



**UNIVERSIDAD DE CASTILLA-LA MANCHA
ESCUELA SUPERIOR DE INFORMÁTICA**

Diseño de red para el I.E.S Berenguela de Castilla

*Juan Manuel Porrero Almansa
Alonso Díaz Sobrino*



Asignatura: Diseño y Gestión de Redes

Titulación: Grado en Ingeniería Informática

Fecha: 26 de mayo de 2021

Contenido

Diseño de red para el I.E.S Berenguela de Castilla	1
1. INTRODUCCIÓN	4
2. ANÁLISIS DE REQUISITOS.....	5
2.1. ANÁLISIS DE METAS DE NEGOCIO	5
2.1.1. Organización del edificio	5
2.2. ANÁLISIS DE METAS DE TÉCNICAS	6
2.3. CARACTERIZACIÓN DE LA RED EXISTENTE.....	8
2.4. CARACTERIZACIÓN DEL TRÁFICO DE REDES.....	8
2.4.1. Cámaras de seguridad.....	8
2.4.2. Alumnado	8
2.4.3. Profesores	8
2.4.4. Personal de administración	8
3. DISEÑO LÓGICO	9
3.1. DISEÑO DE LA TOPOLOGÍA DE RED	9
3.1.1. Capa de núcleo	10
3.1.2. Capa de distribución	10
3.1.3. Capa de acceso	10
3.1.4. Capa de dispositivos finales	11
3.2. DIRECCIONAMIENTO Y ASIGNACIÓN DE NOMBRES.....	11
<i>Direccionamiento privado.....</i>	<i>12</i>
<i>Direccionamiento dinámico.....</i>	<i>12</i>
3.3. PROTOCOLOS DE COMUNICACIÓN/ENRUTADO	13
<i>Conmutación.....</i>	<i>13</i>
<i>Enrutamiento.....</i>	<i>13</i>
3.4. ESTRATEGIAS DE SEGURIDAD	13
3.4.1. Zona Desmilitarizada (DMZ)	13
3.4.2. Listas de Control de Acceso.....	14
4. DISEÑO FÍSICO.....	15
4.1. DISEÑO DEL CABLEADO	15
Tipos y longitudes de cableado entre plantas	15
4.1. DISPOSITIVOS DE INTERCONEXIÓN	19
Plataformas de capa de acceso.....	19
Plataformas de capa de distribución.....	19
Plataformas de capa de núcleo.....	19
5. VALIDACIÓN Y PRUEBAS.....	20
5.1. PROTOTIPO DE RED EN CISCO PACKET TRACER	20
5.1.1. Red interna del instituto.....	20

5.1.2. Internet Service Provider.....	21
5.1.3. DMZ	21
5.2. PRUEBAS DE ACEPTACIÓN.....	23
5.2.1. Listas de control de acceso (ACL).....	23
5.2.2. Servidor de correo electrónico	24
5.2.3. Servidor web	25
APÉNDICE A PRESUPUESTO	26
APÉNDICE A CONFIGURACIÓN DE LOS DISPOSITIVOS.....	27
Configuración switch capa 3 o multicapa del núcleo.....	27
Configuración de los switch capa 2.....	30
BIBLIOGRAFÍA	31

1. INTRODUCCIÓN

La justificación de este trabajo es la de realizar a modo de trabajo teórico de la asignatura Diseño y Gestión de Redes, la distribución e infraestructura de red de un IES, en nuestro caso el **IES Berenguela de Castilla** de Bolaños de Calatrava, que abarca desde el diseño físico y lógico hasta su documentación. Para conseguir este objetivo, trabajaremos sobre los conocimientos adquiridos y tratados en la segunda parte de la asignatura, correspondiendo a Diseño y nos basaremos en varias bibliografías online y no online, siendo el libro Top-down network design de Priscilla Oppenheimer el de mayor importancia.

Top-down consiste en un diseño que se ancla en modelo OSI, comenzando el diseño por las capas superiores y terminando en las inferiores. Define que antes de empezar a asignar y enlazar direcciones IP es importante analizar metas técnicas y de negocio, analizar quién va a utilizar la red y para qué lo harán, dividir estos grupos, y, por último, qué aplicaciones serán utilizadas en esa red.

El diseño de la red lo vamos a dividir en cuatro etapas o fases que se sucederán de forma cíclica. A continuación, se detallarán dichas fases:

- ✦ **Primera fase.** Análisis de Requisitos.
- ✦ **Segunda fase.** Diseño lógico.
- ✦ **Tercera fase.** Diseño físico.
- ✦ **Cuarta fase.** Probar, optimizar y documentar el Diseño de la Red.

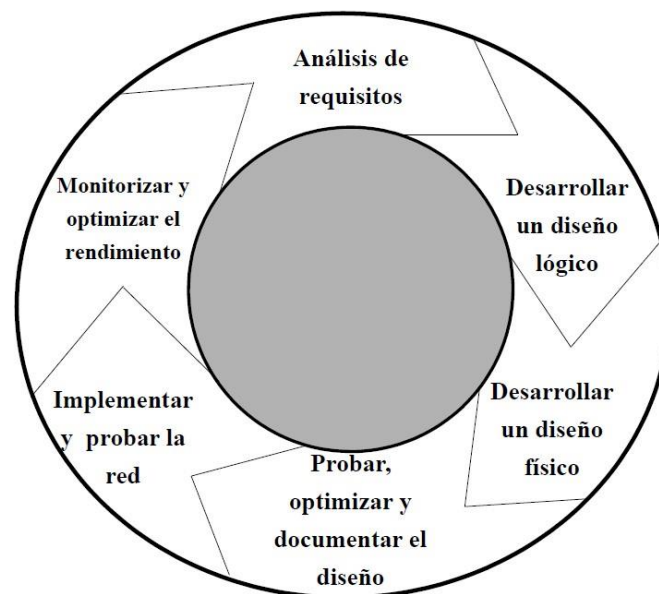


Figura 1.1: Diseño de la red y ciclo de implementación.

2. ANÁLISIS DE REQUISITOS

El análisis de requisitos es lo primero que debemos realizar en un diseño de red de tipo descendente. Vamos a analizar los objetivos de negocio del/los clientes: metas de negocio y restricciones, metas técnicas, caracterización de la red que existe y caracterización del tráfico de la red.

2.1. ANÁLISIS DE METAS DE NEGOCIO

Un objetivo obligatorio para nosotros a la hora de diseñar la red es entender las necesidades de nuestros clientes. Nos piden realizar el diseño del instituto que rigen, el IES Berenguela de Castilla de Bolaños de Calatrava, teniendo en cuenta los siguientes aspectos:

- ✦ **No se puede reutilizar nada de la infraestructura de red existente.** Es un diseño completamente nuevo.
- ✦ Se deben proporcionar todos los servicios de red necesarios. No se permite por lo tanto reutilizar ningún soporte que nos proporciones el IES en base al diseño actual.
- ✦ El diseño debe respetar la organización (edificios, recursos humanos, etc.) de IES elegido

2.1.1. Organización del edificio

El IES Berenguela de Castilla está constituido por un edificio principal, del cual disponemos los planos y será sobre el que vamos a trabajar. También cuenta con edificio anexo del que no disponemos planos, ya que el instituto no podía proporcionarlos al ser relativamente nuevo y que aparece sombreado de color amarillo en la siguiente figura.

