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

GRADO EN INGENIERÍA EN TECNOLOGÍA DE TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

ANÁLISIS Y REDISEÑO DE UNA RED CORPORATIVA Y ESTABLECIMIENTO DE PROTOTIPO DE SUCURSAL REMOTA

Alumno: Martín Ruiz, Mikel

Directora: Ibarrola Armendariz, Ana Eva

Curso: 2018-2019

Fecha: Bilbao, 22, 7, 2019

RESUMEN TRILINGÜE Y PALABRAS CLAVE

[ES]

La sucursal en Bilbao de la empresa SATEC necesita mejorar la infraestructura de su red corporativa. La baja velocidad y las altas latencias están provocando muchos inconvenientes a sus empleados. Desde la migración de oficina en 2017, la falta de recursos para llevar acabo de forma adecuada el diseño y despliegue de la nueva red ha desembocado en que la oficina cuente con una red de carácter temporal de forma indefinida.

El objetivo de este trabajo es desarrollar un profundo análisis orientado a detectar las razones detrás del bajo rendimiento de la red. En base al análisis desarrollado, se propone un diseño adecuado que permita lograr las condiciones necesarias para proporcionar a los usuarios una calidad digna de los servicios disponibles en la sucursal. Con esta propuesta de diseño se pretende establecer un prototipo de referencia para la futura mejora del resto de sucursales de SATEC.

[EUS]

Sukurtsala Bilbon duen SATEC enpresak sare korporatiboko azpiegitura hobetu behar du. Langileek arazo asko dituzte abiadura motela eta mezu atzerapenak direla eta. 2017an bulego honetara mugitu zirenetik, sare berriaren diseinua egiteko beharrezkoak ziren baliabideen ezaren ondorioz bulegoak sare ez eraginkor bat du.

Lan honen helburua azterketa sakon bat egitea da sarearen errendimendu baxuaren arrazoiak bilatzeko. Azterketa egin ostean, sukurtsaleko langileei kalitate duineko zerbitzua eskaintzen duen diseinu bat proposatuko da. Proposamena sareko gainontzeko sukurtsalentzat erreferentziakoa izatea espero da.

[EN]

The SATEC off-site branch office in Bilbao is in need of a better corporative network infrastructure. Its poor bandwidth and huge latencies are giving a hard time to its employees. Since they moved in to this office in 2017, due to budget issues, the design and deployment for the new network was never achieved, so they were stuck with an inefficient temporary one.

The objective is to make a deep analysis of the current situation, detect the reasons for the poor connectivity and propose a new design to achieve the necessary conditions for a rightful quality of the services available at the site. Through this proposal, there is an intention of designing an off-site branch prototype reference for the rest of the networks.

[Palabras clave]

Sucursal, router, switch, túnel, servicio, red, escalabilidad, disponibilidad, seguridad, gestión.

ÍNDICE

Tablas

Figuras

Acrónimos

ARP	*Address Resolution Protocol*
DHCP	*Dynamic Host Configuration Protocol*
DMVPN	*Dynamic Multipoint VPN*
DNS	*Domain Name System*
FGCP	*FortiGate Clustering Protocol*
GRE	*Generic Routing Encapsulation*
HSRP	*Hot Standby Router Protocol*
IOS	*Internetwork Operating System*
IP	*Internet Protocol*
IPsec	*IP security*
ISP	*Internet Service Provider*
LACP	*Link Aggregation Control Protocol*
LAN	*Local Area Network*
LDAP	*Lightweight Directory Access Protocol*
mGRE	*multipoint GRE*
NAT	*Network Address Translation*
NHRP	*Next Hop Resolution Protocol*
OSI	*Open System Interconnection*
OSPF	*Open Shortest Path First*
PoE	*Power over Ethernet*
PTZ	*Parque Tecnológico de Zamudio*
QoS	*Quality of Service*
SD-WAN	*Software Defined WAN*
SNMP	*Simple Network Management Protocol*
SSH	*Secure Shell*
SSID	*Service Set Identifier*
TACACS	*Terminal Access Controller Access Control System*
TI	*Tecnología de la información*
UPS	*Uninterruptible Power Supply*
VDOM	*Virtual Domain*
VRF	*Virtual routing and forwarding*

1 INTRODUCCIÓN

Las redes corporativas de telecomunicaciones han evolucionado de forma significativa en los últimos años. El volumen de tráfico soportado, su alcance y el número y tipo de usuarios se han visto incrementados considerablemente, apareciendo nuevas necesidades con las que no se contaba en un principio. Datos bancarios, conversaciones privadas, información confidencial, alarmas de seguridad, documentos, videos y un largo etcétera de datos de mayor o menor importancia viajan diariamente por las redes corporativas.

Este crecimiento descontrolado junto a la incorporación de nuevos servicios y tecnologías, sin un análisis y rediseño adecuado, puede llevar a que por falta de capacidad, poca escalabilidad, por uso de tecnologías obsoletas e incluso escasa documentación, muchas de ellas acaben colapsándose fácilmente y no proporcionen la calidad de servicio que en un primer instante se deseaba.

En determinadas situaciones, la perdida de una conexión o error de un servicio puede resultar fatal para una empresa. Un fallo o error informático que produzca una interrupción del servicio es un serio problema tanto para empleados como para clientes, así como un mal funcionamiento del mismo.

En CloudEndure [1], empresa de computación en la nube que desarrolla soluciones de software de continuidad empresarial para la recuperación ante desastres, calcularon el coste total por minuto de una interrupción de servicio no planificada, guiándose por un estudio del Instituto Ponemon [2]. Para una pequeña empresa de 20 empleados con una facturación anual de 8,4 millones de euros, estimaron un coste total de 35€ por minuto. Es también lógico pensar que una infraestructura poco eficiente, a pesar de no provocar cortes de servicio, conlleva pequeñas pérdidas de tiempo distribuidas a lo largo de la jornada laboral. Es decir, se puede suponer a pesar de ser de una forma menos apreciable, que, en el caso de una red de bajo rendimiento, está sucediendo un “corte” de servicio, lo que puede suponer a la empresa una repercusión económica semejante a la mencionada en el estudio. Para evitar ese tipo de inconvenientes es pieza clave contar con un diseño óptimo y una gestión adecuada de la topología de la red. Permitiendo así proporcionar a la empresa los servicios de telecomunicación de la forma más idónea.

En este trabajo se analizará cómo identificar y solventar dichos problemas partiendo de una red que no dispone de las características clave anteriormente mencionadas.

2 CONTEXTO

Este proyecto se desarrolla en el marco de un programa de cooperación educativa acordado entre la UPV/EHU y la empresa SATEC para los meses de enero a agosto.

El proyecto global comprende el estudio, análisis y mejora de la red corporativa de la sucursal de Bilbao de esta empresa. Debido a la envergadura del proyecto, el trabajo se ha subdividido en dos subproyectos bien diferenciados:

- Un proyecto inicial que estudia y analiza, tanto el estado de los servicios actualmente soportados y sus requerimientos de mejora, como la necesidad de introducir nuevos servicios y aplicaciones.
- Un segundo proyecto que, en base a los resultados del análisis anterior, estudia las mejoras a implementar en la infraestructura de la red de Bilbao y plantea una propuesta adecuada para el rediseño de la misma, que, además, servirá de base para el rediseño del resto de sucursales de la empresa.

Este trabajo fin de grado comprende el segundo de los proyectos antes mencionados. El primero de ellos se ha desarrollado también en el marco de una cooperación educativa de otro alumno de la EIB [3]. Ha sido imprescindible, por tanto, un trabajo colaborativo para la consecución del objetivo global de mejorar la red de la delegación de Bilbao de la empresa SATEC. Se trata, por tanto, de un proyecto cooperativo relacionado con la especialidad de telemática, y más concretamente con la ingeniería de redes.

SATEC, Sistemas Avanzados de Tecnología, S.A., es una multinacional española integradora de soluciones y servicios avanzados asociados a las nuevas Tecnologías de la Información y Comunicación. A pesar de que su sede principal está en Madrid, cuenta con una sucursal en Bizkaia, más concretamente en el Parque tecnológico de Zamudio (PTZ a partir de ahora).

La delegación cambió de edificio, dentro de ese mismo parque, en 2017, migrando toda la red (equipos, cableado y configuraciones) que disponía en producción a su nueva ubicación.

Para la puesta en funcionamiento de la nueva oficina lo más rápido posible, sus propios técnicos se encargaron de la nueva instalación. Se configuró una maqueta de red provisional sin ningún tipo de presupuesto, es decir, con lo que ya tenían previamente, hasta que se diseñase una infraestructura y trajese el nuevo equipamiento. Esto nunca ocurrió y la red provisional, que funcionaba correctamente en aquel momento, pasó a ser la red corporativa de la delegación.

Dos años después, no se conoce el estado de la red. No hay diagramas ni documentación suficiente que muestre la situación actual de la infraestructura, al menos no de forma fiable. Parte de los miembros del equipo de técnicos que realizaron la instalación inicial ya no se encuentran en la empresa y otros tantos no recuerdan las operaciones que se realizaron, ya que, por ser de origen provisional, no se documentó de forma adecuada.

La red desplegada dispone de un ancho de banda de 400 Mbps contratados (100 Mbps a Sarenet y 300 Mbps a Movistar), de los cuales solo se encuentran en uso en torno a 60 Mbps (Sarenet), los otro 300 Mbps (Movistar) están configurados exclusivamente para el control de accesos y cámaras de seguridad. Una situación claramente desproporcionada e inadecuada para ofrecer una infraestructura acorde al trabajo que realiza el equipo de técnicos y comerciales diariamente a través de dicha red.

A lo largo de los 2 años, se han ido introduciendo “parches” y “workarounds” sin mucho criterio aparente, empeorando la ya delicada situación. Además, al no haber un administrador encargado del mantenimiento de la red, se pueden encontrar numerosas configuraciones de tecnologías que llevan años obsoletas.

Adentrándonos en ciertos problemas de configuraciones concretos, existen varios túneles entre las oficinas de Bilbao y Madrid, principalmente para la monitorización de los equipos de la oficina y el acceso a recursos corporativos. Debido a errores en la configuración actual, se acaba encapsulando parte del tráfico generado desde la oficina hacia Internet, convirtiéndose en una de las principales causas de las altas latencias que experimentas los trabajadores a la hora de acceder a Internet.

Madrid también cuenta con un servicio de monitorización para la red del Parque Tecnológico, cliente de la empresa. A causa de ello, y a causa de tener tanto Madrid como el PTZ direccionamiento privado, existe una doble configuración de NAT (Network Address Translation). Para proporcionar el servicio, se traducen IPs privadas de Madrid a IPs privadas de Zamudio. Ese proceso se realiza a través de dos routers, uno que traduce las direcciones origen y otro que traduce las direcciones destino, con reglas poco adecuadas y excesivamente complejas. Además, esos dos equipos se encuentran en una redundancia de HSRP (Hot Standby Router Protocol) que no funcionaría en caso de ser necesario, ya que los dos routers tienen configuraciones y funcionalidades diferentes. Esto, unido a que el router secundario está prácticamente obsoleto y únicamente sigue en producción por la gran cantidad de rutas y traducciones NAT que tiene configuradas de forma estática.

Como se puede concluir de todo lo mencionado, se hace necesaria una remodelación de la red, previo análisis y estudio de las necesidades y requerimientos.

En este contexto, se enmarca el siguiente proyecto, el cual pretende optimizar y dotar de una infraestructura solida a la red corporativa de la delegación de Bilbao mediante el análisis de la situación actual y el rediseño de la topología de la red en todos los aspectos necesarios y que sirva de prototipo para la mejora del resto de sucursales de la red de SATEC.

3 OBJETIVOS Y ALCANCE

A partir de la situación contextualizada en el apartado anterior, **se establece como objetivo principal de este proyecto el rediseño de la infraestructura de la red corporativa de la sucursal de Bilbao.** Este rediseño se fundamentará en el establecimiento de requerimientos tomando como base los resultados del estudio de los servicios desarrollado en el subproyecto vinculado [3].

Tras el establecimiento de los requerimientos en base al estudio antes mencionado y tras analizar y comprender los problemas actuales de la red y establecer las especificaciones, se planteará el rediseño adecuado de la infraestructura de red. Se busca realizar un diseño sencillo, fiable, seguro y escalable, y que, además, cumpla con todos los requerimientos establecidos como resultado del estudio de los servicios.

En cuanto a objetivos parciales se refiere, el primero de todos consiste en, tras analizar la red, documentar en detalle tanto la arquitectura cómo las problemáticas que provocan o podrían llegar a provocar inconvenientes en su funcionamiento. Como se comentaba anteriormente, es clave conocer por completo la situación inicial y, en este sentido, entender el resultado del análisis preliminar de los servicios. Es por ello, que además de analizar estos resultados, se plantea inicialmente consultar tanto el conexionado como las configuraciones de los equipos actualmente en producción.

El segundo objetivo parcial se trata de realizar un diseño que se ajuste a las necesidades y requerimientos definidos en el ya mencionado estudio de los servicios. Asimismo, se establece el objetivo de que el diseño pueda ser adaptable a cualquiera de las sucursales de la empresa, homologando así una estructura común para todas ellas. Así, se dotaría y aseguraría en todas ellas la capacidad de soportar, de forma adecuada, todos los servicios de los que la empresa dispone. Para ello, el diseño más importante se centra en la conexión de la red LAN, en este caso la de Bilbao, a la WAN corporativa de SATEC.

En tercer lugar, se quiere lograr eliminar todo rastro de previas configuraciones y equipos innecesarios que puedan ir en detrimento del funcionamiento, y por consecuencia, de la calidad del servicio ofrecido por la red actualmente.

Por lo tanto y a modo de resumen, **el proyecto abarca desde el análisis y documentación de la situación actual de la infraestructura de la red corporativa hasta el rediseño de una nueva red.**

4 BENEFICIOS

Este trabajo de fin de grado, como se ha descrito en los apartados anteriores, aborda el rediseño de la infraestructura de red corporativa de la delegación en Bilbao de la empresa SATEC. Como consecuencia del objetivo principal del proyecto, se esperan obtener beneficios de ámbito técnico, económico y social. A continuación, se detalla cada uno de ellos.

4.1 TÉCNICOS

Desde el punto de vista técnico, el proyecto supone grandes beneficios en prácticamente todos los aspectos de la red.

En primer lugar, se identifican cuellos de botella y se eliminan, mejorando el rendimiento general de la red. Esto se traduce en menor porcentaje de uso de CPU y memoria y mayor durabilidad del equipamiento.

En segundo lugar, se facilita la gestión de la red. Por un lado, se simplifican las configuraciones de los equipos para una mayor rapidez en detección de errores o modificaciones futuras. Por otro lado, al haber menos equipos en la red, hay menos equipos que gestionar, lo que implica una gestión más eficaz de manera directa. Además, se reduce el número de equipos vulnerables y se eliminan configuraciones potencialmente peligrosas para la seguridad de la empresa.

En tercer lugar, se abre la posibilidad a continuar escalando la red. Se liberan tanto puertos en los equipos, como enlaces entre ellos. Permitiendo su uso para equipamiento adicional y/o redundancia del equipamiento actual.

De igual forma, al poder tener todas las sucursales la misma topología, se abre la posibilidad a simplificar las tareas de gestión y de provisión de servicios.

Por último, se actualizan las tecnologías en uso, además de incluirse nuevas, como por ejemplo el apilamiento de fuentes de alimentación, lo que se traduce en un beneficio técnico en sí mismo.

4.2 ECONÓMICOS

Los principales beneficios económicos se ven reflejados en la reducción de costes de la empresa.

Para empezar, una red más eficiente, más rápida, significa menos pérdidas de tiempo, menos pérdidas de tiempo se traducen, como bien se ha visto en la introducción del documento, en menores pérdidas económicas.

Asimismo, la simplificación de la red significaría menos equipos encendidos consumiendo recursos eléctricos, lo que directamente implica reducción de costes en la factura eléctrica.

Además, los equipos retirados pueden ser o vendidos o reutilizados para escalar la red de forma adecuada, permitiendo una pequeña inyección económica o una reducción de gastos en futuro equipamiento.

Por último, mayor productividad de los trabajadores significaría trabajo de mayor calidad y clientes más satisfechos, abriendo oportunidades a nuevas contrataciones. De la misma forma, mayor

productividad significaría trabajo realizado en menos tiempo, permitiendo utilizar esos recursos humanos en nuevos proyectos, generando todo ello mayor beneficio económico.

4.3 SOCIALES

En lo que al ámbito social se refiere, los mayores beneficios vienen relacionados con los aspectos emocionales de los empleados.

Una mayor productividad de los trabajadores se refleja de forma directa en su estado de ánimo, los empleados quedarían más satisfechos con el volumen de trabajo completado durante su jornada laboral.

En esa misma línea, la ejecución de las tareas sin largas esperas en las descargas de documentos o en la navegación entre páginas web implica un nivel mucho menor de frustración e impotencia. Mejorando la eficiencia de las personas y evitando una posible pérdida de motivación para continuar trabajando.

Por otra parte, la inclusión de nuevos servicios en la red implica una sensación de avance tecnológico por parte de la empresa, lo que conlleva una motivación extra para continuar realizando las tareas, quizás, de una forma más sencilla.

5 ANTECEDENTES

Antes de pasar al análisis de alternativas para la selección de la topología ideal para las delegaciones, y los equipos que la formarán, se cree necesario mostrar de forma más visual la situación actual de la red.

Se comenzará detallando el nivel de red, tanto especificando los equipos que lo conforman y sus funciones, así como de forma más grafica a través de un diagrama (Figura 1). A continuación, se hará lo mismo con el nivel de enlace (Figura 2) y el nivel físico (Figura 4). Por último, se hará hincapié en los aspectos de la infraestructura que más problemas suponen, es decir, se identificarán los cuellos de botella y los puntos de fallo único.

5.1 NIVEL DE RED

A continuación, se va a explicar en detalle el equipamiento de red en producción, así como sus principales funciones. Al final del apartado se muestra un diagrama (Figura 1) que resume de manera gráfica lo aquí mencionado.

