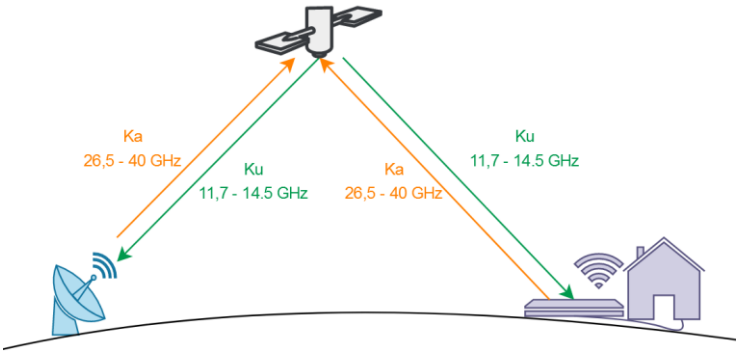
Es interesante señalar que, por otro lado, el sol puede crear interferencias en las señales de los satélites cuando cae directamente detrás de un satélite que se está comunicando con un usuario en tierra, quedando alineado, además, con el haz de la estación terrestre. Este efecto se conoce como apagón solar y suele afectar a los satélites geoestacionarios, incluido el GPS, provocando pérdida de conectividad.

En cambio, el servicio Starlink no se ve afectado por este tipo de interferencias del Sol. En un momento dado, el Starlink tiene varios satélites a la vista. El Starlink se conectará a un satélite que no esté interferido por el Sol [9].

En resumen, Starlink es un sofisticado sistema de transmisión de datos que se basa en una combinación de frecuencias de microondas, terminales de comunicación láser y radios definidas por software. Esta combinación de tecnologías permite al sistema crear una conexión fiable y transmitir datos con rapidez y eficacia.

La constelación Starlink consta de miles de satélites de órbita terrestre baja (LEO) que forman una gran red de satélites interconectados entre sí. Mediante estas dos características SpaceX ofrece un servicio de conectividad a Internet de baja latencia y cobertura mundial, con la posibilidad de ofrecer servicios de *realtime* o *streaming*, entre otros, lo cual era prácticamente imposible con los sistemas satelitales anteriores [8].

En la siguiente imagen (1. Imagen) se puede ver un esquema de la infraestructura de Starlink con las frecuencias utilizadas:



1. Imagen: Infraestructura Starlink

2.2.2 Antenas terminales

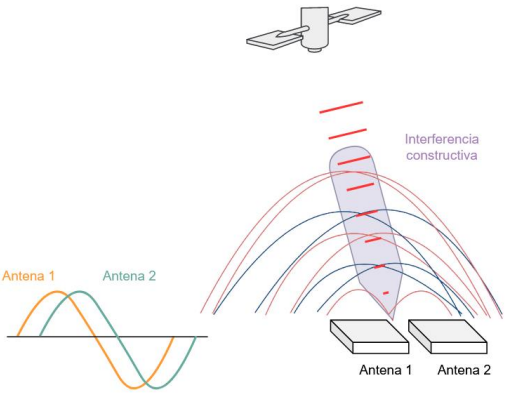
El éxito del servicio Starlink no solo reside en la red de satélites en órbita baja, sino que las antenas de los usuarios también han supuesto un gran cambio.

Al contratar Starlink los usuarios deben colocar una antena en sus instalaciones la cual se conectará a la red de satélites y será la que posteriormente ofrecerá acceso a Internet a través de un cable Ethernet y un router propio de Starlink. Esta antena es una antena de tipo *phased array* [10].

Con una antena *phased array*, los dispositivos de Starlink pueden rastrear satélites por el cielo sin moverse mecánicamente. Esta antena consta de 1280 antenas hexagonales dispuestas en forma de panal, todas ellas alimentadas con la misma señal de GHz para crear un haz similar a un láser que se propaga perpendicularmente.

Este haz debe orientarse de forma que apunte directamente al satélite Starlink. Como se ha indicado anteriormente, un satélite Starlink tarda aproximadamente 90 minutos en dar la vuelta a la Tierra, por lo que la antena debe ir dirigiendo su haz de satélite en satélite. Usar los motores que tiene la antena para dirigir la superficie radiante no es viable porque se romperían fácilmente, teniendo que sustituir la antena del usuario frecuentemente. Como alternativa se usa una técnica llamada *Phased Array Beam Steering*. Esta técnica consiste en cambiar continuamente la fase de las señales enviadas a las 1280 antenas hexagonales.

Concretamente, la solución consiste en desfasar la señal que envía una antena con respecto a las otras y, como resultado, el momento de los picos y valles emitidos por una antena es diferente a la otra. En consecuencia, se crean zonas de interferencias constructivas y zonas de interferencias destructivas. Por lo tanto, cambiando continuamente la fase de las señales enviadas a las antenas, podemos crear una zona de barrido de la interferencia constructiva dirigiendo el haz en una dirección u otra y la zona de interferencias destructivas quedaría en los ángulos restantes. Así, la antena puede cambiar de satélite cada 4 minutos aproximadamente sin tener que mover la antena de forma manual. Para saber el ángulo exacto al que debe apuntar o dirigirse el haz, se utilizan las coordenadas GPS de la antena del usuario [11]. En la siguiente imagen (2. Imagen) se puede ver como se crea la zona constructiva mediante el desfase de las señales que alimentan las antenas:



2. Imagen: Phased Array Beam Steering

En el satélite Starlink hay 4 antenas *phased array*. 2 se utilizan para comunicarse con múltiples antenas terminales y las otras 2 se utilizan para comunicarse con las estaciones terrestres [8].

Una de las grandes desventajas de Starlink es la necesidad de disponer de una exigente visión clara del cielo. Cada antena terminal debe tener una visión clara del cielo a 20° de elevación sobre el horizonte en todas las direcciones. Cualquier nivel de obstrucción afecta negativamente al rendimiento del sistema. Si la obstrucción es superior al 0,27% provocará interrupciones suficientes para que el usuario final lo note, bajando el rendimiento de sistema o incluso generando cortes de la conectividad [12].

Además, como consecuencia del *Phased Array Beam Steering* la antena necesita un campo de visión de 100°, para poder direccionar la zona de barrido de interferencia constructiva. Si en esta franja se detecta algún obstáculo se considera una obstrucción.

Por último, en cuanto a la transmisión de datos, Starlink hace uso de la modulación 64-QAM y del codec H.264 para comprimir los datos, lo que supone un rendimiento mejorado a la hora de la transmisión de los datos gracias a los métodos de compresión que implementan estos protocolos [13].

2.2.3 Política de Uso Razonable y Política de Gestión del Tráfico

La Política de Uso Razonable y Gestión del Tráfico describe cómo se gestiona el tráfico en la red de Starlink y cómo se asignan los datos al cliente en función del Plan de Servicio contratado [14].

Starlink en su política de uso razonable define 4 principios fundamentales [14]:

- Equilibrio entre oferta y demanda. Starlink es un recurso finito y para servir al mayor número de clientes con Internet de alta velocidad, se debe gestionar la red para equilibrar la oferta de Starlink con la demanda de los usuarios, en la que influyen factores como la ubicación del servicio y el tiempo de uso.
- Neutralidad del tráfico. Se trata el tráfico de Internet de forma equitativa, sin discriminación por contenido, remitente, aplicación o servicio. Las prácticas de gestión de red se despliegan sobre la base de requisitos técnicos para categorías específicas de tráfico; esto es, el tratamiento del tráfico es independiente de los datos de contenido.
- Integridad de la red. Garantizar la integridad y seguridad de la red, incluyendo, entre otras cosas, el análisis de patrones de tráfico para optimizar los servicios, evitar la congestión de la red o la distribución de virus u otros códigos maliciosos En estos casos puede llegar a aplicarse una reducción de velocidades para algunos o todos los usuarios.
- Distribución de datos en función del plan de servicio. Se distribuyen los datos entre los usuarios de forma justa y equitativa aplicando políticas de gestión de red cuando la demanda de recursos de red supera la oferta, y permitiendo a los usuarios elegir entre Planes de Servicio a distintos precios en función del Servicio priorizado, adecuado a sus necesidades.

Siguiendo estos principios, Starlink define unos tipos de datos y servicios los cuales, junto con otros parámetros, crean diferentes tarifas para los usuarios.

2.2.4 Infraestructura de red de Starlink

Starlink además de la red de satélites constituye su propio Sistema Autónomo de Internet (AS14593) [15] y por lo tanto, se convierte en un proveedor de servicios de Internet (ISP) el cual debe ofrecer conectividad a Internet a sus usuarios utilizando diferentes políticas.

Starlink proporciona dos políticas IPv4, "default" y "public" [16].

- En el caso de la política "**default**", se utiliza la configuración CGNAT (*Carrier Address Grade Network Translation*) asignando a clientes direcciones privadas desde el prefijo 100.64.0.0/10 mediante DHCP (*Dynamic Host Configuration Protocol*). Después, el protocolo NAT (*Network Address Translation*) es el encargado de traducir entre IPs privadas y públicas de Starlink [16].

  CGNAT es una solución al problema de agotamiento de direcciones IPv4. Para dar servicio de Internet a todos sus clientes, un ISP tendría que asignar una única dirección IPv4 pública a la interfaz externa de cada equipo del cliente, pudiendo agotarse las direcciones IP públicas. CGNAT funciona como el NAT tradicional pero la mayor diferencia es que realiza una doble NAT para así poder asignar IP públicas a un número más amplio de clientes, esto es, realiza dos traducciones IP por cliente.

  Dado que en esta política no se ofrece direccionamiento público, el usuario no puede ofrecer sus servicios a Internet, como por ejemplo en el caso de tener servidores dentro de la red del usuario. Para ello, es necesaria la política "public".

- La política "**public**" de Starlink es una configuración opcional disponible para ciertos clientes. En esta política se asigna una dirección IP pública a los clientes de la red Starlink usando DHCP. Una dirección IP pública es accesible desde cualquier dispositivo en Internet haciendo posible que el cliente ofrezca servicios de Internet desde su propia red.

  Starlink asigna IPs públicas dinámicas, no proporciona IPs estáticas. Esto se debe a que la red de Starlink es dinámica y de vez en cuando cambian las direcciones IP a medida que aumenta la capacidad de la red o cuando se añaden nuevas ubicaciones a la red. Como alternativa Starlink ofrece un sistema de reserva para que la dirección IP pública esté reservada a un cliente incluso cuando el terminal se apaga. Así, se consigue mantener la misma funcionalidad que con las IPs estáticas. Mover la antena Starlink a otra ubicación para conseguir acceso a Internet desde otra ubicación que no sea la inicial, puede causar que la IP pública cambie [17].

Además de políticas de IPv4, siguiendo los principios fundamentales explicados en el apartado anterior, Starlink también diferencia 4 tipos de servicios. Cada tipo de servicio tiene un nivel de prioridad en cuanto a cobertura, disponibilidad y acceso a los recursos de Starlink, como el acceso al ancho de banda. En los siguientes puntos se explican brevemente las implicaciones de cada uno de los niveles de prioridad:

- Standard data: los usuarios que contraten este tipo de servicio se reparten de manera equitativa los recursos entre todos los usuarios de este mismo nivel. Estos usuarios obtienen un paquete de datos ilimitados. Si los patrones de ancho de banda exceden lo que se asigna a un usuario típico, Starlink puede tomar medidas, tales como la reducción temporal de velocidad, para prevenir la congestión de la red.

- Priority data: este tipo de servicio asigna una cantidad fija de datos prioritarios al mes a los clientes que contraten un Plan de Servicio con este nivel de prioridad. Esta cantidad va de 40GB hasta 6 TB. Los datos prioritarios tienen prioridad sobre los datos estándar (*Standard data*) y móviles (*Mobile data*), lo que significa que los usuarios disfrutarán de velocidades de descarga y subida más rápidas y constantes. Los usuarios que agoten la cantidad de datos prioritarios contratada, se les asignará una cantidad ilimitada de datos estándar para el resto del mes. Starlink también ofrece la posibilidad de contratar datos prioritarios adicionales para el resto del mes a un coste adicional.

- Mobile data: este tipo de servicio asigna a los clientes una cantidad ilimitada de datos móviles cada mes. Este nivel de prioridad tiene siempre menor preferencia que todos los demás niveles de prioridad Starlink, por lo que el servicio se puede ver degradado en áreas congestionadas y durante las horas punta. Los Planes de Servicio con este tipo de prioridad no aseguran que se tenga cobertura en movimiento, sino que la antena terminal pueda ser transportada y cambiada de lugar.

- Mobile Priority data: este tipo de servicio asigna una cantidad fija de datos de prioridad móvil cada mes. Los datos de prioridad móvil tienen prioridad sobre los datos estándar y móviles. Los usuarios que agoten la cantidad de datos contratada y si no se encuentran en mar abierto, recibirán datos móviles ilimitados. En el caso de estar en mar abierto los usuarios únicamente podrán acceder a la página web de Starlink y contratar datos de prioridad móvil adicionales.

Por otra parte, Starlink diferencia también 4 Planes de Servicio. Estos planes de servicio tienen asignado cada uno de ellos una política IPv4, un tipo de servicio y una tarifa mensual. Además, cada Plan de Servicio tiene establecidos valores máximos y mínimos en cuanto al rendimiento y, restricciones en la movilidad del usuario. Estos Planes de Servicio son analizados más adelante, en el apartado Diseño del módulo 1: Red del cliente, para poder realizar un diseño con el plan de servicio más adecuado a las necesidades de este proyecto.

2.3 Protocolos de tunelado y redes virtuales privadas (VPN)

Por último, en este apartado se explican brevemente en qué consisten los protocolos de tunelado y las redes virtuales privadas, puesto que, como se verá en el apartado de OBJETIVOS Y ALCANCE, uno de los objetivos es implementar una VPN entre el cliente y el ISP para ofrecer conectividad a Internet. Esta VPN, además de mecanismos de seguridad, debe ofrecer un túnel de nivel 2 del modelo TCP/IP para que el cliente pueda tratar su tráfico como si de la misma red LAN se tratase.

Por ello, en este trabajo se hace una división entre los protocolos de tunelado y los protocolos de redes privadas virtuales (VPN). El primero ofrece al sistema la característica del túnel a nivel 2 del modelo TCP/IP y el segundo, los mecanismos de seguridad para la transmisión del tráfico de datos del cliente.

Por todo ello, se cree relevante describir brevemente en este apartado las características más significativas de estos dos tipos de protocolos.

2.3.1 Tunelado

El tunelado o tunneling se utiliza, entre otras situaciones, cuando se desea conectar redes de origen y destino del mismo tipo a través de una red de tipo diferente. Es decir, los túneles permiten enviar comunicaciones de redes privadas a través de una red pública (como Internet), o transportar un protocolo de red a través de una red incompatible, mediante un proceso llamado encapsulación [18].

El tunelado consiste en encapsular un paquete dentro de otro paquete. La encapsulación es el proceso de añadir un nuevo paquete dentro del paquete existente. Gracias a esta encapsulación la información puede ser transmitida desde un extremo del túnel al otro sin que sea necesaria una interpretación intermedia del paquete encapsulado. De esta manera, se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de entender o analizar el contenido de dichos paquetes. El túnel queda definido por los puntos extremos encargados de llevar a cabo la encapsulación y desencapsulación, y el protocolo de comunicación empleado [18].

Un uso bastante común del tunelado puede ser cuando se quiere conectar dos redes y una de ellas utiliza IPv4 y la otra IPv6. Si un paquete requiere atravesar estas dos redes, el contenido de las cabeceras será incompresible para una de las dos. Por ello, al encapsular paquetes IPv6 dentro de paquetes IPv4 (o viceversa), se podrá intercambiar paquetes entre los dos escenarios de redes.

El uso de protocolos de tunelado puede aumentar la sobrecarga y el tiempo de procesado de un paquete. Puesto que el tunelado se basa en la encapsulación, es necesario añadir datos o cabeceras adicionales al paquete original y esto puede reducir el ancho de banda efectivo y el rendimiento de la red, así como consumir más recurso de CPU y memoria [19].

Los túneles se pueden establecer en diferentes capas del modelo OSI. Dependiendo de la técnica usada, existen diferentes protocolos o técnicas de tunelado.

2.3.2 Redes privadas virtuales

En ciertas ocasiones, como por ejemplo podría ser cuando se requiere interconectar diferentes delegaciones de un banco, es muy importante que la conexión entre dos redes sea segura. Una de las opciones para conseguir una conexión segura es desplegar una línea dedicada la cual sólo será utilizada para la transmisión de datos entre las sedes que se quieren conectar. Pero esta solución resulta muy costosa. Como alternativa una VPN establece conexiones "virtuales" seguras entre las distintas delegaciones, o entre un empleado conectado desde remoto y cualquiera de las sedes.

Una red privada virtual (VPN) es una tecnología que crea una conexión segura y cifrada a través de una red menos segura, como puede ser el caso de Internet. De esta manera, una VPN permite extender una red privada utilizando una red pública [20].

La gran mayoría de los protocolos de VPN emplean el cifrado, la autenticación y la protección de la integridad de los datos, ofrecen un alto grado de seguridad y permiten a los usuarios acceder remotamente a redes privadas asegurando la privacidad e integridad de los datos y autenticación.

Las VPNs, en general, además de utilizar técnicas de seguridad, utilizan protocolos de tunelado para establecer una conexión segura.

Existen dos tipos habituales de VPN [20]:

- **Acceso remoto** (*Remote-Access*): Las VPN de acceso remoto permiten conexiones seguras y cifradas entre la red privada de una empresa y los usuarios remotos a través de un proveedor de servicios externo.

- **De sitio a sitio** (*Site-to-Site*): Mediante el uso de equipos dedicados y un cifrado a gran escala, una empresa puede conectar varias sedes fijas a través de una red pública como Internet. Las VPN de sitio a sitio pueden clasificarse a su vez en intranets o extranets. Una VPN sitio a sitio construida entre oficinas de la misma empresa se dice que es una VPN intranet, mientras que una VPN construida para conectar la empresa con su socio o cliente se denomina VPN extranet.

Para que una VPN sea segura debe ofrecer las siguientes características: confidencialidad (cifrado), fiabilidad (integridad), escalabilidad y gestión de las políticas de seguridad [20].

La seguridad es una de las claras ventajas de los protocolos de VPN. Puesto que se utilizan mecanismos de cifrado, autenticación e integridad, los datos se protegen del acceso no autorizado y la manipulación; incluso evita los ataques del intermediario (*man-in-the-middle*). Además, pueden proporcionar privacidad al ocultar identidades, ubicación y actividad. También pueden llegar a mejorar la velocidad y eficiencia de la red, puesto que se puede reducir la latencia y el consumo de ancho de banda si se utilizan técnicas de compresión u optimización [21].

Al igual que los protocolos de tunelado, el principal problema de los protocolos de VPN es la sobrecarga y el procesamiento extra que se debe hacer al implementar algoritmos de cifrado y autenticación. Aun así, el retardo añadido por el procesamiento se puede minimizar utilizando los algoritmos apropiados [21].

3 OBJETIVOS Y ALCANCE

En este apartado se exponen los objetivos del proyecto describiendo, al mismo tiempo, el alcance del mismo.

El objetivo principal de este proyecto consiste en diseñar, desplegar y analizar el servicio de Starlink como red de acceso viable y asequible para clientes de un proveedor de servicios de Internet (ISP).

El sistema que se define y analiza en este TFM busca dar respuesta a uno de los problemas a los que se enfrentan actualmente los proveedores de conectividad de Internet. En ocasiones, las entidades clientes, principalmente de tipo empresarial, disponen de instalaciones o sucursales en lugares donde instalar líneas de fibra óptica resulta muy costoso y, además, la cobertura 4G es insuficiente. Este puede ser el caso por ejemplo de entidades clientes ubicadas en zonas rurales sin acceso a fibra óptica, los cuales tienen como línea principal un enlace 4G que, al ser muy inestable no cumple con los requisitos necesarios para ofrecer una conectividad a Internet de calidad adecuada. Puede darse el caso también, en el que se disponga de una única línea de fibra óptica pero el cliente necesite una segunda línea de backup en ubicaciones en las que no se puede conseguir, por diversos motivos, una segunda línea de fibra óptica. En estas situaciones, el acceso a definir podría ofertarse como línea de backup.

Para ello, se quiere definir y analizar un sistema de acceso mediante el cual el cliente podría obtener todos los servicios ofrecidos por un ISP, garantizando una conexión a Internet de banda ancha con baja latencia y conectividad continua.

Formando parte de este TFM se propone, por tanto:

- El diseño de la solución de acceso basada en el servicio satelital de Starlink, como sistema de conectividad a Internet a través del ISP. Esta solución debe además proporcionar para los clientes empresariales las siguientes prestaciones:
    - Un rendimiento adecuado para los clientes, en términos de QoS, similares a los que se ofrece a los demás clientes del ISP, que hacen uso de otras tecnologías de acceso.
    - Una solución segura, de forma que la solución proporcionada no ponga en riesgo la conectividad de los clientes, de la misma forma que las soluciones tradicionales cableadas.
    - Conectividad de nivel 2 desde las instalaciones de la empresa cliente hasta el punto de entrada a la red del ISP. Esta característica asegura que el servicio para el cliente es similar al que se presta a quienes se conectan al ISP a través de otro tipo de accesos, como pueden ser las líneas punto a punto.

Además, en este TFM se plantea realizar una implementación de la solución diseñada, para realizar un análisis de viabilidad de dicha solución, considerando que, para ofertar la solución a clientes, ésta debe ser integrada en la infraestructura de red del ISP, sin impactar, ni en el servicio prestado al cliente que contrate esta solución, ni al resto de clientes del ISP.

Por último, como objetivo adicional, se plantea el diseño y la realización de pruebas que permitan analizar el rendimiento de la solución desplegada. Estas pruebas deben permitir conocer si este tipo de acceso resulta adecuado para su comercialización, en cuanto a rendimiento, para los clientes del ISP, así como b) ajustar y optimizar posibles aspectos que se identifiquen como mejorables sobre el despliegue realizado. Además, es importante señalar que se debe asegurar que la prestación de este servicio debe ser también económicamente viable.

Más concretamente, en este proyecto se buscan las características descritas a continuación:

- **Conectividad mediante túnel LAN entre el cliente y el ISP**

El sistema diseñado en este proyecto pretende dotar de conectividad a Internet a toda una infraestructura de un cliente (equipos y usuarios) mediante el sistema satelital Starlink. Este sistema puede funcionar tanto de línea principal en la red de acceso de los clientes que no tengan la opción de obtener líneas de fibra óptica, como de línea de backup en los casos en los que el cliente tiene obtiene una única línea de fibra óptica.

Además, en este trabajo se busca ofrecer al cliente la posibilidad de tratar su tráfico desde el extremo del ISP como si se tratase de su misma red LAN, pudiendo configurar las tecnologías de nivel 2 del modelo TCP/IP, como pueden ser las redes de área local virtual (VLAN). Gracias a esto, el cliente percibe los saltos intermediarios entre su red y la del ISP como si se tratase de un único cable Ethernet. Para ello, es necesario implementar en el sistema un túnel de nivel 2 que encapsule las tramas Ethernet en su totalidad en paquetes IP, las cuales se deben desencapsular en el extremo del ISP.