El edificio principal cuenta con **3 plantas**: la planta baja, donde encontramos aulas, conserjería, sala de profesores y dos aulas ALTHIA; la segunda planta donde encontramos algunos laboratorios, departamentos y aulas; y, por último, la tercera planta, en la cual encontramos aulas.

2.2. ANÁLISIS DE METAS DE TÉCNICAS

A continuación, procederemos a explicar los objetivos técnicos que consideramos más importantes a la hora de desarrollar nuestro diseño de la red del IES Berenguela de Castilla. Se trata de escalabilidad, disponibilidad, rendimiento de la red, seguridad, facilidad de gestionarla y adaptabilidad.

- Hay que tener en cuenta también que no todos los diseños que se pueden hacer tienen la misma capacidad de crecimiento, ya que, por ejemplo, un diseño de red **jerárquico** es mucho más escalable que uno plano. Este aspecto lo trataremos mejor en el apartado 3, el Diseño Lógico.

En cuanto a las **restricciones**, el diseño lo debemos hacer para minimizar el tráfico broadcast. Esto lo conseguiremos mediante la creación de VLAN's.

- ✦ **Disponibilidad.** Cuando hablamos de disponibilidad nos referimos al porcentaje de tiempo (horas, días, meses, años) que una red está funcionando u operativa. Puede ser expresada como el promedio de tiempo entre fallos o tiempo promedio para reparar. El IES Berenguela de Castilla no tiene política de seguridad de las redes, así que, tomando como referencia las de la UCLM hemos propuesto el siguiente esquema:

Vamos a establecer la jornada diurna y nocturna, el tiempo de la jornada nocturna será la mitad que en la diurna. La jornada diurna será todos los días laborables de 8:30 de la mañana a 8:30 de la noche. Todo lo que no sea eso, está considerado como horario nocturno, y, por ende, jornada nocturna.

Se tomarán las medidas técnicas y organizativas oportunas para que estos indicadores no superen los valores límite, que se establecerán en:

- a) 6 horas para una interrupción del servicio en la red troncal o en la red de distribución.
 - b) 10 horas para una interrupción del servicio en la red de acceso a los puestos.
 - c) 14 horas para una interrupción del servicio durante un semestre.
-
- ✦ **Seguridad.** Este es uno de los aspectos más importantes. Ya que vamos a tener un servidor de correo electrónico y un servidor web que deben de ser accesibles desde Internet, vamos a implantar protección frente a ataques de reconocimiento, para evitar que nuestra información no pueda ser eliminada, alterada o interceptada. También nos protegeremos frente a ataques de denegación de servicio (DoS).

Otro aspecto importante en cuanto a seguridad para tener en cuenta sería el de proporcionar un nivel básico de seguridad para que un determinado grupo de usuarios no puedan ser interceptados por usuarios de otro distinto.
 - ✦ **Adaptabilidad.** Hay que hacer un diseño flexible para que se pueda adaptar al patrón de tráfico y otros requisitos o demandas. Para conseguir este objetivo, vamos a evitar la implantación de objetos o elementos de diseño que dificulten usar nuevas tecnologías en un futuro.
 - ✦ **Rendimiento de la Red.** Se deben tener en cuenta los siguientes criterios:

- Ancho de banda
- Carga
- Eficiencia
- Tiempo de respuesta
- Retardo

2.3. CARACTERIZACIÓN DE LA RED EXISTENTE

Un paso importante en el diseño de la red descendente es examinar la red existente del cliente para determinar mejor cómo cumplir con las expectativas de escalabilidad, rendimiento y disponibilidad. El examen de red actual incluye el estudio de la topología física y la evaluación del rendimiento actual. De esta manera, podemos determinar si los objetivos de diseño propuestos por el cliente son realistas, registrar los cuellos de botella o determinar el equipo de red que necesita ser reemplazado.

A pesar de nuestros intentos por recoger datos oficiales sobre el número de conexiones inalámbricas del IES Berenguela de Castilla para mostrarlas en este documento, no nos ha sido posible, ya que ni en Internet hemos encontrado información sobre ello ni en el centro nos han sabido dar un número concreto.

Todos los datos de aquí en adelante son referencias hechas en base a nuestra estancia en nuestra etapa de estudiantes del centro, ya que los dos miembros del grupo somos de Bolaños de Calatrava. Utilizaremos nuestra experiencia en el centro para evaluar el número adecuado de conexiones.

2.4. CARACTERIZACIÓN DEL TRÁFICO DE REDES

Hasta ahora hemos caracterizado la red existente en términos de su estructura e interpretación. Sin embargo, como el análisis de la situación existente es un paso importante, caracterizaremos también la red existente en términos del flujo de tráfico.

Para determinar las fuentes y destinos de tráfico de red debemos identificar previamente las comunidades de usuario y almacenamiento de datos para las aplicaciones existentes. Una comunidad de usuario es un conjunto de personas que hacen el mismo uso de la red. En este sentido, para el diseño de la red del IES de nuestro caso particular, podemos clasificar los usuarios de la red en tres comunidades: **Alumnado, Profesores, Personal de Administración y Cámaras de seguridad.**

2.4.1. Cámaras de seguridad

No tendremos más de 14 cámaras, más que suficientes para tener todo controlado.

2.4.2. Alumnado

Al carecer de datos oficiales como hemos mencionado antes, estimamos que el IES Berenguela de Castilla debe tener entre 600 y 800 alumnos.

2.4.3. Profesores

Estimamos el número de personal docente entre 50 y 70.

2.4.4. Personal de administración

El personal de administración se situaría entre los 15 y 30.

3. DISEÑO LÓGICO

En este apartado nos vamos a encargar de definir la arquitectura de red de nuestro instituto, gracias al **diseño lógico**. Esto es necesario y muy importante antes de pasar a seleccionar productos o tecnologías físicas, para así poder cumplir con los requisitos previamente definidos por el cliente. El primer paso dentro de esta fase de diseño lógico es la topología de red, es decir, un mapa lógico que muestra la forma de la que dispondrá dicha red.

3.1. DISEÑO DE LA TOPOLOGÍA DE RED

Para poder satisfacer los objetivos del cliente, vamos a optar por usar el **modelo jerárquico**. Dicho modelo nos permitirá dividir la red en distintas capas independientes las unas de las otras, de manera que cada una de ellas proporcionen dentro de esa jerarquía distintas funciones específicas dentro de la red. Con esta opción podemos reducir la carga de los dispositivos que estarán conectados a nuestra red, establecer un límite de dominios de broadcast, realizar un diseño lo más simple posible lo que nos hará más fácil las cosas tanto a nosotros (los desarrolladores) como al cliente a la hora de entenderlo, facilitar posibles cambios que se den en la red del instituto y permitir una mayor escalabilidad.