5.1.1 Mikrotik

Router del ISP (Internet Service Provider) Sarenet que provee 100Mbps y una red /29 de IPs públicas. Cabe destacar que este equipo provee su servicio de acceso a internet a través de nuestra propia infraestructura, como se puede ver en el diagrama (Figura 2) y como se comentará más adelante. Además, su ancho de banda se comparte con la infraestructura dedicada a Iberdrola.

5.1.2 HGU

Router del ISP Movistar que provee 300Mbps simétricos, conectado en modo bridge a nuestro router de la serie 7200. Por ello, el router 7204 posee una dirección publica en su interfaz WAN (Wide Area Network).

5.1.3 Cisco 1841

Router conectado a Sarenet, y por lo tanto con una dirección pública de la red /29 que se mencionaba al inicio del apartado. Este equipo cumple varias funciones que se mencionarán brevemente:

- Servidor DHCP (Dynamic Host Configuration Protocol) con IPs públicas.
- Salida por defecto a internet de los equipos de la red de la oficina con direccionamiento público.
- Servidor DHCP para la red de telefonía IP.
- Salida por defecto a internet de la telefonía IP de la oficina.
- Salida por defecto a internet de los equipos de la red de servidores.
- Salida por defecto a internet de los equipos de la red del laboratorio que lo requieran.
- Origen de dos túneles GRE (Generic Routing Encapsulation) con IPSec (Internet Protocol security) idénticos contra dos equipos de SATEC Madrid para recursos corporativos. Ambos se utilizan para anunciar y recibir rutas mediante OSPF (Open Shortest Path First).
- Un túnel GRE contra un equipo de monitorización en Madrid para la gestión de la red del PTZ.
- Traducciones NAT de direcciones destino para la monitorización del PTZ.

5.1.4 Cisco 3640

Router en HSRP (Hot Standby Router Protocol) con el router Cisco de la serie 1800, encargado exclusivamente de traducciones NAT de direcciones origen de Madrid al PTZ.

Contiene una gran cantidad de configuraciones adicionales, como se comentaba en anteriores apartados, pero se ha llegado a la conclusión de que ninguna de ellas está siendo utilizada.

5.1.5 Fortigate 101E

Primero de todo mencionar que este equipo se encuentra en la oficina para dar servicio a los empleados de SATEC Bilbao que trabajan para Iberdrola. Tanto el equipo, como la infraestructura y los empleados para dichas labores no son objeto de este proyecto.

A pesar de ello, por motivos de necesidad de ancho de banda, existe una VDOM (Virtual Domain) para los empleados de SATEC Bilbao que no trabajan para Iberdrola. En ese dominio se ha creado una red de IPs privadas. El tráfico de esta red tiene como router por defecto el Firewall, el cual posee una de las IPs públicas de la red /29 de Sarenet. Dicho tráfico sale a internet sin cruzar ninguno de los túneles GRE con Madrid.

5.1.6 Cisco 7204 VXR

Router conectado a Movistar, encargado de dos túneles GRE contra Madrid. Como se puede ver en el diagrama de red (Figura 1), su única función en estos momentos es proveer de conexión a internet a las cámaras y controles de acceso. Mediante los túneles y el uso de OSPF, se logra que dicha red pueda ser monitorizada desde Madrid.

5.1.7 Diagrama del nivel de red

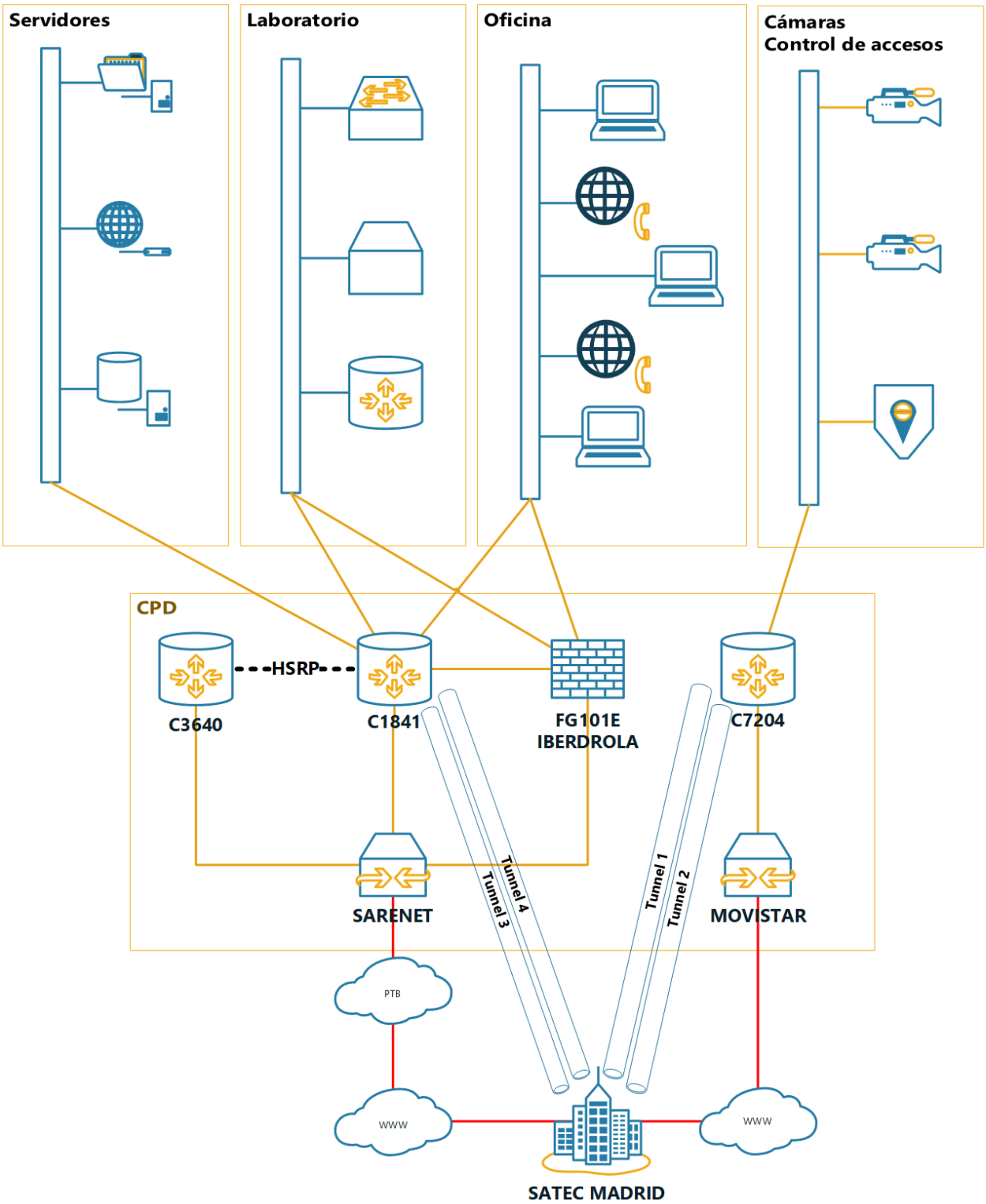

Figura 1: Nivel de red inicial

5.2 NIVEL DE ENLACE

En este apartado se va a detallar el esquema del nivel de enlace, enumerando las diferentes VLANs existentes actualmente en producción (se obvian el resto de VLANs que hay configuradas sin ninguna función aparente) y definiendo su uso concreto. Al final del apartado se van a mencionar los equipos que actúan a nivel de enlace y sus funciones en concreto.

5.2.1 VLANs

Todas ellas se pueden ver en el diagrama que se muestra al final del apartado (Figura 2).

- *VLAN 1*

  VLAN nativa de Cisco, utilizada por todo el PTZ para el tráfico de datos.

- *VLAN 6*

  Utilizada para la gestión de los UPSs (Uninterruptible Power Supply) de los diferentes edificios del PTZ.

- *VLAN 7*

  Utilizada para conectarse a uno de los clientes de la empresa en el PTZ sin necesidad de rutar a nivel de red. Esta VLAN se propaga por el parque a través de un enlace directo.

- *VLAN 10*

  Utilizada para la voz IP de la oficina.

- *VLAN 13*

  Utilizada para separar el laboratorio de la red de datos corporativos.

- *VLAN 15*

  Utilizada para el acceso a la red por los equipos que requieran direccionamiento público.

- *VLAN 16*

  Utilizada para el acceso a la red por los equipos que requieran direccionamiento privado y no necesiten cruzar los túneles con Madrid.

- *VLAN 20*

  Utilizada para las cámaras y los controles de acceso.

- *VLAN 22 (Sarenet)*

  VLAN gestionada por Sarenet para dar servicio de acceso a internet a la oficina. Como se ha comentado anteriormente, y como se puede ver al final del apartado en el diagrama (Figura 2), esta VLAN se propaga al PTZ a través de nuestro switch core. Ello implica que parte de su configuración está gestionada por SATEC Bilbao.

5.2.2 Switches

Los modelos de los equipos y su ubicación en la infraestructura se pueden ver en el diagrama (Figura 2). A continuación, se describen cada uno de ellos.

5.2.2.1 Switch core

Switch que conecta Sarenet, y los 3 routers que de Sarenet dependen, a prácticamente todo el resto de equipos de la delegación.

- PCs de los técnicos
- PCs de los comerciales
- Telefonía
- Salas de reuniones
- Impresoras
- Servidores
- Switch del laboratorio

5.2.2.2 Switch laboratorio

Switch de acceso con la única función de enviar el tráfico del laboratorio con destino internet a través de un trunk al switch core.

5.2.2.3 Switch de acceso oficina

Switch de acceso con la única función de enviar el tráfico de varios empleados de la oficina a través de un Port-Channel en modo trunk al switch core. Se añadió por falta de puertos en el switch core para todos los empleados.

5.2.2.4 Switch de cámaras y controles de acceso

Como se puede apreciar en el diagrama mencionado (Figura 2), se encarga de conectar las cámaras y los controles de acceso al router 7204.

5.2.3 Diagrama de nivel de enlace

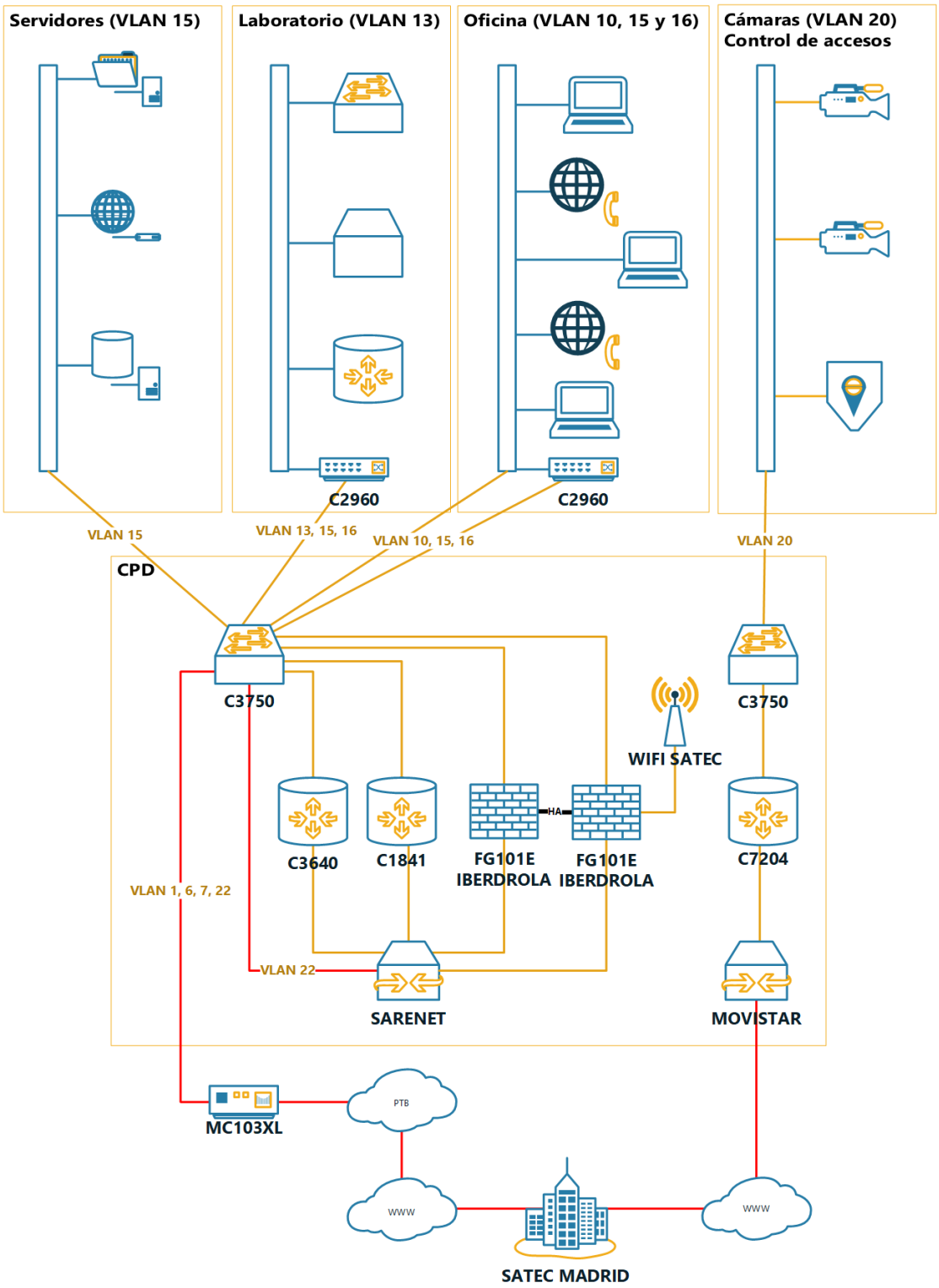

Figura 2: Nivel de enlace inicial

5.3 NIVEL FÍSICO

En este apartado se va a explicar muy brevemente la ubicación de los equipos físicamente y el grado de utilización de sus puertos.

5.3.1 Rack Principal CPD

Como se ha podido ir observando en los dos diagramas previos (Figura 1 y Figura 2), la mayoría de la infraestructura se encuentra en el CPD de la delegación. En él también se encuentra un conversor eléctrico-óptico con una capacidad máxima de 100Mbps. Este pequeño dispositivo es el único cable entre la red y el PTZ, es decir, entre la red de la oficina e internet.

5.3.2 Rack Iberdrola CPD

En este rack se encuentra la infraestructura de la delegación dedicada exclusivamente a Iberdrola. Se menciona por el simple motivo de que, como se comentaba previamente, se utilizan ciertos equipos de esa infraestructura para la red de la oficina.

5.3.3 Rack Laboratorio

Rack con una gran cantidad de equipos de clientes y maquetas de prueba, solo se hace mención al equipo que interconecta ese rack con el CPD.

5.3.4 Rack Pasillo

Rack situado en un armario del pasillo de la oficina, este armario contiene tanto equipos de Iberdrola como de la oficina, además en él se encuentra el panel de parcheo con todas las tomas de red de la delegación. Por ello, en él también se encuentra el switch de acceso de la oficina, con la intención de reducir los 8 puertos adicionales que necesitan ser parcheados al switch core a 2 del trunk entre los dos switches.

5.3.5 Cisco Air-CAP 1702

Punto de acceso inalámbrico dedicado a la creación del SSID (Service Set Identifier) de SATEC para proveer de acceso inalámbrico a la red a los empleados de la oficina.

5.3.6 Diagrama de nivel físico – Puertos

En la siguiente figura (Figura 3) se muestra el nivel de ocupación y el propósito de los puertos de los switches de la red.

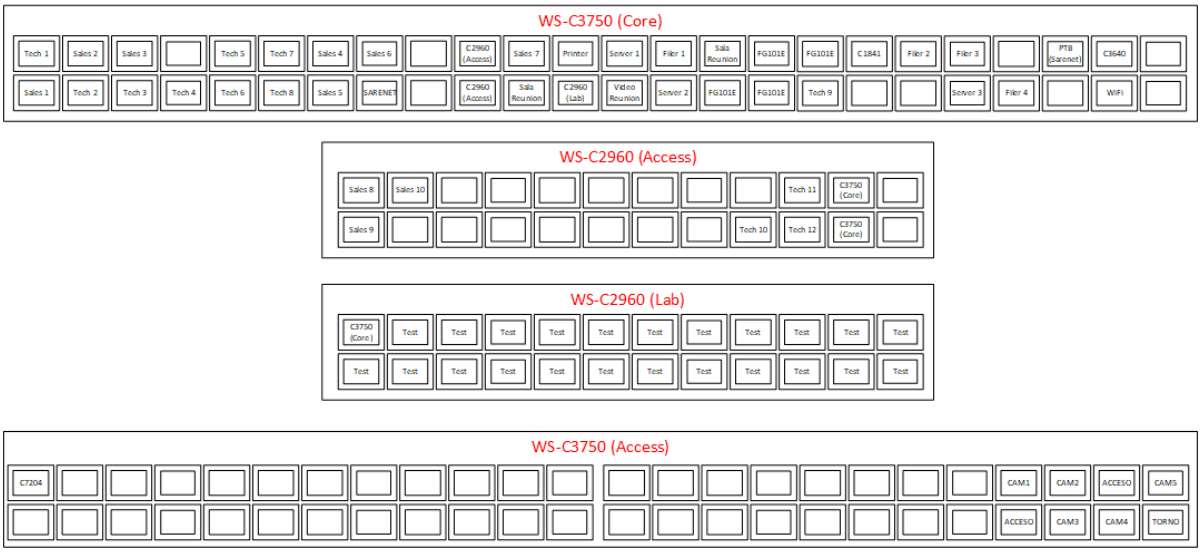

Figura 3: Uso de puertos inicial

A continuación, se resume el porcentaje de utilización de cada uno de ellos.

- **Core (94%):** 48 puertos disponibles, 6 conectados sin uso, 3 libres.
- **Acceso red (33%):** 24 puertos disponibles, 16 libres.
- **Acceso equipos seguridad (20%):** 48 puertos disponibles, 39 libres.
- **Laboratorio:** 24 puertos disponibles, se encuentra prácticamente aislado de la red de producción y se manipulan constantemente por lo que no es relevante su ocupación actual.

5.3.7 Diagrama de nivel físico – Racks

En la siguiente figura (Figura 4) se muestra la ubicación del equipamiento y su correspondiente cableado de interconexión. Se han obviado, con el fin de simplificar el esquema, los cables de red provenientes de equipos finales.