- **Seguridad en las comunicaciones del cliente con flexibilidad de cambios de direcciones IP**

Considerando las necesidades de la mayoría de los clientes, es recomendable implementar un sistema que garantice la seguridad en las comunicaciones entre el cliente y el ISP. Específicamente, se busca asegurar la confidencialidad del tráfico, la autenticación de los extremos y la disponibilidad del servicio. Para cumplir con estos requisitos, se propone la implementación de dos tecnologías: una VPN y HA (*High Availability*).

La VPN proporcionará confidencialidad y autenticación a través del uso de claves criptográficas. Starlink hace uso de direcciones IP dinámicas, por lo que esta VPN debe ser capaz de gestionar cambios en las direcciones IP de los extremos del túnel, pudiendo mantener la sesión iniciada sin cambios en la configuración del mismo y sin que el usuario perciba ninguna interrupción del servicio.

Por consiguiente, en este trabajo se diferencian los protocolos de tunelado y los protocolos de redes privadas virtuales (VPN). El primero ofrece al sistema la característica del túnel a nivel 2 del modelo TCP/IP y el segundo, los mecanismos de seguridad para la transmisión del tráfico de datos del cliente.

En cuanto a la disponibilidad, se debe aplicar la duplicación de los servicios que el ISP ofrece al cliente, asegurando así servicios en alta disponibilidad (HA).

- **Análisis de validación del sistema**

Una vez implementado el sistema, se debe comprobar el correcto funcionamiento del sistema y la correcta integración de todos los componentes que lo forman. Para ello, se han hecho pruebas de validación garantizando que el cliente obtiene conectividad a Internet y que las tecnologías implementadas funcionan correctamente haciendo que los componentes cumplan con el diseño realizado.

- **Análisis de rendimiento del sistema**

Después de validar el sistema, se han llevado a cabo pruebas de rendimiento de red para poder analizar el rendimiento general del sistema. Estas pruebas se han hecho en diferentes situaciones y, así, poder concluir la influencia de algunos de los componentes y factores del sistema.

- **Optimización de la implementación del sistema**

Por último, después de haber validado y analizado el diseño y la implementación de sistema, se ha ajustado el sistema para conseguir la optimización de la implementación del sistema. Estos ajustes son mejoras en relación a distintos aspectos de la implementación que permiten que el despliegue llevado a cabo obtenga mejor rendimiento.

4 BENEFICIOS

En este apartado se describen los beneficios que el proyecto puede aportar en diferentes áreas. Los beneficios se han clasificado en tres tipos: beneficios técnicos, beneficios económicos y beneficios sociales. En los siguientes subapartados se exponen sucesivamente los beneficios.

4.1 Beneficios técnicos

1. **Mayor cobertura y disponibilidad**

Como se ha mencionado previamente, uno de los escenarios de aplicación para este proyecto se presenta cuando un cliente enfrenta obstáculos significativos para acceder a conexiones de fibra óptica y, además, la cobertura de red 4G disponible no cumple con las necesidades requeridas para una conexión a Internet estable y eficaz. Ante esta situación, el proyecto propone la utilización de una tecnología de acceso innovadora que es la comunicación satelital como red de acceso a Internet. En particular, se propone hacer uso del sistema satelital Starlink ya que es la única empresa a día de hoy que ofrece una cobertura global de Internet de baja latencia.

Desde la perspectiva del proveedor de servicios de Internet (ISP), el uso de Starlink permite ampliar la cobertura de servicio a más clientes, especialmente aquellos ubicados en regiones donde las infraestructuras de conexión a Internet habituales son insuficientes o inexistentes.

Por otro lado, en los casos en los que se considera la opción de utilizar un enlace 4G como red de acceso, se ha de mencionar que, aunque pueda lograrse cierta cobertura, esta suele ser inestable y variable, lo que puede afectar negativamente a la experiencia del usuario. En contraste, Starlink ofrece una disponibilidad del 99%, ofreciendo una alternativa mucho más confiable y constante. Esta alta disponibilidad asegura que los clientes tengan acceso continuo a Internet, un aspecto importante para muchas aplicaciones que dependen de una conexión ininterrumpida para su funcionamiento.

Por lo tanto, este proyecto no solo mejora la accesibilidad al servicio de Internet, sino que también mejora la calidad de la conexión en cuanto a disponibilidad y rendimiento.

2. **Innovación en tecnologías de acceso**

El análisis de la viabilidad de esta nueva tecnología de acceso, así como su optimización, contribuye a la innovación y mejora continua que permite los despliegues de tecnologías de comunicación satelital como red de acceso entre la red de un cliente y su ISP. De esta manera, tanto el cliente como el proveedor de servicios de Internet se benefician de la innovación y ventajas que ofrecen los sistemas satelitales.

3. Conexión segura resistente a cambios de configuración

Gracias a la utilización del protocolo de VPN escogido en el análisis de alternativas, es posible asegurar una conexión cifrada y autenticada sin interrupciones ni cambios de configuración independientemente de la dirección IP. En muchas ocasiones, los protocolos de VPN dependen de la dirección IP del cliente, puesto que el cliente suele ser identificado mediante esta dirección. En el caso del protocolo escogido los clientes son identificados con una clave pública estática y, en consecuencia, los cambios de dirección no afectan a la conectividad.

Por ello, el sistema en su totalidad debe estar adecuadamente configurado para soportar cambios en la dirección IP del cliente. Como se explicará posteriormente, el sistema ha sido diseñado de tal manera que se mantenga la conexión segura independientemente de la dirección del cliente y, si se produce un cambio, no sea necesario ninguna configuración adicional y los túneles no experimenten ninguna interrupción.

4. Obtención túnel LAN entre el cliente y el ISP

El sistema diseñado en este proyecto proporciona al cliente la capacidad de establecer una conexión segura de nivel 2 del modelo TCP/IP en el extremo de la red del proveedor de servicios de Internet (ISP). Esto permite al cliente manejar su tráfico como si estuviera dentro de su propia red LAN, incluso cuando se transmita a través de redes públicas de Internet. Esta funcionalidad se logra mediante la implementación de una combinación de protocolos de tunelado como se verá después.

4.2 Beneficios económicos

En relación con los beneficios económicos, cabe destacar que el beneficio técnico de capacidad para lograr una mayor cobertura y disponibilidad también conlleva, de manera indirecta, ventajas económicas significativas.

1. **Reducir costes y captación de clientes**

Es innegable que la solución de red de acceso más eficiente tanto técnicamente como económicamente para conseguir conectividad a Internet actualmente es la tecnología FTTH (*Fiber-To-The-Home*). Esta tecnología consiste en llevar líneas de fibra óptica hasta el edificio del propio cliente. En la mayoría de las ocasiones, esta tecnología se encuentra ya desplegada y para ofrecer este servicio únicamente se debe alquilar una de las fibras ópticas ya instaladas en el mismo edificio del cliente o lo más cercano a este. Pero, volviendo al mismo caso en el que se quiere dar conectividad a Internet a una empresa o cliente que se encuentra en una zona de difícil acceso, puede ocurrir que las grandes empresas proveedores de Internet no tengan desplegadas líneas de fibra óptica. Por lo tanto, si se quiere ofrecer FTTH la única opción es realizar una obra civil para desplegar esas líneas de fibra óptica.

Esto puede resultar realmente costoso en tiempo y dinero para las empresas y, un sistema de conexión por satélite como el aquí diseñado, ofrece una conectividad a Internet de baja latencia a menos coste. Hasta ahora, el principal desafío asociado a este tipo de soluciones eran las bajas velocidades y la alta latencia inherentes de cualquier sistema satelital, circunstancias que impedían la oferta de ciertos servicios de Internet. Sin embargo, Starlink ha logrado superar estas limitaciones proporcionando una conexión a Internet de alta velocidad y baja latencia. Es por ello que, es una solución muy apropiada para obtener conexión a Internet y ofrecer todo tipo de servicios en lugares remotos.

Por último, en la actualidad es imprescindible para muchas empresas contar con una conexión a Internet de alta calidad y estabilidad. Por lo tanto, desde la perspectiva de un proveedor de servicios de Internet, ofrecer un servicio de acceso de este tipo permite atender a nuevos clientes que tengan estas necesidades. Además, este sistema mejora la calidad de la conexión en términos de disponibilidad y rendimiento, lo que a su vez mejora la imagen del ISP y facilita la captación de nuevos clientes gracias a la introducción de innovaciones tecnológicas.

2. **Facilidad de instalación y movilidad**

Para conseguir conexión a la red satelital Starlink es necesario la instalación de una antena terminal en la red del cliente. Esta antena contiene un sistema de orientación automatizado, por lo que únicamente requiere una visión despejada del cielo para establecer la conexión con la red satelital. Todo ello es transparente para el usuario final ofreciendo, así, una gran facilidad de instalación.

Además, tras realizar un análisis de los diferentes servicios ofrecidos por Starlink en el presente documento, se ha optado por contratar un servicio que permite la reubicación de la antena terminal, con lo que se consigue cierta movilidad. Para que dicha movilidad sea efectivamente

implementada, es necesario que todo el sistema esté adecuadamente configurado para ello. En consecuencia, se ha diseñado el sistema de manera que el único requisito para la activación de todos los componentes sea la obtención de una dirección IP a través del protocolo DHCP. El diseño permite, además, que la IP pueda ser tanto pública como privada, y estática o dinámica. Al recibir esta dirección, el sistema establecerá automáticamente los protocolos propuestos y conseguirá conectividad a Internet.

Esta característica puede ser ventajosa si el cliente decide cambiar de ubicación. Normalmente, cuando un cliente cambia de ubicación es necesario realizar cambios de configuración en la red de acceso, pero, en este caso, el sistema se adapta automáticamente.

Otro claro ejemplo puede ser si se quiere ofrecer conexión a Internet de forma temporal. Si el cliente tiene una avería en sus líneas principales, el sistema propuesto en este documento puede ser una solución temporal para que el cliente siga obteniendo conexión a Internet.

Todos los casos anteriores suponen un claro beneficio económico para el ISP, puesto que ofrece opciones novedosas y más flexibles para sus clientes.

4.3 Beneficios sociales

Por último, ofrecer una mayor cobertura de conexión a Internet supone también una ventaja social puesto que ayuda a disminuir la llamada “brecha digital”. La brecha digital hace referencia a la desigualdad en el acceso, uso o impacto de las Tecnologías de la Información y la Comunicación (TIC) entre grupos sociales. La geografía suele ser una de las causas de este fenómeno.

Además, el sistema propuesto en este documento podría ser fácilmente adaptado para proporcionar conexión a Internet a usuarios finales en ubicaciones remotas, conectando sus domicilios a través de Starlink y garantizando la seguridad de dicha conexión.

5 ANÁLISIS DE ALTERNATIVAS

En este apartado se analizan las alternativas que se han valorado en distintos aspectos a lo largo del desarrollo de este proyecto, para seleccionar, teniendo en cuenta los objetivos del proyecto, las tecnologías que mejor se adapten. Las alternativas se han analizado una a una, identificando los aspectos positivos y negativos de cada una de ellas, para posteriormente elegir de forma justificada entre las distintas alternativas.

Como se ha explicado anteriormente, uno de los objetivos principales es ofrecer conectividad a Internet mediante Starlink, garantizando la seguridad y la protección de datos de las comunicaciones del cliente. Además, otro de los requisitos es ofrecer al cliente la posibilidad de tratar su tráfico en el extremo del ISP como si de su red LAN se tratase. Para conseguir esto de la mejor forma posible, en este apartado se analizan diferentes tecnologías de VPN, para proteger los datos mediante algoritmos de cifrado y autenticación, y diferentes protocolos de tunelado de red para ofrecer una conexión entre el cliente y el ISP como si fuese un solo cable Ethernet.

Para elegir la alternativa que mejor se adapte a los objetivos del proyecto, primero se ha valorado en profundidad cada opción. En este apartado, para cada alternativa, en cada aspecto asociado, se han definido y valorado distintos criterios para tomar la decisión y para finalizar, se ha seleccionado una de las opciones de manera justificada. Para tomar la decisión se ha asignado a cada criterio un porcentaje en función de su importancia y se ha estimado el grado de cumplimiento de los criterios de cada opción estableciendo una nota del 0 al 10.

5.1 Protocolo de red privada virtual (VPN)

Como se ha mencionado en el apartado de objetivos del proyecto, uno de los requisitos para dar conectividad a Internet al cliente es añadir seguridad a sus comunicaciones. Esto se proporciona mediante el uso de tecnología VPN.

Como se verá posteriormente, esta VPN se ha implementado desde la red del cliente hasta la red del ISP, ofreciendo seguridad de extremo a extremo. Esto hace que el cliente obtenga seguridad sobre su tráfico hasta la red de su proveedor sin importar las redes intermedias. Por todo ello, esta VPN debe ofrecer protección de datos mediante la confidencialidad y autenticación de los extremos.

Existen varios protocolos VPN que ofrecen diferentes niveles de seguridad y rendimiento. La elección del protocolo VPN adecuado depende de las necesidades específicas del usuario, el nivel de seguridad requerido, el rendimiento y, desde el punto de vista del ISP, de la escalabilidad.

5.1.1 Alternativas de protocolo VPN

A continuación, se analizan los protocolos de VPN más utilizados en la actualidad que se han valorado en este TFM, para después, calificarlos según los criterios escogidos para este proyecto y finalmente escoger el más adecuado.

- **SSTP (*Secure Socket Tunneling Protocol*)**

SSTP (*Secure Socket Tunneling Protocol*) es un protocolo de túnel de red privada virtual (VPN) que proporciona un mecanismo para transportar tráfico PPP a través de un canal SSL/TLS. SSL (*Secure Socket Layer)* proporciona seguridad a nivel de transporte con negociación de claves, cifrado, comprobación de la integridad del tráfico y autenticación.

SSTP funciona estableciendo una conexión segura y cifrada entre un cliente VPN y un servidor SSTP. Utiliza el mismo puerto que HTTPS, lo que garantiza la compatibilidad y la facilidad de acceso a través de Internet.

El protocolo encapsula paquetes PPP sobre un canal SSL, proporcionando la seguridad mediante la aplicación de los mecanismos de SSL/TLS. La fase inicial consiste en un proceso de "handshake" para establecer una conexión segura entre el cliente y el servidor. Durante esta fase, el servidor se autentica ante el cliente mediante certificados SSL. Tras el handshake, los paquetes PPP cifrados se transmiten a través del canal SSL establecido.

El uso del puerto TCP 443 para la transmisión del tráfico permite a SSTP atravesar sin problemas la mayoría de cortafuegos y servidores proxy. Por esa razón, el protocolo es especialmente eficaz en entornos en los que las conexiones VPN pueden bloquearse o no conectarse a través de cortafuegos o dispositivos NAT.

Aunque el protocolo ofrece varias ventajas, tiene ciertos inconvenientes. Al ser un protocolo propietario desarrollado por Microsoft, no ofrece la transparencia de las soluciones de código abierto y es posible que no satisfaga las necesidades de clientes con requisitos de seguridad muy específicos. Otra de las desventajas es que el proceso de cifrado intensivo de SSTP puede ralentizar la velocidad de conexión.

- **IPSec (*Internet Protocol Security*)**

IPSec (*Internet Protocol Security*) es un conjunto de protocolos estándar de IETF (*Internet Engineering Task Force*) que proporcionan autenticación, integridad y confidencialidad de los datos entre dos puntos de comunicación a través de la red IP.

IPSec utiliza dos protocolos para proteger el tráfico o el flujo de datos. Estos protocolos son ESP (*Encapsulation Security Payload*) y AH (*Authentication Header*). Todos estos componentes son importantes para proporcionar los tres servicios principales: confidencialidad, autenticación e integridad. Además, IPSec define también los protocolos necesarios para el intercambio seguro de claves.

El protocolo de cabecera de autenticación (AH) proporciona la autenticación del origen de los datos, integridad de los datos y protección contra la repetición. Sin embargo, AH no ofrece confidencialidad de los datos, lo que significa que toda la información se transmite en texto claro. AH garantiza la integridad de los datos mediante una suma de verificación. Para asegurar la autenticación del origen de los datos, AH utiliza una clave secreta compartida entre los extremos y para evitar la repetición, añade en la cabecera un campo de número de secuencia.

La diferencia entre ESP y AH es que ESP proporciona cifrado, mientras que ambos protocolos ofrecen autenticación y verificación de integridad. Con ESP, ambos sistemas de comunicación utilizan una clave compartida para cifrar y descifrar los datos intercambiados.

IPSec ofrece la posibilidad de combinar estos dos protocolos de manera que se protege el datagrama IP en su totalidad. Aunque la combinación de ambos protocolos ofrece mayor seguridad, el esfuerzo de procesamiento adicional puede suponer una pérdida de rendimiento considerable.

Aunque IPSec es un protocolo estándar abierto que cuenta con un amplio respaldo de los proveedores, puede tener problemas de compatibilidad con algunos dispositivos y aplicaciones de red, lo que puede provocar problemas de interoperabilidad.

- **OpenVPN**

OpenVPN es un proyecto de software de código abierto que implementa un protocolo de tunelado VPN. Funciona en la capa de transporte (nivel 4) del modelo OSI creando túneles cifrados para paquetes de datos y autenticación de los extremos, garantizando una transmisión segura entre el cliente y el servidor.

OpenVPN utiliza la librería OpenSSL para manejar el cifrado y descifrado, proporcionando un canal seguro para el intercambio de datos. Utiliza el protocolo SSL/TLS para el intercambio de claves, lo que permite mecanismos de cifrado de hasta 256 bits. Además, OpenVPN utiliza PFS (*Perfect Forward Secrecy*). PFS crea una clave de cifrado única para cada sesión o transferencia de datos. La sustitución de las claves de cifrado dificulta significativamente a los atacantes externos el robo de claves y la manipulación de los cifrados.

El protocolo OpenVPN funciona en dos modos: TCP y UDP. El modo TCP garantiza que los paquetes de datos se entregan en el orden correcto y retransmite cualquier paquete perdido. El modo TCP proporciona fiabilidad en términos de pérdidas de paquetes gracias sus mecanismos de acknowledge y temporizadores, aunque a expensas de la velocidad. El modo UDP suele ser el predeterminado. UDP es más rápido, pero no garantiza el orden de los paquetes, por lo que es menos fiable pero más eficaz para las comunicaciones en tiempo real.

Una de las ventajas más significativas de OpenVPN es que soporta una amplia configuración, tanto para mejorar el rendimiento como también la seguridad. Ofrece flexibilidad, por ejemplo, en sus métodos de autenticación, ya que admite la autenticación mutua entre clientes y servidores VPN mediante diversos métodos. Los métodos incluyen claves precompartidas, autenticación basada en certificados digitales y autenticación por nombre de usuario/contraseña. Esta flexibilidad garantiza que las empresas puedan aplicar políticas de seguridad sin verse limitadas por el software VPN.

Sin embargo, OpenVPN requiere un consumo alto de los recursos comparando con otros protocolos y en consecuencia se obtiene un menor rendimiento.

OpenVPN es más reciente que SSTP. Además, OpenVPN es de código abierto y se beneficia de las revisiones y actualizaciones de los colaboradores. También utiliza el cifrado AES, que es el estándar en cifrado simétrico.

- **WireGuard**

WireGuard es software de código abierto para establecimiento de túneles de red que funciona en la capa 3 del modelo TCP/IP. Ofrece confidencialidad de los datos y autenticación mediante claves criptográficas.

WireGuard proporciona una interfaz virtual que puede ser administrada utilizando las utilidades estándar ip e ifconfig. Una vez configurada, esta interfaz actúa como interfaz de túnel encapsulando de forma segura los paquetes IP sobre UDP.

Se basa en un principio fundamental: una asociación entre una clave pública de un peer y una dirección IP de origen del túnel. Debido a esa asociación se puede decir que WireGuard es una VPN peer-to-peer. La interfaz virtual de WireGuard puede mantener uno más peers. Los túneles son identificados mediante peers y estos, a su vez, son identificados por claves públicas. En resumen, un peer es una clave pública con la que se establece un túnel.

A diferencia de algunas tecnologías VPN, WireGuard no tiene roles estrictos de cliente o servidor. Todos los peers de WireGuard son igualmente capaces de desempeñar lo que podría ser un rol de cliente o servidor. Esto abre la posibilidad de poder diseñar diferentes topologías.

WireGuard ha sido diseñado pensando en la facilidad de implementación y simplicidad. Está pensado para ser fácilmente implementado en muy pocas líneas de código, y fácilmente auditable en busca de vulnerabilidades de seguridad.

Además, WireGuard garantizar que los paquetes procedentes de una interfaz WireGuard serán autenticados y cifrados.

Una de las grandes ventajas de WireGuard respecto a otros protocolos de VPN es su capacidad de hacer roaming entre direcciones IP. Puesto que los peers se identifican con claves y no con direcciones IP, cuando una dirección cambia WireGuard es capaz de almacenar el cambio y seguir manteniendo el túnel establecido siendo totalmente transparente para el usuario.

WireGuard ofrece mejores resultados en cuanto a rendimiento y facilidad de implementación comparado con IPSec y OpenVPN. Esto se debe, mayormente, a que WireGuard tiene como objetivo proporcionar una VPN que sea simple y altamente efectiva. Otras tecnologías VPN populares, como OpenVPN e IPsec, son a menudo complejas de configurar, se desconectan fácilmente, toman un tiempo considerable negociando reconexiones, pueden usar cifrados obsoletos y tienen un código relativamente masivo, de 400,000 a 600,000 líneas de código para los dos ejemplos dados.

El diseño de WireGuard busca reducir estos problemas, haciendo el túnel seguro y fácil de implementar y administrar, gracias a que el software es implementado como interfaz de red virtual del kernel para Linux y, además, está definido en menos de 4 000 líneas de código.

5.1.2 Selección de protocolo de VPN

Después de conocer las diferentes alternativas de protocolos de VPN, en este apartado se describen los criterios de selección para esta tecnología y se le asigna una ponderación a cada uno de ellos dependiendo de la importancia que tienen respecto a este proyecto. A continuación, se establece un valor del 0 al 10 a cada una de las alternativas según el cumplimiento de cada criterio. Finalmente, se calcula la nota media de cada una de las alternativas y se selecciona justificadamente una de ellas.

Los criterios de selección para el protocolo de VPN son los siguientes:

- **Rendimiento (30 %)**: Este criterio representa la medida de rendimiento de red que ofrece el protocolo. Mediante este criterio se tiene en cuenta la sobrecarga de los algoritmos de cifrado y descifrado, el retardo añadido por el procesamiento de los paquetes y la cantidad de recursos de procesado que supone. Este criterio es importante a la hora de la selección por lo se le asigna una ponderación del 30 %.