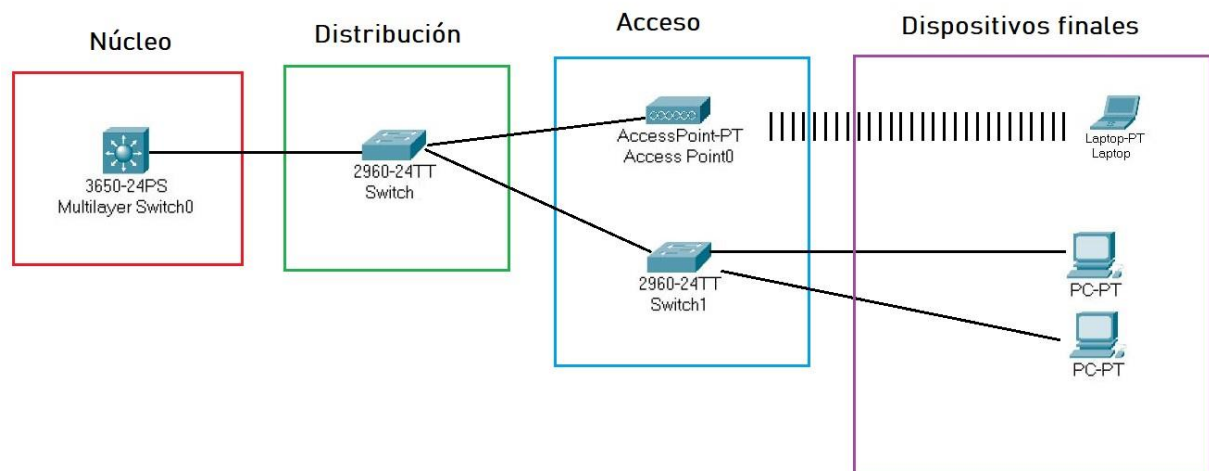


Figura 3.1: Ejemplo de diseño jerárquico de red

Por tanto, la topología de red para el IES Berenguela de Castilla de Bolaños de Calatrava (Ciudad Real) que estamos diseñando tendrá una jerárquica de 4 capas: una capa que contendrá al **núcleo** donde se encuentra el rack y el switch multicapa que proporcionarán un transporte rápido entre los distintos switches de distribución; una capa de **distribución** que nos sirva de enlace entre las capas de acceso y ofrezca conectividad a los servicios; una capa de **acceso** para ofrecer acceso a la red a los terminales y grupos de usuarios; y una última capa conocida como **dispositivos finales** que contendrá a los dispositivos a través de los cuales las personas podrán conectarse a la red y desempeñar las tareas oportunas.

3.1.1. Capa de núcleo

La capa de núcleo o también conocida como “backbone de red” es una pieza fundamental de la red escalable, y de las más sencillas de diseñar. Esta capa proporciona la conectividad para las capas de distribución en entornos LAN de gran tamaño, ya que interconecta los módulos de distribución, el centro de datos y el perímetro de la **WAN (Wide Area Network)**. Los dispositivos que la componen deben estar diseñados para conmutar los paquetes lo más rápido que se pueda.

En nuestro caso hemos utilizado un **switch multicapa** de alta velocidad, exactamente el modelo 3650, que va conectado a los distintos dispositivos, a través, de fibra. Este se encuentra dentro de un **rack** (armario metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones), que hemos colocado en la planta baja del instituto, ciertamente en una habitación que se encuentra céntrica en todo el edificio. Del switch multicapa colocado en el rack, subirán cables hacia las demás plantas para conectarlo a los **switches de distribución** (uno por cada planta) que darán soporte a los dispositivos que se encuentren ahí.

3.1.2. Capa de distribución

La capa de distribución admite muchos servicios importantes. En una red donde la conectividad necesita atravesar la LAN de extremo a extremo, ya sea entre diferentes dispositivos de capa de acceso o desde un dispositivo de capa acceso a la WAN, la capa de distribución facilita dicha conectividad. Como la red que tenemos que hacer abarca un diseño de LAN grande, nos vemos obligados a utilizar varios switches de distribución, uno por cada planta. Sin embargo, en la planta baja no colocaremos ningún switch de distribución ya que aprovecharemos el propio multicapa para conectar los dispositivos pertenecientes de la capa de acceso.

Uno de los motivos es ahorrarnos la instalación de fibra óptica entre las distintas plantas. Por tanto, en el presupuesto debemos incluir la adquisición de 2 switches para la capa de distribución.

3.1.3. Capa de acceso

Esta capa es por donde los dispositivos que controla el usuario se conectan a la red. De esta manera dicha capa nos permite la conectividad a la red tanto de forma inalámbrica como por cable. Además, posee ciertos servicios y cualidades que dotan a la red de seguridad y recuperabilidad.

Para proporcionar acceso a la red a grupos de trabajo y usuarios del instituto, instalaremos distintos puntos de acceso en las diferentes plantas, ya que al tratarse de un instituto la conexión por cable no será muy demandada en los dispositivos debido a que los profesores no usan internet con tanta frecuencia para enseñar como podría ser en la universidad. Sin embargo, en zonas como althias si colocaremos switches para conectar los ordenadores por cable.

De esta manera los dispositivos que vamos a utilizar van a ser:

- **Planta baja**

Vamos a utilizar 5 puntos de acceso para dotar de internet a las diferentes aulas y pasillos que la componen. Un switch para conectar las distintas cámaras que instalaremos, otros 2 switches (uno por althia) para dar conectividad por cable a los ordenadores que allí se encuentren y un último switch para el personal de administración que se encuentra trabajando en dicha planta. En cuanto a los puntos de acceso, vamos a colocar dos por pasillo uno para la red de alumnos y otro para la red de profesores. En uno de los pasillos únicamente colocamos un punto de acceso para la red de profesores, esto es debido a que esa zona es exclusivamente para ellos, los alumnos solo deben ir ahí para preguntar dudas o cualquier tema educativo o privado. Por último, hemos decidido colocar un cable directo entre el rack y el ordenador del director, ya que es el máximo representante del instituto y necesita una conexión rápida y eficaz para poder desempeñar las distintas labores que le conciernen.

- **Primera planta**

En esta planta vamos a utilizar 6 puntos de acceso (dos por pasillo) como hemos comentado antes para dar conectividad a las redes de profesores y alumnos. Contamos con un switch para las cámaras de esta planta y otro último de distribución para poder interconectar todos los demás.

- **Segunda planta**

Por último, en la segunda planta vamos a colocar 4 puntos de acceso, ya que en esta únicamente hay dos pasillos. Además de los correspondientes switches, uno para cámaras y otro de distribución como hemos comentado en apartados anteriores.

3.1.4. Capa de dispositivos finales

Esta última capa alberga los dispositivos finales con los cuales los usuarios podrán acceder a la red y navegar por internet. En nuestro caso, hemos colocado dispositivos tales como impresoras, móviles, portátiles y ordenadores de sobremesa. Incluyendo aquellos ordenadores con los que se podrán ver las grabaciones de las cámaras de seguridad.

3.2. DIRECCIONAMIENTO Y ASIGNACIÓN DE NOMBRES

Es fundamental usar un modelo estructurado para hacer el direccionamiento y la asignación de nombres. De esta manera, haciendo un uso adecuado evitaremos desperdiciar direcciones, duplicaciones o nombres que no sean fáciles de utilizar. Para la asignación de direcciones a cada dispositivo utilizaremos el protocolo **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol), que asigna de forma automática direcciones a los hosts dentro del rango establecido.