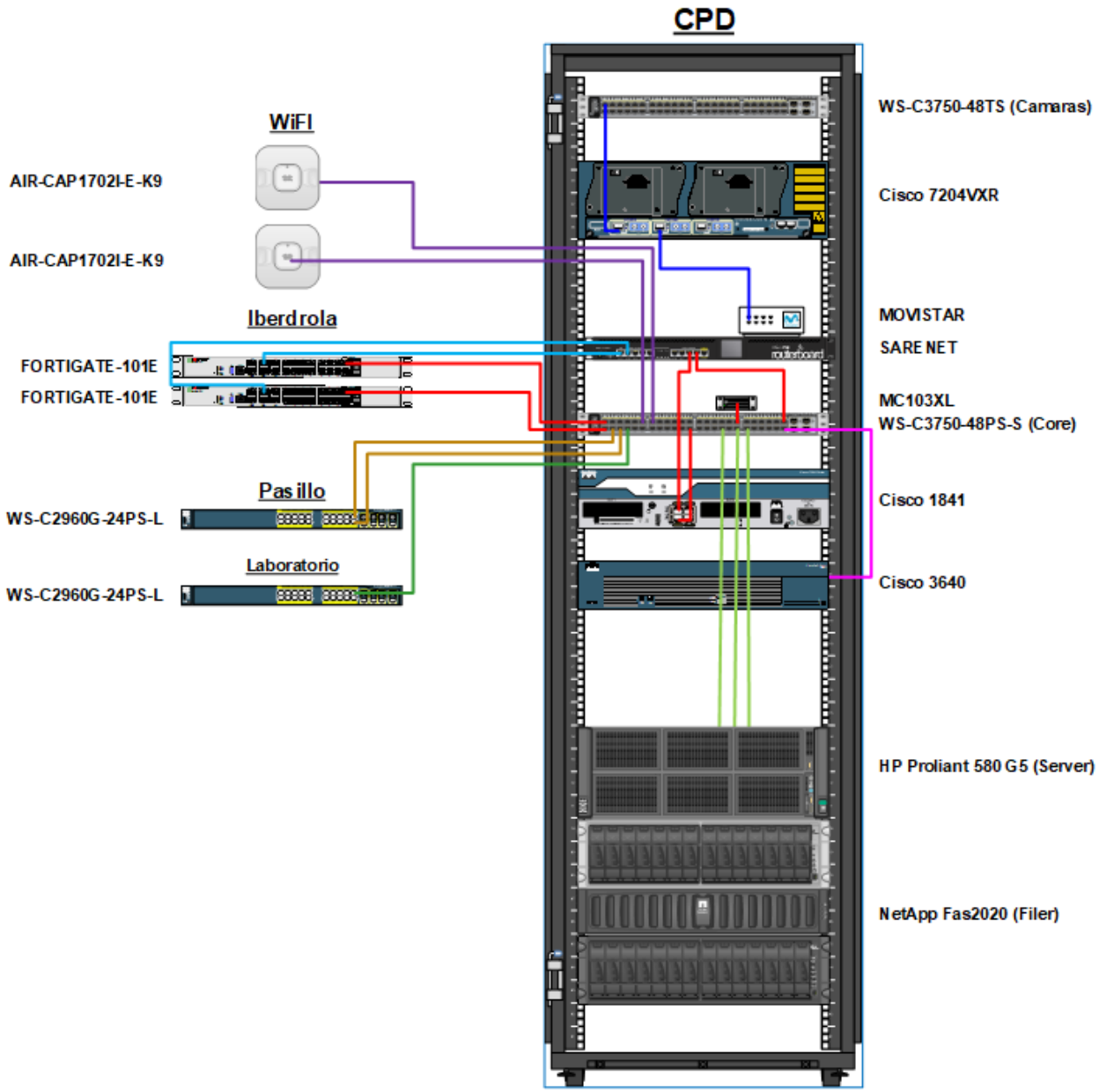

Figura 4: Distribución de equipos inicial

5.4 PROBLEMAS IDENTIFICADOS

Como se venía comentando desde un principio, para gestionar una red, es necesario conocerla en detalle. Una vez realizada dicha tarea, es el momento de tratar de mejorarla. Para ello, es imprescindible identificar los principales problemas que originan la necesidad de hacerlo: los cuellos de botella, los puntos de fallo único, las vulnerabilidades de seguridad y la gestión indebida.

Se expondrán los problemas identificados de la misma forma que se ha hecho con el análisis de la situación, estudiando los 3 niveles inferiores del modelo OSI (Open System Interconnection) de forma independiente.

5.4.1 Nivel de red

5.4.1.1 Acceso a internet

Como se ha podido comprobar, la oficina cuenta con 2 salidas a internet. A pesar de ello, no están siendo correctamente aprovechadas. Una de ellas, la de Movistar concretamente, se encuentra aislada del tráfico de datos de la red. Es decir, se encuentra dedicada exclusivamente a tráfico de monitorización de 8 dispositivos que, además, apenas requieren de ancho de banda. Por lo tanto, en caso de algún problema en la red de acceso a internet por parte de Sarenet, la oficina quedaría incomunicada. Además, los 100Mbps de Sarenet son compartidos con los empleados de Iberdrola.

5.4.1.2 Baja fiabilidad

HSRP es un protocolo propietario de Cisco Systems que permite el despliegue de un router virtual con una dirección IP común compartida por varios routers físicos. Es decir, desacopla las direcciones IP de la interfaz física y las asocia a grupos de interfaces, habilitando la redundancia del hardware. Es un protocolo activo-pasivo en el que solo uno de los routers es el encargado de realizar las tareas, si el router primario deja de funcionar, el secundario ocupará su lugar, mientras que la dirección IP virtual seguirá siendo la misma. Este protocolo evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers. Se ha mencionado con anterioridad, y se puede apreciar en el diagrama de red (Figura 1), que los routers C1841 y C3640 cuentan con este protocolo configurado entre ellos.

El problema surge al comprobar el resto de configuraciones de los equipos, ya que estos dos routers están configurados para dos funciones totalmente diferentes. Por ello, aun existiendo la clara intención de contar con redundancia en el router que proporciona la salida a internet, su “backup” teórico no está correctamente configurado. Lo mismo pasa con la monitorización y su NAT. Si cualquiera de los dos fallase, el otro no podría asumir las funciones correspondientes, por el simple motivo de que no están debidamente configurados para ello.

5.4.1.3 Acceso a WAN corporativa

Los túneles mencionados y mostrados en el apartado anterior utilizan el protocolo GRE, en conjunto con IPsec, para proporcionar el servicio de encapsulado con Madrid.

Los túneles tienen un ancho de banda muy limitado, además, para llegar a otras sucursales como la de Vigo, el tráfico debe pasar por el túnel con Madrid, y después, llegar a Vigo a través de otro túnel Madrid-Vigo, generando tráfico innecesario en el extremo de Madrid. Además, algunos problemas de

rutado estático provocan que el tráfico de acceso a internet tenga que viajar a través de esos túneles, con las consecuencias de latencia y reducción del ancho de banda que ello conlleva.

5.4.1.4 Gestión

Después del análisis realizado, se ha llegado a conocer todo el direccionamiento IP de los equipos de la red, pero aún no se tiene acceso remoto a todos ellos. Gran parte de la gestión se tiene que realizar de forma presencial a través del puerto de consola. Además, no existe el rol de administrador de red, por lo que cualquier persona que requiera de alguna configuración específica, ha de hacerla personalmente, desplazándose hasta el equipo que corresponde. Esto conlleva que múltiples personas modifiquen la red a su antojo sin ningún tipo de orden, criterio y/o responsabilidad, con el añadido de que los cambios no se documentan ni eliminan tras su uso.

5.4.2 Nivel de enlace

5.4.2.1 Diseño

No existe una estructura jerarquizada tal y como recomienda Cisco para facilitar la gestión y asegurar la escalabilidad de la red. No están correctamente definidas ni la capa de acceso ni la de distribución. Algunos de los equipos finales de los usuarios de la red están directamente conectados al switch core, y algunos otros a un switch de acceso, provocando confusión a la hora de gestionar el acceso a la red.

5.4.2.2 VLANs

Las VLANs no están definidas adecuadamente, cada equipo tiene una descripción diferente, y algunas de ellas no se propagan debidamente.

5.4.2.3 Redundancia de caminos

A excepción de los enlaces del FG101E y el del switch de la oficina con el switch core, ningún enlace contempla la redundancia. Cualquier fallo provocaría la caída de la conexión entre los equipos involucrados.

5.4.3 Nivel físico

5.4.3.1 Puertos

El switch core tiene conectados equipos finales de forma directa. Se han tenido que añadir switches adicionales para subsanar el hecho de que el switch core se encuentre sin puertos libres. En caso de ser necesario añadir algún switch más con el propósito de dar acceso a internet a nuevos equipos, habría que reestructurar el cableado.

5.4.3.2 Convertidor de Medios MC103XL

El conversor óptico-eléctrico de Allied Telesis que se encuentra en el rack del CPD es el último elemento entre la red del PTZ, es decir, internet, y la sucursal. Un fallo en ese equipo o la fibra óptica que a él se conecta supondría una caída total del servicio.

6 DESCRIPCIÓN DE REQUERIMIENTOS

Partiendo de la problemática presentada y basándonos en el estudio previamente mencionado [3], se va a realizar una descripción detallada de los requerimientos que han de cumplirse. A través de estos, se podrán más adelante definir las especificaciones concretas de la infraestructura para asegurar un diseño acorde a los objetivos establecidos al inicio del trabajo.

En una primera instancia se va presentar una lista con el resumen de los servicios que contempla el estudio, para posteriormente, mostrar los requerimientos de esos servicios.

Por un lado, los servicios de usuarios:

- Aplicaciones de datos (corporativas y no corporativas)
- Telefonía IP
- Conferencia por video
- Control de accesos
- Cámaras de seguridad
- Gestión y mantenimiento de red
- Servidor de almacenamiento

Estos servicios tienen unos requerimientos de rendimiento. En base al estudio de los servicios y la recomendación de la ITU-T G.1010 [4], se pueden resumir en la siguiente tabla:

	Ancho de banda	**Retardo**	**Fluctuación de retardo**	**Perdidas**	**Otros**
Datos corporativos	10% del enlace	<100 ms	Best effort	<0,5%	-
Datos no corporativos	25% del enlace	<100 ms	Best effort	<2%	-
Telefonía IP	384 kbps/llamada	<100 ms	<1 ms	<1%	PoE
Conferencia por video	460 kbps/sesión	<100 ms	<10 ms	<1%	-
Control de accesos	100 kbps/sistema	<100 ms	Best effort	<2%	PoE
Cámaras de seguridad	1,5 Mbps/cámara	<200 ms	<50 ms	<1%	PoE
Gestión de red	1% del enlace	<100 ms	Best effort	<1%	-

Tabla 1: Requerimientos de rendimiento

En segundo lugar, se muestra una lista de los servicios de red que contempla el estudio:

- Acceso inalámbrico.
- Segmentación del dominio de difusión.
- Asignación dinámica de direccionamiento.
- Traducción de direccionamiento de red.
- Resolución de nombres de dominio.
- Monitorización.
- Autenticación.
- Red virtual privada.
- Rutado.
- Almacenamiento en red.

Para proporcionar estos servicios, se ha establecido como requerimiento que el equipamiento de red cuente con las tecnologías y protocolos que se mencionan a continuación:

- VLAN VoIP: Gestión de QoS para telefonía sobre IP.
- PoE: Alimentación sobre ethernet para los equipos que lo requieren (teléfonos, control de accesos y cámaras).
- VLAN: Segmentación del dominio de difusión y separación de servicios.
- NAT: Traducción del direccionamiento privado de la red al direccionamiento público.
- DHCP: Asignación dinámica de direcciones a equipos finales.
- DNS: Resolución de nombres de dominio.
- SNMP: Monitorización.
- TACACS: Autenticación de credenciales para acceso a equipos y recursos de red.
- SSH: Acceso a consola para gestión de los equipos de red.
- VPN: Interconexión con WAN de SATEC.
- OSPF: Anuncio de redes entre sucursales.

Por último, se ha tomado como base el estudio de los requerimientos de dimensionamiento mínimos, para, posteriormente, poder realizar un diseño adecuado a las dimensiones de la sucursal de Bilbao.

ELEMENTOS DE LA RED	**Cantidad**
Puestos de trabajo	40
Salas de reuniones	5
Sistemas de control de accesos	4
Vigilancia por video	5
Laboratorio	20

Tabla 2: Dimensionamiento sucursal de Bilbao

7 ESPECIFICACIONES

En este apartado se recogen las especificaciones que han de cumplirse para ajustarse a los requerimientos planteados en el apartado anterior. En base a estas especificaciones se ha realizado el análisis, la selección y la descripción de la solución de diseño propuesta en apartados posteriores.

Se va a comenzar con la descripción de las especificaciones de rendimiento. Partiendo de la tabla de requerimientos del apartado anterior (Tabla 1), se van a diferenciar 4 grupos. Para cada grupo, se definen los parámetros de rendimiento que se desean cumplir para asegurar sin problemas la QoS esperada, también se calcula el ancho de banda total que necesita cada grupo. Partiendo de un ancho de banda de 300 Mbps y un caso de máxima actividad:

	Ancho de banda	**Retardo**	**Fluctuación de retardo**	**Perdidas**
Datos no corporativos	40% del enlace	<100 ms	<50 ms	<1%
Control de accesos	100 kbps/sistema			
Cámaras de seguridad	1,5 Mbps/cámara			
Gestión de red	0,5% del enlace			
Total	129,4 Mbps			

Tabla 3: Especificaciones de rendimiento grupo 1

Suponiendo los 4 controles de acceso simultáneos y las 5 cámaras activas, se requiere un ancho de banda máximo de 129,4 Mbps.

	Ancho de banda	**Retardo**	**Fluctuación de retardo**	**Perdidas**
Datos corporativos	30% del enlace	<50 ms	<50 ms	<0,5%
Total	90 Mbps			

Tabla 4: Especificaciones de rendimiento grupo 2

	Ancho de banda	**Retardo**	**Fluctuación de retardo**	**Perdidas**
Telefonía IP	0,5 Mbps/llamada	<100 ms	<1 ms	<1%
Total	22,5 Mbps			

Tabla 5: Especificaciones de rendimiento grupo 3

Suponiendo los 40 teléfonos de cada puesto de trabajo y los 5 de las salas de reuniones al mismo tiempo, se requiere un ancho de banda máximo de 22,5 Mbps.

	Ancho de banda	**Retardo**	**Fluctuación de retardo**	**Perdidas**
Conferencia por video	0,5 Mbps/sesión	<50 ms	<10 ms	<1%
Total	2,5 Mbps			

Tabla 6 Especificaciones de rendimiento grupo 4

En la suma total de ancho de banda, podemos comprobar que serían necesario asegurar un máximo de 244,4 Mbps.

A continuación, se van a especificar las características que deben tenerse en cuenta a la hora de seleccionar los componentes de red de la infraestructura a desplegar, para así asegurar el correcto funcionamiento de los servicios de red. Además, se va a tener en cuenta la necesidad de varias características adicionales para proporcionar una infraestructura segura, escalable y de alta disponibilidad.

Antes de nada, se quiere hacer hincapié en que todo el equipamiento a utilizar debe ser equipamiento del fabricante Cisco Systems, con excepción del firewall de Fortinet que pertenece a Iberdrola, y ya que no puede ser sustituido, se podrá utilizar a conveniencia.

7.1 LAN

Los switches son los equipos básicos de una red LAN. Su función es tan necesaria y amplia que es imprescindible que cumplan las especificaciones adecuadas para el tipo de red en la que operan. Para ello, existen 5 tipos de switches predefinidos que ayudan a acotar la selección del equipamiento en función de su propósito.

- Switches de campus
- Switches de data center
- Orientados a la nube
- Switches de ISP
- Switches para rutado virtual

En nuestro caso, **se van a utilizar switches de campus**. Dentro de estos, existen variedad de modelos en función del factor de forma. En nuestro caso, se van a seleccionar **tanto equipos de configuración fija como apilables**.

Adicionalmente, el espacio que estos ocupan en el rack del CPD también es importante, ya que solo se dispone de uno. La unidad de rack es un término para describir el grosor de un equipo de red enrackable. Definido en el EIA-310, una unidad (U) describe un equipo con una altura estándar de 4,45 centímetros y una anchura de 48,26 centímetros. **Los equipos a seleccionar deben cumplir un tamaño de 1 unidad rack (U).**

Por último, se han de tener varias consideraciones adicionales:

- **Densidad de puertos:** los equipos de factor apilable o fijo varían entre 24 y 48 puertos. En el apartado de diseño se decidirá, en función del dimensionamiento planteado en

el apartado anterior, y en función de la topología seleccionada en el siguiente apartado, el número de switches y su densidad concreta para cada situación. **Se** podrán seleccionar **tanto de 24 como de 48 puertos.**

- **Velocidad de puertos:** se seleccionarán obligatoriamente equipos con puertos de un mínimo de **1 Gbps**.

- **Soporte de PoE:** permite a los switches entregar alimentación a equipos finales a través del mismo cable ethernet que los conecta. **Es necesario provisionar a la red de al menos un número de puertos de este tipo igual al número de equipos finales que lo requieran.** Teléfonos IP, puntos de acceso inalámbricos, cámaras de seguridad y controles de acceso.

- **Escalabilidad:** los equipos de core y/o distribución deben tener características de nivel 3. Los de acceso pueden o no poseerlas, siendo suficiente con capacidades de nivel 2.

7.2 WAN

Cualquier red básica que necesite acceso a la WAN, necesita equipos con capacidad de rutado, sin ellos, el tráfico no puede salir de la red LAN. Estos, determinan la vía más adecuada para enviar los paquetes. Interconectan múltiples redes IP entre sí, de carácter público o privado, e incluso son el medio de traducción entre ciertas tecnologías y protocolos.