- **Open source (10 %)**: Este término se refiere al software que se desarrolla de forma descentralizada y colaborativa, basándose en la revisión por pares y la producción comunitaria. El software de código abierto suele ser flexible y customizable a las necesidades del proyecto, puesto que lo desarrollan comunidades y no un único autor o empresa. Este criterio, aunque no se considera crucial, es interesante ya que gracias a la comunidad y las constantes revisiones el software de este tipo obtiene mejores resultados y se adapta más rápido a las necesidades que van surgiendo en la actualidad. Por ello se le ha asignado una ponderación del 10 %.

- **Flexibilidad ante los cambios de direcciones IP (60 %)**: Este criterio se refiere a la capacidad del protocolo de VPN para admitir los cambios de direcciones IP con los que se establece el túnel sin verse afectada la conexión. Se considera que este criterio es esencial para este proyecto, puesto que, como se ha explicado anteriormente, Starlink asigna direcciones IP dinámicas que pueden cambiar a lo largo del tiempo. Por ello, este criterio adquiere una ponderación elevada, siendo ésta del 60 %.

A continuación, se muestran las puntuaciones asignadas a cada alternativa, desglosadas por criterio y ponderación:

	Rendimiento	Open source	Flexibilidad	TOTAL
SSTP	4	0	2	2,4
IPSec	7	10	1	3,7
OpenVPN	5	10	5	5,5
WireGuard	8	10	9	**8,8**

1. Tabla: Matriz de evaluación de alternativas para el protocolo VPN

Como se puede observar en la tabla anterior (1. Tabla), la alternativa seleccionada para el protocolo de VPN a implementar es WireGuard. El punto más determinante en la selección de esta alternativa, dadas las ponderaciones previamente establecidas para cada criterio, ha sido la flexibilidad que ofrece ante los cambios de direcciones IP. Gracias a que los extremos del túnel se identifican mediante claves criptográficas y que las direcciones IP de los extremos no intervienen en el funcionamiento del protocolo, WireGuard permite crear túneles con direcciones IP dinámicas sin verse afectado ni interrumpido el funcionamiento cuando estas cambian. Además, WireGuard obtiene el mejor rendimiento comparando con los demás protocolos debido a que es implementado en el kernel Linux y a su facilidad de implementación en términos de necesidad de recursos y líneas de código. Por todo ello, se puede decir que WireGuard es la solución más adecuada para este proyecto.

5.2 Protocolo de tunelado

Además de implementar un protocolo de VPN con algoritmos de cifrado y autenticación, en este proyecto se ha implementado ofrecer al cliente la posibilidad de tratar su tráfico en el extremo del ISP como si fuese de su misma red LAN, pudiendo, por ejemplo, configurar VLANs. Para ello, se debe implementar en el sistema diseñado un protocolo de tunelado que encapsule las tramas Ethernet de la red LAN en paquetes IP para después desencapsularlas en el extremo del ISP y así, ofrecer un túnel de nivel 2 en el modelo TCP/IP entre el cliente y el ISP. De esta manera, el cliente además de obtener un túnel seguro percibe el salto entre su red y el ISP como si fuese un único cable Ethernet. Los protocolos analizados en este apartado no requieren de mecanismos de seguridad. Esta característica que obtiene con el protocolo escogido en el apartado anterior (5.1 Protocolo de red privada virtual (VPN)).

5.2.1 Alternativas de protocolo de tunelado

A continuación, se analizan diferentes protocolos de para después, calificarlos según los criterios escogidos para este proyecto y finalmente escoger el más adecuado.

- **GRE (*Generic Routing Encapsulation*)**

GRE es un mecanismo para encapsular cualquier protocolo de capa de red sobre cualquier otro protocolo de capa de red. La especificación general se describió originalmente en el RFC 1701, y la encapsulación de paquetes IP sobre IP se define en el RFC 1702 como una implementación específica de GRE. GRE se utiliza frecuentemente para encapsular paquetes IPv4 e IPv6 dentro de paquetes IPv4. GRE no ofrece mecanismos de seguridad por lo que generalmente se implementa junto con otros protocolos de VPN como IPSec para obtener servicios de seguridad como cifrado y autenticación.

GRE se usa ampliamente en las VPN para transportar paquetes IP entre redes IP privadas a través de redes públicas con direcciones IP rutadas globalmente. GRE permite a los hosts de una red IP privada comunicarse con hosts de otra red IP privada proporcionando un túnel entre dos routers a través de Internet. La ventaja de GRE sobre otros protocolos de tunelado es que puede encapsular tráfico broadcast, multicast u otros protocolos no IP.

GRE es un protocolo sin estado y no tiene conocimiento de la configuración; ni siquiera de la existencia del punto final del túnel remoto. Una vez configurado GRE, los paquetes se encapsulan y se reenvían, esté o no presente el dispositivo que los desencapsula.

Los paquetes IP de una red privada destinados a un host en otra red IP privada son encapsulados por el router de salida de la red origen y reenviados al router de la red destino. Los routers intermedios encaminan los paquetes utilizando las cabeceras exteriores sin analizar las cabeceras del paquete original. El router destino extrae del paquete la carga útil original y lo ruta al destino apropiado dentro de la red a la que está conectado.

- **L2TP (*Layer 2 Tunneling Protocol*)**

L2TP opera en la capa de acceso de red (nivel 2) del modelo TCP/IP, que se encarga de establecer y mantener conexiones directas entre dispositivos de una red. L2TP facilita la creación de túneles, o conexiones encapsuladas, para transportar datos a través de una red pública, como Internet, manteniendo la privacidad mediante mecanismos de cifrado ya utenticación.

L2TP por sí mismo no proporciona funciones de cifrado o autenticación. Para garantizar una comunicación segura, L2TP suele combinarse con el protocolo de seguridad de Internet (IPsec), que añade funciones de cifrado y autenticación. Esto protege los datos que se transmiten por el túnel L2TP.

El túnel L2TP se crea encapsulando una trama L2TP (una trama PPP con un datagrama IP encapsulado) dentro de un paquete del Protocolo de Datagramas de Usuario (UDP), que a su vez se encapsula dentro de un paquete IP. Las direcciones de origen y destino de este paquete IP definen los puntos finales de la conexión.

En la práctica, hay dos puntos finales de un túnel creado a través de L2TP: el Concentrador de Acceso L2TP (LAC) y el Servidor de Red L2TP (LNS).

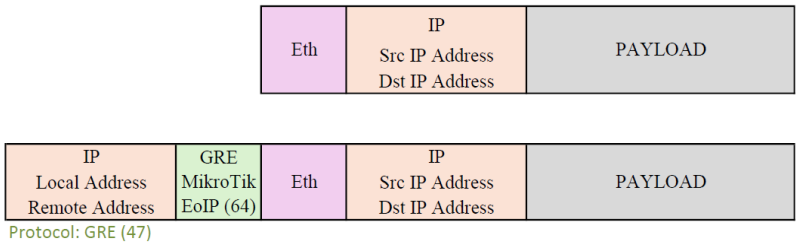
El LAC recibe el tráfico de dispositivos remotos y lo ruta de forma segura al LNS. El LAC negocia una conexión Punto a Punto (PPP) para transmitir tramas de datos. El LNS se encuentra en el otro extremo del túnel L2TP y funciona como punto de terminación de las sesiones PPP.

- **EoIP (*Ethernet over IP*)**

Ethernet over IP (EoIP) Tunneling es un protocolo de MikroTik RouterOS que crea un túnel Ethernet entre dos routers sobre una conexión IP. Encapsula tramas Ethernet dentro de paquetes IP. Esto permite transportar tráfico Ethernet a través de una red IP, y puede utilizarse para conectar redes Ethernet remotas a través de Internet o redes IP privadas. Además, EoIP puede utilizarse para conectar redes Ethernet a través de diversos tipos de infraestructura, ya sean conexiones por cable, inalámbricas o incluso por satélite.

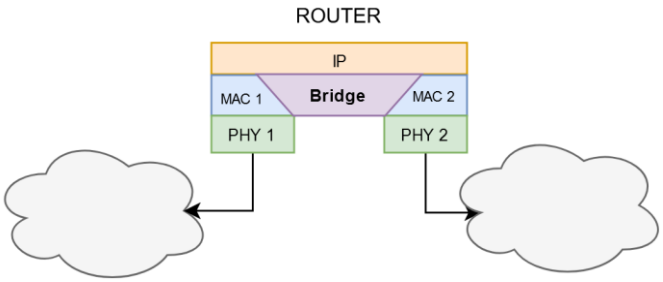
EoIP se basa en el protocolo GRE anteriormente explicado en este mismo apartado. EoIP añade a una trama Ethernet completa la cabecera GRE y la cabecera IP exterior. Esta cabecera IP exterior menciona el punto de entrada del túnel (*Local Address*) y el punto de salida del túnel (*Remote*

Address), pero el paquete interior se mantiene sin modificaciones. Este proceso se puede ver en la siguiente imagen (3. Imagen)



3. Imagen: Encapsulación protocolo EoIP

Cuando la función de puenteo (*bridging*) del router está activada, todo el tráfico Ethernet se transfiere a través de este puente como si existiera una conexión directa mediante una interfaz Ethernet física y un cable entre ambos routers, como se puede observar en la siguiente imagen (4. Imagen).



4. Imagen: Bridging

Gracias a todo esto, las configuraciones de red con interfaces EoIP ofrecen diversas posibilidades para la conexión de redes LAN. Una de estas posibilidades es conectar redes LAN a través de Internet, permitiendo una interconexión global. Por otro lado, también se pueden conectar redes LAN mediante redes inalámbricas 802.11b en modo "ad-hoc".

EoIP es una solución propietaria, lo que puede suponer que no todos los fabricantes de equipamiento de red acepten este protocolo. Los demás protocolos analizados en este mismo apartado son soluciones estándar, por lo que EoIP tiene una desventaja significativa respecto a los demás protocolos en este sentido.

5.2.2 Selección de protocolo de tunelado

Al igual que en el apartado anterior, después de describir las diferentes soluciones, se establecen los criterios más importantes para hacer una selección justificada entre las diferentes opciones. En esta ocasión, los criterios de selección establecidos son los siguientes:

- **Facilidad de implementación (5 %)**: este criterio depende de una combinación de factores que incluyen la complejidad del protocolo, la configuración necesaria y el entorno de implementación. Dado que este criterio no es transcendental, se valora con una ponderación del 5 %.

- **Sobrecarga de los paquetes de datos (30 %)**: este criterio se refiere a la información adicional que se le añade a cada paquete a la hora de enviarlo por el túnel. Esta información suele ir en forma de cabeceras y, precisamente, son estas mediante las cuales se crea el túnel. Dependiendo del tipo de túnel y del protocolo la información necesaria para la creación del túnel es mayor o menor. Estas cabeceras adicionales suponen una bajada en el rendimiento, puesto que se percibe una reducción del ancho de banda efectivo y un aumento en la latencia por el procesamiento de los paquetes. Además, en este proyecto este túnel se quiere implementar dentro del protocolo de VPN, por lo que el rendimiento se puede ver doblemente afectado. Dada la importancia y la influencia de este criterio se le ha asignado una ponderación del 30 %.

- **Adaptabilidad a la solución planteada y a la infraestructura del ISP (65 %)**: como se ha explicado anteriormente, el protocolo de tunelado escogido debe encapsular tramas Ethernet en su totalidad, para que de este modo el cliente pueda tratar su tráfico en el extremo del ISP como si se tratase de la misma red LAN. El protocolo debe ser adaptable a este requisito. Además, debe ser adaptable también a la red del ISP sin interferir en otros protocolos. Al ser un criterio esencial, adquiere una ponderación del 65 %.

A continuación, se muestran las puntuaciones asignadas a cada alternativa, desglosadas por criterio y ponderación:

	Implementación	Sobrecarga	Adaptabilidad	TOTAL
GRE	7	8	5	6,0
L2TP	6	2	3	2,8
EoIP	5	8	9	8,5

2. Tabla: Matriz de evaluación de alternativas para el protocolo de tunelado

Como se muestra en la tabla anterior (2. Tabla), el protocolo seleccionado para la implementación del túnel es EoIP, puesto que este protocolo está precisamente diseñado para la conexión de redes LAN encapsulando las tramas Ethernet en su totalidad en la red de origen. Gracias a esto, el cliente tiene la posibilidad de identificar su tráfico en el extremo del ISP, por ejemplo, mediante VLANs. Además, Además, a pesar de ser una solución propietaria, el equipamiento de red de

5.3 Estrategia para el despliegue del sistema

Una vez finalizado el diseño del sistema, en este TFM se plantea su implementación y despliegue con el objetivo de analizar su validación y rendimiento en equipamiento real. Para llevar a cabo este proceso, existen diversas estrategias.

5.3.1 Alternativas de la estrategia para el despliegue del sistema

A continuación, se describen y se analizan las distintas alternativas para el despliegue del sistema.

- **Despliegue de una maqueta**

Esta primera estrategia consiste en desplegar el sistema en una maqueta dedicada únicamente a este proyecto. Como se ha explicado más adelante en el aparatado DESCRIPCIÓN DE LA SOLUCIÓN PROPUESTA, el sistema consta de varios componentes por lo que si se sigue esta estrategia se deben desplegar todos los componentes para crear la maqueta y después realizar las pruebas sobre ella. La maqueta estaría aislada de cualquier otro componente de red.

En esta situación, al estar la maqueta aislada, el sistema no se ve afectado por factores externos y no interfiere con otros sistemas. Esto garantiza un entorno seguro y controlado para realizar pruebas sin riesgos de comprometer otros sistemas o redes. Además, los posibles errores durante la implementación o durante las pruebas no tienen consecuencias graves, ya que no afectan la red en producción. Esto permite un margen de error elevado y un análisis más profundo de las características y limitaciones del sistema. Se pueden realizar pruebas exhaustivas y repetitivas sin preocuparse por el impacto en usuarios finales.

Sin embargo, crear y mantener una maqueta aislada puede ser costoso, ya que requiere equipamiento y/o configuración adicional. Además, existe una falta de realismo. Aunque se intente replicar el entorno real, una maqueta aislada puede no capturar todas las complejidades y variabilidades del sistema, lo que podría llevar a resultados de pruebas menos representativos. Además, no permite valorar el impacto de implementar un nuevo sistema a una red real ya en operación, dónde se pretende que el sistema aquí diseñado opere.

- **Integración en la infraestructura en operación del ISP**

Otra de las opciones para el despliegue del sistema es integrarlo directamente en la infraestructura del proveedor de servicios de Internet. El ISP mantiene una red en operación con conectividad a sus clientes y a Internet por lo que si se sigue esta estrategia el sistema diseñado en este trabajo debería ser implementado e integrado en la red ya desplegada.

La clara ventaja de esta estrategia es que permite evaluar su rendimiento y comportamiento en un entorno real y con tráfico auténtico. Esto proporciona una visión precisa de cómo el sistema funcionará en la práctica en la infraestructura para la que se ha definido. Además, al estar en un entorno de producción, es posible identificar y resolver problemas que solo aparecen en condiciones de uso reales, como problemas de latencia, congestión o interferencias. Por otro lado, facilita la evaluación y retroalimentación de los usuarios finales, lo que puede ser valioso para realizar mejoras y ajustes en el sistema.

En cambio, las pruebas en una red de producción conllevan el riesgo de causar interrupciones o degradaciones del servicio de la red en operación, lo que puede afectar a los clientes del ISP. Por ello, tanto en la configuración como en la realización de las pruebas se dispone de menos flexibilidad. Las pruebas de validación y rendimiento que se van a realizar en este proyecto pueden estar restringidas en cuanto a la cantidad y variedad.

Esta estrategia resulta más costosa, ya que implica un mayor tiempo y esfuerzo en la configuración y puesta en marcha del sistema y de cada prueba. Esto se debe a la necesidad de analizar el impacto en la red antes de cada instalación y prueba.

5.3.2 Selección de la estrategia para el despliegue del sistema

Una vez descritas las diferentes estrategias para el despliegue del sistema, se analizan los criterios de selección más significativos para después elegir, de manera justificada, entre las diferentes opciones.

- **Precisión en los resultados (60 %)**: este criterio se refiere a la capacidad de precisión del despliegue ajustándose a la realidad. Es decir, se busca que el despliegue llevado a cabo en este trabajo sea lo más cercano posible a lo que un usuario final cliente del ISP percibe. De esta manera, los resultados de las pruebas realizadas sobre el despliegue serán realistas, lo que permite hacer una valoración y un análisis más exhaustivo y cercano al servicio que se va a ofrecer a los usuarios de este acceso, así como su impacto en la infraestructura de red actual, y por ello en los demás clientes del ISP. Dada la importancia y la influencia de este criterio, se le ha asignado una ponderación del 60 %.
- **Flexibilidad en la configuración y realización de pruebas (20 %)**: este criterio se refiere a la flexibilidad que ofrece el sistema implementado para configurar y probar diferentes escenarios, con el fin de dotar a la propuesta del proyecto de mayor ámbito de evaluación y, con ello, valor. Un despliegue flexible permite realizar cambios en las configuraciones sin afectar a otros componentes ajenos a este sistema o incluso a la red del ISP y, gracias a ello, se pueden realizar diversas pruebas en diferentes escenarios para obtener unos resultados más precisos. Este criterio se valora con una ponderación del 20 %.
- **Feedback directo (20 %)**: este criterio se refiere a la posibilidad de obtener realimentación directo de los usuarios finales del sistema. Gracias a la valoración directa de los usuarios finales, el sistema puede ser mejorado y ajustado para ofrecer una conectividad a Internet de mayor calidad. En consecuencia, los clientes del ISP manifiestan su valoración real lo que le da un valor mayor al proyecto.

A continuación, se muestran las puntuaciones asignadas a cada alternativa, desglosadas por criterio y ponderación:

	Precisión en los resultados (60 %)	Flexibilidad (20 %)	Feedback directo (20 %)	TOTAL
Maqueta	5	9	3	5,4
Integración	8	2	8	**6,8**

3. Tabla: Matriz de evaluación de alternativas para la estrategia de despliegue

Como se puede observar en la tabla anterior (3. Tabla), la estrategia seleccionada para el despliegue del sistema es la integración en la infraestructura en operación del ISP. Esta estrategia destaca por su capacidad de ajustarse a la realidad ofreciendo resultados cercanos a los que un usuario final percibe. Además, permite recibir una valoración directamente de los usuarios y posibles clientes, pudiendo ajustar mejor el sistema. Debido a todo ello, el análisis del sistema es más cercano a la realidad y con ello, se aumenta el valor de este trabajo.

6 ANÁLISIS DE RIESGOS

En este apartado del documento se analizan los diferentes riesgos que han tenido en cuenta durante el desarrollo de este TFM. La identificación y análisis de riesgos es muy importante, ya que permite evitar imprevistos e inconvenientes a lo largo del proyecto y, además, la previsión de problemas puede disminuir posteriormente el impacto negativo de los mismos.

Por ello, en este apartado se identifican los riesgos de este proyecto y se describen de forma individualizada. A continuación, se cuantifica la probabilidad de ocurrencia de cada uno de ellos y su posible impacto para, después, realizar una comparación de entre estos mediante la matriz probabilidad-impacto. Finalmente, se describe el plan de prevención de los riesgos identificados.

6.1 Riesgos

1. **Problemas de cobertura Starlink**

Aunque anteriormente se haya mencionado que Starlink ofrece una cobertura global, puede darse el caso en el que el lugar o el país donde se encuentra el cliente al que se le quiere dar conectividad a Internet mediante el sistema diseñado en este trabajo, Starlink no ofrezca sus servicios.

Starlink comenzó a ofrecer su servicio de conexión a Internet en 2020 lanzando unos 60 satélites a la órbita LEO. Gracias a estos satélites junto con ciertas estaciones terrestres, Starlink comenzó a ofrecer su servicio en EE.UU. A lo largo de los años, Starlink ha ido ampliando su cobertura a medida que ha puesto en órbita más satélites e instalando estaciones terrestres. Es así que, hoy en día, Starlink ofrece sus servicios en la gran mayoría de países, pero, todavía existen ciertos lugares donde no está disponible.

Esto se debe a que, como se ha explicado anteriormente, la infraestructura de Starlink se compone de varios elementos además de la red satelital. Para poder ofrecer cobertura en un lugar es necesario tener alguna estación terrestre cercana y que esta esté conectada al Sistema Autónomo de Starlink.

Este problema es un riesgo externo, esto es, no puede ser controlado por la propia empresa que quiere dar conectividad a Internet al cliente. Este riesgo puede surgir cuando una empresa tiene diversas delegaciones en distintos países, en algunos de los cuales Starlink podría no ofrecer sus servicios.

Por todo ello, se ha asignado la siguiente probabilidad de ocurrencia e impacto:

- Probabilidad de ocurrencia: 10 %
- Impacto: 90 %

2. Problemas de instalación de equipos

Como se explicará posteriormente, la implementación del sistema diseñado en este trabajo se ha hecho con equipos reales. Para ello se han instalado varios equipos, tales como la antena terminal Starlink y un router entre otros. Como en cualquier instalación, pueden aparecer ciertos problemas.

La antena terminal de Starlink exige tener una visión despejada del cielo de unos 100º para poder establecer una conexión eficiente con la red satelital. Esta condición puede limitar la instalación, ya que cualquier obstáculo como árboles y edificios contiguos puede impedir que se establezca la conexión. Es por ello que, es recomendable instalar la antena en un lugar elevado como en un tejado, pero aun así la instalación puede llegar a ser complicada puesto que Starlink recomienda que la antena esté lo más horizontal posible y algunos tejados tienen cierta inclinación. Por lo tanto, es muy importante encontrar un lugar adecuado para la instalación de la antena.

Por otro lado, los equipos de Starlink están adaptados para poder ser instalados en el exterior. Es así que, tanto los equipos como los conectores tienen protección ante la entrada del agua como la de la lluvia. Pero, como el router que se quiere conectar detrás de la antena no está adaptado para ser instalado en la intemperie, esto puede suponer algunos problemas. Por ejemplo, si se instala la antena en un tejado el cable que irá desde la antena al router debe ser lo suficientemente largo como para poder colocar el router en el interior del edificio del cliente. Por ello, se han establecido los siguientes parámetros:

- Probabilidad de ocurrencia: 50 %
- Impacto: 70 %

3. Problemas de hardware

Los fallos en la infraestructura de red son los fallos más habituales en cualquier proyecto de ingeniería de red. Estos fallos suelen aparecer en hardware de los propios equipos que constituyen la infraestructura. Como se explicará después, el sistema aquí diseñado se ha implementado en equipo real, por lo que, cabe la posibilidad de que dicho equipamiento sufra fallos técnicos que se deriven en problemas para cumplir con los plazos y costes establecidos. Estos fallos pueden ser tanto internos como externos y no son de fácil solución, puesto que la única opción recae en cambiar el propio hardware.