Direccionamiento privado

El direccionamiento que hemos decidido utilizar dentro del instituto es privado, es decir, hemos utilizado **direcciones IP privadas**, ya que nos proporcionan seguridad porque la red interna no es visible desde internet. La comunicación con internet nos la proporciona **ISP** (Internet Service Provider) empresa encargada de proveernos de conexión a internet. En este caso dicha empresa será **Orange**.

En base a las metas de escalabilidad de nuestro cliente y al número de conexiones que se han hecho al instituto en los recientes años, hemos optado por utilizar el rango de direcciones privadas de clase B **172.16.0.0-172.16.15.255**, ya que va dirigido a un centro de estudios, el cual nos permite direccionar 4094 direcciones IP. Es decir, usamos la **dirección red 172.16.0.0/20**. Como hemos dicho al principio de este apartado, para seguir un modelo estructurado hemos usado **VLSM**, con el fin de dividir la red en cuatro VLANS en relación con los grupos que hemos comentado en la fase de análisis, aquí podemos ver una tabla con la información de cada VLAN:

VLANs	HOST	Dirección de red	Máscara	Rango de direcciones		Broadcast
				Inicio	Fin	
Alumnos	2046	172.16.0.0/21	255.255.248.0	172.16.0.1	172.16.7.254	172.16.7.255
Profesores	254	172.16.8.0/24	255.255.255.0	172.16.8.1	172.16.8.254	172.16.8.255
Personal administrativo	62	172.16.9.0/26	255.255.255.192	172.16.9.1	172.16.9.62	172.16.9.63
Cámaras	14	172.16.9.64/28	255.255.255.240	172.16.9.65	172.16.9.78	172.16.9.79

Figura 3.2: Asignación de direcciones a los distintos grupos

Direccionamiento dinámico

Al igual que hemos comentado al principio de este apartado, utilizaremos como protocolo de asignación DHCP, ya que además de que asigna dinámicamente direcciones IP a los hosts, también agrega otros parámetros de configuración a cada dispositivo de la red. El motivo por el que lo utilizamos es que hay una gran cantidad de usuarios que utilizarán la red, así podrán integrarse rápidamente en la red, sin necesidad de configurar absolutamente nada de forma manual. No utilizamos servidores específicos para dicha tarea, sino que DHCP será proporcionado por los dispositivos de interconexión que utilizamos en el núcleo. Es decir, dicho protocolo será configurado el switch multicapa del rack y mediante VTP será transferido a los demás dispositivos para que alberguen esas VLANs.

Asignación de nombres

Para cumplir con los objetivos marcados al principio por el cliente vamos a utilizar un nombre de dominio significativo. Es decir, el servicio de correo electrónico va a utilizar el nombre del instituto como domino **@berenguela.es**, y el servidor web alojará el sitio www.berenguela.es.

3.3. PROTOCOLOS DE COMUNICACIÓN/ENRUTADO

Conmutación

Como objetivo de lograr adaptabilidad y seguridad para el cliente, utilizaremos las VLANS antes comentadas en el diseño de la red. De esta manera, conseguiremos que los datos sensibles pertenecientes a distintos grupos queden separados, aumentando así la seguridad y disminuyendo la probabilidad de que ocurran violaciones de confidencialidad. Concretamente, las VLANS serán para alumnos, profesores, personal administrativo y cámaras. Así gozamos de seguridad y de otras ventajas como pueden ser la reducción del tamaño de los dominios de difusión y el ahorro de costos, ya que el uso de enlaces y ancho de banda es más eficiente.

Al igual que hemos comentado en el apartado anterior utilizaremos el protocolo de gestión de VLANS **VTP** (**VLAN TRUNK PROTOCOL**). Dicho protocolo ofrece una serie de beneficios para administrar la red, como la consistencia en la configuración de VLAN a través de la red o la posibilidad de realizar seguimiento y monitoreo preciso de las VLANS.

Enrutamiento

El protocolo de enrutamiento que utilizaremos será dinámico para que los dispositivos de enrutado como pueden ser un router o un switch multicapa aprendan como alcanzar automáticamente las distintas redes y host. El protocolo utilizado para dicha función es **RIP** (**Routing Information Protocol**).

RIP tiene múltiples ventajas con respecto a otros ya que implementa un algoritmo de encaminamiento más simple, haciendo que el cálculo de la mejor ruta sea más rápido. Es soportado por la mayoría de los fabricantes y es más fácil de configurar.

3.4. ESTRATEGIAS DE SEGURIDAD

El diseño y desarrollo de estrategias de seguridad es una de las tareas más importantes y difíciles. Esto nos permite proteger todos los componentes de la topología creada, sobre todo en las que alberguen servidores públicos. Para ello, cada uno de los switches están protegidos con una contraseña (1234), permitiendo así acceder a su configuración solo el personal autorizado

3.4.1. Zona Desmilitarizada (DMZ)

En nuestro diseño de red para el instituto Berenguela de Castilla debemos tener en cuenta que se gestionará un servidor de correo electrónico y un servidor web que deben ser accesibles desde Internet. Incluso, los mismos usuarios de la red demandarán rápido acceso a los recursos. Pero hay que tener cuidado ya que, si estas **pasarelas de aplicaciones** o **bastion host** se conectan directamente a la red local, corremos el peligro de que un servidor infectado pueda afectar a la red entera.

Para ello hay que buscar soluciones que eviten un fallo en cadena como este anterior. En ese sentido, vamos a utilizar redes perimetrales, también conocidas como zonas desmilitarizadas (DMZ), los cuales permiten **externalizar servidores vulnerables a**

ataques. Una DMZ consiste en una red con un rango de direcciones IP privadas que funciona como franja de seguridad entre dos redes, separándolas mediante reglas de acceso. De esta manera, aunque estos servidores se encuentren de forma física dentro de la red del instituto, no están conectados directamente con los equipos de la red local.

Para implementar una DMZ en nuestra red de instituto de una forma que nos sea más económica, ya que no es un estatuto que requiera de una seguridad muy fuerte, hemos decidido utilizar un único cortafuegos, es decir, un router con firewall con terminales para cuatro conexiones de red separadas: una para la red interna, otra para internet, otra para el ISP y otra para la DMZ.

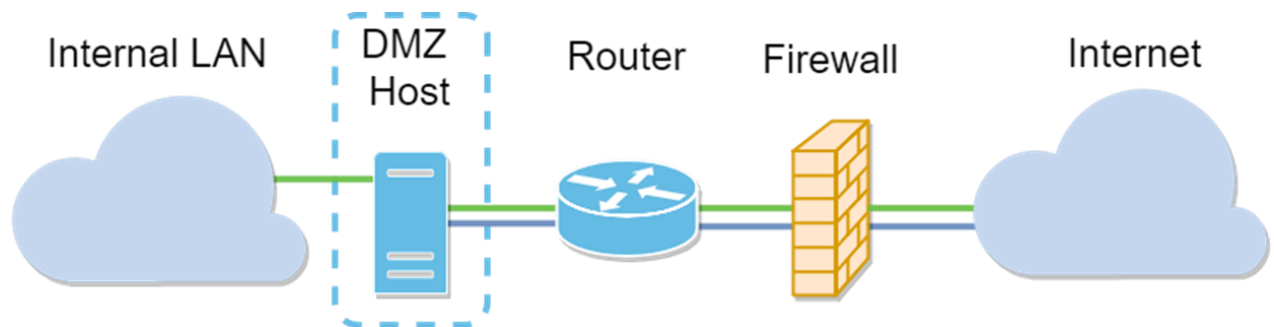


Figura 3.3: DMZ para proteger la red del instituto.