Todos los equipos de red conocen la dirección del router adyacente que les va a permitir llegar a su destino fuera de su propia red. La habilidad de rutado eficiente y de recuperación frente a fallos de red es crítico para ofrecer el servicio para el que están diseñados. Adicionalmente a esta capacidad de rutado, también ofrecen otro tipo de beneficios:

- Segmentación del dominio de difusión.
- Seguridad avanzada.
- Interconexión de sucursales remotas.
- Agrupar usuarios de forma lógica en función de aplicación o departamento.

Existen variedad de modelos disponibles. Al igual que los switches, existen varios tipos predefinidos para acotar las características requeridas por la red concreta en la que operan.

- Routers de sede
- Routers frontera
- Routers de ISP
- Routers virtuales
- Agregación de WAN
- Industriales
- Pequeños negocios

En nuestro caso **se van a utilizar routers de agregación de WAN**. A diferencia de los switches, no se va a especificar el factor de forma que deben tener, pero **se recomendaría utilizar routers modulares**, ya que sus funciones y propósitos son mucho más amplios que los de un switch y ofrecen mayor versatilidad frente a los prefijados.

Por último, se han de tener varias consideraciones adicionales:

- **Tipo de puertos:** deben tener al menos 3 puertos Ethernet de 1 Gbps.
- **Seguridad:** deben soportar encriptación mediante IPsec.
- **Redundancia:** deben soportar al menos el protocolo HSRP.
- **Rutado:** el protocolo a soportar será OSPFv3, ya que se encuentra desplegado actualmente y no provoca ningún inconveniente.

Independientemente del equipo, modelo o función, los dispositivos de red requieren de una Cisco IOS (Internetwork Operating System). Algunas características de red no están definidas por el equipo físico sino por su versión de IOS, por lo que es imprescindible saber cómo gestionarlas. **Todos los equipos deben tener la última versión estable disponible en la página web del fabricante.**

Es imprescindible, además, que todos los equipos cuenten tanto con una interfaz fuera de banda como una interfaz en banda para su gestión**. Se utilizará el puerto de consola para la gestión fuera de banda y los protocolos SSHv2 y/o HTTPS para la gestión en banda.**

Finalmente, se van a establecer una serie de recomendaciones a tener en cuenta a la hora de realizar el dimensionamiento de la red de acceso:

- **Tomas de red de usuario:** al menos 2 por cada puesto de trabajo.
- **Tomas de red para el resto de equipos:** al menos 1 por cada equipo final, 4 tomas en el caso de servidores y equipos de red.
- **Tomas para salas de conferencia:** Tamaño de aforo + 2 para sistemas de conferencia.
- **Despachos y otras salas independientes:** al menos 4.
- **Laboratorio:** 24-48 puertos, con al menos un 50% con PoE.

8 ANÁLISIS DE ALTERNATIVAS

Tras analizar el estado de la red y los requerimientos de los servicios que debe soportar, y tras establecer las especificaciones, se van a plantear una serie de alternativas que conduzcan a la selección del diseño de la solución adecuada a desplegar.

Para realizar el análisis, se presentan las alternativas a estudiar para resolver las problemáticas y cumplir las especificaciones y, a continuación, se hace una comparación entre ellas. Para tomar una decisión y seleccionar las alternativas apropiadas se van a definir una serie de criterios de selección. Estos criterios pueden o no tener la misma relevancia para la decisión final, es decir, cada criterio pondera un porcentaje concreto en función de lo importante que se considere. Finalmente, teniendo en cuenta los criterios más importantes que repercuten sobre el desarrollo de este trabajo, se muestra una tabla resumen con las valoraciones y la consecuente selección de la alternativa.

8.1 WAN

La característica más importante de esta red, y la que más va a condicionar el diseño final, es su integración en la VPN de SATEC. Por medio de los túneles con Madrid, mencionados en apartados anteriores, se crea la WAN que conecta todas las sucursales de la empresa. Esto permite el acceso a todos los servicios y recursos corporativos que ofrece la empresa. Es decir, proporciona una vía de comunicación segura con otras sucursales de la empresa a través de la red pública de internet.

Desplegar una WAN tiene un coste muy elevado, y, al ser el presupuesto uno de los factores más determinantes en este trabajo, se van a analizar otro tipo de alternativas. Para la creación de una WAN privada sin tener que asumir los grandes costes de desplegar toda la infraestructura, existen infinidad de soluciones. En este análisis solo se contemplan las compatibles con Cisco, ya que todas las redes de SATEC están desplegadas con equipamiento del fabricante y es uno de los requisitos impuestos por Madrid. Además, solo se van a considerar las tecnologías que trabajan en el nivel 3 del modelo OSI.

Se van a analizar 3 tecnologías para esta alternativa.

- **GRE + IPsec**: La tecnología en uso en estos momentos. La más simple, pero la más compleja de gestionar y mantener.
- **DMVPN**: Con su base en GRE+IPsec, pero con grandes mejoras en la escalabilidad y gestión.
- **Auto VPN (SD-WAN):** Tecnología definida por software, basada también en IPsec, pero extremadamente sencilla de utilizar, ya que se gestiona todo de forma automática. Por ello, su precio no es del todo asequible.

8.1.1 Túneles estáticos

GRE es un protocolo de encapsulado que trabaja en la capa 3 del modelo OSI. Es un protocolo punto a punto básico y no seguro desarrollado por Cisco Systems, propuesto como estándar en el RFC 2784 [5] y ampliado en el RFC 2890 [6].

IPsec es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre IP autenticando y/o cifrando cada paquete en un flujo de datos. Está implementado por un conjunto de protocolos criptográficos para asegurar el flujo de paquetes, garantizar la autenticación mutua y establecer parámetros criptográficos. También incluye protocolos para el establecimiento de claves de cifrado. Todos los protocolos de IPsec actúan en la capa de red, la capa 3 del modelo OSI.

En la siguiente figura (Figura 5) se muestra de forma simplificada el funcionamiento de la combinación de Ipsec con GRE.

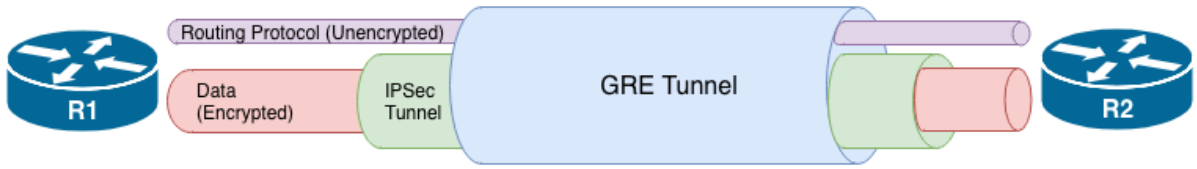

Figura 5: IPsec sobre GRE (REF: www.jannet.hk)

Mediante el uso de ambas tecnologías en conjunto se pueden crear túneles estáticos punto a punto seguros, capaces de soportar paquetes IP broadcast o multicast, utilizados por protocolos de rutado como OSPF.

8.1.2 DMVPN

Es un software del IOS de Cisco, usado por los dispositivos de red para crear conexiones encriptadas seguras, dinámicas y escalables entre sucursales a través de internet, utilizando túneles tanto persistentes como dinámicos. Se basa en varios protocolos de la capa 3 del modelo OSI, entre ellos destacan NHRP [7], mGRE e IPsec. Su característica principal es la capacidad de crear túneles punto a multipunto en una subred de forma dinámica.

Además, es compatible con VRF (Virtual routing and forwarding), permitiendo segregar de forma muy sencilla el tráfico corporativo del tráfico corriente de acceso a internet.

8.1.3 Auto VPN

Meraki MX es una gama de productos de seguridad y SD-WAN de Cisco basados en la nube, con características de red y seguridad totalmente integradas. Todos los productos soportan Auto VPN, la habilidad de configurar VPNs sobre IPsec de forma totalmente automática en cuestión de minutos. Cuentan con una interfaz gráfica que permite gestionar toda la red en varios clics de ratón.

8.1.4 Comparativa

En una topología genérica "Hub and Spoke" (Figura 6) se implementan túneles estáticos (usando GRE + IPSEC) entre un router "hub" ubicado en el centro y sus "spokes", los cuales conectan oficinas sucursales a la sede central.

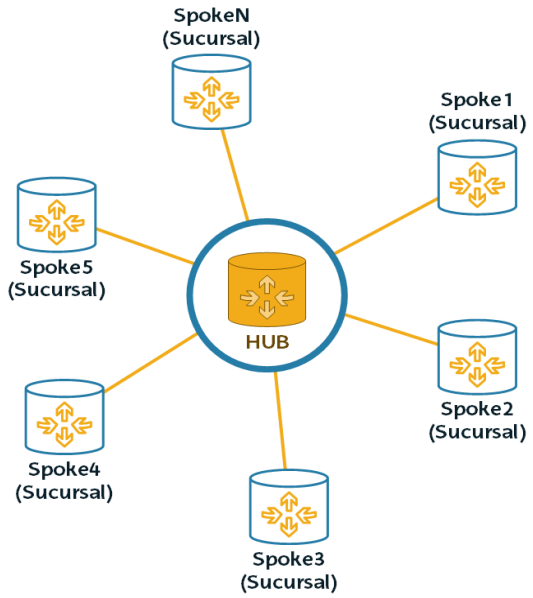

Figura 6: Topología "Hub and Spoke"

Cada nuevo "spoke" requiere que se haga una configuración adicional en el router "hub" y el tráfico entre los "spokes" debe ser desviado a través del "hub" para que salga de un túnel y luego ingrese en otro. Mientras que esta podría ser una solución aceptable a pequeña escala, se vuelve difícil de gestionar cuando los "spokes" van multiplicándose y creciendo en número. Ya que haría falta configurar el "hub" cada vez que se quiere añadir un nuevo "spoke".

En ese momento aparece la necesidad de implementar túneles de forma dinámica (DMVPN), de manera que los "spokes" puedan comunicarse y crear túneles seguros entre ellos sin la necesidad de ocupar un ancho de banda extra en el "hub". Además, cada nuevo "spoke" no requiere la necesidad de configurar un túnel exclusivo e independiente entre él y el "hub". A esto se le conoce como una topología "VPN mesh".

Nuestra red en concreto tiene su "hub" ubicado en Madrid. Supongamos, para simplificar el ejemplo, que contiene tres "Spokes", uno en Bilbao, otro en Vigo y un último en Barcelona. Mientras que una configuración en estrella de "Hub and Spoke" requeriría tres túneles separados expandiéndose desde el router "hub" hacia cada uno de los router "spoke", el GRE multipunto permite que los cuatro routers puedan comunicarse usando una sola única interfaz túnel en la misma subred IP. Esta configuración es habilitada por el NHRP (Next Hop Resolution Protocol) el cual permite que los túneles multipunto sean construidos dinámicamente. En caso de querer incluir una nueva sucursal en Cádiz, por ejemplo, tan solo sería necesario incluir una interfaz túnel en su router y añadirla a la subred IP del DMVPN desplegado.

Por último, Auto VPN se basa en el mismo principio de crear túneles IPsec, con la gran diferencia en que las configuraciones básicas de túnel, e incluso las adicionales para nuevos "spokes" que facilita DMVPN, son realizadas por el equipo de forma automática. Por lo que la gestión se convierte en una tarea muy simple. En cambio, el coste de cambiar el equipamiento es considerablemente superior.

A continuación, se muestran los 4 criterios considerados junto a su ponderación:

- **Coste (50 %)**: El desembolso adicional que supondría para el proyecto, en nuestro caso, al tener un presupuesto muy limitado, es el indicador más importante.

- **Gestión (20 %)**: La dificultad que supondría al administrador de la red el mantenimiento y gestión de dicha tecnología.

- **Simplicidad (15 %)**: El nivel de facilidad que supondría la ejecución de dicha alternativa.

- **Escalabilidad (15%)**: La capacidad de la tecnología de adaptarse a cambios y/o crecimiento.

Se realizarán puntuaciones (1-5) de los criterios para cada alternativa con la mayor precisión y objetividad posible, siendo 5 la mejor nota y 1 la peor. Se tomará la que obtenga la mayor puntuación una vez realizada la media ponderada. En la siguiente tabla (Tabla 7) se muestra el resumen de las puntuaciones y su correspondiente resultado.

Comparativa	**Estático**	**DMVPN**	**Auto VPN**
Coste (50%)	4	4	1
Gestión (20%)	2	4	5
Simplicidad (15%)	2	3	5
Escalabilidad (15%)	1	4	5
Resultado	2,85	3,85	3,00

Tabla 7: Análisis de alternativas 1

Se puede apreciar que Auto VPN es la mejor solución para WANs corporativas, por ello la gran atención que está recibiendo el concepto de SD-WAN en los últimos años. A pesar de ello, por restricciones de presupuesto, **la mejor de las alternativas para este proyecto, es decir, para la sucursal de Bilbao, es DMVPN.**

8.2 LAN

Si anteriormente se analizaba la característica más importante de la red WAN de SATEC, que era la interconexión entre sucursales, ahora se va a analizar la característica más determinante de la red LAN, que es su topología. En ella, se deben cumplir los principales requisitos de dimensionamiento de la red. Además, es la infraestructura base que debe soportar todos los servicios mencionados en los requerimientos.

Para el diseño de las alternativas en lo que a topología respecta, se han analizado y seguido las propuestas de diseño del marco de trabajo de Cisco SONA (Service-Oriented Network Architecture). Más concretamente el componente de "Enterprise Branch Arquitecture" [8] de la capa de infraestructura de red creado por el ESE (Cisco Enterprise Systems Engineering).

En realidad, no existe un diseño de red único válido para cualquier sucursal, cada una tiene sus características, necesidades y peculiaridades concretas. Aun así, en este apartado se van a analizar 3 alternativas de coste, disponibilidad, tamaño y escalabilidad diferentes, de una forma genérica, ofreciendo la posibilidad de adaptarlas de forma sencilla y oportuna al diseño de la red de cada sucursal en concreto.

A pesar de ello, sí que existen componentes de red comunes para todas. Los usuarios hacen uso de ordenadores, portátiles, teléfonos y equipos de video y audio diariamente, estos elementos son los comúnmente conocidos como equipos finales. En las topologías a analizar no se van a contemplar directamente, sino que se englobaran con una nube llamada EF, para así poder observar la estructura de la topología de forma más simple y visual. El diseño de esa nube se mostrará más adelante, en el diseño final de la red, a fin de poder dimensionarla de forma adecuada a nuestra sucursal una vez seleccionada la topología más indicada.

Las alternativas a analizar son las siguientes:

- **Un perfil simple** muy económico que integra el máximo posible de servicios en una única plataforma, aunque no proporciona redundancia ni gran capacidad de usuarios

- **Un perfil de doble nivel** que no necesita un gran esfuerzo de despliegue y es capaz de soportar gran cantidad de usuarios y servicios.

- **Un perfil de nivel múltiple** con gran redundancia y alta disponibilidad.

8.2.1 Perfil simple

Se trata de un perfil recomendado para redes pequeñas que no contienen una gran cantidad de usuarios. A través de la figura (Figura 7) se puede apreciar que consiste en un router de servicios integrados como router por defecto para interconectar tanto la WAN de SATEC como Internet, con la red de área local. Esa interconexión cuenta con alta disponibilidad gracias a su enlace de "backup" con otro ISP. Por otro lado, los switches de acceso directamente conectados al router permiten aumentar considerablemente la capacidad de usuarios.

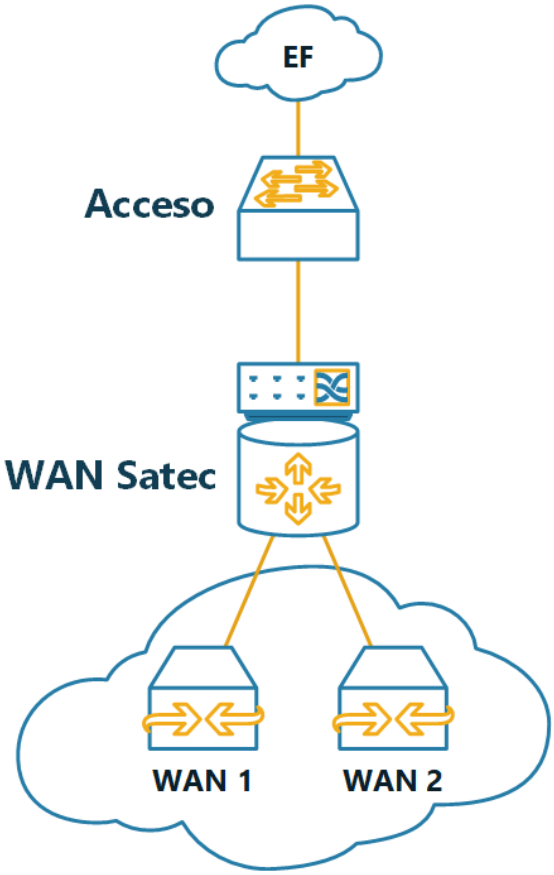

Figura 7: Diagrama perfil simple

Este perfil es de coste muy reducido, y contiene el mínimo número de dispositivos necesarios a gestionar por el equipo de administración. Los puntos negativos se encuentran en la robustez y capacidad de dimensionamiento. Por tener todos los servicios en la misma plataforma existe un punto de fallo único en el router. No existen ningún tipo de redundancia de equipos por lo que cualquier fallo de hardware supondría un corte de servicio. La capacidad de acceso también está limitada al número de puertos del router. Para futuro crecimiento sería necesario incluir un switch de distribución, de tal forma que se evolucionaría a una arquitectura de la capa de enlace en dos niveles.

8.2.2 Perfil doble nivel

Este perfil se basa en redes muy habituales existentes hoy en día. La intención es ilustrar como aplicar servicios avanzados en una sucursal sin necesidad de un gran rediseño de la red actual. Como se puede ver en la figura (Figura 8), consiste en dos routers de servicios integrados conectados a un switch externo de distribución. En este caso la redundancia de ISP también se proporciona, así como redundancia en el router por defecto, para eliminar ese punto de fallo único comentado en la alternativa anterior, con la consecuencia de duplicar el coste en equipamiento de red y labores de gestión.

La red WAN y LAN no se interconectan directamente en este caso, sino que el router se encarga de la red WAN y un switch adicional entre los switches de acceso y el router se encarga de la LAN.