- Probabilidad de ocurrencia: 30 %
- Impacto: 90 %

4. Incompatibilidad con versiones de equipamiento

Para la implementación y valoración de la viabilidad de la solución del sistema diseñado se ha utilizado un router MikroTik. La empresa MikroTik publica diferentes versiones de su Sistema Operativo continuamente para implementar mejoras y funcionalidades de manera que sus equipos puedan adaptarse a la evolución constante de las tecnologías de red y comunicación. Estas actualizaciones pueden afectar al sistema en diferentes ámbitos, pero existe una limitación importante que consiste en que uno de los protocolos que se ha implementado en el despliegue del sistema es WireGuard, un protocolo de red privada virtual (VPN). Este protocolo es compatible únicamente con versiones de MikroTik a partir de la versión 7.

- Probabilidad de ocurrencia: 30 %
- Impacto: 90 %

6.2 Matriz Probabilidad – Impacto

Tras identificar los riesgos principales del proyecto, se empleará una herramienta conocida como Matriz de Probabilidad-Impacto. Esta herramienta se utiliza para priorizar los distintos riesgos asociados al proyecto, evaluando tanto la probabilidad de su ocurrencia como la magnitud de su impacto en el proyecto.

A continuación, se presenta la mencionada Matriz Probabilidad-Impacto de este proyecto:

		Impacto				
		%10	%30	%50	%70	%90
Probabilidad	%10					**1**
	%30					**3, 4**
	%50				**2**	
	%70					
	%90					

4. Tabla: Matriz Probabilidad - Impacto

Como se puede observar en la tabla anterior (4. Tabla), el riesgo (1) tiene una probabilidad muy baja en el contexto de este proyecto, puesto que en el momento de hacer este TFM, Starlink ofrece cobertura en la mayoría de los países y, antes de comenzar con el trabajo se ha comprobado que el servicio estaba disponible y que el ISP escogido no ofrece servicio en otros países.

Sin embargo, los riesgos (2) y (3) tienen una relevancia más importante en este proyecto. El riesgo (2) aunque tenga una probabilidad de ocurrencia no muy alta, su impacto es significativo, puesto que cualquier problema de instalación puede causar problemas importantes, principalmente en los plazos del proyecto. De la misma manera, al riesgo (3) se le ha asignado una probabilidad de ocurrencia menor, pero, su impacto es del 90 %. Los problemas de hardware no son muy habituales, pero pueden afectar significativamente a los costes del proyecto.

Por último, el riesgo (4) es el de mayor importancia para este proyecto, aunque tenga una probabilidad de ocurrencia del 50 % su impacto es muy alto, del 90%. Cuando el sistema aquí diseñado se quiere llevar a implementarlo en un cliente, los problemas con las versiones de MikroTik pueden afectar al despliegue. Es por ello por lo que se deben analizar las versiones del equipamiento que se quiere instalar.

Por todo ello, es importante diseñar un plan de prevención para los riesgos más relevantes, concretamente los riesgos (2), (3) y (4).

6.3 Plan de prevención

El paso final en el análisis de riesgos es desarrollar un plan de prevención para reducir las posibilidades de que los riesgos identificados sucedan y formular un plan de respuesta para actuar si alguno de estos ocurre. Para los riesgos mencionados previamente, se definen las siguientes acciones:

- **Hardware de respaldo:**

Si alguno de los equipos utilizados sufre problemas técnicos que lo inutilicen, conviene contar con equipamiento de back up como reserva para evitar riesgos del tipo (3). Además, se recomienda planificar la instalación de todos los equipos involucrados para prevenir el riesgo (2). Sobre todo, se debe asegurar que se puede acceder a un lugar donde la vista del cielo sea totalmente despejada en unos 100° de ángulo de visión y, que esté disponible un lugar como un rack para instalar el router MikroTik lo suficientemente cerca para que la largura del cable entre la antena y el router sea apto.

- **Análisis de compatibilidad de versiones instaladas con los protocolos a implementar:** (4)

Para este proyecto es esencial comprobar la compatibilidad entre las versiones del equipamiento con el que se quiere hacer el despliegue del sistema y los protocolos que se deben implementar. Exactamente, para poder implementar WireGuard en un router MikroTik se necesita como mínimo la versión 7, por lo que es totalmente necesario tener esta versión o una versión superior a esta.

Adicionalmente, como en cualquier aspecto relacionado con la seguridad, es muy importante mantener los equipos actualizados, ya que las actualizaciones frecuentemente incluyen la implementación de nuevos parches de seguridad, esenciales para la protección de los datos.

Esto se podría hacer monitorizando las versiones de los equipos instalados mediante algunos scritps y, cuando un equipo esté desactualizado respecto con la última versión estable publicada o con la última versión que el ISP quiere instalar en sus equipos, que este mismo genere una alerta para que algún técnico actualice el equipo o que, de manera automática, el propio equipo descargue la última versión desde un repositorio y lo instale.

7 DESCRIPCIÓN DE LA SOLUCIÓN PROPUESTA

Una vez analizadas las diferentes alternativas, en este apartado se explica con detalle la solución propuesta para hacer uso de la red satelital Starlink como red de acceso entre un cliente y un ISP.

Para ello, en primer lugar, se presenta una visión general del sistema implementado, con todos los componentes que lo forman. Después, se describen con detalle los componentes de este sistema diferenciando el diseño y la implementación de cada uno de ellos.

Además de la implementación, también se ha hecho un análisis de validación y rendimiento del sistema. Por ello, en este apartado también se detallan las pruebas llevadas a cabo y sus resultados. Por último, tras haber analizado el rendimiento, se detallan algunos aspectos con el objetivo de optimizar la implementación del sistema.

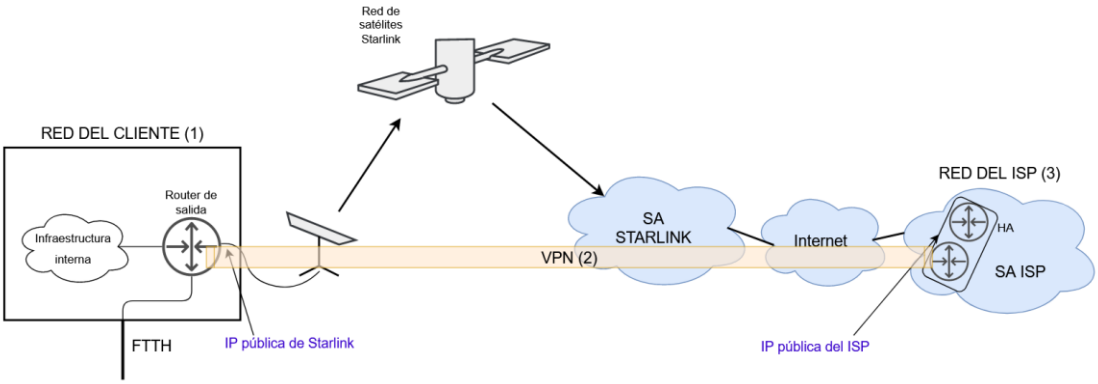
7.1 Visión general del sistema

Como se ha explicado anteriormente, el objetivo principal de este proyecto es diseñar, desplegar y analizar el servicio de Starlink como red de acceso entre la red de un cliente y la de un ISP. Para ello, primero, se ha realizado un diseño del sistema teniendo en cuenta los objetivos de este proyecto que después se ha implementado. En este apartado, se presenta una visión general de todo el sistema para, después, explicar detalladamente cada componente que lo forma.

Un claro caso de uso de este sistema es implementarlo como solución al problema de la accesibilidad a la conectividad a Internet en lugares remotos. En ocasiones, un cliente puede encontrarse en un lugar donde la instalación de una línea de fibra sea muy costosa y la cobertura de 4G no sea suficiente. En otras situaciones, aunque el cliente obtenga una línea de fibra óptica como línea principal, se puede dar el caso en el que conseguir otra línea de fibra óptica como back-up es prácticamente imposible. Una de las grandes ventajas de los sistemas satelitales es el gran alcance de cobertura, y es por ello que una red de acceso entre el cliente y el ISP mediante un enlace satelital puede ser la solución en estas situaciones.

Puesto que el servicio Starlink opera en la órbita baja LEO y, en consecuencia, ofrece conectividad a Internet de banda ancha y baja latencia, pudiendo ofrecer adecuadamente la mayoría de servicios de Internet, en este trabajo se plantea el uso de este servicio como alternativa para conectar la red de un cliente a la de su ISP. Además, el objetivo de la empresa Starlink es llegar a ofrecer una cobertura global llegando incluso a los lugares más remotos, lo que hace, junto con lo anteriormente mencionado, que el servicio Starlink sea el más adecuado para este proyecto.

Para ello, se ha diseñado la siguiente topología (5. Imagen):



5. Imagen: Visión general del sistema

Como se puede ver en la imagen anterior (5. Imagen), la topología puede separarse en 3 partes principales: la red del cliente, una VPN y la red del ISP. La VPN comienza en la red del cliente, pasa por la conexión satelital, el SA de Starlink e Internet y acaba en la red del ISP. La VPN es el módulo encargado de proporcionar conectividad a Internet al cliente. A continuación, se describen los detalles de cada una de las partes:

1. La red del cliente (módulo 1)

Dentro de la red del cliente se pueden diferenciar otros 3 componentes: la antena terminal de Starlink, el router de salida de la red del cliente y la infraestructura interna del cliente.

1.1. Antena terminal Starlink

La antena Starlink es la encargada de establecer una conexión con la red de satélites y estos a su vez, están conectados a las estaciones terrestres del Sistema Autónomo de Starlink y, mediante Internet, se establece la conexión con la red del ISP.

1.2. Router de salida de la red del cliente

El router de salida es el encargado de conectar la red interna del cliente a Internet. Si el cliente se encuentra en un lugar remoto donde instalar fibras ópticas hasta sus instalaciones es costoso en cuanto a tiempo y dinero, el router tiene una única conexión con Starlink como línea principal para el acceso a la red del cliente. En el caso en el que se disponga de una línea principal de fibra óptica pero no sea posible conseguir una segunda línea de FTTH como backup, este router puede mantener dos conexiones a Internet: una conexión tipo FTTH como línea principal y la conexión con el sistema Starlink como línea de backup. En todos los casos, el router tiene una conexión directa con la antena terminal de Starlink, dispuesta también en las instalaciones del cliente. Este router debe mantener la conexión a Internet y rutar todo el tráfico de la red del cliente.

1.3. Infraestructura interna del cliente

En cuanto a la red interna del cliente, esta se compone de todos los equipos e infraestructura que ofrecen conectividad a Internet a los usuarios finales, como por ejemplo ordenadores personales, cableado, switches o redes WiFi. Este TFM no abarca el diseño de esta red y es totalmente independiente del sistema diseñado en este proyecto.

2. VPN (módulo 2)

Este módulo es el encargado de proveer de conectividad a Internet a la red del cliente mediante una VPN. Esta VPN comienza en el router de salida de la red el cliente y acaba en los terminadores de VPN situados en la red del ISP. Abarca los saltos de la conexión satelital, el Sistema Autónomo de Starlink y todos los saltos intermedios necesarios entre el SA de Starlink y el SA del ISP (Internet).

Además, se quiere que esta VPN ofrezca mecanismos de seguridad en cuanto a cifrado y autenticación, y un túnel de nivel 2 del modelo TCP/IP para que el cliente pueda tratar su tráfico en el extremo del ISP como si fuese de la misma red LAN. Es por ello que esta VPN la componen dos protocolos diferentes: un protocolo de VPN que ofrezca mecanismos de seguridad (cifrado de los datos y autenticación de los extremos) y un protocolo de tunelado que ofrezca el encapsulamiento de las tramas de Ethernet de la red LAN del cliente en su totalidad.

3. Red del ISP (módulo 3)

Por último, en la red del ISP se propone que estén los terminadores del túnel mencionado. Se propone que estos terminadores se desplieguen en HA (*High Availability*), es decir, los terminadores están duplicados de forma que si uno de los dos cae el cliente es capaz de establecer el túnel con el otro terminador.

7.2 Diseño del sistema

Para poder poner en marcha el sistema es necesario diseñar previamente sus 3 componentes principales. En los siguientes apartados se procede a describir detalladamente cada uno de los componentes individualmente, identificando las necesidades de cada uno de ellos y ofreciendo un diseño acorde.

7.2.1 Diseño del módulo 1: Red del cliente

Este módulo, como ya se ha indicado, consiste en 3 componentes: la antena terminal de Starlink, el router de salida y la infraestructura interna del cliente.

1. Antena terminal Starlink

Esta antena es la encargada de establecer la conexión con la red satelital Starlink mediante la cual el cliente obtiene conectividad a Internet. La antena debe estar instalada en las instalaciones del cliente, y tal y como se ha explicado en el apartado de CONTEXTO TECNOLÓGICO, la antena necesita una visión despejada del cielo de 100° con una elevación de 20° sobre el horizonte. Por ello, es recomendable instalar la antena en el tejado de las instalaciones del cliente, puesto que cualquier árbol o edificio contiguo podría impedir el funcionamiento del sistema. Se ha de mencionar que, tanto la antena como el cable y todos los equipos de Starlink están preparados para poder ser instalados en el exterior.

2. Router de salida de la red del cliente

Una vez instalada la antena, esta debe ir conectada directamente al router de salida del cliente, el cual, es el encargado de rutar el tráfico desde la red interna del cliente hacia Internet o viceversa. Este router no está acondicionado para ser instalado en el exterior, por lo que será un factor a tener en cuenta a la hora de llevar a cabo el montaje.

El router de salida recibe una dirección IP de Starlink mediante DHCP en la interfaz en la que esté conectada la antena. Teniendo en cuenta que este sistema se quiere implementar como red de acceso entre la red de un cliente y su ISP, es necesario tener la posibilidad de obtener una IP pública. Si un cliente desea instalar servidores públicos en su red interna es imprescindible tener direccionamiento público.

Además de la conexión a Internet, el router tiene conectado la red LAN del cliente, esto es, se considera como un *Border router*. En consecuencia, debe establecer una sesión BGP de tipo eBGP con el Sistema Autonomo del ISP. El neighbour de esta sesión será el terminador de la VPN. Una vez establecida la sesión BGP, el router recibe las rutas necesarias por parte de su ISP y será capaz de direccionar hacia y desde Internet todo el tráfico de su red LAN, aplicando cuando sea necesario el protocolo NAT con la IP pública recibida.

3. Infraestructura interna del cliente

Como se ha mencionado anteriormente, este TFM no abarca el diseño de la red interna del cliente. El único requisito de esta es que debe tener direccionamiento público para que, en el caso de que el cliente tenga servidores públicos dentro de su propia red, se puedan direccionar las peticiones a estos.

Starlink ofrece 4 Planes de Servicio diferentes para obtener la conexión a su red. Cada plan de servicio tiene ciertas características marcadas en cuanto a rendimiento, direccionamiento IP, movilidad y tipos de datos contratados. Teniendo en cuenta todo lo anteriormente explicado, se ha escogido el Plan de Servicio que mejor se ajusta a las necesidades de este proyecto. En la siguiente tabla (5. Tabla) se pueden observar los parámetros de rendimiento y las condiciones de cada plan de servicio [22]:

PLANES DE SERVICIO	DOWNLOAD	UPLOAD	LATENCIA	DISPONIBILIDAD	IP PÚBLICA	MOVILIDAD	DATOS
STANDARD FIXED	177 – 268 Mbps (España)	20 – 35 Mbps (España)	33 – 46 ms	≥ 99 %	No CGNAT	Sin movilidad	Datos ilimitados (Standard data)
PRIORITY FIXED	40 – 220 Mbps (España)	8 – 25 Mbps	25 – 60 ms	≥ 99 %	Sí	Sin movilidad. Sí cambios de ubicaciones	Prioridad sobre Standard y Mobile. Paquetes de 40 GB, 1 TB, 2 TB, 6 TB (Priority)
MOBILE STANDARD	5 -50 Mbps	2 – 10 Mbps	< 99 ms	≥ 99 %	No CGNAT	Sin conectividad en movimiento, portátil	Sin ninguna prioridad. Paquetes de 50 GB, 1 TB, 5 TB (Mobile data)
MOBILE PRIORITY	40 – 220 Mbps	8 – 25 Mbps	< 99 ms	≥ 99 %	Sí	Conectividad en movimiento	Prioridad ante Standard y Mobile. Paquetes de 50 GB, 1 TB, 5 TB (Mobile Priority)

5. Tabla: Planes de Servicio Starlink

Puesto que se necesita direccionamiento público, los planes Standard Fixed y Mobile Fixed no son aptos para este proyecto. El plan Mobile Priority está pensado para aquellos usuarios que necesiten mantener la conectividad a Internet en movimiento, como por ejemplo en el caso de las embarcaciones, característica que no es necesaria para este proyecto y que supone un sobrecoste. El plan Priority Fixed, aunque no ofrece movilidad, permite cambios de ubicaciones, esto es, no se mantiene la conectividad a Internet mientras el usuario esté en movimiento, pero se puede conseguir conectividad en diferentes ubicaciones. Además, el tráfico de datos del plan Priority Fixed tiene prioridad ante el tráfico de los demás planes de servicio ya que con este plan se obtienen datos del tipo “Priority data”.

Por todas estas razones, se ha seleccionado el plan Fixed Priority de 40 GB, ya que se ajusta a las necesidades del proyecto. Las características ofrecidas por otros planes, como la movilidad, no son necesarias para el tipo de clientes que actualmente tiene el ISP seleccionado. Optar por estos planes resultaría en un aumento innecesario de los gastos, dado que son más caros que el plan escogido.

Por lo tanto, con el plan escogido se adquieren las siguientes características:

- 40 GB de Priority data
- CGNAT y opción de obtener una IP pública
- Se permiten los cambios de ubicaciones
- Entre 40 y 220 Mbps en Donwload
- Entre 8 y 25 Mbps en Upload
- Entre 25 y 60 ms de latencia
- 99 % de disponibilidad del servicio

7.2.2 Diseño del módulo 2: Conectividad entre red del cliente y red del ISP (VPN)

Este módulo debe ofrecer al sistema dos importantes características: la conectividad entre la red del cliente y su ISP, y seguridad en las comunicaciones del cliente.

- **Conectividad**

Como se ha mencionado previamente, uno de los objetivos de este módulo es proporcionar conectividad a Internet a la red del cliente mediante una VPN. Dado que no existe una conexión directa entre la red del cliente y la red del ISP, y que el tráfico del cliente debe ser transmitido a través de Internet, es necesario implementar una tecnología que establezca una conexión directa entre la red del cliente y el ISP y que proteja dicho tráfico durante los saltos intermedios (Internet). Mediante la implementación de una VPN entre las dos redes, el cliente puede percibir como si estuviese directamente conectado a la red del ISP con un único salto. Como se puede observar en la imagen de la visión general del sistema (5. Imagen), la VPN comienza en el router de salida de la red del cliente y termina en los terminadores de la red del ISP, abarcando todos los saltos intermedios de la red satelital, el SA de Starlink e Internet.

Además, es esencial que la VPN sea capaz de gestionar los cambios de las direcciones IP de los extremos, puesto que el extremo del cliente recibe una IP pública dinámica de Starlink la cual es probable que a lo largo del tiempo cambie.

En este sistema se propone que sea el cliente el responsable de comenzar con el establecimiento del túnel, ya que los servidores de la VPN del ISP tienen una dirección IP pública estática y la dirección IP del cliente para los estos es incierta, puesto que puede ir cambiando.

- **Seguridad**

Por otro lado, en este tipo de sistemas es interesante añadir seguridad a las comunicaciones del cliente. En este caso se requiere que el protocolo de red privada virtual (VPN) aplique el cifrado del tráfico entre el cliente y el ISP y la autenticación de los extremos del túnel.

Teniendo en cuenta todos los requisitos anteriores y como se ha explicado en el apartado de ANÁLISIS DE ALTERNATIVAS, se ha seleccionado el protocolo WireGuard para su implementación en este sistema como un protocolo de tunelado seguro debido a su mejorado rendimiento en comparación con otras soluciones VPN y, particularmente, por su capacidad para gestionar eficientemente los cambios de direcciones IP. La totalidad del proceso, desde el establecimiento del túnel hasta la transmisión de paquetes, se basa en el uso de claves criptográficas lo cual asegura que los cambios en las direcciones IP no afectan en la operatividad del sistema. Este protocolo añade al sistema mecanismos de cifrado y autenticación.

WireGuard es un protocolo peer-to-peer y cada peer tiene su par de claves privada y pública. Los peers se identifican con la clave pública y es con esta con la que se establece el túnel seguro en vez de con una dirección IP.

A pesar de que WireGuard sea peer-to-peer en este trabajo se ha diseñado una topología servidor-cliente, donde cada cliente tenga configurado un único peer, el servidor que le corresponde, y el servidor tenga un peer por cada cliente. Además, en la lista de las direcciones IP permitidas del cliente se debe configurar sólo la dirección IP de la interfaz virtual WireGuard del servidor y, del mismo modo, en el servidor en la lista de direcciones IP permitidas del peer del cliente se debe configurar únicamente la dirección IP de la interfaz virtual WireGuard del cliente. De esta manera se aumenta la seguridad, puesto que se impide que el tráfico de diferentes clientes se cruce.

A su vez, el extremo del túnel de la red del ISP se identifica mediante un registro DNS. Este registro DNS identifica los dos servidores de VPN en HA y debe estar configurado como registro DNS estático en el router del cliente. Cada cliente tiene establecido uno de los dos servidores como principal y el otro de backup, por lo que el cliente debe tener dos registros DNS configurados con las direcciones IP públicas de los servidores. El registro del servidor principal debe estar activado y el del backup desactivado. La VPN se establece con este registro DNS y no con la dirección IP del servidor para, así, poder cambiar entre los dos servidores e implementar la propiedad de HA.

Por último, para hacer efectiva la propiedad de HA de los terminadores, se debe monitorizar el estado del túnel. Esto se consigue ejecutando continuamente un script en el router del cliente que comprueba si la sesión BGP está levantada o no, puesto que la sesión BGP únicamente se establece cuando el túnel está establecido. Si la sesión BGP está caída el cliente detecta que existe algún problema con el túnel y, por lo tanto, debe cambiar el terminador del túnel al servidor de backup. Para ello, gracias a que el extremo del túnel del ISP se identifica mediante un nombre de dominio, el cliente únicamente debe modificar sus registros DNS y desactivar el registro principal y activar el registro secundario.

Adicionalmente, teniendo en cuenta la necesidad de algunos clientes, es interesante utilizar un protocolo de tunelado que ofrezca Ethernet sobre IP, de la manera que, sin importar los saltos intermediarios, los extremos del túnel se vean como si todo fuese una conexión de un solo cable Ethernet. De esta manera, además de tener una conexión segura, el cliente puede tratar su tráfico como si todo fuese de la misma red, pudiendo configurar, por ejemplo, VLANs.

Para obtener la propiedad de tunelado Ethernet sobre IP, se ha optado por implementar el protocolo EoIP dentro del túnel WireGuard y, de esta forma, el sistema se beneficia de las ventajas de ambos protocolos. Por un lado, se obtienen mecanismos de cifrado y autenticación y la posibilidad de cambios de direcciones IP de WireGuard y, por otro, la facilidad de configuración de las redes LAN que ofrece EoIP junto con la función de puentes de red.