3.4.2. Listas de Control de Acceso

Uno de los factores clave para construir una red segura y fiable es saber identificar y fortalecer las comunicaciones, es decir, quien debe hablar con quién y el tipo de tráfico que se intercambia. En base a los cuatro grupos que hemos definido en los requisitos, tenemos que tratar de que los datos y la información de un grupo no sea interceptada, analizada, alterada o eliminada por otro grupo. Esto es lo que llamamos integridad de la información.

Como posible solución a este tipo de problemas que se plantean cuando creamos una red, vamos a optar por **listas de control de acceso (ACL)**, que nos permiten controlar ese tráfico que viaja por la red. De esta manera, lograremos limitar el tráfico de la red y mejorar el rendimiento global, ya que reducimos la carga de red.

Los grupos que hemos restringido han sido los alumnos con las cámaras y los profesores con las cámaras, de esta manera ninguno de estos tendrá acceso a ellas, delegando así el trabajo de revisión de estas únicamente al personal administrativo.

En caso, de que ocurra cualquier problema o situación desagradable en el centro y los alumnos o profesores quieran ver lo ocurrido para solucionar el problema, tendrán que contactar con el personal administrativo para que estos se encarguen de revisarlas y solucionar el problema.

4. DISEÑO FÍSICO

Tras completar el diseño lógico y haber establecido la topología de la red, es turno de escoger la tecnología física y dispositivos de red para el IES. En esta fase de Diseño Físico tendremos que estudiar y analizar las mejores opciones en cuanto a cableado y dispositivos de conexión tales como routers, puntos de acceso y switches.

4.1. DISEÑO DEL CABLEADO

Tipos y longitudes de cableado entre plantas

Utilizaremos un **esquema de cableado centralizado**, que tendrá como núcleo el RACK de la planta baja, lugar donde está el switch multicapa o de capa 3.

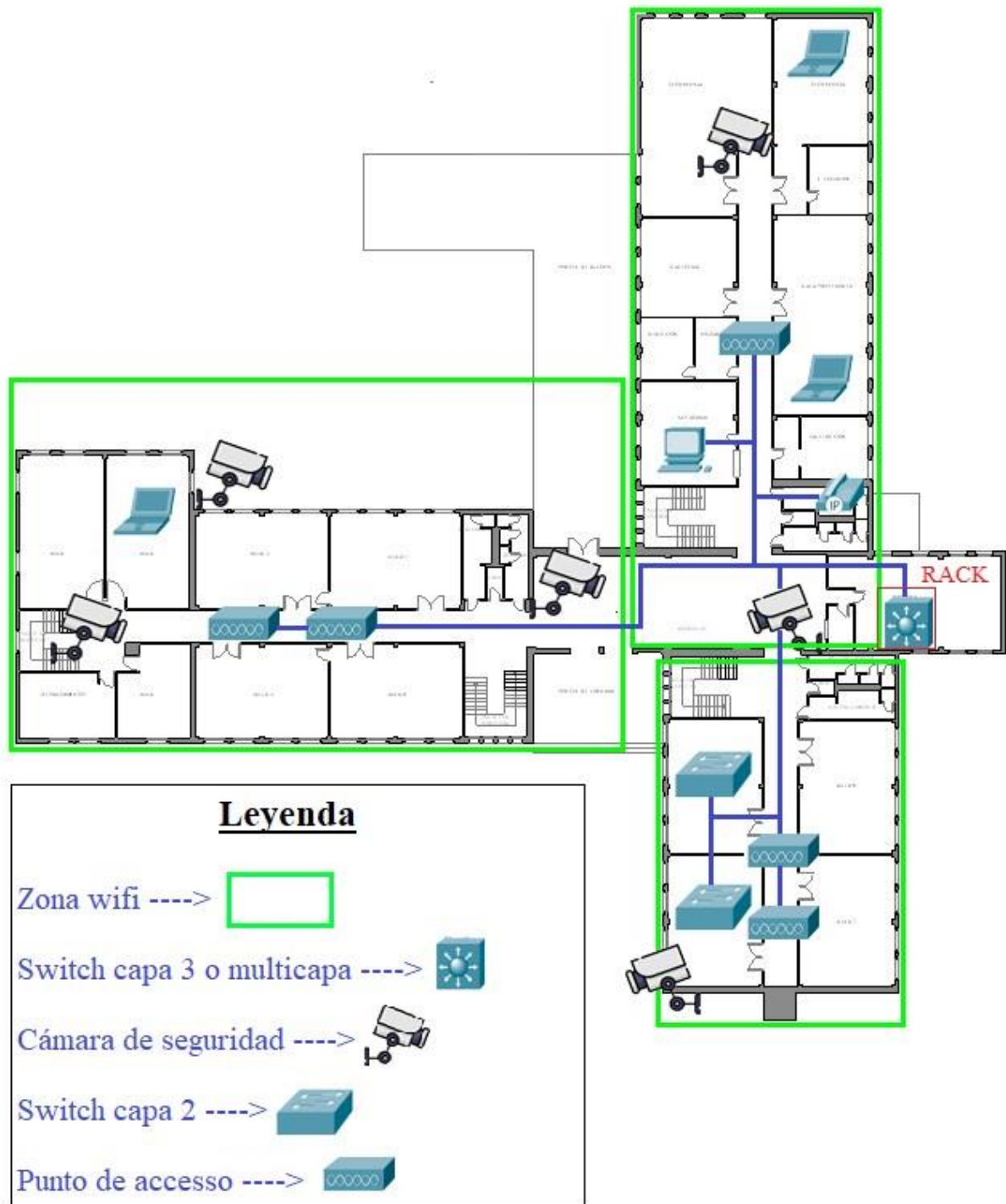
Habrà un RACK por planta, principalmente albergarán un switch de capa 2 en cada uno de ellos, que se conectarán al núcleo por medio de **fibra multimodo (MMF)** ya que son conexiones de corta distancia.

Para la capa de acceso se utilizará un **medio de cobre de par trenzado no blindado** (UTP, Unshielded Twisted-Pair). Las ventajas de este tipo de cable UTP es que su instalación es barata y sencilla, proporciona un aceptable rendimiento y a la hora de solucionar problemas también en relativamente fácil encontrarlos y solucionarlos. Para estar preparados en el futuro hemos instalado **UTP Cat 6** que llevarán conectores de Cat 5, con lo cual, en caso de querer aumentar la velocidad únicamente habría que cambiar los conectores.