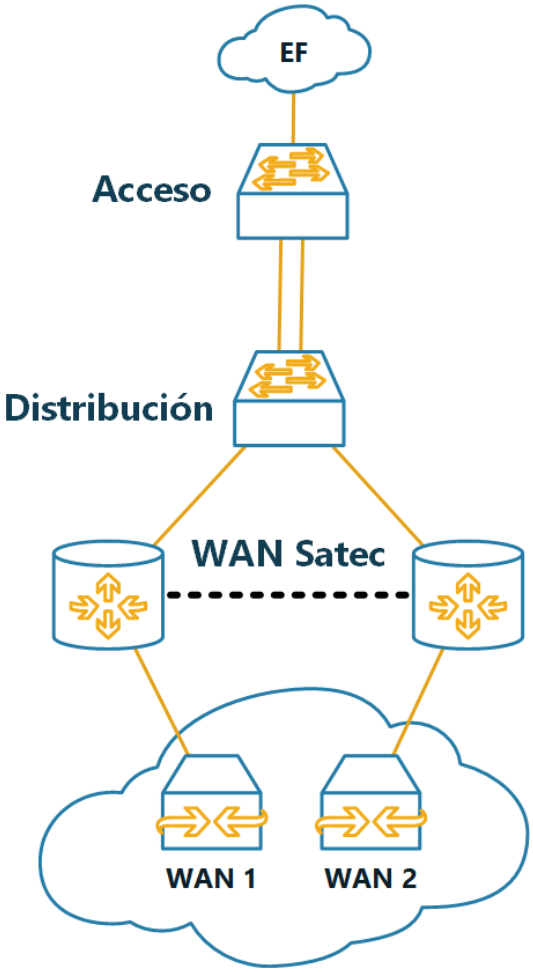

Figura 8: Diagrama perfil nivel doble

Este perfil está ampliamente desplegado y es un paso adelante con respecto al anterior en la migración a perfiles más avanzados de WAN. Es un perfil de coste bajo, con cierto grado de redundancia que permite asegurar un buen nivel de alta disponibilidad. La escalabilidad de este perfil también es considerablemente alta.

8.2.3 Perfil multinivel

Como se observa en la siguiente figura (Figura 9), consiste en un primer nivel de acceso a Internet de alta disponibilidad y redundancia, gracias a sus dos enlaces de conexión con la WAN. Un segundo nivel de seguridad, también de alta disponibilidad, y un tercer nivel de red para la integración de los servicios de la WAN de SATEC. En el nivel de enlace nos encontramos otra vez con un a topología en dos niveles, en este caso con alta disponibilidad en el nivel de distribución a través de una tecnología de apilamiento. Por último, una serie de switches de acceso para dar acceso a los equipos finales a la LAN.

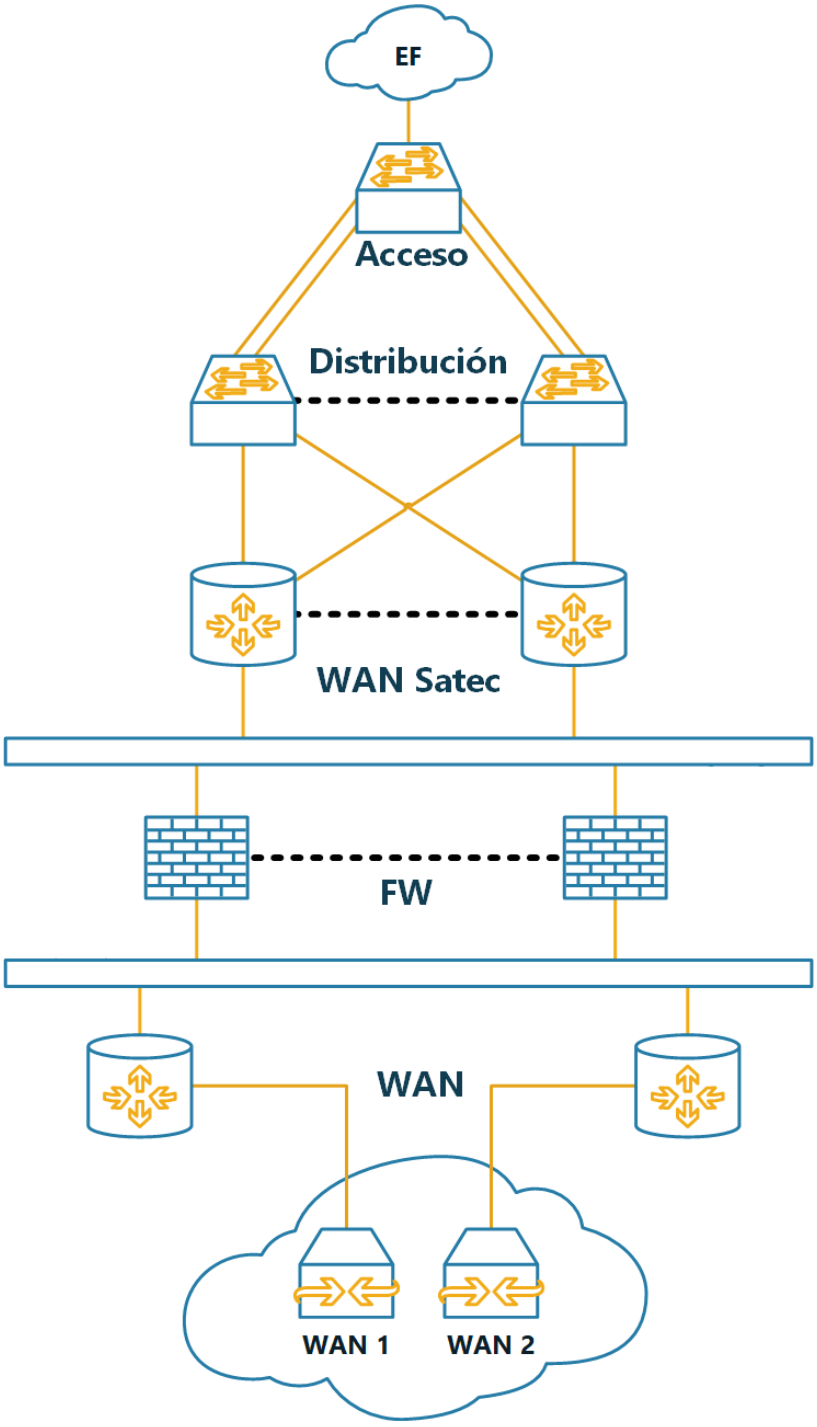

Figura 9: Diagrama perfil multinivel

En resumen, los routers inferiores proporcionan la conectividad a Internet, los firewalls seguridad, los routers internos integración de servicios y los switches apilados la extensión de la LAN.

Este perfil multinivel se asemeja a una pequeña red de campus o una de grandes redes corporativas. El nivel de distribución puede ser fácilmente escalado gracias a la tecnología de apilamiento. En definitiva, con un alto grado de equipamiento a gestionar, pero un coste no muy elevado, se proporciona un muy alto nivel de disponibilidad y redundancia, así como de seguridad y robustez.

8.2.4 Comparativa

Los tres perfiles cumplen los requerimientos y especificaciones definidos en anteriores apartados. Pero, para seleccionar la topología adecuada, se han propuesto, con los componentes habituales de una red, tres perfiles de coste, disponibilidad, dimensión, escalabilidad y funcionalidad variados. Estas tres alternativas proveen la base para el diseño de las redes de las sucursales de SATEC.

Para este trabajo en concreto, se va a seleccionar la topología más adecuada para la sucursal de Bilbao, ya que a pesar de que todas ellas son válidas y cumplen con los requerimientos y especificaciones, es necesario seleccionar la que mejor se adapta a las particularidades de la red bajo estudio.

El perfil simple provee el mayor grado de integración de servicios, a expensas de redundancia y baja tolerancia a fallos.

El perfil de doble nivel incorpora cierto grado de disponibilidad con conectividad WAN y LAN distribuida.

El perfil multinivel ofrece la mayor disponibilidad, pero no ofrece integración de servicios en una sola plataforma.

A continuación, se muestran los 4 criterios considerados junto a su ponderación:

- **Coste (40 %)**: El desembolso que supondría para el proyecto, en nuestro caso, al tener un presupuesto muy limitado, es el indicador más importante.

- **Disponibilidad (20 %)**: El grado de disponibilidad y redundancia que aportaría la topología a la continuidad del servicio. Al contar con servicios a clientes, es muy importante.

- **Escalabilidad (20%):** La capacidad de la topología de adaptarse a cambios y/o crecimiento. Como se ha podido ver, una topología sin posibilidad de escalar como la que se tenía hasta ahora conlleva muchos problemas.

- **Seguridad (10 %):** El grado de seguridad que posee la red frente a ataques externos.

- **Gestión (10 %)**: La complejidad y/o necesidad de gestión y mantenimiento del equipamiento de red.

Se realizarán puntuaciones (1-5) de los criterios para cada alternativa con la mayor precisión y objetividad posible, siendo 5 la mejor nota y 1 la peor. Se tomará la que obtenga la mayor puntuación una vez realizada la media ponderada.

En la siguiente tabla (Tabla 8) se muestra el resumen de las puntuaciones y su correspondiente resultado.

Comparativa	**Simple**	**Doble nivel**	**Nivel Múltiple**
Coste (40%)	4	3	2
Disponibilidad (20%)	1	2	4
Escalabilidad (20%)	1	4	5
Seguridad (10%)	2	2	4
Gestión (10 %)	5	4	3
Resultado	2,7	3,0	3,3

Tabla 8: Análisis de alternativas 2

Se puede apreciar que según se añaden características, a pesar de que aumenta el coste, su rendimiento se ve aumentado, por lo **que la mejor opción para la sucursal de Bilbao es la de utilizar una topología con un perfil multinivel.**

9 ANÁLISIS DE RIESGOS

Este es un proyecto con riesgos considerablemente reducidos, pero a pesar de ello, es importante haber realizado un análisis. Se realizaron los ejercicios de identificación de riesgos al inicio del proyecto, pero, han sido revisados periódicamente para detectar con mayor exactitud riesgos surgidos posteriormente que podrían haber tenido un impacto sobre el proyecto no detectado con anterioridad.

Primeramente, se evaluarán los riesgos para identificar la severidad de las medidas a tomar. Tanto para evitar que sucedan como para mitigar su impacto en el caso de que sí sucedan. Posteriormente se propondrá un plan de contingencia en función del nivel de riesgo que supongan.

A cada riesgo identificado se le asignará:

- Probabilidad: 1 a 10, siendo 1 la más baja y 10 la más alta.
- Impacto: 1 a 10, siendo 1 la más baja y 10 la más alta.

La prioridad e importancia del riesgo (PIR) se calcula mediante la fórmula:

PIR = Probabilidad x Impacto

En función del resultado obtenido, se le asignará a cada riesgo un color identificativo:

- Si PIR > 40 se le asigna un identificador **ROJO,** se tomarán medidas drásticas.
- Si 40 ≥ PIR > 16 se le asigna un identificador **NARANJA**, se tomarán medidas moderadas.
- Si 16 ≥ PIR ≥ 1 se le asigna un identificador **VERDE**, se tomarán ligeras medidas de precaución.

No lograr acceder a alguno de los equipos de la red: en caso de no lograr acceder al cliente de consola de alguno de los equipos, ya sea por no conocer la contraseña de acceso o incluso la de permisos de administración, dificultaría mucho las tares de análisis y/o administración del equipo.

- Probabilidad: 6
- Impacto: 9
- PIR: 54

Plan de contingencia: sería necesario probar con técnicas y herramientas de fuerza bruta para la obtención de la clave. En caso de no lograrse, habría que inspeccionar todas sus conexiones y tráfico generado para identificar si se trata de un equipo de función crítica sobre el servicio. En caso de serlo, se detendría la continuación del proyecto para realizar un plan detallado.

Pasar por alto parámetros de la configuración: no analizar cada parámetro de la configuración de los equipos actualmente en producción podría suponer el diseño incorrecto de las mejoras a introducir.

- Probabilidad: 5
- Impacto: 4
- PIR: 20

Plan de contingencia: será necesario al inicio del proyecto realizar un "backup" de todas las configuraciones de los equipos en producción, así como del estado y la información técnica de los mismos.

Provocar caída del servicio durante manipulación: podría darse la situación de hallarse siguiendo uno de los cientos de latiguillos que interconectan los equipos de la red y provocar un corte.

- Probabilidad: 3
- Impacto: 5
- PIR: 15

Plan de contingencia: se avisará a un superior el comienzo de la revisión de cableado para estar alerta por si algún servicio pudiera ser interrumpido.

Sobredimensionamiento: Diseñar una red excesivamente grande y robusta supone, al igual que excesivamente pequeña y frágil, un grave problema. A pesar de que en estos momentos el bajo rendimiento de la red esté dando lugar a pérdidas económicas, un sobredimensionamiento conllevaría una inversión de baja amortización, con un alto grado de recursos en desuso.

- Probabilidad: 5
- Impacto: 5
- PIR: 25

Plan de contingencia: Se realizará un análisis de dimensionamiento y previsión de crecimiento previa consulta con el director técnico de la sucursal.

10 DESCRIPCIÓN DE LA SOLUCIÓN PROPUESTA

En este apartado se va a plantear el diseño final al que se ha llegado tras analizar los problemas de la red, los requerimientos de QoS, las especificaciones y las alternativas.

En la siguiente figura (Figura 10) se va a mostrar un diagrama de la solución completa, sin mucho grado de detalle, para poder visualizar, a lo largo del apartado, dónde encajan cada una de las partes de la red que se van ir explicando. La descripción del diseño se ha dividido en dos grandes apartados, el de interconexión con la WAN y el de despliegue de la propia red LAN de la sucursal de Bilbao.

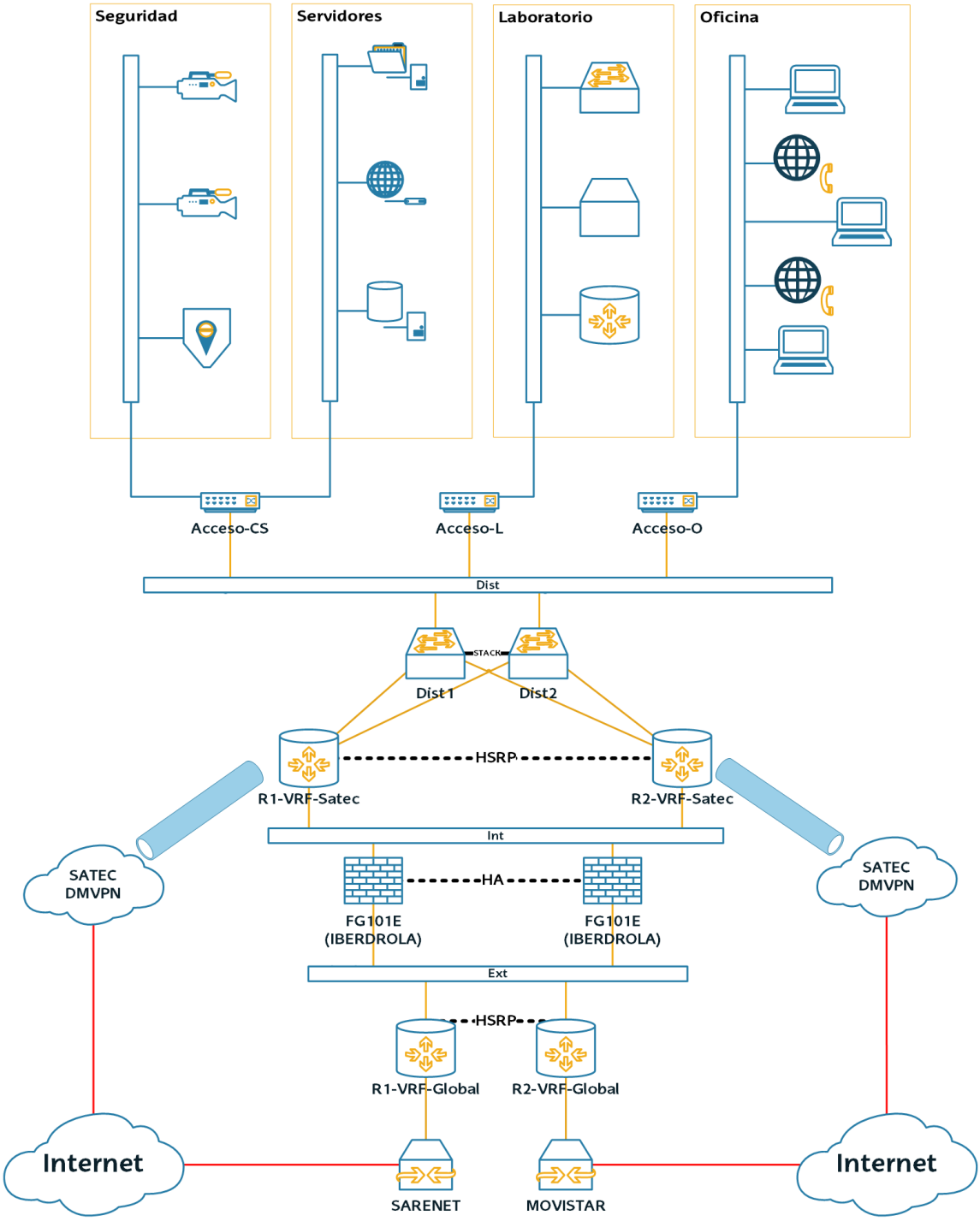

Figura 10: Red de Satec Bilbao

10.1 WAN

El primero de los apartados es el de la integración de la red con la WAN de SATEC e Internet. Como se ha podido observar en el análisis de alternativas (Tabla 7), la mejor solución para realizar esa integración es utilizar la tecnología DMVPN de Cisco, que junto al uso de VRFs nos permite hacerlo de forma totalmente independiente a la interconexión con Internet. A continuación, se van a explicar el diseño de ambas interconexiones, además del uso de la tecnología VRF.

10.1.1 DMVPN

Se va a comenzar mostrando el esquema de DMVPN, para, posteriormente, describir su papel en la red de Bilbao.