Por lo tanto, cada cliente debe tener asociado un túnel EoIP con ID único, el mismo ID que se utiliza después para la VLAN asociada a ese cliente en el extremo del ISP. Una vez se establece el túnel EoIP, el router del cliente debe ser capaz de establecer una sesión BGP con la que obtener las rutas necesarias.

7.2.3 Diseño del módulo 3: Red del ISP

Este módulo abarca la parte de la red del ISP necesaria para poner en funcionamiento el sistema. Más concretamente, el ISP debe ofrecer al cliente los terminadores de la VPN que se establece entre el cliente y el ISP.

Como se ha mencionado anteriormente, en este diseño es el cliente el responsable de comenzar el establecimiento de la VPN, por lo que es necesario que estos terminadores tengan una dirección IP pública contra la que establecer el túnel y un puerto abierto en el que escuchar y aceptar estas peticiones.

Además, se propone que los terminadores de la VPN se desplieguen en HA (*High Availability*). Esta propiedad se adquiere manteniendo duplicada la configuración en los dos servidores del ISP en todo momento. Así, cuando el cliente detecte algún problema este debe ser capaz de cambiar el extremo del túnel al otro terminador y el nuevo servidor debe aceptar la petición estableciéndose el túnel con el otro terminador.

Por último, estos servidores deben tener asociado al tráfico del cliente una VLAN. Puesto que uno de los requisitos de la VPN es que ofrezca Ethernet sobre IP, los servidores reciben una trama Ethernet y deben marcarlo con la VLAN asociada al cliente. Para ello debe tener activada la configuración de puente de red entre la interfaz de la VPN y la VLAN.

7.2.4 Diseño de pruebas de validación y rendimiento

Finalmente, en este TFM también se han llevado a cabo diferentes pruebas tanto de validación como de rendimiento. Puesto que este trabajo consiste en un proyecto de ingeniería de red dirigido a clientes, se le debe garantizar al cliente que el sistema aquí propuesto funciona correctamente y que es efectivo dentro de unos parámetros de rendimiento. Es por ello que es importante también diseñar las pruebas que se van a realizar para poder después interpretar los resultados.

- **Validación**

En cuanto a la prueba de validación, el objetivo principal es poder validar la integración de todos los componentes del sistema diseñado. Esta prueba consiste en generar tráfico desde el router del cliente hasta la red del ISP y comprobar que se obtiene conectividad entre las dos redes, tanto desde el cliente hasta el ISP como en dirección contraria.

Para ello, se ha utilizado el protocolo ICMP (*Internet Control Message Protocol*). Mediante este protocolo se han mandado ciertos mensajes de tipo ping desde el router de salida del cliente hasta una dirección IP dentro de la red del ISP. Después de comprobar la conectividad entre el cliente y el ISP, se ha comprobado que se hace la correcta integración de los componentes del sistema mediante la herramienta Wireshark. Wireshark es una herramienta pasiva que captura u observa el tráfico de una interfaz. Por lo tanto, mientras se mandan los mensajes ping se ha capturado el tráfico saliente en las diferentes interfaces del router de salida del cliente para poder comprobar el formato de los paquetes y con ello la integración de los componentes y protocolos del sistema.

- **Rendimiento**

Una vez validada la integración de los componentes del sistema, se han realizado pruebas de rendimiento. En este proyecto el rendimiento se va a medir mediante 3 diferentes parámetros: RTT (*Round-Trip Time*), jitter y el ancho de banda de upload y de download. Se ha optado por medir estos parámetros debido a su importancia en el rendimiento de las redes y su impacto directo en la experiencia del usuario final. La latencia influye en el tiempo de respuesta de las solicitudes del usuario, el jitter afecta a la calidad de muchos servicios como video y voz y el ancho de banda determina la capacidad de la red para manejar grandes volúmenes de datos. Estos factores son significativamente importantes para garantizar una experiencia de usuario fluida y eficiente.

  - RTT (*Round-Trip Time*)

El RTT es el tiempo que necesita una solicitud de red para viajar por la red más el tiempo de la respuesta a esta solicitud que hace el viaje inverso. La latencia de red se mide, en general, mediante este parámetro. La latencia muestra el tiempo que tardan los datos en transferirse a través de la red. Una latencia, y por lo tanto un RTT, más baja mejora la experiencia de uso de una aplicación o servicio. En este caso el RTT se va a medir también con el protocolo ICMP mandando desde el router del cliente 100 solicitudes de ping a diferentes servidores: al servidor DNS de Google (8.8.8.8) y a un servidor interno del ISP. De esta manera, se quiere medir la latencia entre el router de salida del cliente y Google, y entre el router de salida del cliente y la red del ISP. Se cree importante medir la latencia al servidor DNS de Google, dado que es el servidor DNS por defecto que se configura en los equipos de los usuarios finales y, por lo tanto, uno de los servidores más utilizados.

  - Jitter

El jitter, por otro lado, tiene que ver con la variabilidad. Es la irregularidad en el tiempo de llegada de los paquetes de datos a su destino y el viaje de vuelta. Mientras que la latencia mide el tiempo medio que tarda un paquete en llegar a su destino y volver, el jitter se centra en las fluctuaciones o variaciones de esos tiempos. El jitter es especialmente crítico en aplicaciones en tiempo real como las llamadas de voz y vídeo, en las que un flujo de datos consistente y predecible es crucial para una experiencia de usuario fluida. Para calcular el jitter se han mandado 100 mensajes ping a un dispositivo remoto y, después, se ha calculado la diferencia media de tiempo entra cada secuencia de paquetes de respuesta. Al igual que para el RTT, se ha calculado el jitter entre el router de salida del cliente y el servidor DNS de Google y un servidor interno de la red del ISP.

  - Bandwidth

Además de la latencia y del jitter, se debe analizar el ancho de banda efectivo que el cliente percibe, puesto que es uno de los parámetros más importantes para la experiencia del usuario. Para ello, se han ejecutado diferentes pruebas de velocidad tanto de upload (desde el cliente al servidor de bandwidth test) como de download (desde el servidor al cliente). El servidor contra el que se han realizado estas pruebas es un servidor colocado dentro de la red interna del ISP, por lo que se va a medir el ancho de banda efectivo entre el cliente y el ISP. Se ha de mencionar que este servidor es el mismo contra el que se han hecho las pruebas de latencia y de jitter para poder medir los parámetros de rendimiento entre los mismos extremos.

Para evaluar los 3 parámetros de rendimiento (latencia, jitter y ancho de banda), se han realizado 10 repeticiones de las pruebas mencionadas y, posteriormente, se ha calculado la media de todas ellas. Con el objetivo de que las medias obtenidas reflejen de manera más precisa la realidad, dichas repeticiones se han llevado a cabo en distintos días y horas. La selección de los momentos específicos para realizar las pruebas se ha basado en los periodos de mayor actividad o críticos en el horario laboral y los fines de semana, ya que en esos momentos las redes pueden estar más congestionadas, lo que podría afectar el rendimiento del sistema. Más concretamente las pruebas se han realizado en los siguientes días:

- Lunes a las 08:30
- Lunes a las 18:00
- Martes a las 10:00
- Miércoles a las 12:30
- Miércoles a las 22:00
- Jueves a las 13:30
- Jueves a las 20:00
- Viernes a las 17:00
- Sábado a las 14:00
- Domingo a las 16:00

Además de realizar las pruebas en diferentes días y en diferentes horas, se ha medido cada parámetro en diferentes situaciones o escenarios. Se cree de interés medir el rendimiento del sistema en diferentes escenarios de tal manera que se pueda medir la influencia de algunos parámetros del sistema, como por ejemplo la disminución del rendimiento por la implementación de la VPN por la sobrecarga de los paquetes o el impacto de haber consumido el paquete de datos prioritarios. Una vez analizado las diferentes situaciones, se ha escogido el escenario más eficiente y cercano a la realidad que percibe el usuario final.

Una vez hechas las pruebas y calculado las medias, se espera que los parámetros en todos los casos cumplan con los siguientes valores [23] :

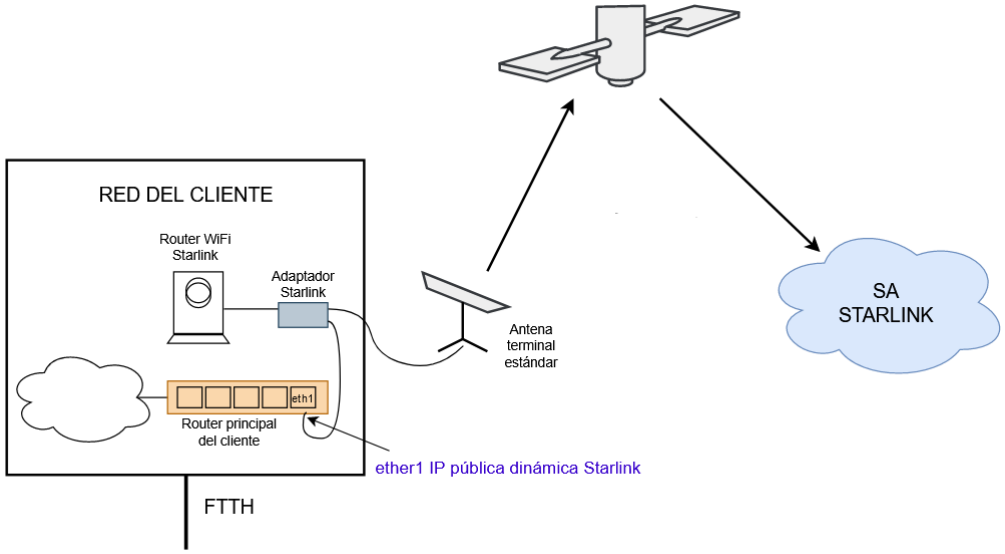
- Ancho de banda download: entre 40 y 220 Mbps
- Ancho de banda upload: entre 8 y 25 Mbps
- Latencia: entre 25 y 60 ms
- Jitter: menor de 30 ms

7.3 Implementación de la solución

Una vez finalizado el diseño de la solución, se puede proceder al desarrollo de la propuesta. A continuación, en este subapartado, se describe la implementación llevada a cabo en este proyecto.

7.3.1 Implementación del módulo 1: Red del cliente

Primero, se ha llevado a cabo el montaje de la red del cliente instalando la antena terminal Starlink junto con los equipos necesarios. El montaje es el siguiente:



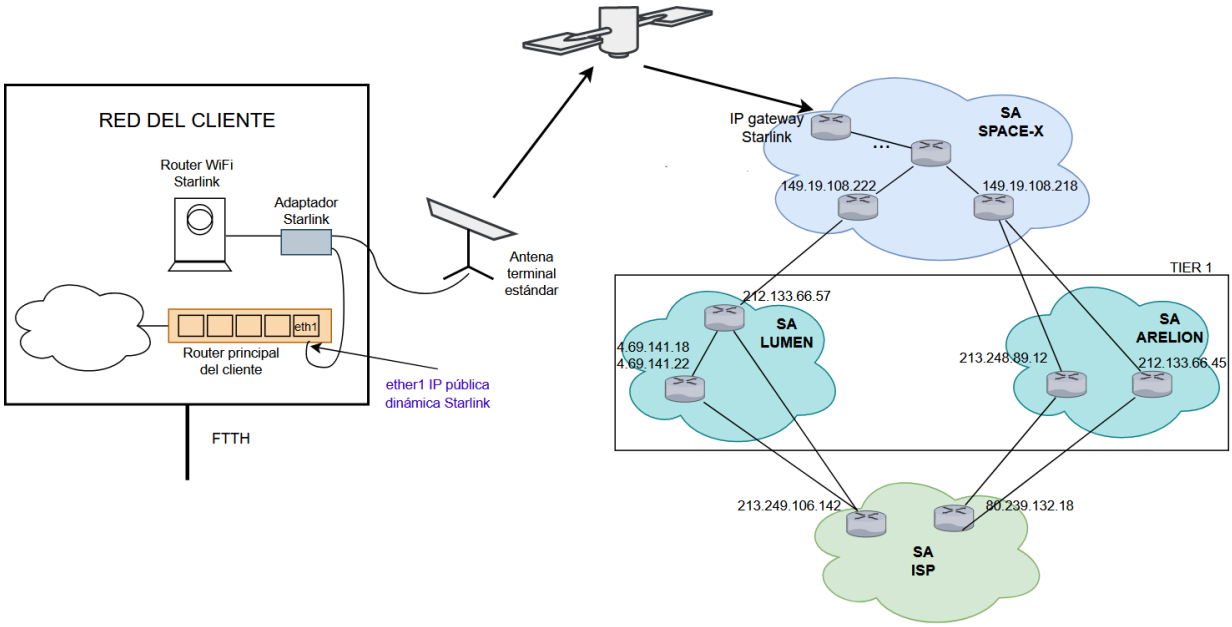
6. Imagen: Montaje red del cliente

Según las especificaciones, la antena terminal necesita 100° de campo de visión, por lo que lo primero a tener en cuenta es que se debe encontrar un lugar donde se tenga esta visibilidad completamente despejada del cielo. Esto es importante, ya que, si la antena encuentra alguna obstrucción, la conexión se verá afectada o incluso la antena no será capaz de establecer la conexión con el satélite. Una solución puede ser instalar la antena en un tejado. Una vez instalada, la propia antena cuenta con un sistema de orientación automática motorizada para encontrar la orientación óptima para establecer la conexión con la red de satélites Starlink.

La antena debe ser alimentada por PoE (*Power over Ethernet*) mediante el cable que también transmitirá los datos del cliente. En el kit escogido para este proyecto este cable debe ir conectado directamente al router WiFi Starlink, ya que es el propio router el que funciona como fuente de alimentación de la antena. Esta configuración sería para el caso en el que se quiera obtener acceso a Internet mediante WiFi (Escenario 1). Pero, el WiFi limita el ancho de banda que percibe el usuario final, por lo que Starlink ofrece una configuración llamada “Bypass” en la que se anula el WiFi y se debe añadir, entre la antena y el router WiFi de Starlink, un adaptador específico de tal manera que se obtiene un conector RJ45 para poder conectar el router del cliente. Aun así, con este tipo de antena, el router WiFi sigue siendo necesario para que le dé alimentación a la antena. De esta manera, el router WiFi se convierte en un elemento pasivo.

Finalmente, se ha conectado el conector RJ45 del adaptador al interfaz ether1 del router principal de la red del cliente. Esta interfaz será la que recibe la dirección IP pública de Starlink una vez se establece la conexión con la red satelital.

Una vez hecho todo el montaje, para comprobar su correcto funcionamiento se han realizado diversas pruebas de traceroute. Además, se ha analizado el camino que un paquete hace para llegar hasta la red del ISP. Ambos, el ISP escogido y Starlink, mantienen una relación de tránsito con dos Sistemas Autónomos de tier 1: Lumen y Arelion, entre otros. Por lo tanto, en las pruebas realizadas se han detectado diferentes posibles caminos los cuales se han resumido en la siguiente imagen:

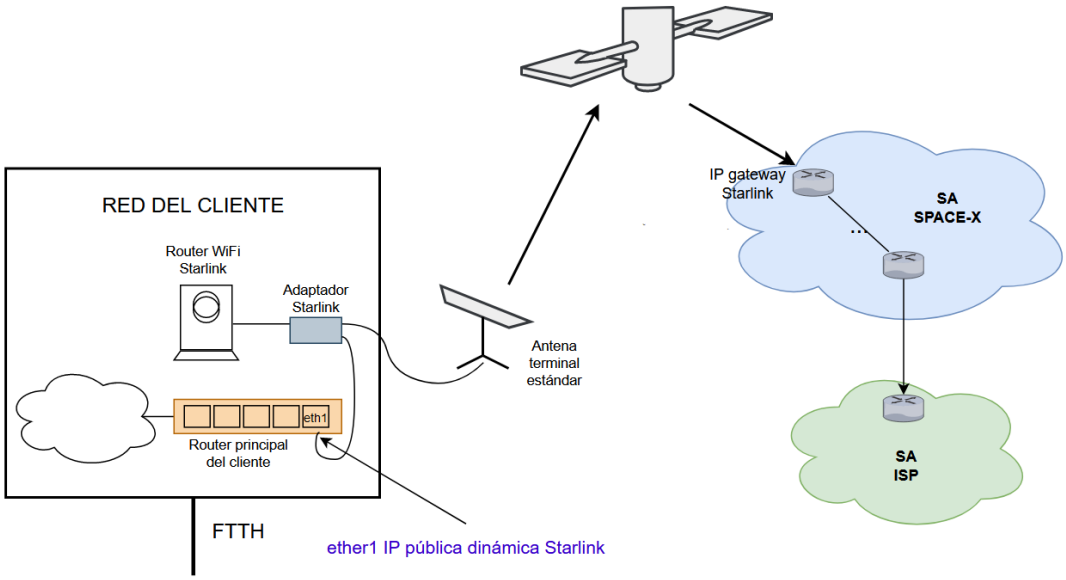


7. Imagen: Traceroute

Una vez analizado el recorrido predeterminado que deben realizar los paquetes entre la red del cliente y el ISP, se propone optimizar el tránsito entre ambos mediante el establecimiento de una relación de peering entre el Sistema Autónomo de Starlink y el Sistema Autónomo del ISP.

Cada salto puede añadir ciertos milisegundos de retraso en el paquete, por lo que, si se quiere reducir la latencia y el RTT, es deseable reducir la cantidad de saltos. Para ello, una de las mejores opciones es establecer peering entre Starlink y el ISP [15]. De esta manera, el Sistema Autónomo del ISP escogido y el Sistema Autónomo de Starlink estarán directamente conectados, sin la necesidad de tener que utilizar redes de tránsito y así, facilitar la conectividad entre las redes y optimizar el tráfico de datos mejorando la calidad de los servicios.

Se ha de mencionar que durante el desarrollo de este proyecto no se ha podido establecer el peering entre los dos Sistemas Autónomos, pero, si se quiere comercializar el sistema diseñado en este TFM se debería considerar hacer el contrato de peering para mejorar el rendimiento del sistema.



8. Imagen: Peering entre ISP y Starlink

7.3.2 Implementación del módulo 2: Conectividad cliente – ISP

Como se ha explicado anteriormente, la conectividad entre el cliente y el ISP se obtiene mediante una VPN. Esta VPN se compone por dos protocolos: WireGuard y EoIP. El primero ofrece mecanismos de cifrado de los datos ya autenticación de los extremos y el segundo ofrece un túnel de nivel 2 entre las dos redes. En este apartado se detalla la implementación de los dos protocolos.

- **WireGuard**

El funcionamiento de WireGuard se basa principalmente en un concepto llamado *Criptokey Routing*. Este mecanismo consiste en asociar claves públicas con una lista de direcciones IP que están permitidas dentro del túnel. Esa asociación se hace mediante el uso de unas tablas que se deben configurar a la hora de implementar el protocolo.

Para poner en funcionamiento WireGuard primero se debe crear una interfaz virtual tanto en el servidor como en el cliente. Al crear esta interfaz se le debe asignar un nombre y un valor de MTU que en este caso se ha utilizado el valor por defecto, 1420 bytes. En esta implementación los nombres asignados han sido *wireguard.104* en el caso del cliente *y WG-Server* en el caso del servidor. Cualquier interfaz WireGuard escucha en un puerto determinado y para este proyecto se ha escogido el puerto UDP 13262. Después de crear la interfaz virtual, se le debe asignar una dirección IP. Todos los clientes tienen una dirección IP asignada a su interfaz WireGuard del grupo 10.250.1.0/24 y el servidor mantiene la dirección IP 10.250.0.1.

Cada interfaz tiene una clave privada, una clave pública y una lista de peers los cuales se identifican por su propia clave pública. Al crear la interfaz se crean automáticamente una clave privada y, derivada de ella, una clave pública. La clave pública del servidor debe estar configurada en el peer de todos los clientes y la clave pública de los clientes en los peers del servidor. Estas claves se pueden intercambiar mediante archivos de configuración o por cualquier método fuera de banda.

Una vez configuradas las interfaces, se pueden crear los peers de WireGuard con los cuales se va a establecer la VPN. Como se ha mencionado anteriormente, el cliente tiene un único peer: el servidor. Para ello, se debe crear un peer asignado a la interfaz *wireguard.104*. Este peer tiene como identificador la clave pública del servidor y en la lista de direcciones IP permitidas tendrá configurada la IP 10.250.0.1/32. Para este proyecto es necesario que el cliente sea quien comience con el proceso de establecimiento del túnel, puesto que la IP del cliente puede cambiar y de esta manera, el servidor no tiene la necesidad de saber de antemano la IP del cliente. Además, para poder aplicar HA, en el cliente se debe configurar como endpoint con el que establecer la conexión el dominio con el que se identifican los servidores: wireguard1ba. El cliente, entonces, debe tener configurado un registro DNS estático para este dominio con la dirección pública de uno de los servidores. También debe tener un segundo registro de DNS, pero esta vez desactivado, con la dirección IP pública del otro servidor que va a funcionar como backup.

[Interface: *wireguard.104*]			
Interface Public Key	JqNs...1dpn		
Interface Private Key	**********		
Listening UDP Port	13262		
[Peers]			
Peer Public Key	**Allowed Source IPs**	**Endpoint**	**Persistent keepalive**
aDLn...q2fg	10.250.0.1/32	wireguard1ba:13262	00:00:05

6. Tabla: Configuración interfaz WireGuard del cliente

La configuración del servidor, en cambio, no tiene ningún endpoint inicial de sus peers (los clientes). Esto se debe a que el servidor descubre el punto final de sus pares examinando desde dónde se originan los datos correctamente autenticados. Si el propio servidor cambia su punto final y envía datos a los clientes, éstos descubrirán el nuevo punto final del servidor y actualizarán la configuración igualmente. Tanto el cliente como el servidor envían datos cifrados al punto final IP más reciente para el que han descifrado datos de forma auténtica. Por lo tanto, hay itinerancia IP completa en ambos extremos. Es por eso por lo que el peer asociado a este cliente en el servidor, únicamente debe tener configurado la clave pública del cliente y en la lista de direcciones IP permitidas la dirección del cliente: 10.250.1.4/32.

[Interface: *WG-Server*]			
Interface Public Key	aDLn...q2fg		
Interface Private Key	**********		
Listening UDP Port	13262		
[Peers]			
Peer Public Key	**Allowed Source IPs**	**Endpoint**	**Persistent keepalive**
JqNs...1dpn	10.250.1.4/32	-	-
...	...	...	...

7. Tabla: Configuración interfaz WireGuard del servidor

Cuando un paquete va a ser transmitido por una interfaz WireGuard, estas tablas son consultadas para determinar, por la dirección IP de destino, qué clave pública se debe usar para el cifrado del paquete. Es por eso que se dice que en el proceso de envío de un paquete la lista de direcciones IP permitidas funciona como una tabla de rutado.

En cambio, cuando la interfaz recibe un paquete cifrado, después de descifrarlo y autenticarlo mediante la clave pública, sólo aceptará el paquete si su IP de origen se encuentra dentro de las direcciones IP permitidas a ese peer. En esta ocasión, la lista de direcciones IP permitidas cumple la función de lista de acceso o Access control.