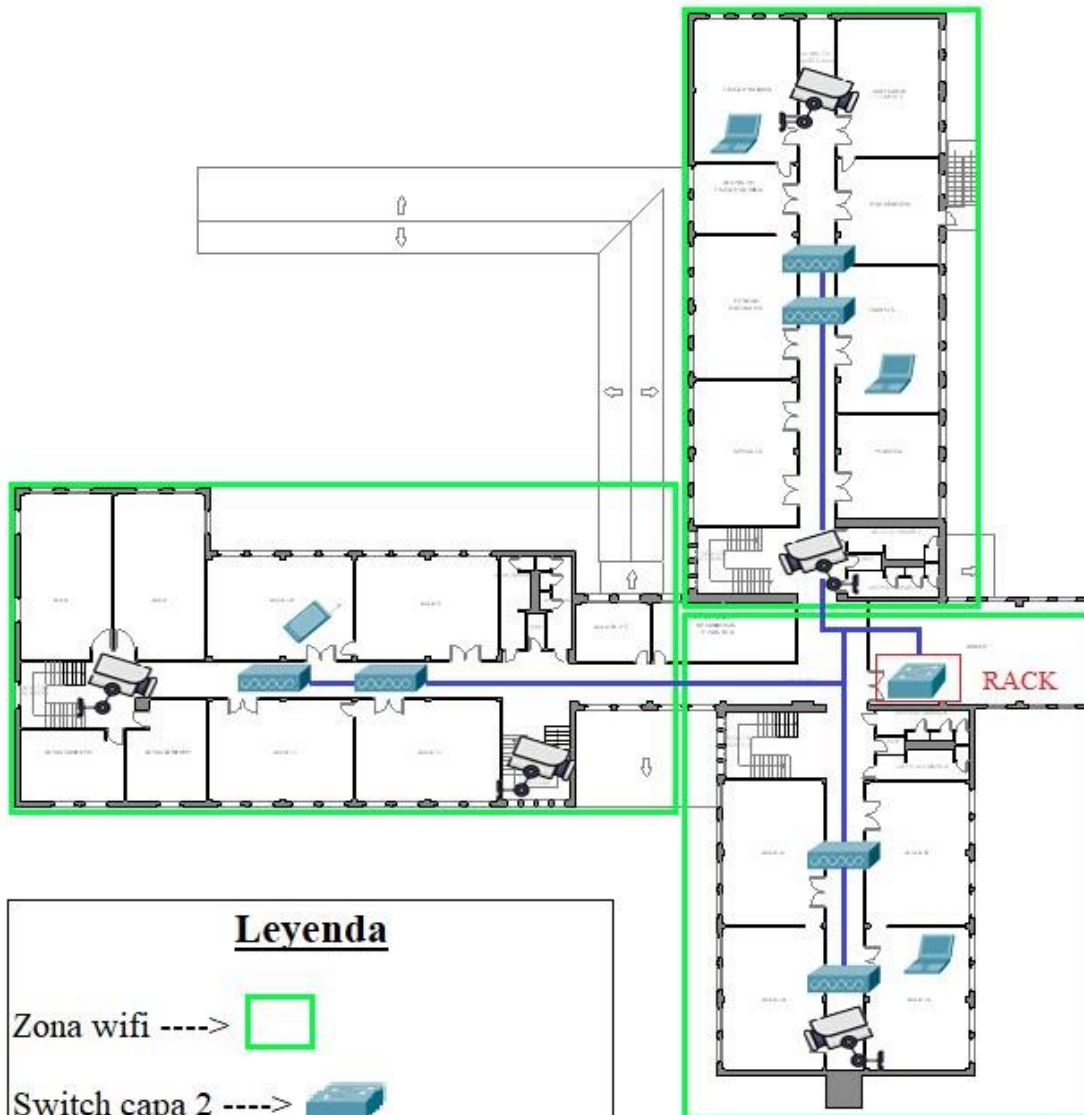
Adicionalmente, se instalarán puntos de acceso para proporcionar una cobertura WiFi.

A continuación, se adjuntan imágenes de la distribución física:

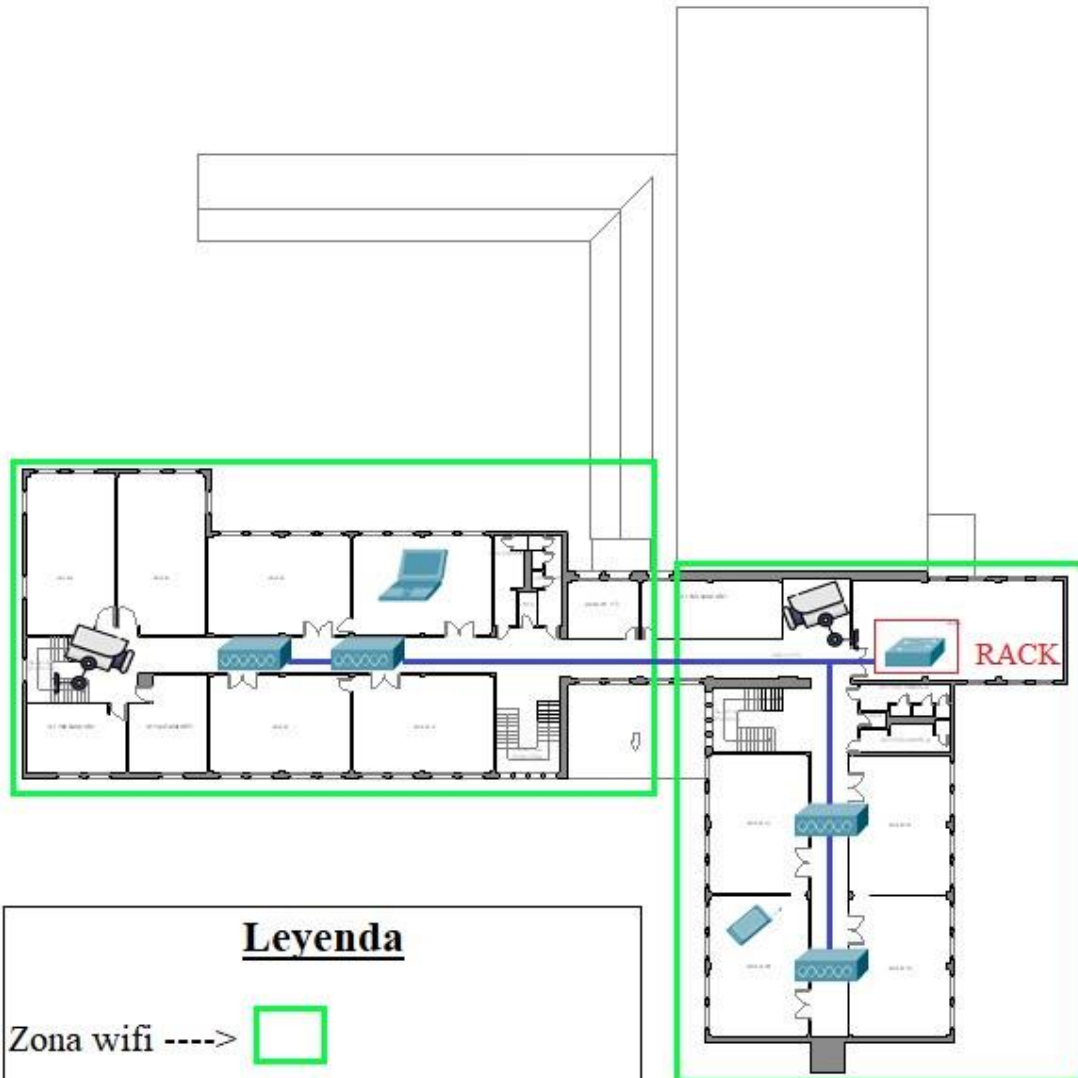
PLANTA BAJA



PRIMERA PLANTA



SEGUNDA PLANTA



Leyenda

Zona wifi ---->



Switch capa 2 ---->



Smartphone ---->



Punto de acceso ---->



4.1. DISPOSITIVOS DE INTERCONEXIÓN

Plataformas de capa de acceso

El conmutador de la capa de acceso se ejecuta en la capa 2 del modelo OSI y proporciona servicios como la asociación de VLAN. El objetivo principal del conmutador de capa de acceso es permitir que los usuarios finales accedan a la red. El conmutador de la capa de acceso debe proporcionar esta función a bajo costo y alta densidad de puertos. Por lo tanto, decidimos comprar los switches de la serie **Cisco Catalyst 2960-S**.

El switch Cisco Catalyst 2960-S son de capa 2 apilables de configuración fija que proporcionan conexión Gigabit y Fast Ethernet. Tienen dos modelos: de 24 puertos y de 48 puertos y son confiables y seguros, permitiendo la realización de gestiones y operaciones empresariales, además son más baratos, por lo que el costo total será menor. De este modelo instalaremos: 4 para la planta baja, 1 para la planta primera y 1 para la segunda planta, haciendo un total de **6 unidades**.

Otro aspecto a tratar es el de los puntos de acceso. Tras realizar varias comparaciones, y tantear varios y marcas, la más popular y la más fiable es Ubiquiti. Nos hemos decidido por instalar el modelo Ubiquiti UAP-AC-LR. Ofrecen una buena calidad en cuanto al precio que tienen, y tienen largo alcance y rendimiento. Además, cuenta con doble banda simultánea 3x3 MIMO a 2.4GHz, y 2x2 MIMO en 5GHz. De este dispositivo compraremos: 5 para la planta baja, 6 para la primera planta y 4 para la segunda planta, haciendo un total de **15 puntos de acceso**.

Plataformas de capa de distribución

Los switches de capa de distribución son los puntos de conexión de los múltiples switches de la capa de acceso. Por tanto, debemos seleccionar una familia de switch que soporte la cantidad tráfico que llega desde la capa de acceso. En este sentido, el switch de capa de distribución debe tener alto rendimiento, pues el un punto que se encuentra delimitando el dominio de broadcast. Instalaremos un **Cisco Catalyst WS-C3850-24T-S** como elemento de distribución en cada planta del IES.

Plataformas de capa de núcleo

Instalaremos switches, siendo necesario que estos dispositivos se encarguen del enrutamiento de paquetes mediante el direccionamiento lógico y el control de VLANs. El switch de capa 3 **WS-C3650-48PS-S Cisco Catalyst 3650** nos ofrece todas las prestaciones que necesitamos: 48 puertos, redundancia de alimentación, soporte de Access Control List (ACL) y Quality of Service (QoS).

En la fase de Diseño Lógico hablamos de la implementación de una zona desmilitarizada para proteger los servidores accesibles desde Internet. Es fundamental conseguir un cortafuegos que sea capaz de hacer frente al tráfico de Internet, así como a los diferentes accesos a la red interna. Compraremos un **Cisco ASA 5500-X con servicios FirePOWER**, un dispositivo de firewall que ofrece protección contra amenazas integrada para toda la secuencia de ataque. Este NGFW recibió las mejores calificaciones de eficacia en seguridad en pruebas de terceros por NGIPS y AMP, al bloquear el 99,4% y el 99,2% de las amenazas, respectivamente.

5. VALIDACIÓN Y PRUEBAS

Para verificar que nuestro diseño de red cumple satisfactoriamente con los objetivos técnicos y de negocio planteados al principio con el cliente, vamos a pasar a mostrar el prototipo que hemos realizado en el simulador **Cisco Packet Tracer 8**, el cual nos permite configurar los distintos dispositivos necesarios para la creación de la red y probar su correcto funcionamiento. Para esto último, realizaremos las llamadas pruebas de aceptación de los diferentes elementos que le hemos introducido, tales como los servidores web y de correo y las listas de acceso que nos permiten restringir la comunicación entre VLANs determinadas.

5.1. PROTOTIPO DE RED EN CISCO PACKET TRACER

Como hemos comentado en la introducción de este apartado, hemos realizado un prototipo con la herramienta de simulación Cisco Packet Tracer 8, en la cual hemos podido diseñar la topología de red y configurar sus diferentes componentes para comprobar que efectivamente funciona y cumple con los requisitos inicialmente establecidos con el cliente.

A la izquierda del prototipo, podemos ver las cuatro conexiones de red para llevar a cabo la implementación de una **DMZ** utilizando para ello únicamente un cortafuegos. Las zonas que podemos distinguir son la red jerárquica interna del instituto, el ISP (Orange) que nos proporciona accesos a Internet, la DMZ con los servidores del instituto (web y de correo) y finalmente una pequeña simulación a Internet.

5.1.1. Red interna del instituto

Como hemos comentado en ocasiones anteriores, aquí podemos ver el modelo jerárquico que hemos seguido para diseñar dicha red. Las capas de núcleo, distribución, acceso y dispositivos finales. En el **núcleo** hemos optado por añadir un switch 3650 multicapa o de capa 3, con los puertos hacia los switches de distribución truncados para así poder transmitir las distintas VLANs que hemos configurado. Además, para añadir velocidad hemos puesto cables de fibra permitiendo así un transporte rápido. En la parte de **distribución** hemos incluido un switch de capa 2 por planta, menos en la planta baja que hemos conectado todos los elementos directamente al multicapa para ahorrar dinero, ya que disponemos de suficientes puertos en este para dicho cometido. En **acceso** hemos utilizado switches 2960 para dotar de conexión a las dos althias de la planta baja y a las cámaras de todo el edificio, además, de puntos de acceso para permitir que la conexión inalámbrica. Finalmente, los **dispositivos finales** que hemos utilizado han sido portátiles, impresoras, ordenadores de sobremesa y teléfonos móviles

5.1.2. Internet Service Provider

Para poder proveer al instituto de internet hemos optado por contratar un ISP, en este caso Orange, que nos proporciona dicha conectividad. También, hemos usado un DNS (Servidor de Domino de Nombres) que nos permite registrar la dirección de nuestro instituto www.berenguela.es

5.1.3. DMZ

Por último, volvemos a recalcar la zona desmilitarizada en la cual se encuentran alojados el servidor web y de correo electrónico, que dotan al instituto de tales servicios.