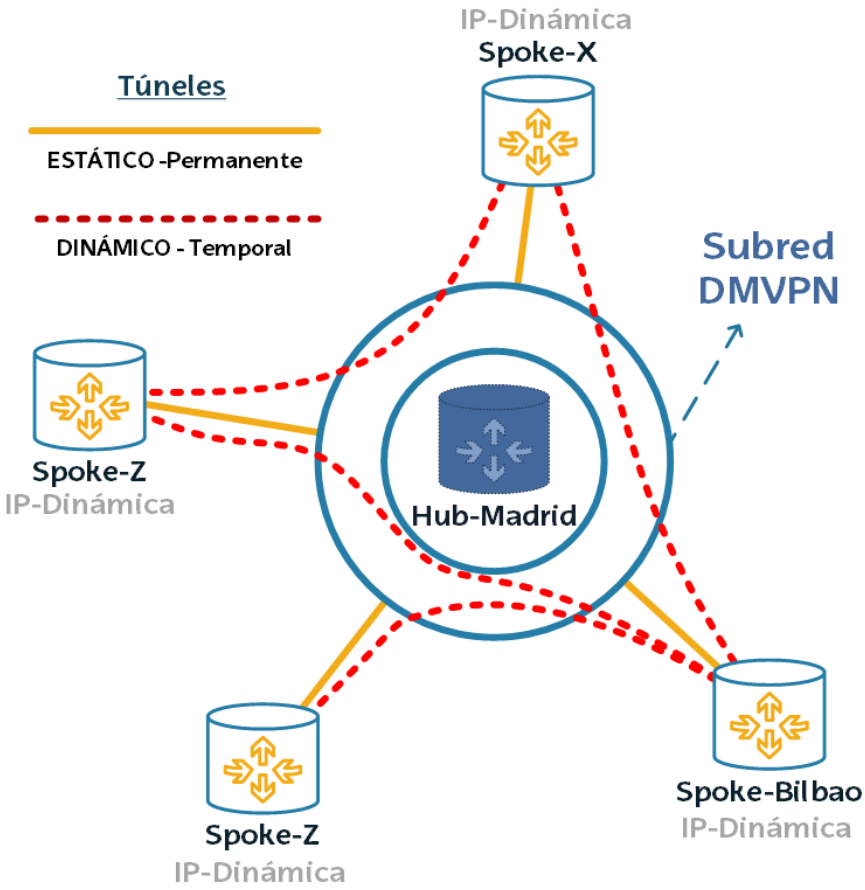

Figura 11: DMVPN Satec

El router encargado de permitir el acceso de los equipos de la sucursal de Bilbao a la WAN de SATEC y viceversa posee una de sus interfaces en la subred de la VPN dinámica multipunto. Gracias a ello, y a través de comandos del protocolo NHRP, el hub en Madrid no necesita conocer datos de par del spoke en Bilbao. El spoke se encarga de crear túneles GRE de forma dinámica con el hub en Madrid.

Por medio de ese túnel, el spoke es capaz de registrarse en la red de SATEC. En el caso del hub, se encarga de redistribuir la información de rutado dinámico (en nuestro caso OSPF) que le llega por el túnel. Así, muestra la red de Bilbao a otros spokes que quieran comunicarse con la sucursal. De la misma forma, el spoke de Bilbao conoce el direccionamiento del resto de sucursales gracias al túnel que ha creado con Madrid y por el que recibe información de OSPF de otras redes que se hayan registrado, también, con NHRP.

Con esa información, el spoke es capaz de crear túneles temporales con otros spokes de la WAN. Se evita con ello la necesidad de reenviar todo el tráfico a través del túnel con Madrid, para después, el hub de Madrid, reenviarlo por el túnel con la otra sucursal en cuestión.

Para todo ello, tan solo es necesario conocer la IP del hub y los respectivos parámetros de seguridad de la subred DMVPN. Gracias a esto, la IP de los spokes puede ser dinámica, y como se verá a continuación se puede disponer de redundancia de túneles e ISPs.

10.1.2 VRF

En este apartado se va a mostrar el diseño que se ha planteado para segregar, de forma virtual, el spoke que realiza las funciones arriba mencionadas, y el router que da salida a Internet a través del ISP.

Como se puede apreciar en el diagrama que se muestra al final del apartado (Figura 12), ambas instancias del router están separadas por un firewall que realiza las tareas de seguridad para el tráfico con origen y destino en Internet. El tráfico con origen o destino la WAN de SATEC no necesita de dichas características ya que el propio conjunto de protocolos de IPsec que utiliza DMVPN proporciona la seguridad requerida.

Por lo tanto, el tráfico corporativo de SATEC proveniente de la LAN o saliente del túnel se desencapsula/encapsula en el router de la instancia de VRF “SATEC”. El resto del tráfico se envía al firewall. Finalmente, todo el tráfico, entrante o saliente, encapsulado o no, se procesa a través del router virtual denominado “Global”.

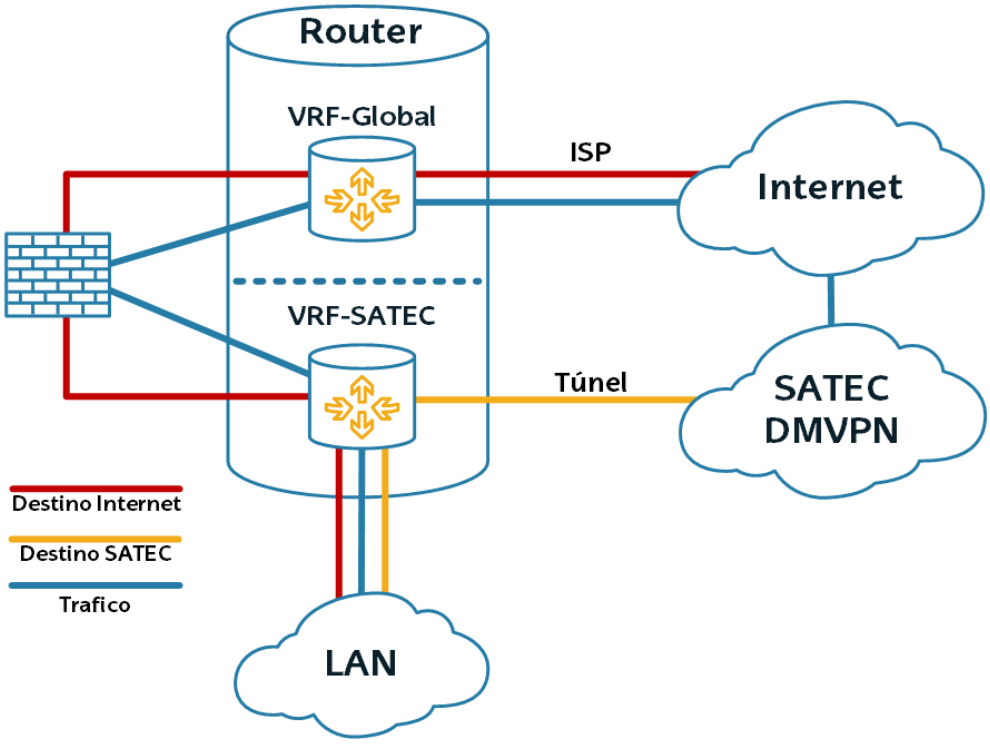

Figura 12: Implementación de VRF

En caso de que, para esta o cualquier otra sucursal hiciera falta incluir otra DMVPN independiente, se podría crear otra VRF con la misma función que la VRF denominada "SATEC".

10.1.3 ISPs

Por último, se va a mostrar el diseño para el acceso a Internet. En lo que a proveedores de servicio respecta, se van a mantener los dos accesos que se tenían en un principio. De todas formas, se va a comenzar a utilizar la salida que proporciona Movistar (300Mbps) para poder asegurar la QoS de 240 Mbps que requieren todos los servicios en un caso de máxima demanda.

El acceso a través de Sarenet (<100Mbps) solo se utilizará en caso de pérdida del acceso a través de Movistar, dejando todo el ancho de banda que proporciona para el uso por los empleados que trabajan de forma independiente para Iberdrola.

Para ello, se establecerá el router conectado a Movistar como primario (HSRP) en la interfaz LAN, aplicando mayor prioridad en su configuración. Por otro lado, el router en espera, es decir, el router conectado a Sarenet, monitorizará la interfaz de Movistar, para poder establecerse como activo en caso de esa mencionada pérdida de acceso a internet en el router conectado a Movistar.

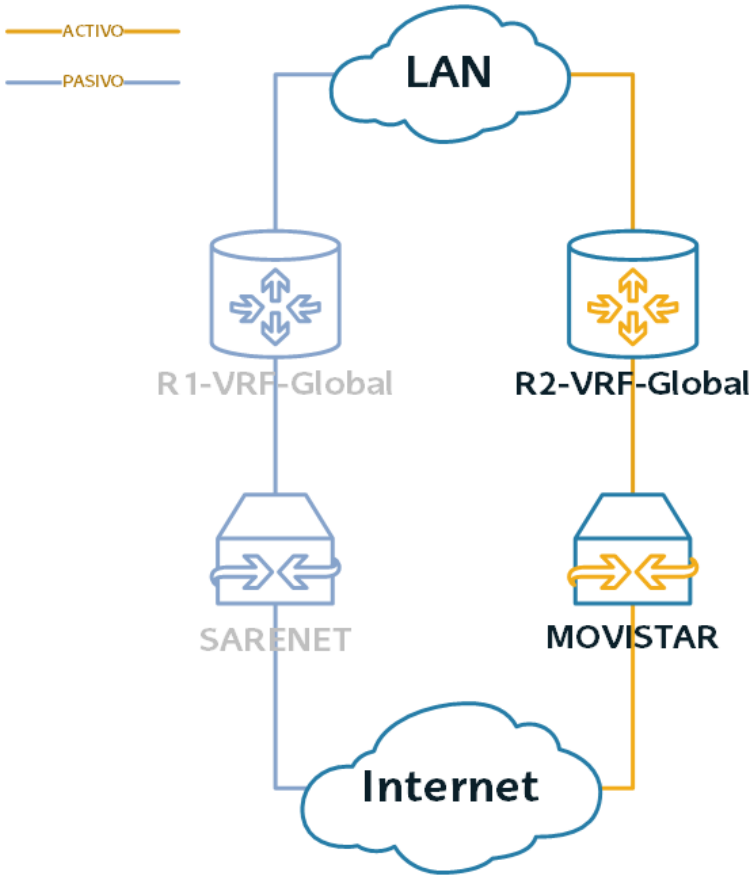

Figura 13: Terminación ISPs

Además, se tendrán que reducir las políticas de QoS especificadas, ya que los menos de 100Mbps de Sarenet no podrían soportar todo el tráfico generado por la red.

10.2 LAN

Una vez expuestos los aspectos más importantes de la interconexión con la WAN, se van a desarrollar los aspectos de diseño que caracterizan la infraestructura de la propia red de la sucursal de Bilbao.

Como se adelantaba en el análisis de alternativas, se ha seleccionado una topología multinivel. Esta se encuentra compuesta por una capa de red en tres niveles y una capa de enlace en dos, divididas de la siguiente forma:

- Capa de red
  - Internet
  - Seguridad
  - Servicios corporativos de Satec
- Capa de enlace
  - Core/Distribución
  - Acceso

Los tres niveles de la capa de red, es decir, el de acceso a Internet, el de seguridad, y el tercero para servicios corporativos, en lo que a WAN respecta, ya se han comentado en el apartado anterior. En este apartado se van a explicar los aspectos de la LAN.

Los dos niveles de la capa de enlace se encuentran ambos de forma íntegra en esa LAN. El nivel Core/Distribución es el nivel intermedio entre la capa de red y el nivel de acceso, es el encargado de intercomunicar todos los equipos de la sucursal a nivel 2 de la capa OSI. El nivel de acceso es el último nivel entre la red y los equipos finales, es decir, es el encargado de extender el dominio del core hasta los dispositivos que realmente hacen uso de la red de la sucursal.

10.2.1 Capa de red – Core

Se va comenzar explicando la topología seleccionada para la capa de red. En el diagrama que se muestra a continuación (Figura 14), se contemplan los 6 elementos que la componen, a pesar de que físicamente, solo actúan 2. Estos 2 equipos son el router y el firewall, divididos de la siguiente forma:

- Router
    1. R1
        - VRF-Satec
        - VRF-Global
    2. R2
        - VRF-Satec
        - VRF-Global
- Firewall
    1. FG101E-1
    2. FG101E-2

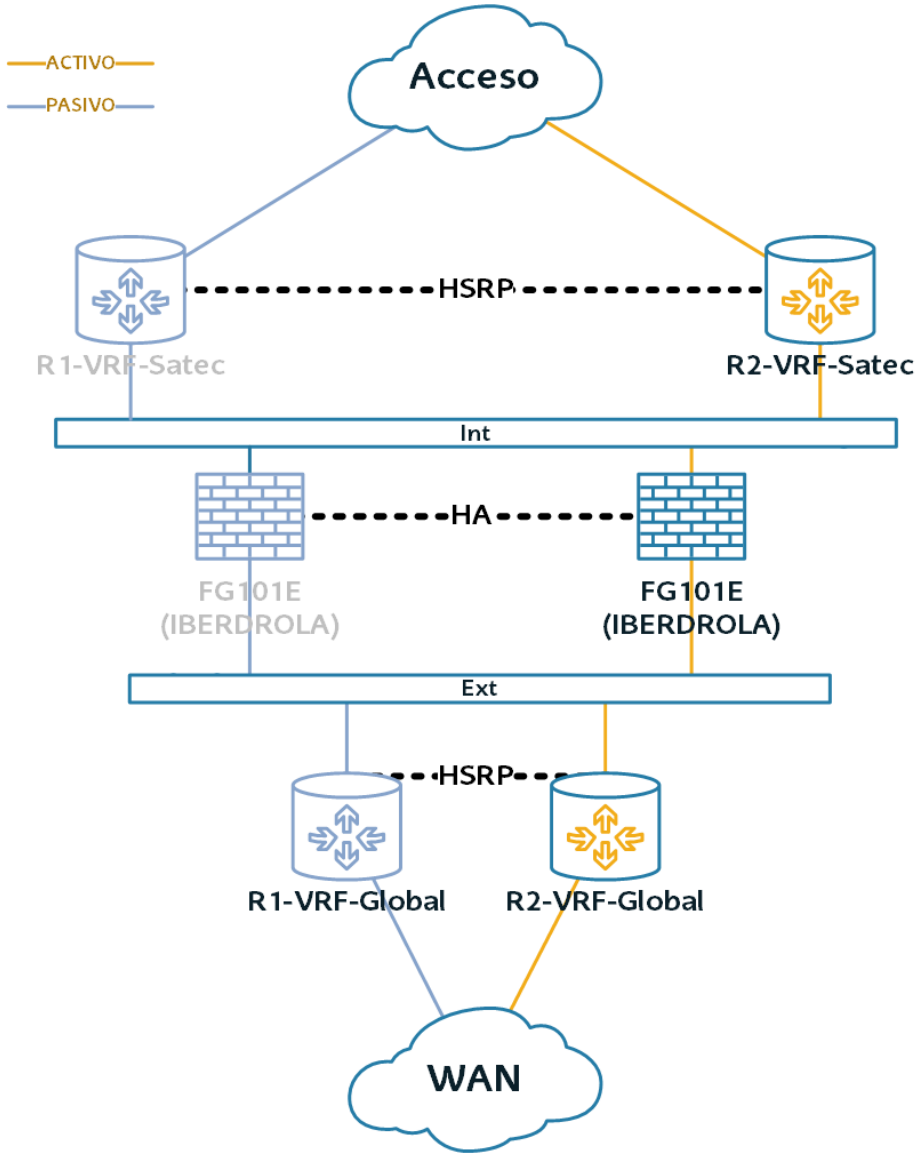

Figura 14: Capa de red Satec Bilbao – LAN Core

Como ya se ha podido apreciar en apartados anteriores, el acceso a servicios corporativos de SATEC y el acceso global a internet se encuentran desplegados de forma virtual con VRFs en un mismo router. El nivel de seguridad, formado por una pareja de firewalls, se encuentra, como se ha podido ya apreciar, entre esos dos routers.

Centrándonos ahora en las características concretas de la red, se van a desarrollar los aspectos de redundancia y alta disponibilidad. Tanto el firewall, como los dos routers están diseñados de la misma forma.

Los 3 equipos se encuentran duplicados, es decir, existe, para cada equipo, un segundo equipo desplegado con funcionalidades idénticas. Dichas funcionalidades se encuentran virtualizadas de tal forma que ambos equipos pueden físicamente desempeñarlas. En el diagrama (Figura 14) se han dibujado de color más oscuro los equipos que se encuentran en estado de espera. Esto se realiza mediante los protocolos HSRP (Cisco) y FGCP (Fortinet). Gracias a este diseño, en caso de avería de cualquiera de los equipos, el otro pasaría a estar activo y la red seguiría funcionando de forma normal.

En el caso de caída de alguno de los enlaces, a través de comandos de tracking de HSRP y configuraciones de "remote link failover" de FGCP también se puede lograr redundancia de caminos.