Una vez establecida la VPN WireGuard, se deberá ver en el lado del servidor como current-endpoint la dirección IP pública de Starlink que recibe el router del cliente en su interfaz ether1 y el puerto UDP 13262.

- **EoIP**

Una vez configurado el protocolo WireGuard tanto en el cliente como el servidor se debe implementar el túnel EoIP dentro de la VPN WireGuard, de tal manera que se encapsule primero una trama Ethernet en su totalidad y después, se le aplique el cifrado de WireGuard a todo el paquete encapsulado.

En este caso también, se debe crear interfaces virtuales la cuales actuan de interfaz túnel. El cliente tiene una interfaz denominada *eoip.104*, con el *tunnel-id* 104. Dado que el protocolo EoIP realiza fragmentación de forma autónoma, se debe configurar el MTU de esta interfaz en 1500 bytes. El tamaño máximo permitido que puede tener un paquete en enlaces físicos de Ethernet es 1500 bytes. El propio EoIP aplicará la fragmentación correspondiente teniendo en cuenta los bytes de las cabeceras que añade para que el paquete tenga en total 1500 bytes. Por ello, el MTU de EoIP debe ser 1500 bytes, de lo contrario EoIP fragmentaría paquetes de tamaño menor.

Como se ha dicho anteriormente, el túnel EoIP se establece dentro del túnel WireGuard. Por ello, las direcciones IP con las que se establece el túnel deben ser las asignadas a las interfaces de WireGuard. El cliente debe tener configurado como Local Address la dirección IP 10.250.1.4 y como Remote Address 10.250.0.1. El servidor tiene configurada la misma interfaz con el mismo *tunnel-id* asociado (104) pero con las direcciones IP intercambiadas: la dirección Local Address debe ser 10.250.0.1 y la dirección Remote Address 10.250.1.4.

Después de configurar el túnel EoIP se puede configurar la VLAN asociada al cliente en el extremo del ISP. Para ello, en el servidor se debe crear una VLAN denominada *vlan.104* con el mismo ID que el túnel EoIP: 104 y, posteriormente, crear un puente de red entre la interfaz *eoip.104* y la *vlan.104*. De esta manera, cuando el servidor reciba un paquete en la interfaz eoip.104 detectará que tiene un puente de red relacionado y enviará el paquete marcado por ese puente con el ID 104. Gracias a esta configuración se consigue que el tráfico del cliente sea tratado como si todo fuese de la misma red Ethernet.

Por último, se debe configurar la sesión BGP en el cliente para que este reciba las rutas necesarias. Como se ha explicado anteriormente, el cliente mantiene una sesión de tipo eBGP con uno de los

routers detrás del servidor de VPN configurado. Es por ello que se ha configurado como neighbour address una dirección IP interna de la red del ISP, la cual es la encargada de anunciar las rutas al cliente. También se debe configurar como remote AS el identificador del Sistema Autónomo del ISP escogido para este trabajo.

Una vez que se ha completado la configuración de todos los componentes del sistema, se debe verificar la integración de los túneles WireGuard y EoIP. Una vez que estos túneles se hayan establecido, el cliente debe recibir las rutas por el protocolo BGP, lo que permite que el cliente acceda a la conectividad a Internet mediante el servicio Starlink.

7.3.3 Implementación del módulo 3: Red del ISP

En este caso, se han instalado dos routers en la red del ISP que actúan como servidores de VPN y se le ha asignado a cada uno de ellos una dirección IP pública contra la que se establecen todos los túneles.

Para el establecimiento de los túneles los servidores deben escuchar en un puerto UDP, ya que uno de los protocolos escogidos es WireGuard. En esta ocasión, se ha escogido el puerto UDP 13262.

Además, como se ha explicado anteriormente, la configuración de los servidores debe estar duplicada en todo momento para ofrecer la propiedad de HA. Esto se consigue gracias a un script mediante el cual, cuando se quiere configurar un cliente nuevo, toda la configuración correspondiente se lleva a cabo en los dos servidores. Esta configuración abarca tanto la configuración necesaria para crear los túneles de WireGuard y EoIP, como la configuración de la VLAN correspondiente al cliente y la del protocolo BGP para anunciar al cliente las rutas necesarias. Toda la configuración se explica en el siguiente apartado.

7.4 Prueba de integración y validación del sistema

Con esta prueba se pretende comprobar que la configuración definida es adecuada y que todos los componentes y protocolos del sistema funcionan adecuadamente consiguiendo su integración.

Como se ha explicado, se han enviado mensajes ICMP mediante la herramienta ping para, primero, comprobar la conectividad entre el cliente y la red del ISP. Concretamente se han mandado mensajes ICMP Echo Request desde la red LAN del cliente (192.168.0.1) a una dirección IP pública dentro de la red del ISP (194.30.10.41). Puesto que se reciben los mensajes de ICMP Echo Reply, se puede concluir que tanto el túnel WireGuard como el túnel EoIP están establecidos y que, además, se ha establecido la sesión BGP y se han recibido las rutas necesarias para poder enviar y recibir estos mensajes. Adicionalmente, si se hace una prueba de traceroute desde el cliente hacia la misma dirección IP del ISP, se puede ver cómo la dirección IP del primer salto pertenece a la VLAN configurada dentro de la red del ISP y que, comparando con los resultados de las pruebas de traceroute hechas en el apartado de la implementación de la red del cliente, no se ven ninguna de las IPs de los saltos intermediarios del Sistema Autónomo Starlink, ya que el tráfico viaja por el túnel.

```
[sarenet@ETH6851904] /tool> ping 194.30.10.41
  SEQ HOST                                     SIZE TTL TIME       STATUS
    0 194.30.10.41                               56  62 33ms569us
    1 194.30.10.41                               56  62 36ms4us
    2 194.30.10.41                               56  62 34ms346us
    sent=3 received=3 packet-loss=0% min-rtt=33ms569us avg-rtt=34ms639us max-rtt=36ms4us
```

9. Imagen: Prueba de conectividad entre la red del cliente y el ISP

```
[sarenet@ETH6851904] > /tool/traceroute 194.30.10.41 src-address=192.168.0.1
Columns: ADDRESS, LOSS, SENT, LAST, AVG, BEST, WORST, STD-DEV
#  ADDRESS         LOSS  SENT  LAST    AVG   BEST  WORST  STD-DEV
1  10.100.67.190   0%       3  25.8ms  26.4  25.7  27.6   0.9
2  194.30.10.41    0%       3  31.8ms  30.4  27.7  31.8   1.9
```

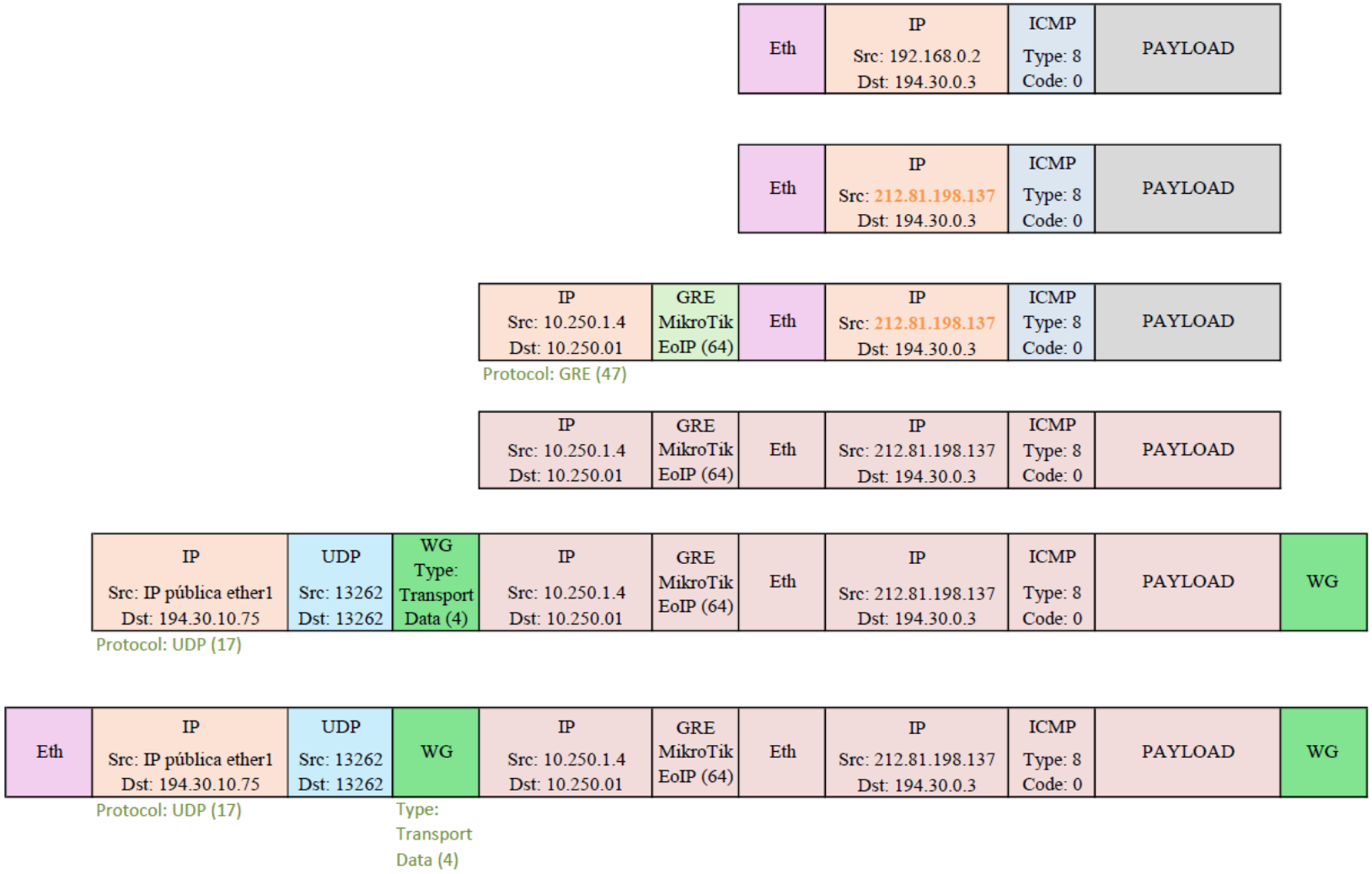
10. Imagen: Traceroute desde la red del cliente al ISP

Adicionalmente se ha usado la herramienta Wireshark para capturar el tráfico en diferentes interfaces mientras se envían los mensajes ICMP. En concreto, se ha capturado el tráfico en las interfaces virtuales *wireguard.104* y *eoip.104* y en la interfaz de salida *ether1*. Con ello se quiere ver que se aplican correctamente los protocolos WireGuard y EoIP y que se hace correctamente la integración entre los dos. Para ello, se ha analizado el formato de los paquetes que se envían y las operaciones que realiza tanto el router del cliente como el servidor.

A continuación, se describen las operaciones llevabas a cabo por el cliente:

1. El cliente crea la trama que contiene el mensaje ICMP con las cabeceras ICMP, IP y Ethernet.
2. Consulta la tabla de rutado y, dependiendo de la dirección IP de destino, escoge la ruta por defecto. La ruta por defecto indica que todo tráfico saliente se debe mandar por la interfaz *eoip.104*. Además, aplica NAT y cambia la dirección IP de origen a la IP pública del ISP asociada al cliente.
3. Aplica el protocolo EoIP:
    3.1. Añade la cabecera GRE indicando que el paquete de dentro es una trama Ethernet (EtherIP).
    3.2. Añade la cabecera IP utilizando los parámetros Remote Address y Local Address.
    3.3. Si es necesario, aplica la fragmentación.
4. Después, vuelve a consultar la tabla de rutado, pero en esta ocasión la dirección IP de destino es 10.250.0.1, por lo que coincide con el registro de la interfaz de *wireguard.104*.
5. Aplica el protocolo WireGuard:
    5.1. Consulta la tabla WireGuard y compara la dirección 10.250.0.1 con las listas de direcciones IP permitidas de todos sus peers. En este caso, el cliente tiene un único peer con una sola dirección: 10.250.0.1. En consecuencia, identifica el peer y obtiene la clave simétrica de envío.
    5.2. Encripta el paquete recibido desde la interfaz EoIP en su totalidad con la clave simétrica.
    5.3. Añade las cabeceras WireGuard.
5.4. Consulta el último endpoint guardado para ese peer. El endpoint, en este caso, es el dominio wireguard1ba, por lo que, seguido, consulta sus registros DNS y obtiene la IP del servidor. Con esta información añade las cabeceras IP y UDP.
6. Vuelve a consultar la tabla de rutado y esta vez, compara la dirección IP del servidor con sus rutas. Puesto que el cliente tiene rutas estáticas a los dos servidores en HA, sabe a dónde debe mandar el paquete. El gateway de estas rutas coincide con el gateway obtenido mediante DHCP en la interfaz ether1.
7. Por último, añade la cabecera Ethernet y manda la trama por la interfaz ether1.

En la siguiente figura (11. Imagen) se muestra el proceso anteriormente explicado:

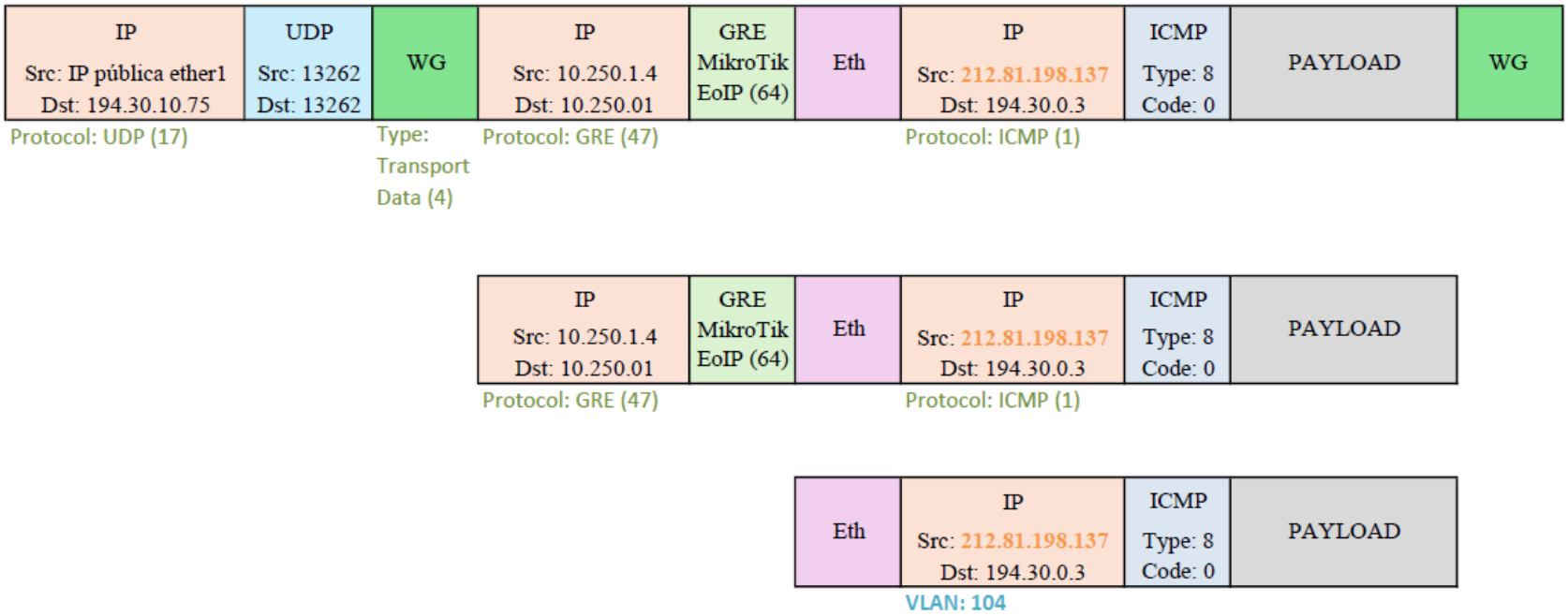


11. Imagen: Prueba integración en el router del cliente

El servidor recibe una trama en el puerto 13262:

1. Puesto que en el puerto 13262 el servidor mantiene la interfaz WG-Server escuchando, aplica el protocolo WireGuard:
    1.1. Analiza a cabecera WireGuard e identifica el peer correspondiente. Una vez identificado puede desencriptar el paquete con la clave simétrica de recepción. Si no puede identificar el peer, desencriptar el paquete o autenticarlo lo descarta.
    1.2. Si el paquete es autenticado, guarda la dirección IP de origen y el puerto UDP de origen de las cabeceras exteriores como último endpoint de ese peer (el cliente).
    1.3. Después, consulta si la dirección IP origen de la cabecera interna, la recientemente desencriptada, coincide con las direcciones permitidas de ese peer. En este diseño, se ha configurado como única IP permitida la 10.250.1.4, por lo que aceptará el paquete.
    1.4. Descarta las cabeceras WireGuard, IP y UDP.
2. A continuación, entrega el paquete sin las cabeceras de WireGuard a la interfaz *eoip.104*.
    2.1. Consulta la cabecera IP y comprueba que el parámetro *protocol* se ha establecido a 47 (GRE).
    2.2. Extrae los valores de la cabecera GRE e identifica que el paquete que se encuentra en el interior es una trama Ethernet entera.
    2.3. Descarta las cabeceras IP y GRE.
3. El servidor detecta que tiene un bridge configurado con la interfaz eoip.104 y la VLAN 104.
    3.1. Marca el paquete con el ID correspondiente a esa VLAN (104).
4. Envía el paquete por el bridge

En la siguiente figura (12. Imagen) se muestra el proceso anteriormente explicado:



12. Imagen: Prueba integración servidor del ISP

7.5 Análisis del rendimiento del sistema

Después de haber comprobado la integración de todos los componentes y la conectividad entre la red del cliente y el ISP, en este TFM se ha analizado el rendimiento del sistema diseñado.

Para ello, como se ha descrito anteriormente, se han analizado 3 parámetros por la importancia en el funcionamiento adecuado de las redes de telecomunicaciones: la latencia, el jitter y el ancho de banda. Estos parámetros han sido evaluados repetidamente en diferentes días y diferentes horas para, después, calcular un valor medio de cada uno de ellos y en diferentes escenarios para poder analizar la influencia de ciertos aspectos. Los escenarios son los siguientes:

- **Escenario 1**: Con salto WiFi entre la antena y el router del cliente.
- **Escenario 2**: La antena y el router del cliente conectados mediante cable, sin establecer la VPN y con datos prioritarios.
- **Escenario 3**: La antena y el router del cliente conectados mediante cable, con el túnel establecido y con los datos prioritarios.
- **Escenario 4**: La antena y el router del cliente conectados mediante cable, con el túnel establecido y con el paquete de datos prioritarios gastados.
- **Escenario 5**: La antena y el router del cliente conectados mediante cable, sin establecer la VPN y con el paquete de datos prioritarios gastados.

De esta manera, se quiere analizar también la influencia de establecer una VPN entre el cliente y el ISP, el impacto de haber consumido el paquete de los datos prioritarios y las limitaciones de ofrecer la conectividad a Internet mediante WiFi en vez de por cable. Para analizar esto último, se debe instalar el router WiFi de Starlink. Starlink ofrece también la posibilidad de conectar directamente la antena a un router propio de Starlink el cual únicamente ofrece WiFi para dar conectividad a los usuarios.

En esta sección se presentan y se analizan las medias calculadas de los tres parámetros en cada uno de los escenarios previamente mencionados. En todos los casos, se deben considerar los valores esperados de los parámetros medidos:

- Ancho de banda download: entre 40 y 220 Mbps
- Ancho de banda upload: entre 8 y 25 Mbps
- Latencia: entre 25 y 60 ms
- Jitter: menor de 30 ms

En la siguiente tabla (8. Tabla) se presenta un resumen de las medias calculadas:

Rendimiento del sistema	Latencia		Jitter		Upload	Download
	Google	ISP	Google	ISP		
Escenario 1	48,90 ms	43,10 ms	4,13 ms	4,38 ms	30 Mbps	89 Mbps
Escenario 2	29,48 ms	35,02 ms	4,01 ms	3,97 ms	49,94 Mbps	229,62 Mbps
Escenario 3	47,92 ms	41,57 ms	4,05 ms	4,60 ms	17,88 Mbps	200,82 Mbps
Escenario 4	44,83 ms	36,90 ms	4,26 ms	3,93 ms	16,47 Mbps	203,19 Mbps
Escenario 5	30,57 ms	31,10 ms	3,96 ms	4,43 ms	43,45 Mbps	232,41 Mbps

8. Tabla: Resumen de valores del análisis del rendimiento del sistema

- **Escenario 1**:

En el escenario 1, aunque el ancho de banda de subida y bajada se encuentra dentro de los límites establecidos, se observa claramente una limitación debido al WiFi, ya que el router WiFi de Starlink ofrece únicamente hasta 100 Mbps. La latencia en ambos casos se encuentra dentro de los valores esperados; sin embargo, se obtienen valores más altos que en los demás escenarios, lo cual se debe también principalmente a la tecnología WiFi. En cuanto al jitter, se puede afirmar que es considerablemente menor que el límite establecido de 30 ms.

- **Escenario 2**:

El escenario 2 sirve de referencia para los demás casos, ya que se trata de una configuración simple. Conectando el router del cliente y la antena mediante el cable se evita cualquier límite por tecnología de transmisión de datos y al no implementar ninguna tecnología adicional, como puede ser la VPN, se obtienen los valores que Starlink provee a sus usuarios. Es así que el bandwidth obtenido supera los valores esperados tanto en upload como en download. Esto se debe a que se ha contratado un servicio con datos prioritarios y en el lugar donde se ha escogido instalar el sistema no existe sobrecarga de clientes Starlink, por lo que no existe competitividad para conseguir los recursos de Starlink. En este caso, el jitter también se encuentra significativamente por debajo de los 30 ms, con valores similares entre el cliente y Google, y entre el cliente y el ISP, siendo de aproximadamente 4 ms. Además, este escenario presenta la latencia más baja en comparación con los demás escenarios. Cabe destacar que la latencia hacia Google es más baja que hacia la red del ISP, debido a que un paquete debe realizar menos saltos entre el Sistema Autónomo de Starlink y el Sistema Autónomo de Google que hacia el Sistema Autónomo del ISP.