10.2.2 Capa de enlace – Core/Distribución

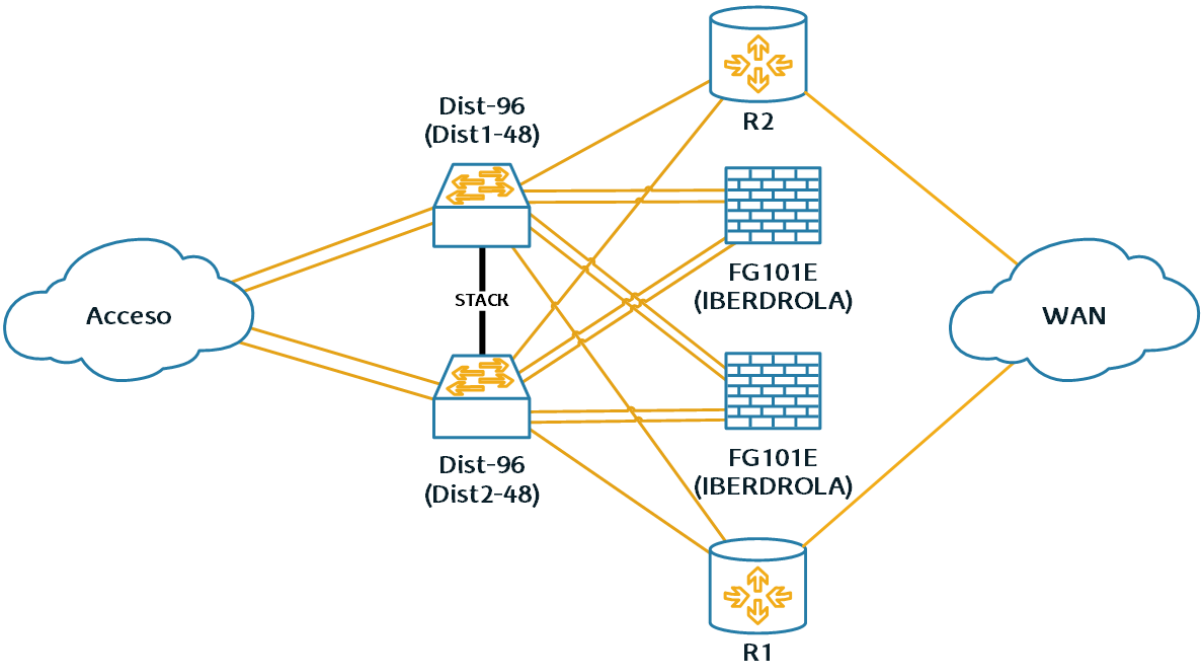

Figura 15: Capa de enlace Satec Bilbao – LAN Core

Como se puede observar, los routers y los firewalls no se encuentran directamente conectados entre sí, sino que lo hacen a través del switch de distribución.

Excepto por el enlace entre los routers y la WAN, todos los enlaces se encuentran duplicados mediante LACP, que además de proveer redundancia, duplica la capacidad. El switch de distribución se encuentra también duplicado, al igual que lo estaban los equipos de la capa de red. En este caso, a través de la tecnología StackWise de Cisco, que permite controlar ambos equipos desde el maestro. En caso de avería de cualquiera de ellos, el otro tomaría el control, proporcionando una alta disponibilidad.

10.2.3 Capa de red – Acceso

Este apartado está dedicado al diseño del nivel 3 de la capa OSI de la red LAN, más concretamente al protocolo de asignación de direccionamiento dinámico (DHCP) y la separación de las diferentes redes que componen la red de la sucursal de Bilbao en función de los equipos finales que hacen uso de ella.

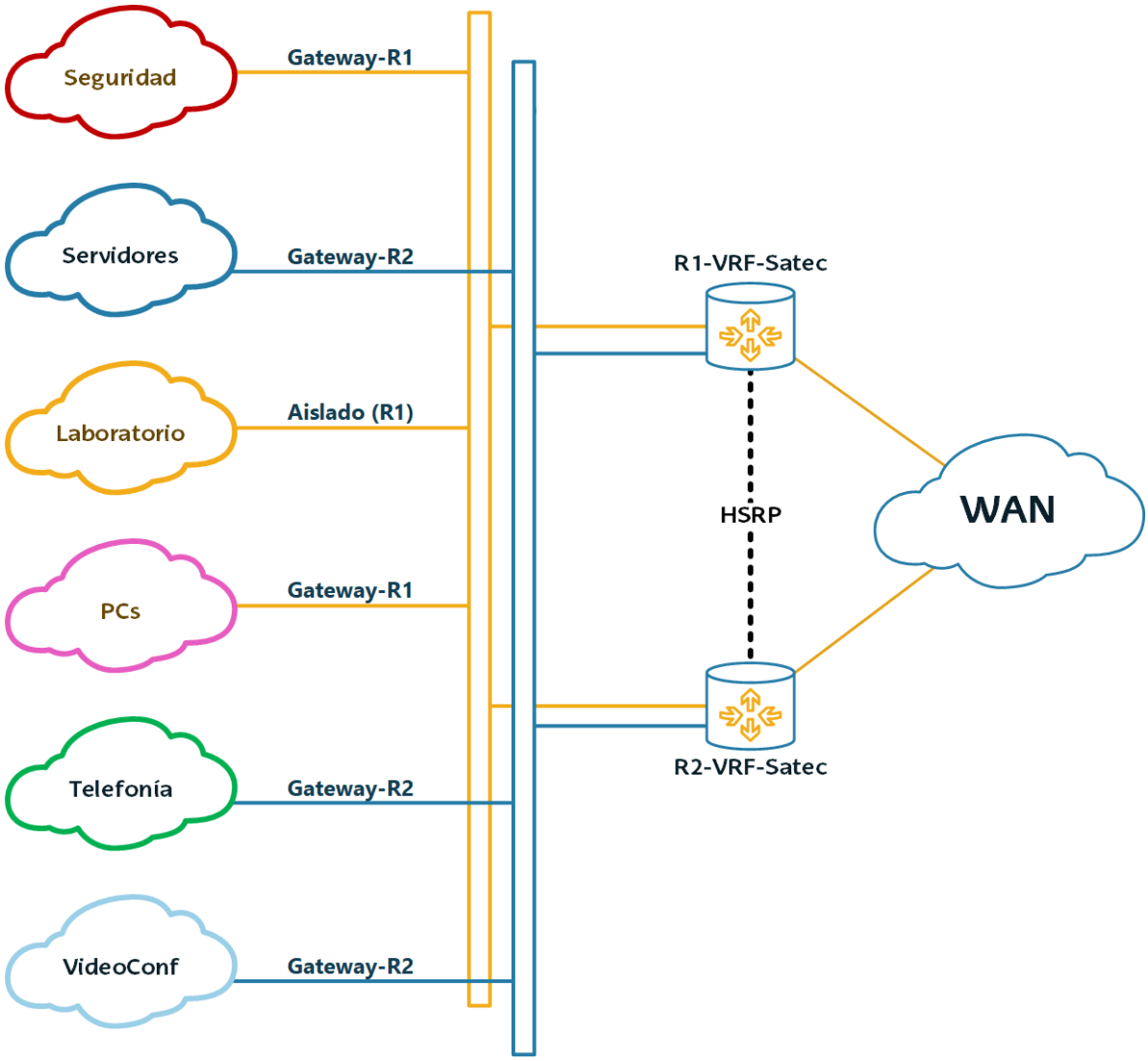

Figura 16: Capa de red Satec Bilbao – LAN Acceso

A la hora de diseñar la estructura de dominios de broadcast y direccionamiento, es importante prestar atención a dos factores clave. Por un lado, el tipo de dispositivo que se va a conectar a dicha red. Es decir, la función que va a desempeñar, la necesidad de IP fija o dinámica, los requerimientos de ancho de banda y/o la disponibilidad que requiere. Por otro lado, el router que va a hacerse cargo de esa red, es decir, el router por defecto que se va a encargar de proveer el acceso a los servicios que el dispositivo requiere.

Para esto, se han identificado los diferentes dispositivos que harán uso de la red y los routers por defecto disponibles para proporcionar los servicios. A cada dispositivo, se le ha asignado una red diferente, con un router por defecto diferente, y sus propias características de direccionamiento.

Se han identificado un total de 6 tipos de dispositivos diferentes:

1. Equipamiento de seguridad perimetral
    a. Direccionamiento: Fijo
    b. Router por defecto: R1
2. Servidores
    a. Direccionamiento: Fijo
    b. Router por defecto: R2
3. Equipamiento de laboratorio
    a. Direccionamiento: DHCP
    b. Router por defecto: Aislado (R1 a través de la red de PCs)
4. Ordenadores portátiles de los empleados
    a. Direccionamiento: DHCP
    b. Router por defecto: R1
5. Teléfonos
    a. Direccionamiento: DHCP
    b. Router por defecto: R2
6. Sistemas de videoconferencia
    a. Direccionamiento: DHCP
    b. Router por defecto: R2

Para lograr este diseño, la configuración de ambos routers será idéntica excepto en 1 parámetro. El de configuración de HSRP. Para lograr el balanceo de carga de routers por defecto se va a utilizar MHSRP, una opción de HSRP que permite asignar de forma independiente prioridades de Activo-Pasivo diferentes para cada red.

10.2.4 Capa de enlace – Acceso

Por último, se va describir el diseño de la capa de enlace del nivel de acceso. Para ello, previamente, ha sido necesario la realización de un análisis de dimensionamiento. En base a los requerimientos y las especificaciones, se van a tomar una serie de decisiones para proporcionar acceso a todos los equipos que puedan requerir hacer uso de la red.

1. Equipamiento de seguridad perimetral
    - Puertos (Total/Con PoE): 9/9
2. Servidores
    - Puertos (Total/Con PoE): 8/0
3. Equipamiento de laboratorio
    - Puertos (Total/Con PoE): 24/24
4. Ordenadores portátiles de los empleados
    - Puertos (Total/Con PoE): 110/0
5. Teléfonos
    - Puertos (Total/Con PoE): 45/45
6. Sistemas de videoconferencia
    - Puertos (Total/Con PoE): 10/10

Para llevar esto a cabo sin utilizar una cantidad innecesaria de switches, se han agrupado los 6 tipos de dispositivos en 3 de mayor similitud y cercanía.

- Oficina (165 puertos/55-PoE)
  - Ordenadores portátiles
  - Teléfonos
  - Sistemas de videoconferencia
- Laboratorio (24-puertos/24-PoE)
- Seguridad y servidores (17-puertos/9-PoE)
  - Controles de acceso
  - Cámaras
  - Servidores

Estos 3 grupos suman un total de 196 puertos, de los cuales 88 requieren de PoE. A continuación, se muestra el diseño más adecuado para ofrecer las capacidades propuestas sin comprometer la escalabilidad de la red (Figura 17).

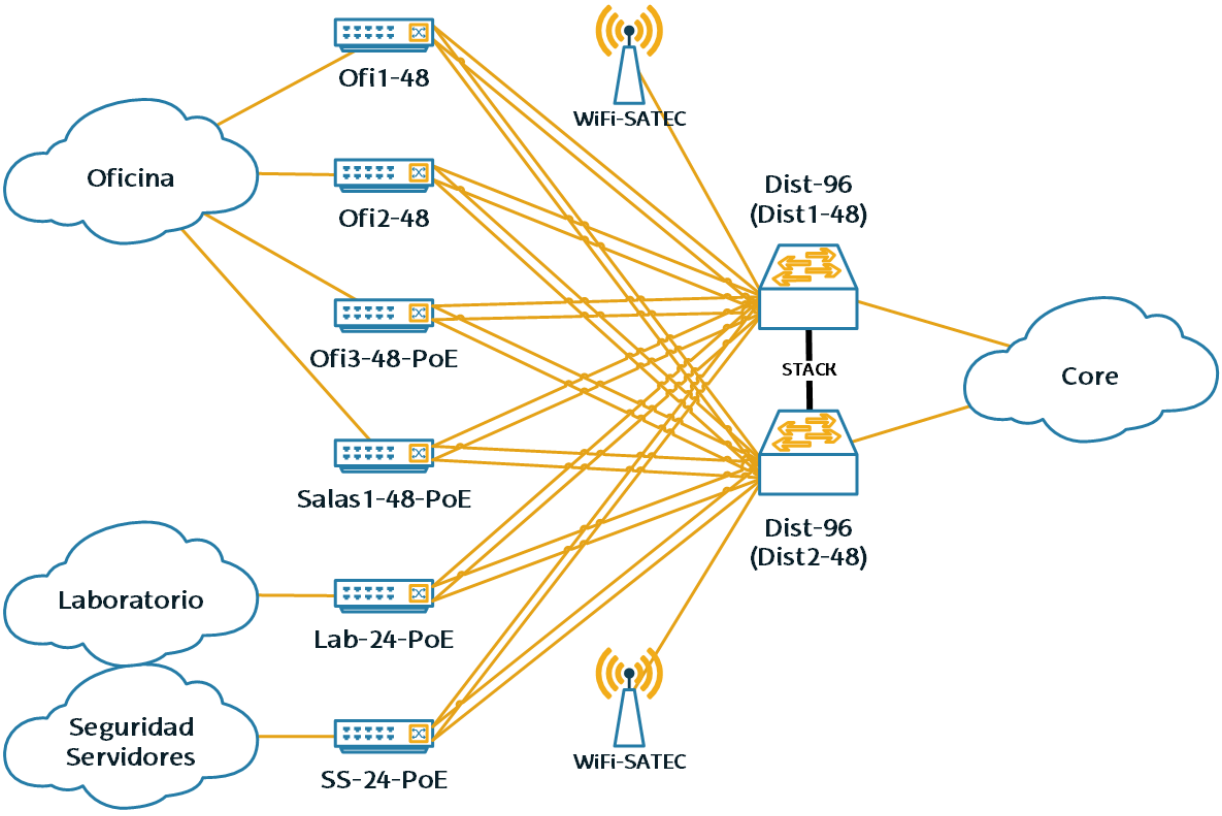

Figura 17: Capa de enlace Satec Bilbao – LAN Acceso

Un total de 8 switches, 4 de 48 puertos sin PoE, 2 de 48 puertos con PoE y 2 de 24 puertos con PoE. Todos los switches de nivel 2, es decir, los de la capa de acceso, poseen 4 enlaces reservados para el la conexión con el nivel superior. La capacidad total de la red de acceso es de 240 puertos, de los cuales 144 poseen PoE. La capacidad total de la red de distribución es de 96 puertos, de los cuales 38 se encuentran ocupados por equipos propios de la red.

10.2.5 Nivel físico

Finalmente, se muestra el esquema de conexionado y ubicación de todos los equipos de la infraestructura, así como el modelo de los mismos (Figura 18).

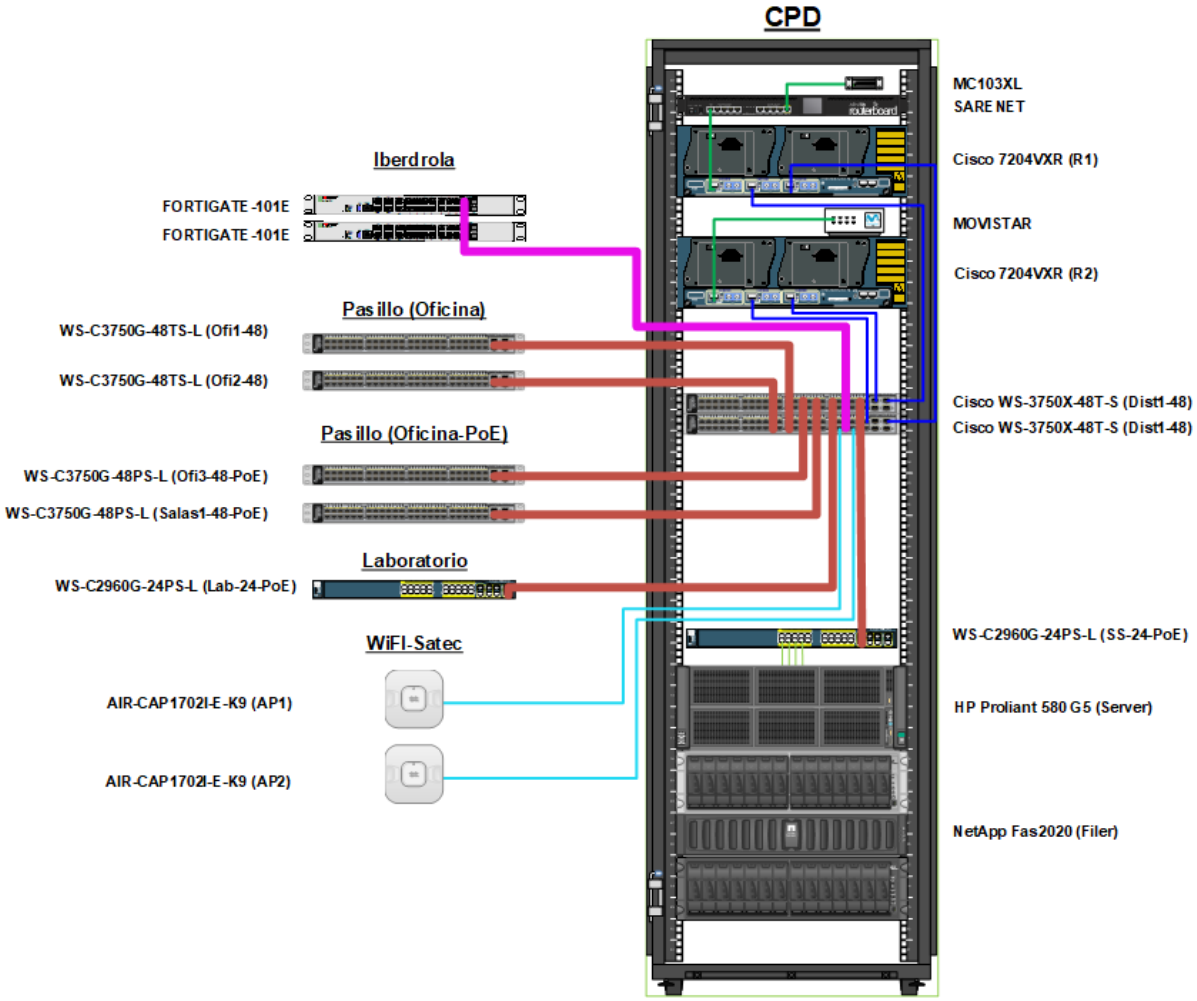

Figura 18: Capa física - Satec Bilbao

El grosor de las líneas indica el número de cables. Las líneas más gruesas indican cuatro latiguillos, es decir, representan cuatro enlaces. Las líneas más delgadas representan un solo latiguillo.

11 METODOLOGÍA

11.1 DESCRIPCIÓN DE TAREAS

En este apartado se presenta la descripción de las tareas realizadas para la consecución del trabajo. Antes de nada, se mencionan brevemente y a continuación, se detalla cada una de ellas.

Se ha divido la realización del trabajo en 13 fases consecutivas fácilmente diferenciables, sin incluir la tarea general de llevar a cabo la documentación pertinente correspondiente a cada una de las fases, realizada de forma paralela a la ejecución de cada una de las fases descritas. A continuación, se presenta un resumen de dichas fases:

1. Establecimiento de objetivos
2. Análisis de situación
3. Análisis de problemas
4. Análisis de los requerimientos
5. Definición de especificaciones
6. Análisis de alternativas
7. Selección de alternativas
8. Diseño de la solución
9. Descripción de la solución
10. Presupuesto
11. Análisis de rentabilidad
12. Plan de migración
13. Manual de administración

Para lograr que el proyecto no perdiese el sentido y se descontrolase, era imprescindible comenzar estableciendo de forma clara tanto el objetivo principal del proyecto como el alcance del mismo, por lo que la tarea inicial fue el establecimiento de los objetivos. Para ello, se realizaron varias reuniones con diferentes personas, incluyendo a la directora del TFG, el director de la cooperación educativa, el director técnico de la oficina y el departamento de TI de la empresa. A partir de esa definición de objetivos, se comenzaron con las tareas para lograr alcanzarlos.