- **Escenario 3**:

Por otro lado, el escenario 3 representa la implementación en su totalidad del sistema diseñado en este trabajo. Comenzando por el ancho de banda, se ve una clara bajada de 30 Mbps tanto en el ancho de bando de subida como en el de bajada, debido al procesamiento y sobrecarga adicional de los paquetes por la VPN. Como se ha explicado, los protocolos escogidos para la implementación de la VPN añaden ciertas cabeceras a los paquetes lo que supone un mayor procesamiento a la hora de transmitir paquetes y, por consiguiente, el ancho de banda efectivo se reduce. Además, se aplican protocolos de cifrado y descifrado entre otros mecanismos, lo que hace que el procesamiento de los paquetes sea más lento y la latencia sea mayor que en el escenario 2. Aun así, se mantiene dentro de los límites establecidos por lo que se puede decir que este aumento es

aceptable. Es interesante mencionar que en este caso la latencia obtenida hacia la red del ISP es menor que la latencia obtenida hacia la red de Google, ya que todo el tráfico saliente del cliente se envía primero a los terminadores de la VPN en a la red del ISP. En cuanto al jitter se detecta también un cierto aumento respecto al escenario 2 pero sigue siendo considerablemente menor que 30 ms.

- **Escenario 4 y 5**:

Por último, en el escenario 4 no se han detectado grandes cambios respecto al escenario 3. Esto se debe a que se ha contratado un servicio con datos prioritarios y en el área seleccionada para la instalación del sistema actualmente no hay una saturación de clientes de Starlink, por lo que no hay competencia por los recursos de Starlink y se obtienen valores similares a los obtenidos en el caso en el que el sistema completo está desplegado. Por la misma razón, en el escenario 5 tampoco se observan grandes cambios respecto al escenario 2. Si aumenta la cantidad de usuarios de Starlink, es posible que en el futuro se obtengan valores inferiores a los aquí presentados puesto que, una vez agotado el paquete de datos prioritarios, se pierde la prioridad y se debe competir con los demás usuarios de alrededor.

En conclusión, cogiendo de referencia el escenario 2 se ha visto que ofrecer al usuario final en la red LAN conectividad a Internet mediante WiFi limita a la mitad el ancho de banda y, por lo tanto, se puede decir que no es una opción efectiva. Cuando se añade una VPN para ofrecer seguridad a las comunicaciones del cliente se percibe también una bajada del ancho de banda, de unos 30 Mbps. Aun así, se considera que este escenario es totalmente aceptable puesto que la seguridad es un requisito para el diseño del sistema y los parámetros de rendimiento se mantienen dentro de las condiciones establecidas. Además, en este mismo escenario el jitter se encuentra significativamente por debajo del límite establecido y se mantiene en unos 4 ms, lo que hace que el usuario final sea capaz de hacer uso de servicios con requisitos de red exigentes, como lo son las aplicaciones de video y voz.

Por último, se puede concluir que en el momento del desarrollo de este proyecto el hecho de gastar el paquete de datos prioritarios contratado no supone ningún cambio, puesto que la red de Starlink no se encuentra saturada y se pueden optar a los mismos recursos de la red Starlink.

En resumen, el sistema diseñado e implementado en este trabajo cumple con todas las condiciones establecidas tanto de funcionamiento como de rendimiento. En concreto, cogiendo el escenario 3 como la implementación en su totalidad del sistema diseñado en este trabajo, el sistema obtiene los siguientes resultados:

- Latencia: entre 40 ms y 50 ms
- Bandwidth upload: 17,88 Mbps
- Bandwidth download: 200,82 Mbps
- Jitter: entre 4 ms y 5 ms

7.6 Optimización de la implementación

En este trabajo se propone también añadir ciertas configuraciones para conseguir la optimización de la implementación llevada a cabo. A continuación, se indican los aspectos que han sido objeto de ajuste en este TFM.

- Time sensitive:

WireGuard es un protocolo sensible al tiempo, por lo que cualquier desfase temporal puede afectar al funcionamiento de este.

Una de las principales características de WireGuard es que evita el almacenamiento de cualquier estado previo a la autenticación y, por lo tanto, no envía ninguna respuesta a paquetes no autenticados. Sin embargo, esta propiedad requiere que el primer mensaje recibido autentique al iniciador [24].

Para evitar esto, se incluye una marca de tiempo cifrada y autenticada en el primer mensaje del handshake. El receptor lleva la cuenta de la mayor marca de tiempo recibida por cada peer y descarta los paquetes que contengan marcas de tiempo inferiores o iguales a ella [24].

Es por eso que, un desfase temporal puede incluso causar que no se establezca el túnel WireGuard. A la hora del establecimiento del túnel si el iniciador no tiene sincronizada la hora, el receptor recibirá un mensaje handshake initiation que, a pesar de ser autenticado, contiene una marca de tiempo inferior a la del receptor y, por lo tanto, descartará el mensaje y no se establecerá el túnel. Esto no sucede si el iniciador hace un cierre ordenado del túnel, puesto que, de esta manera el servidor borrará la información guardada para ese peer y el servidor aceptará el próximo handshake de ese peer.

Un claro ejemplo de esta situación puede ser un cliente el cual pierde la alimentación por un tiempo prolongado. En este caso, el cliente se apagará y perderá, lógicamente, la repentinamente conexión sin avisar al servidor, por lo que no se realizará un cierre ordenado del túnel. Puesto que anteriormente el túnel estaba establecido, el servidor tendrá guardado para ese peer un endpoint address, un endpoint port y una marca de tiempo y, además, mantendrá la sesión anterior activa. Al estar la sesión activa, pasado un cierto tiempo sin recibir ningún paquete del cliente, el servidor intentará mandar mensajes de handshake initiation al endpoint que tiene guardado, por lo que se verá esta conexión activa en el firewall del servidor. Si después de un lapso de tiempo el cliente vuelve a recuperar la alimentación mantendrá la hora en la que ha sido desconectado y si la dirección IP que recibe en la interfaz de salida o incluso la dirección con la que se hace NAT ha cambiado, el servidor rechazará los mensajes de handshake nuevos puesto que estos tendrán una marca de tiempo menor a la anteriormente guardada.

Para evitar esto, en este trabajo se propone hacer uso del protocolo NTP (*Network Time Protocol*).

En el cliente es necesario tener acceso, mediante el gateway recibido por DHCP, a los terminadores de WireGuard sin haber recibido ninguna ruta por BGP para poder establecer el túnel. Es por ello que, se propone configurar los servidores WireGuard como servidores NTP. En el ejemplo anterior,

el cliente al recuperar la alimentación, primero sincronizará la hora con el servidor WireGuard y una vez tenga la hora sincronizada, el servidor aceptará las peticiones de handshake del cliente.

En este caso, como el sistema se ha desplegado en HA, a la hora de configurar el servidor NTP se debe definir el dominio *wireguard1ba* de tal manera que se pueda cambiar entre servidores sin ningún problema.

- Sobrecarga:

Generalmente, cuando se implementa un protocolo de VPN el rendimiento se ve afectado. Esto se debe, entre otras cosas, a la sobrecarga que suponen estos protocolos en relación al procesado de las cabeceras que se añaden y se deben procesar. En este caso, EoIP añade 42 bytes en las cabeceras IP, GRE y Ethernet y WireGuard añade otros 60 bytes en las cabeceras IP, UDP y WireGuard.

EoIP aplica la fragmentación de paquetes de manera transparente, por lo que, aunque el paquete que se quiera mandar tenga un tamaño que sobrepase los 1550 bytes de MTU de la capa física, EoIP aplicará la fragmentación y el paquete podrá ser transmitido.

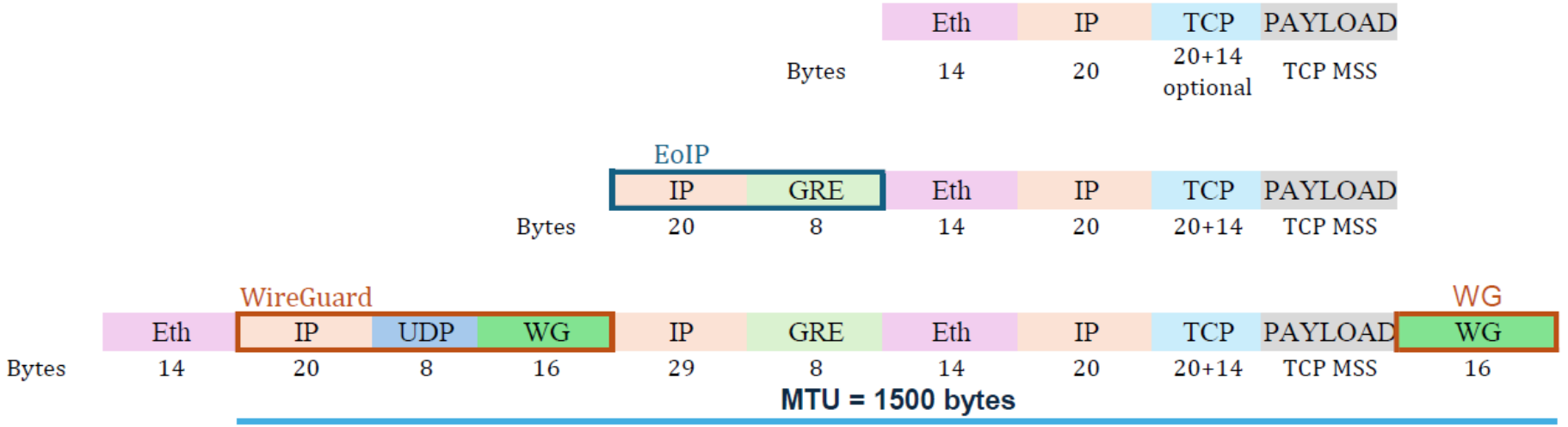
Aun así, al añadir tanta sobrecarga a todos los paquetes, la cantidad de paquetes que puedan sobrepasar el MTU de 1500 bytes es mayor y, en consecuencia, los equipos deberán aplicar en su interfaz EoIP la fragmentación más veces de lo habitual disminuyendo así el rendimiento.

Con el objetivo de aliviar el procesamiento de los paquetes en los equipos, en este trabajo se propone un ajuste del valor MSS (*Maximum Segment Size*).

El MSS es la cantidad máxima de bytes que un equipo puede aceptar en un segmento TCP. El protocolo TCP cuenta con un método que permite que ambos extremos de una conexión negociar el valor de MSS a utilizarse cuando se establece una conexión. Para hacerlo, cada extremo utiliza el campo OPTIONS de la cabecera TCP para proponer un MSS. El MSS que finalmente se adopta es el menor de los valores sugeridos por ambos extremos.

Durante el desarrollo de este TFM, se ha hecho el cálculo del valor máximo de bytes que un segmento puede tener teniendo en cuenta las cabeceras de los dos protocolos WireGuard y EoIP. Este cálculo se ha realizado tomando como base en el tamaño de MTU de la interfaz física de red (1500 bytes) y restando el tamaño de las cabeceras de los protocolos de VPN, IPv4 y la propia cabecera de TCP.

Teniendo en cuenta los diferentes tamaños de las cabeceras, el valor de MSS se ha fijado en 1344 bytes:



13. Imagen: Cálculo TCP MSS

8 PLANIFICACIÓN

En este apartado se presenta la planificación seguida para llevar a cabo el proyecto. Para desarrollar con éxito cualquier proyecto es conveniente dividir el desarrollo del proyecto en fases y tareas. Por ello, el desarrollo de este proyecto se dividirá en paquetes de trabajo y tareas.

En primer lugar, se presenta el equipo de trabajo. A continuación, se describen cada uno de los paquetes de trabajo (PT) y las tareas (T) correspondientes a cada paquete de trabajo. El tiempo invertido en cada paquete de trabajo y tarea se indica en horas. En cada paquete de trabajo, además, se establecen algunos hitos para poder realizar un seguimiento del desarrollo del proyecto. Por último, en este apartado se presenta un diagrama de Gantt con todas las tareas y paquetes de trabajo anteriormente descritas.

8.1 Equipo de proyecto y recursos técnicos

A continuación, en la tabla siguiente (9. Tabla), se muestra el equipo de trabajo encargado tanto del diseño, implementación y análisis de la solución propuesta en este proyecto, como de la redacción de la documentación pertinente.

Nombre y apellidos	Nivel	Responsabilidad
Higuero Aperribai, María Victoria	Ingeniera superior (L1)	Directora de proyecto
Omagojeaskoa Insunza, Jon Mikel	Ingeniero superior (L1)	Director técnico de la empresa
Aguiar Bilbao, Irati	Ingeniera junior (L2)	Proyectista

9. Tabla: Equipo de proyecto

El nivel se clasifica en L1 y L2, y dicha clasificación indica lo siguiente:

- **Nivel de conocimiento L1**:

Ingeniera senior con un alto nivel de conocimiento en el campo de las Telecomunicaciones. Su principal función es guiar a la proyectista, estableciendo las pautas y tareas esenciales para asegurar un desempeño exitoso del proyecto. Como directora de proyecto define el plan de trabajo y los objetivos a alcanzar, supervisa las tareas de la proyectista y se encarga de corregir y evaluar la documentación del proyecto.

- **Nivel de conocimiento L2**:

Ingeniera junior en Telecomunicaciones, con conocimientos adecuados para el diseño e implementación de la solución descrita en este documento. Su función es llevar a cabo las tareas del proyecto y seguir las instrucciones de la directora para lograr los objetivos fijados. Desempeñará las tareas asignadas por la directora del proyecto y redactará los informes necesarios para la elaboración del documento final del Trabajo Fin de Máster.

8.2 Descripción de paquetes de trabajo y tareas

Como se ha indicado anteriormente, la planificación del proyecto consta de diferentes paquetes de trabajo (PT) y, a su vez, cada paquete de trabajo está compuesto por diferentes tareas (T). En los siguientes apartados se describe cada paquete de trabajo y cada tarea con su duración correspondiente.

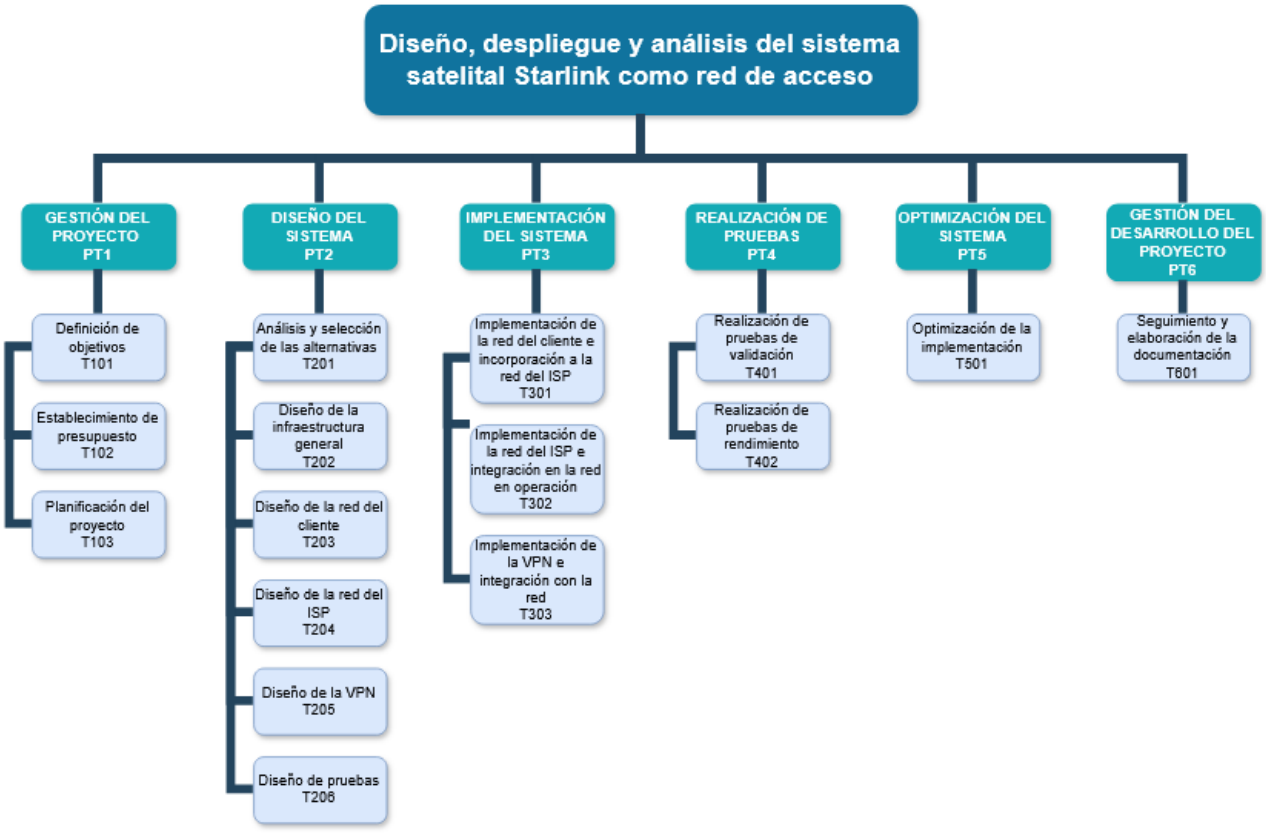
El proyecto comienza el 1 de septiembre de 2023 y finaliza el día 6 de junio de 2024 con la entrega de la memoria final del proyecto. En la tabla mostrada a continuación (10. Tabla) se pueden observar las fechas de inicio y fin de proyecto, así como la duración y la carga de trabajo del mismo.

Fecha de inicio	Fecha de finalización	Duración	Carga de trabajo
1 de septiembre de 2023	6 de junio de 2024	200 días	728 horas

10. Tabla: Resumen duración del proyecto

Para facilitar la compresión de la planificación del proyecto, a continuación, se presenta un diagrama WBS (14. Imagen). Este diagrama permite organizar de manera visual las diferentes actividades que conforman el desarrollo del proyecto.

El proyecto se compone de 6 paquetes de trabajo, cada uno conformado por diversas tareas. A cada paquete se le ha asignado un código con el prefijo "PT" y a cada tarea se le ha asignado un código con el prefijo "T". Este sistema de codificación se ha implementado con el objetivo de mejorar la identificación de cada paquete de trabajo y cada tarea a lo largo de la planificación del proyecto.



14. Imagen: Diagrama WBS

A continuación, se detallan cada uno de los paquetes de trabajo y las tareas correspondientes, junto con los recursos humanos y técnicos asignados, así como la duración y la carga de trabajo de cada uno de ellos.

PT1 - GESTIÓN DEL PROYECTO

Este paquete de trabajo incluye las tareas iniciales del desarrollo del proyecto. En ellas, se establecen los objetivos a alcanzar durante el desarrollo del proyecto, el presupuesto para alcanzar los objetivos y la planificación necesaria para la realización del trabajo en el plazo adecuado.

Duración total: 60 h

- **T101 - Definición de objetivos**

Esta tarea consiste en definir los objetivos que se quieren lograr con el desarrollo del proyecto.

  - Recursos humanos: directora de proyecto y proyectista
  - Recursos técnicos: PC
  - Duración: 5 días
  - Carga de trabajo: 20 h

- **T102 - Establecimiento de presupuesto**

Esta tarea es ejecutada al comienzo de la duración del proyecto para calcular el coste que va a suponer su realización y desarrollo. Tiene que ser tenido en cuenta a lo largo del proyecto para el establecimiento de medidas correctoras en caso de ser requerido (imprevistos, retrasos...).

  - Recursos humanos: directora de proyecto y proyectista
  - Recursos técnicos: PC
  - Duración: 5 días
  - Carga de trabajo: 20 h

- **T103 - Planificación del proyecto**

En esta tarea se plantean las pautas de trabajo y la organización necesaria para llevar a cabo dicho desarrollo. Se desglosa todo el desarrollo del proyecto en diferentes paquetes de tareas y se establecen los plazos disponibles para cada uno.

  - Recursos humanos: proyectista
  - Recursos técnicos: PC
  - Duración: 5 días
  - Carga de trabajo: 20 h

- **H1 – Documento de objetivos, presupuesto y planificación del proyecto**

PT2 - DISEÑO DEL SISTEMA

Este paquete de trabajo constituye una de las fases de mayor importancia en el proyecto, puesto que incluye todas las tareas de diseño del sistema. Estas tareas abarcan desde el diseño de todos los componentes del sistema hasta el diseño de las pruebas que se han realizado después de desplegar el sistema.

Duración total: 145h

- **T201 - Análisis, valoración y selección de las alternativas**

Una parte importante del proyecto consiste en analizar las diferentes alternativas que deben valorarse a la hora de realizar el diseño e implementación, evaluar las características de cada una de ellas, y seleccionar finalmente aquella que mejor se adapte a las necesidades de cada escenario. Esta parte resulta fundamental para elaborar el análisis de alternativas y el posterior diseño de la solución.

  - Recursos humanos: proyectista
  - Recursos técnicos: Internet, artículos de investigación, PC
  - Duración: 10 días
  - Carga de trabajo: 20 h

- **T202 – Diseño de la infraestructura general**

Esta tarea consiste en diseñar la infraestructura general de la solución propuesta en este trabajo, para después, diseñar cada componente individualmente.

  - Recursos humanos: proyectista
  - Recursos técnicos: Internet, artículos de investigación, PC
  - Duración: 5 días
  - Carga de trabajo: 10 h

- **T202 - Diseño de la red del cliente**

Esta tarea consiste en la definición de todas las características correspondientes a la red del cliente. Teniendo en cuenta los objetivos del proyecto, se deben determinar los requisitos y configuraciones de las tecnologías necesarias.

  - Recursos humanos: proyectista
  - Recursos técnicos: PC
  - Duración: 40 días
  - Carga de trabajo: 30 h

- **T203 - Diseño de la red del ISP**

Esta tarea consiste en la definición de todas las características correspondientes a la red del ISP. Teniendo en cuenta los objetivos del proyecto, se deben determinar los requisitos y configuraciones de las tecnologías necesarias.

  - Recursos humanos: proyectista
  - Recursos técnicos: PC
  - Duración: 40 días
  - Carga de trabajo: 30 h

- **T204 - Diseño de la VPN**

Esta tarea consiste en la definición de todas las características correspondientes a la VPN entre la red del cliente y el ISP. Esta tarea abarca tanto las características y configuraciones necesarias de la VPN, con mecanismos de cifrado y autenticación, como las características y configuraciones necesarias del túnel de nivel 2 del modelo TCP/IP.

  - Recursos humanos: proyectista
  - Recursos técnicos: PC
  - Duración: 40 días
  - Carga de trabajo: 40 h

- **T205 - Diseño de las pruebas de validación y rendimiento**

Esta tarea consiste en la definición de las pruebas de validación y de rendimiento que se han realizado en el despliegue del sistema. Esta parte resulta fundamental para obtener resultados significativos y ajustados a la realidad.

Por un lado, se deben definir las pruebas de validación, con el objetivo de validar la conectividad entre el cliente y el ISP. Por otro lado, se deben definir también las pruebas de rendimiento para analizar el rendimiento del sistema. En esta ocasión se deben establecer, además, los parámetros que definen el rendimiento del sistema y los valores esperados de cada uno de ellos.

  - Recursos humanos: proyectista
  - Recursos técnicos: PC
  - Duración: 10 días
  - Carga de trabajo: 15 h

- **H2 - Descripción del diseño de la solución**

PT3 - IMPLEMENTACIÓN DEL SISTEMA

Este paquete de trabajo incluye las tareas necesarias para llevar a cabo la implementación del sistema diseñado, instalando y configurando desde la red del cliente, el protocolo de VPN, el protocolo de túnel de nivel 2, hasta los terminadores en la red del ISP, todo ello sobre la infraestructura actual en operación de la red del ISP escogido.

Duración total: 185 h

- **T301 – Implementación de la red del cliente e incorporación a la red del ISP**

En esta tarea se lleva a cabo la instalación y configuración de los equipos de la red del cliente: la antena terminal Starlink y los equipos añadidos, y el router de salida de la red del cliente. Además, se debe incorporar esta red a la red actual en operación del ISP.

  - Recursos humanos: proyectista
  - Recursos técnicos: PC, kit Starlink, router del cliente, cableado
  - Duración: 15 días
  - Carga de trabajo: 35 h

- **T302 – Implementación de la red del ISP e integración en la red en operación**

En esta tarea se lleva a cabo la instalación y configuración de los terminadores de VPN en la red del ISP. Los terminadores se deben implementar en HA en la infraestructura ya desplegada del ISP.

  - Recursos humanos: proyectista
  - Recursos técnicos: PC; terminadores, cableado
  - Duración: 15 días
  - Carga de trabajo: 25 h

- **T303 – Implementación de la VPN e integración con la red**

En esta tarea se lleva a cabo toda la configuración pertinente para la implementación de los protocolos de VPN y de tunelado, para conseguir la confidencialidad y autenticación, y el túnel de nivel 2, respectivamente. Además, se debe integrar la VPN creada a la infraestructura en operación del ISP.

  - Recursos humanos: proyectista
  - Recursos técnicos: PC, router del cliente, terminadores, cableado
  - Duración: 15 días
  - Carga de trabajo: 40 h

- **H3 – Despliegue del sistema**

PT4 - REALIZACIÓN DE LAS PRUEBAS

Este paquete de trabajo incluye las tareas necesarias para llevar a cabo las pruebas de validación y de rendimiento diseñadas en el PT2 en el despliegue realizado en el paquete de trabajo anterior (PT3).

Duración total: 98 h

- **T401 - Realización de pruebas de validación**

En esta tarea se comprueba la correcta conectividad entre el cliente y el ISP. Para ello, se genera tráfico desde la red del cliente para después comprobar que este tráfico llega correctamente a los terminadores de VPN situados en la red del ISP. Además, se comprueba la correcta integración entre las tecnologías implementadas tanto de VPN como de tunelado de nivel 2 para la conectividad.

  - Recursos humanos: proyectista
  - Recursos técnicos: PC, kit Starlink, router del cliente, terminadores, cableado
  - Duración: 15 días
  - Carga de trabajo: 40 h

- **T402 - Realización de pruebas de rendimiento**

En esta tarea se llevan a cabo las pruebas de rendimiento diseñadas en la tarea T205. Concretamente, se realizan medidas de latencia, jitter y bandwidth del sistema en diferentes escenarios, para después calcular las medias de dichos resultados y poder comparar los escenarios identificando la influencia de diferentes parámetros.

  - Recursos humanos: proyectista
  - Recursos técnicos: PC, kit Starlink, router del cliente, terminadores, cableado
  - Duración: 30 días
  - Carga de trabajo: 58 h

- **H4 – Documento de análisis de pruebas de validación y de rendimiento**

PT5 - OPTIMIZACIÓN DEL SISTEMA

Este paquete de trabajo incluye la tarea correspondiente para llegar a la optimización de la implementación llevada a cabo en el paquete de trabajo PT3.

Duración total: 40 h.

- **T501 - Optimización de la implementación**

Esta tarea consiste en realizar los ajustes necesarios para conseguir la optimización de la implementación hecha. Para ello, se propone añadir las configuraciones necesarias. Estas configuraciones son mejoras en relación a distintos aspectos identificados en la implementación del sistema.

  - Recursos humanos: proyectista
  - Recursos técnicos: PC, kit Starlink, router del cliente, terminadores, cableado
  - Duración: 15 días
  - Carga de trabajo: 40 h

- **H5 – Implementación de la optimización**

PT6 - GESTIÓN DEL DESARROLLO DEL PROYECTO

Este paquete de trabajo incluye una seria de tareas que se centran en la organización y gestión del trabajo a realizar dentro del mismo.

Duración total: 200 h.

- **T601 - Seguimiento y elaboración de la documentación**

Esta tarea abarca todo el trabajo de puesta en marcha, seguimiento del desarrollo, finalización y cierre del proyecto para garantizar el existo del mismo. Además, en esta tarea la proyectista realiza también el documento que recoge toda la información del proyecto y que consiste en este documento de memoria del TFM.

  - Recursos humanos: directora de proyecto y proyectista
  - Recursos técnicos: PC
  - Duración: 200 días
  - Carga de trabajo: 200 h

- **H6 – Memoria y entrega final del proyecto**

8.3 Diagrama de Gantt

En este apartado del documento, la planificación seguida se representa mediante un diagrama de Gantt. Este diagrama permite visualizar gráficamente los paquetes de trabajo y las tareas descritas anteriormente, así como el tiempo dedicado a las mismas.

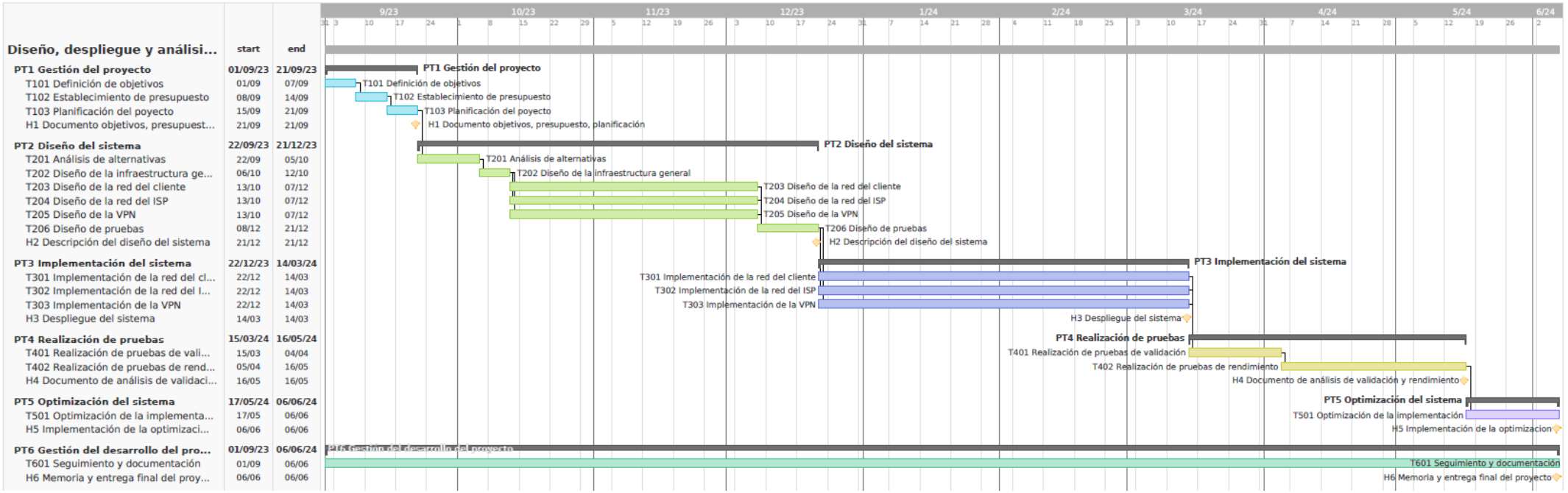
Como se ha mencionado anteriormente, el proyecto comienza el 1 de septiembre de 2023 y finaliza el 6 de junio de 2024 con la entrega del proyecto y la documentación correspondiente.

En lo referente a los hitos del proyecto, se han definido los mostrados en la siguiente tabla (11. Tabla) :

Código	Descripción
H1	Documento de objetivos, presupuesto y planificación
H2	Descripción del diseño de la solución
H3	Despliegue del sistema
H4	Documento de análisis de pruebas de validación y rendimiento
H5	Implementación de la optimización
H6	Memoria y entrega final del proyecto

11. Tabla: Resumen de hitos del proyecto

A continuación, se muestra el diagrama de Gantt de la planificación de este proyecto:



15. Imagen: Diagrama de Gantt

9 ANÁLISIS DE COSTES

Una vez descrita la planificación del proyecto, en este apartado se realiza un resumen de los costes derivados del desarrollo del proyecto. En primer lugar, se desglosan los costes de los recursos humanos. Posteriormente, se exponen los costes de los recursos materiales separados en amortizaciones y gastos. Por último, se presenta un resumen del coste total del proyecto.

9.1 Horas internas

Este apartado se refiere a los costes de recursos humanos pertenecientes al equipo que ha llevado a cabo el proyecto.

Los costes de recursos humanos se han calculado considerando las horas dedicadas al proyecto por cada miembro del equipo y la tasa horaria de cada uno de ellos. En la siguiente tabla (12. Tabla) se muestra la distribución de los costes de los recursos humanos:

Concepto	Número de horas	Coste unitario (IVA incluido)	Coste total (IVA incluido)
Ingeniera junior	500 h	13 €/h	6.500,00 €
Ingeniera senior (x2)	228 h	40 €/h	9.120,00 €
TOTAL (IVA incluido)			**15.620,00 €**

12. Tabla: Coste horas internas del proyecto

9.2 Amortizaciones

Además de los costes en recursos humanos, se deben de tener en cuenta los costes de los recursos materiales utilizados en el desarrollo del proyecto. En la siguiente tabla (13. Tabla) se describen los recursos de equipamiento utilizados en el desarrollo de este proyecto:

Material	Descripción	Cantidad
Kit de Starlink	Consiste en la antena terminal Starlink, el adaptador, el router WiFi y los cables Starlink necesarios.	1
Router del cliente	Router principal del cliente.	1
Terminadores VPN	Routers situados en la red del ISP cumpliendo las funciones de terminadores de VPN.	2
PC	Ordenador personal para los trabajos de la proyectista	1
Cableado	Cables Ethernet necesarios para conectar los routers tanto de la red del cliente como del ISP.	1

13. Tabla: Recursos técnicos

Por lo tanto, se calcula un coste unitario por cada material utilizado, considerando el coste total de cada uno de ellos y su vida útil. Se considera que un año de vida útil equivale a 1760 horas laborables. El coste unitario de las amortizaciones de este proyecto se muestra en la siguiente tabla (14. Tabla):

Amortizaciones	Coste (IVA incluido)	Vida útil	Coste unitario (IVA incluido)
Kit Starlink	429,00 €	5 años	0,049 €/h
Router cliente	300,00 €	3 años	0,057 €/h
Terminadores	600,00 €	3 años	0,114 €/h
PC	1.500,00 €	4 años	0,213 €/h
Cableado	100,00 €	3 años	0,019 €/h

14. Tabla: Coste unitario de las amortizaciones del proyecto

Una vez calculado el coste unitario de cada material, se debe de tener en cuenta la cantidad de horas que ha sido utilizado cada material durante el desarrollo del proyecto para calcular el valor de amortización de cada uno de ellos.

El tiempo de utilización del PC equivale a las horas internas de la proyectista, puesto que ha sido el material de referencia para llevar a cabo todas las tareas del proyecto. En cuanto a los demás materiales, el equipamiento de redes necesario para desplegar el sistema, para calcular la utilización en horas de todos ellos se ha tenido en cuenta la duración de los paquetes de trabajo de Implementación, Realización de pruebas y Optimización de la implementación. Los detalles de estos paquetes pueden verse en el apartado 8.2 Descripción de paquetes de trabajo y tareas.

El desglose del cálculo de las amortizaciones de este proyecto se muestra, a continuación (15. Tabla):

Concepto	Número de horas	Coste unitario (IVA incluido)	Coste total (IVA incluido)
Kit Starlink	268 h	0,049 €/h	13,07 €
Router cliente	268 h	0,057 €/h	15,23 €
Terminadores	268 h	0,114 €/h	30,45 €
PC	600 h	0,213 €/h	127,84 €
Cableado	268 h	0,019 €/h	5,08 €
TOTAL (IVA incluido)			**191,66 €**

15. Tabla: Amortizaciones del proyecto

9.3 Gastos

Por último, en este apartado se incluyen los gastos directos que ha supuesto el desarrollo del proyecto. En este caso, se han considerado el coste mensual de Starlink por la utilización de su sistema satelital y el acceso a Internet, y el gasto en electricidad durante todo el proyecto. El desglose de los gastos se describe en la siguiente tabla (16. Tabla):

Concepto	Coste unitario (IVA incluido)	Número de meses	Coste total (IVA incluido)
Mensualidad Starlink	61,00 €	7 meses	427,00 €
Facturas electricidad	-	-	530,00 €
TOTAL (IVA incluido)			**957,00 €**

16. Tabla: Gastos directos del proyecto

9.4 Coste total del proyecto

Puesto que en este proyecto no se han realizado subcontrataciones, para calcular el coste total del desarrollo de este proyecto basta con sumar el coste de las horas internas, las amortizaciones y los gastos directos. Además, es importante señalar que se ha añadido una partida de costes indirectos (10 % del resultado de la suma de los costes anteriores), con la intención de considerar gastos no atribuibles a un solo proyecto, así como los gastos de los imprevistos que han surgido a lo largo del desarrollo de este proyecto.

Partida	Coste total (IVA incluido)
Horas internas	15.620,00 €
Amortizaciones	191,66 €
Gastos	957,00 €
SUBTOTAL	16.768,66 €
Costes indirectos (10 %)	1.676,87 €
TOTAL (IVA incluido)	**18.445,53 €**

17. Tabla: Resumen de los costes del proyecto

El desarrollo de este proyecto supone un coste total que asciende a la cifra de 18.445,53 € (IVA incluido).

Como se observa en el desglose anterior, la mayor parte del coste de este proyecto se ha destinado a cubrir los gastos en recursos humanos (horas internas). El diseño e implementación de la solución propuesta en este proyecto requieren una gran cantidad de horas de trabajo, lo que ha incrementado significativamente los costes de personal.

10 CONCLUSIONES

El objetivo principal de este proyecto ha sido diseñar, desplegar y analizar tanto la integración como el rendimiento del servicio de Starlink como red de acceso entre la red de un cliente y la de un proveedor de servicios de Internet.

Por un lado, se ha conseguido dotar de conectividad a Internet toda la infraestructura de un cliente mediante la integración de una tecnología de acceso innovadora como lo son las comunicaciones satelitales de órbita baja. Hasta ahora, los sistemas satelitales suponían grandes latencias en las comunicaciones, lo que prácticamente hacía imposible ofrecer conectividad a Internet mediante estos sistemas, puesto que, servicios como el audio y la voz se ven afectados negativamente. En este TFM se ha propuesto utilizar la tecnología Starlink, la cual opera en la órbita baja, posibilitando un acceso a Internet de banda ancha y baja latencia. En este trabajo se ha diseñado y desplegado todo un sistema para poder implementar la tecnología Starlink como red de acceso entre la red de un cliente y su ISP, ofreciendo al cliente conectividad a Internet de baja latencia mediante una VPN.

Adicionalmente, con la implementación del protocolo EoIP se ha logrado que la conectividad entre el cliente y su ISP sea de nivel 2 del modelo TCP/IP. Esto es, las tramas Ethernet de la red LAN del cliente se encapsulan y son enviadas hasta la red del ISP donde pueden ser tratadas como si fuese de la misma red LAN. En este caso, se ha configurado una VLAN en el extremo del ISP, pudiendo así identificar todo el tráfico del cliente.

Por otro lado, se ha conseguido proporcionar seguridad a las comunicaciones entre el cliente y el ISP en términos de confidencialidad del tráfico de datos, autenticación de los extremos y alta disponibilidad del servicio. Para ello, se ha utilizado el protocolo de VPN WireGuard el cual aplica el cifrado y autentica los extremos del túnel mediante claves criptográficas. Gracias a la asociación que hace el protocolo entre claves públicas y direcciones IP, la VPN queda definida por claves criptográficas y no por las direcciones IP de los extremos. Por lo tanto, el sistema propuesto en este trabajo se beneficia de esta característica ofreciendo, así, una conexión segura y sin interrupciones con direcciones IP dinámicas. Se ha de mencionar que, todo el sistema ha sido adaptado a la flexibilidad de los cambios en las direcciones IP mediante scripts y registros DNS. Además, una vez se crea el túnel el cliente establece una sesión BGP con el ISP por la que recibe las rutas necesarias para la completa conectividad.

Del mismo modo, el ISP ofrece una alta disponibilidad del servicio mediante dos terminadores de VPN duplicados. El cliente monitoriza periódicamente el estado de la conexión con el terminador que tiene establecido la VPN y si se detecta que la conexión se ha caído, automáticamente, establece la conexión contra el otro terminador.

En este TFM se han llevado a cabo diferentes pruebas tanto de validación como de rendimiento. Por una parte, se ha verificado la conectividad entre el cliente y el ISP generando tráfico entre ellos y comprobando el correcto funcionamiento del sistema desplegado. Además, se ha confirmado la integración de todos los componentes del sistema y la integración de este en la red en operación del ISP.

Por otra parte, se ha analizado el rendimiento del sistema mediante la medición de 3 parámetros: el ancho de banda, la latencia y el jitter. Para ello, se han realizado diferentes pruebas repetidamente y posteriormente se ha calculado la media de todos los resultados. Para que las medidas obtenidas representen mejor la realidad, se han realizado repeticiones de las pruebas para la medición de los parámetros en diferentes días y horarios. La elección de los momentos específicos para las pruebas se ha basado en los periodos de mayor actividad, cuando es más probable que las redes estén congestionadas, lo que influye en el rendimiento del sistema. Adicionalmente, las pruebas se han llevado a cabo también en diferentes escenarios, pudiendo analizar la influencia de varios factores del sistema.

Por último, en este proyecto se han añadido las configuraciones necesarias para conseguir la optimización de la implementación del sistema en cuanto a sincronización de los relojes de los equipos y la sobrecarga de los paquetes debido a las cabeceras adicionales de los protocolos de tunelado y VPN. En concreto, se ha implementado el protocolo NTP para la sincronización de la hora de tal manera que los equipos se mantienen sincronizados en todo momento evitando así problemas de conexión entre el cliente y los terminadores, y se ha ajustado el valor del MSS de TCP para mejorar el procesamiento del router del cliente, e indirectamente mejorar el rendimiento del sistema.

En conclusión, se han conseguido alcanzar los objetivos definidos al principio del proyecto en los plazos y costes previstos. Desde una perspectiva técnica, el proyecto ha conseguido diseñar, desarrollar e implementar una solución que cumple con los objetivos planteados y se ha demostrado la viabilidad de la propuesta mediante pruebas realizadas sobre equipamiento de red real, evidenciando los beneficios de este proyecto.

11 REFERENCIAS

[1] J. L. Ordoñez, “Comunicaciones Por Satélite,” 2013.

[2] “Satellite Communication - Introduction.” https://www.tutorialspoint.com/satellite_communication/satellite_communication_introduction.htm (accessed Mar. 08, 2024).

[3] “A straightforward introduction to satellite communications.” https://www.inmarsat.com/en/insights/corporate/2023/a-straightforward-introduction-to-satellite-communications.html (accessed Mar. 08, 2024).

[4] “ESA - Satellite frequency bands.” https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Satellite_frequency_bands (accessed Mar. 08, 2024).

[5] “Satellite Basics | Intelsat.” https://www.intelsat.com/resources/tools/satellite-101/ (accessed Mar. 08, 2024).

[6] “Advantages and Disadvantages of Satellite Communication - GeeksforGeeks.” https://www.geeksforgeeks.org/advantages-and-disadvantages-of-satellite-communication/ (accessed Mar. 08, 2024).

[7] Starlink, “Starlink | Cómo funciona Starlink.” https://www.starlink.com/technology (accessed Mar. 08, 2024).

[8] A. Simmons, “Elon Musk’s Starlink and Satellite Broadband - Dgtl Infra,” *December 2, 2020*. https://dgtlinfra.com/elon-musk-starlink-and-satellite-broadband/ (accessed Mar. 08, 2024).

[9] Starlink, “Interference.” https://starlink-enterprise-guide.readme.io/docs/interference (accessed Apr. 20, 2024).

[10] Starlink, “Starlink | Especificaciones - High Performance.” https://www.starlink.com/specifications?spec=2 (accessed Mar. 11, 2024).

[11] J. J. Mathew, N. HS, D. J. V V, and D. R. S, “Implementation of Beam Steering using Phased Array Antennas,” *Int. J. Innov. Sci. Res. Technol.*, vol. 5, no. 6, pp. 1006–1008, 2020, doi: 10.38124/ijisrt20jun716.

[12] Starlink, “Monitoring Your Starlink.” https://starlink-enterprise-guide.readme.io/docs/monitoring-your-starlink (accessed Apr. 20, 2024).

[13] G. Gopal, “Exploring Starlink’s Magic,” *19/07/2023*. https://www.linkedin.com/pulse/exploring-starlinks-magic-how-does-work-govind-v-gopal (accessed Apr. 20, 2024).

[14] Starlink, “Política de Uso Razonable y Política de Gestión Del Tráfico - Starlink.” https://www.starlink.com/legal/documents/DOC-1469-65206-75 (accessed Mar. 08, 2024).

[15] PeeringDB, “AS14593 - SpaceX Starlink - PeeringDB.” https://www.peeringdb.com/net/18747 (accessed Apr. 20, 2024).

[16] Starlink, “IP Addresses.” https://starlink-enterprise-guide.readme.io/docs/ip-addresses (accessed Mar. 08, 2024).

[17] Starlink, “DHCP Configuration.” https://starlink-enterprise-guide.readme.io/docs/dhcp-configuration (accessed Mar. 11, 2024).

[18] GeeksforGeeks, “Tunneling,” Apr. 13, 2023. https://www.geeksforgeeks.org/tunneling/ (accessed Apr. 20, 2024).

[19] LinkedIn, “Túnel IP: pros y contras para el rendimiento de la red.” https://www.linkedin.com/advice/0/what-advantages-disadvantages-using-ip-tunneling (accessed Apr. 20, 2024).

[20] Cisco, “How Virtual Private Networks Work - Cisco,” Oct. 13, 2008. https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html#conv (accessed Apr. 20, 2024).

[21] LinkedIn, “Beneficios de la tunelización VPN para la ingeniería de redes.” https://www.linkedin.com/advice/1/how-do-you-integrate-vpn-tunneling-other-network (accessed Apr. 20, 2024).

[22] Starlink, “Starlink Especificaciones - Rendimiento.” https://www.starlink.com/legal/documents/DOC-1470-99699-90 (accessed Apr. 20, 2024).

[23] W. Stallings, T. Case, A. K. Bhattacharjee, and S. Mukherjee, *Business data communications : infrastructure, networking and security*. 2012.

[24] J. A. Donenfeld, “WireGuard: Next Generation Kernel Network Tunnel,” *24th Annu. Netw. Distrib. Syst. Secur. Symp. NDSS 2017*, pp. 1–20, 2017, doi: 10.14722/ndss.2017.23160.