En primer lugar, se intentó reunir toda la información y documentación disponible para conseguir el direccionamiento de nivel 3 de los equipos. Toda ella era de carácter dudoso y con fecha de 2017, por lo que se optó por desplazarse físicamente hasta el CPD (centro de procesado de datos) que se encuentra en el laboratorio de la oficina para comprobar, tanto el conexionado, como la configuración en producción.

Una vez comprendida la situación, se realizó un análisis detallado de los problemas de la infraestructura que podían estar afectando al rendimiento de la red, así como los que podrían suponer un inconveniente en el fututo.

Posteriormente, se analizó el ya mencionado estudio de los requerimientos de los servicios realizado por otro de los alumnos en cooperación educativa en la empresa [3], para a continuación, definir las especificaciones para la realización de un diseño de red adecuado.

Tras analizar las alternativas existentes para la resolución de los problemas identificados, se llevó a cabo una selección de las alternativas más adecuadas.

Más adelante, se realizó tanto un diseño de red como una descripción del mismo acorde a los requerimientos, las especificaciones y las alternativas seleccionadas en fases previas.

Finalmente, una vez realizadas todas las tareas descritas, se hizo una estimación de los costes del proyecto de diseño y un presupuesto de su implantación, así como un análisis de rentabilidad.

11.2 CRONOGRAMA

En este apartado se representan de forma gráfica (Tabla 9) los paquetes de trabajo llevados a cabo, junto a su dedicación en horas, su duración en semanas y sus fechas de realización. Al final, se muestra el número de horas dedicadas al proyecto a la semana durante las 10 semanas de su duración, y el cómputo total de horas dedicadas al mismo.

Cronograma		Mayo			Junio				Julio			T(h)
		S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	
PT0	Familiarización y Formación	10 semanas										34
T001	Definición del proyecto	8										8
T002	Establecimiento de objetivos		8									8
T002	Asistencia a cursos de CCNA		2	2	2	2	2	2	2	2	2	18
PT1	Analisis de situación	4 semanas										52
T101	Analisis del nivel fisico	8	8									16
T102	Analisis del nivel de enlace		8									8
T103	Analisis del nivel de red			16								16
T104	Identificación de problemas			8	4							12
PT2	Especificaciones	2 semanas										32
T201	Especificaciones de servicios de usuario				8							8
T202	Especificaciones de servicios de red				8							8
T203	Especificaiones de hardware				8							8
T204	Especificaciones de diseño					8						8
PT3	Estudio de alternativas	3 semanas										72
T301	Estudio de tecnologias actuales					8	8					16
T302	Estudio de tecnologias futuras					8	8					16
T303	Estudio de tecnologias validas						8					8
T304	Estudio de alternativas para VPN						8	8				16
T305	Estudio de alternativas para topología							16				16
PT4	Diseño	4 semanas										56
T401	Diseño de topología							8	8			16
T402	Diseño de acceso WAN								8			8
T403	Diseño de seguridad								8			8
T404	Diseño de acceso LAN								4	8		12
T405	Diseño de redundancia									4	8	12
PT7	Gestión	10 semanas										112
T701	Seguimiento	2	2	2	2	2	2	2	2	2	2	20
T702	Documentación del proyecto	6	6	6	6	8	8	8	8	16	20	92
Horas a la semana:		24	34	34	38	36	44	44	40	32	32	358

Tabla 9: Cronograma

12 ASPECTOS ECONÓMICOS

En este apartado se van a realizar dos cálculos de costes diferentes. Por un lado, el coste correspondiente a la realización de los análisis y diseños de red que en este documento se recogen. Por otro lado, un presupuesto que resume los costes de ejecución del diseño propuesto para la mejora de la red corporativa.

12.1 COSTES DE PROYECCIÓN

Este apartado recoge, por un lado, los costes de horas internas que engloban las tareas realizadas por la directora del proyecto en la UPV/EHU, el director del proyecto en SATEC, y el alumno en cooperación educativa que ha desarrollado el trabajo. Estos se calculan a partir del cronograma mostrado anteriormente. Se calcula también el coste por amortización del material utilizado para el desarrollo. Por otro lado, se calculan los gastos derivados del uso del material de oficina.

Todo ello se recoge en una última tabla resumen en la que se consideran los costes indirectos (10%) y el margen de imprevistos (10%).

Horas internas	**Horas**	**Coste**	**Total**
Ingeniero Junior	358h	12€/h	4.296€
Directores de proyecto	54h	50€/h	2.700€
			6.996€

Tabla 10: Calculo horas internas (proyección)

Amortizaciones	**Coste**	**Vida**	**Uso**	**Total**
Lenovo L440	799€	5 años	3 meses	40€
Windows 10 Pro	259€	5 años	3 meses	13€
Microsoft Office	68€	1 año	3 meses	17€
Visio	150€	1 año	2 meses	25€
				95€

Tabla 11: Calculo amortizaciones (proyección)

Gastos	**Coste**	**Total**
Material	100€	100€

Tabla 12: Calculo gastos (proyección)

Finalmente se calcula el coste total:

Concepto	Total
Horas internas	6.996€
Amortizaciones	95€
Gastos	100€
Subtotal	7.191€
Costes indirectos	719€
Subtotal	7.910€
Imprevistos	791€
Total	**8.701€**

Tabla 13: Calculo coste total (proyección)

12.2 PRESUPUESTO DE IMPLANTACIÓN

Este presupuesto recoge los costes de la implantación del diseño realizado para el prototipo de la red corporativa. En los costes se va a considerar que un ingeniero junior sería capaz de realizar las instalaciones adecuadamente, pero las configuraciones, por su complejidad, debe hacerlas un ingeniero senior.

El principal coste de la implantación reside en la adquisición del equipamiento de red. Por ello, se van a realizar dos presupuestos diferentes, uno enfocado a servir de referencia para un despliegue desde 0 y un segundo considerando que una gran parte del equipamiento ya se encuentra en el almacén de Bilbao o en producción.

Para mayor precisión, se utilizarán precios de equipamiento de segunda mano, ya que parte de los equipos ya no se encuentran en venta. y/o con descuento. Las licencias de soporte técnico de cisco se calcularán para una duración de uso de 5 años, además, se incluirán directamente en el precio.

No se van a considerar amortizaciones ni gastos en material ya que constituyen un valor muy inferior al margen de error en la estimación del valor de los equipos. Todo ello se recoge en una última tabla resumen en la que se considera el margen de imprevistos.

Horas internas	**Horas**	**Coste**	**Total**
Ingeniero Junior	40h	12€/h	480€
Ingeniero Senior	80h	40€/h	3.200€
			3.680€

Tabla 14: Calculo horas internas (implantación)

Material	Precio/u	Unidades	Descuento	Total
Cisco 7204VXR	18.656,00€	2	60%	14.924,80€
Cisco WS-3750X-48T-S	13.234,00€	2	60%	10.587,20€
Cisco WS-3750G-48TS-L	9.729,00€	2	60%	7.783,20€
Cisco WS-3750G-48PS	10.245,00€	2	60%	8.196,00€
Cisco WS-2960G-24PS-L	7.183,00€	2	60%	5.746,40€
AIR-CAP1702I-E-K9	300,00€	2	60%	240,00€
FortiGate 101E	19.789,00€	2	60%	15.831,20€
UTP CAT6 RJ45	2,60€	300	-	650,00€
				63.958,80€

Tabla 15: Calculo costes equipamiento (implantación)

Finalmente se calcula el coste total considerando los imprevistos:

Concepto	Total
Horas internas	3.680,00 €
Gastos	63.958,80 €
Subtotal	67.638,80 €
Imprevistos	6.763,88 €
Total	**74.402,68 €**

Tabla 16: Calculo coste total (implantación)

12.2.1 Presupuesto de ejecución

Por último, se va a calcular el coste real de ejecución para la sucursal de Bilbao, puesto que varios equipos ya se encuentran actualmente en producción y/o en el almacén, por lo que no sería necesaria su adquisición.

Horas internas	Horas	Coste	Total
Ingeniero Junior	40h	12€/h	480€
Ingeniero Senior	80h	40€/h	3.200€
			3.680€

Tabla 17: Calculo horas internas (ejecución Bilbao)

Material	Coste/u	Unidades	Descuento	Total
Cisco WS-3750X-48T-S	13.234,00€	2	60%	15.880,80 €
Cisco WS-3750G-48TS-L	9.729,00€	1	60%	5.837,40 €
Cisco WS-3750G-48PS	10.245,00€	2	60%	12.294,00 €
				34.012,20 €

Tabla 18: Calculo costes equipamiento (ejecución Bilbao)

Finalmente se calcula el coste total considerando los imprevistos:

Concepto	Total
Horas internas	3.680,00 €
Gastos	34.012,20 €
Subtotal	37.692,20 €
Imprevistos	3.769,22 €
Total	**41.461,42 €**

Tabla 19: Calculo coste total (ejecución Bilbao)

12.3 ANÁLISIS DE RENTABILIDAD

Con base en los estudios realizados por CloudEndure [1] mencionado en la introducción, se va a tratar de realizar una estimación de la rentabilidad del proyecto planteado. Para ello, con el fin de contextualizar la situación, se va a realizar un resumen de las conclusiones extraídas de ambos estudios.

Para una empresa con los siguientes datos:

- Tamaño de empresa: Pequeña
- Número de empleados: 20
- Facturación anual: 8,4 millones

Supone unos costes de:

- Coste por minuto de una interrupción de servicio no planificada: 35€

A continuación, se presentan los datos para la sucursal de Bilbao:

- Tamaño de la sucursal: Pequeña
- Número de empleados: 25
- Facturación anual: 7,3 millones

Se puede observar que la situación es muy similar, quizás con un coste inferior para la sucursal de Bilbao ya que posee un 25% más de empleados, pero entorno a un 10% menos de facturación. Por ello, se van a actualizar los datos para intentar realizar un cálculo más preciso:

- Coste por minuto de una interrupción de servicio no planificada: 26€

A partir de los datos obtenidos, se podría estimar el coste por la pérdida de tiempo a costa del rendimiento. Suponiendo que cada empleado pierde entre 15 y 20 minutos diarios en esperar a que se descarguen los correos, páginas web y/o ficheros almacenados en la nube, se calcula un coste diario de entre 390€ y 520€. Con la media, es decir, 455€ diarios, en torno a los 250 días laborables anuales y 22 de vacaciones, obtenemos un gasto anual a causa del bajo rendimiento de la red de entorno a los 103.740€.

Ahora se va a realizar un cálculo similar, pero esta vez, sin considerar costes indirectos, es decir, teniendo en cuenta tan solo el coste por hora de cada empleado.

Supongamos que cada empleado pierde entre 15 y 20 minutos diarios en esperar a que se descarguen los correos, páginas web y/o ficheros almacenados en la nube. Supongamos también que el coste/h de cada empleado, de media, es de 24€/h. Eso supone un coste de entre 6€ y 8€ por empleado al día. En una empresa de 25 empleados, supone unos costes en tiempo no productivo diario de entre 150€ y 200€. Haciendo la media, es decir, 175€ diarios, estimando en torno a los 250 días laborables anuales y restando los 22 días de vacaciones, obtenemos un gasto anual a causa de las pérdidas de tiempo de los empleados provocado por el bajo rendimiento de la red entorno a los 39.900€.

A continuación, se realiza un resumen de todo ello:

Concepto	**CloudEndure**	**Coste/h**
Coste minuto	1,04€	0,40€
Empleados	25	25
Minutos	15-20 minutos	15-20 minutos
Coste diario	455€	175€
Días	228 días	228 días
Anual	**103.704€**	**39.900€**

Tabla 20: Resumen del estudio de coste anual

El análisis basado en el estudio de CloudEndure ha resultado en un coste más de dos veces superior al realizado en base a los costes/h de los empleados. A pesar de que a primera vista se puede observar una gran diferencia, esta no es tan alarmante si se reconsideran ciertos factores que han sido pasados por alto en las suposiciones realizadas inicialmente.

Cabe destacar que el coste por una pérdida de servicio total puede ser muy superior al coste por pérdida de tiempo en rendimiento pobre de ciertos servicios. Esto se fundamenta en que el bajo rendimiento de la red no afecta de igual forma a todos los servicios. El servicio de telefonía, por ejemplo, se ha supuesto que funciona correctamente en el segundo caso, aun así, en el primero, se ha dado por hecho una caída total del servicio de red, y, por ende, el de telefonía. Lo mismo ocurre con otros servicios más concretos de la red de la sucursal de Bilbao.

Por todo ello, se cree que, **basándose en ambos análisis, y realizando una estimación a gran escala, la sucursal de la empresa SATEC en Bilbao puede llegar a estar perdiendo entre 40.000€ y 100.000€ anuales**. Esto significa que el presupuesto total (costes de diseño + implantación) de 50.000€ para la mejora de la red se encuentra en el rango del coste anual que supone no disponer de una red adecuada.

13 CONCLUSIONES

Cualquier persona que haya tratado o trate habitualmente con tecnologías de las telecomunicaciones ha sufrido alguna vez la frustración de no lograr realizar lo que desea a causa del bajo rendimiento de su conexión a internet. La dependencia de Internet en el siglo XXI es innegable, sobre todo en el mundo profesional. Por ello, el bajo rendimiento de la red de la sucursal de Bilbao de la empresa SATEC ha conducido a la necesidad de un profundo análisis y rediseño, con el fin de solventar los problemas que lo provocaban.

El rediseño de la red buscaba cumplir 4 características principales:

- Simplicidad
- Disponibilidad
- Seguridad
- Escalabilidad

Como se ha podido observar a lo largo del proyecto se han ido teniendo en cuenta cada uno de los factores en cada toma de decisión, desde las especificaciones, hasta el diseño final, cobrando su máxima importancia en el análisis de alternativas. Se ha seleccionado un diseño sencillo, provisto de duplicidad de equipos y enlaces para una alta disponibilidad, varios niveles de seguridad y un análisis de dimensionamiento y previsión de crecimiento para proporcionar escalabilidad.

Tras establecer ese claro objetivo de mejora, y a fin de facilitar el éxito, se habían establecido una serie de objetivos parciales:

- Analizar y documentar la situación.
- Eliminar todo rastro de configuraciones y tecnologías obsoletas y/o erróneas.
- Proporcionar un prototipo de sucursal remota.

Los dos primeros fueron logrados con éxito al inicio del proyecto, aportando, sin siquiera comenzar con el rediseño para la mejora, una base de optimización y reducción de riesgos. El último objetivo parcial también ha sido llevado a cabo con éxito. A través de un diseño de LAN simple y una propuesta de acceso WAN muy versátil ampliamente adoptada en entornos corporativos se ha logrado un diseño capaz de soportar todos los servicios que requiere una red de las características y dimensiones expuestas.

A través de todos los pasos mencionados también se ha logrado plantear una solución a cada problema que había sido identificado en la red. El acceso a internet de Movistar, y sus 300 Mbps, pasarían a ser la salida principal de la sucursal, logrando aumentar en cinco veces el ancho de banda inicial. La gestión de la red se ha simplificado a través de la documentación correspondiente al nuevo despliegue. Y finalmente, la utilización de puertos se ha jerarquizado de tal forma que proporciona las capacidades necesarias de adaptación a cualquier posible aumento de plantilla.

Por último, se quiere hacer hincapié en el análisis de costes realizado. Por un lado, se ha conseguido ahorrar un total de 33.000€ en equipamiento reutilizable. Por otro lado, tras calcular los costes que provoca una red de bajo rendimiento sobre la productividad de la oficina, se ha llegado a la conclusión de que se trata de un proyecto muy rentable. En cuestión de un año es capaz de recuperar la totalidad de la inversión, sin tener en cuenta siquiera los beneficios técnicos y sociales que este aporta.

14 BIBLIOGRAFÍA

[1] «CloudEndure | Disaster Recovery, Cloud Backup, and Cloud Migration,» 2012. [En línea]. Available: https://www.cloudendure.com/.

[2] «Ponemon Institute - Measuring Trust In Privacy And Security,» Ponemon Institute, 2002. [En línea]. Available: https://www.ponemon.org/.

[3] E. C. García, «ESTUDIO Y ANÁLISIS DE LOS SERVICIOS PARA LA MEJORA DE UNA RED CORPORATIVA,» UPV/EHU, Bilbao, 2019.

[4] ITU-T, G.1010 : End-user multimedia QoS categories, 2001.

[5] IETF, «Generic Routing Encapsulation (GRE),» 2000. [En línea]. Available: https://tools.ietf.org/html/rfc2784.

[6] IETF, « Key and Sequence Number Extensions to GRE,» 2000. [En línea]. Available: https://tools.ietf.org/html/rfc2890.

[7] IETF, «NBMA Next Hop Resolution Protocol (NHRP),» 1998. [En línea]. Available: https://tools.ietf.org/html/rfc2332.

[8] Cisco Systems, «Enterprise Branch Architecture Design Overview,» [En línea]. Available: https://docstore.mik.ua/.

[9] Cisco Systems, «IPsec VPN WAN Design Overview,» 2008. [En línea]. Available: https://www.cisco.com.

[10] Cisco Systems, «VPN WAN Technology Design Guide,» 2014. [En línea]. Available: https://www.cisco.com.

[11] Cisco Systems, «Enterprise Branch Security Design Guide,» [En línea]. Available: https://fenix.tecnico.ulisboa.pt/.

[12] T. Szigeti, C. Hattingh, R. Barton y K. Briley, «End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks,» 2013. [En línea]. Available: http://www.ciscopress.com.

[13] Cisco Systems, «Configure ISP Redundancy on a DMVPN Spoke with the VRF-Lite Feature,» 2015. [En línea]. Available: https://www.cisco.com.