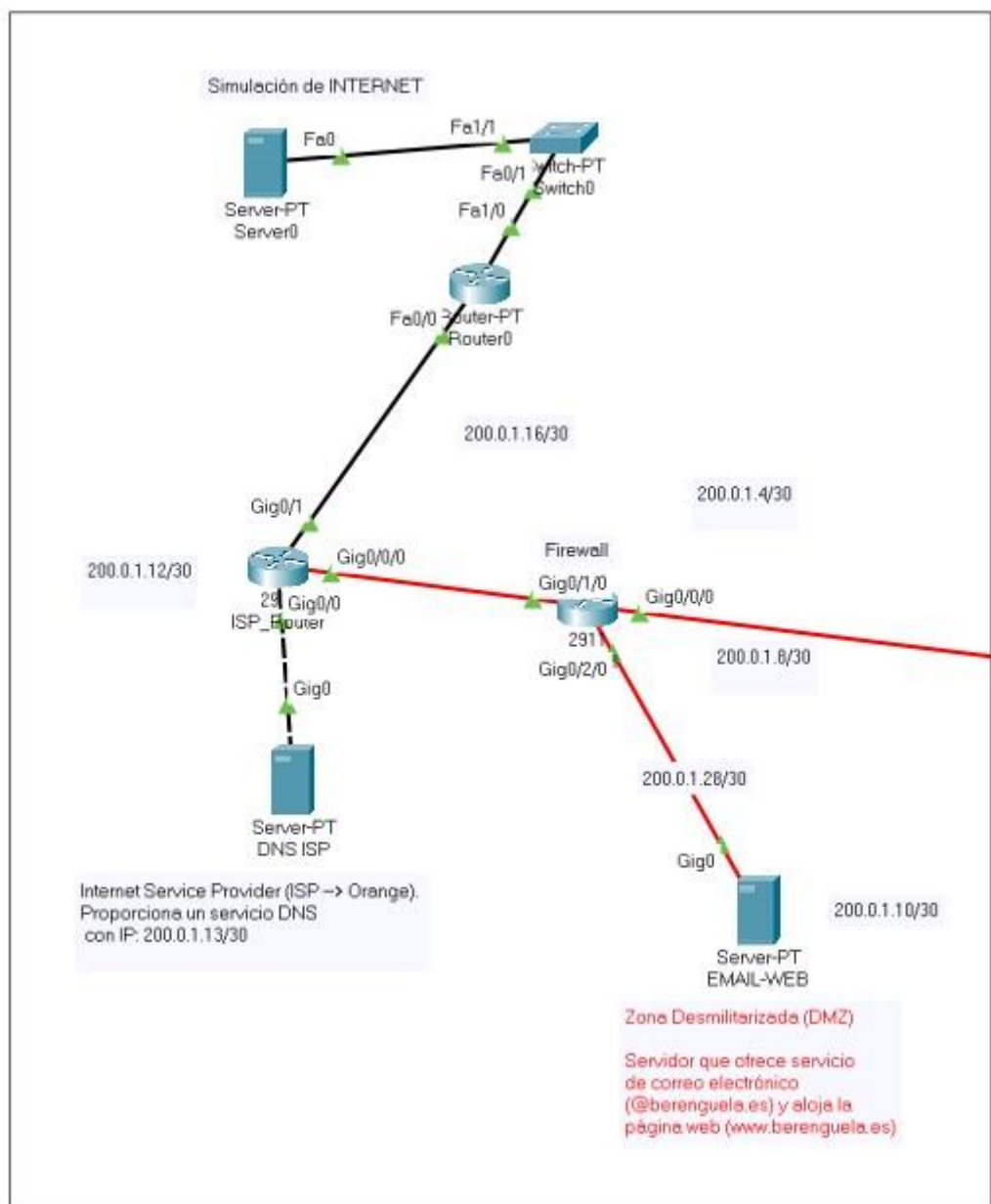
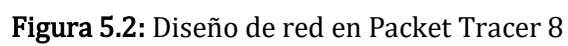


Figura 5.1: DMZ, ISP y Simulación de Internet.



5.2. PRUEBAS DE ACEPTACIÓN

En este apartado vamos a mostrar las pruebas de aceptación para comprobar el correcto funcionamiento de la red.

5.2.1. Listas de control de acceso (ACL)

Con estas listas lo que tratamos es de restringir el acceso de unas VLANs a otras, para dar seguridad a nuestra red. Por tanto, el **objetivo** de esta será probar la capacidad de las ACL que hemos configurado en el switch multicapa y se han heredado al resto de dispositivos. De esta manera, denegamos ciertas comunicaciones entre grupos específicos y permitimos que los miembros de un mismo grupo o comunidad si puedan intercambiar información.

Una vez dicho esto, los **criterios de aceptación** que tendremos serán que los switches bloquen un ping desde un punto A, que intente contactar con un punto B perteneciente a grupos distintos y restringidos. Esto es el caso de cualquier alumno o profesor que intente acceder a las cámaras. Sin embargo, si deben permitir la comunicación entre dos dispositivos pertenecientes a la misma comunidad y a otras comunidades no restringidas.

Una vez dicho esto, vamos a pasar a probar que lo citado anteriormente funciona enviando un mensaje ICMP desde un ordenador alumno a otro que se encargue de las cámaras. Lo mismo haremos con los profesores y entre miembros de la misma comunidad.







Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Laptop3Profesor	Laptop1Profesor	ICMP		0.000	N	0	(edit)	
	Successful	Laptop2Alumno	Laptop3Profesor	ICMP		0.000	N	1	(edit)	
	Successful	Smartphone AlumI	PC3PDA	ICMP		0.000	N	2	(edit)	

Figura 5.3: Tráfico de paquetes exitoso entre comunidades permitidas









Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	Laptop1Profesor	Cámaras PS	ICMP		0.000	N	0	(edit)	
	Failed	Smartphone AlumI	Cámaras PS	ICMP		0.000	N	1	(edit)	
	Failed	Laptop3Alumno	PC1 cámaras	ICMP		0.000	N	2	(edit)	
	Successful	PC3PDA	PC1 cámaras	ICMP		0.000	N	3	(edit)	

Figura 5.4: Tráfico de paquetes fallido entre alumnos y profesores con las cámaras y exitoso con el personal de administración

5.2.2. Servidor de correo electrónico

Los **objetivos** marcados en esta prueba consisten en probar la funcionalidad del servicio de correo electrónico (SMTP + POP3) gracias al envío de emails por parte de usuarios pertenecientes a comunidades diferentes, tales como alumno a personal de administración.

Como **criterio de aceptación** los switches deben alcanzar el servidor de correo y permitir el tráfico de emails. Además, los usuarios deben de poder recuperar en una bandeja de entrada los correos electrónicos que les han llegado gracias a POP3.

Para probar que todo lo anterior funciona de manera adecuada, vamos a proceder a enviar un correo desde un ordenador alumno a un profesor. En el servidor de correo electrónico hemos dado de alta tres usuarios distintos:

- **Sebastian.reyes** con contraseña 1234.
- **Alonso.diaz** con contraseña 1234.
- **Juanma.porrero** con contraseña 1234.

A continuación, mostramos los emails enviados y recibidos:

```
Sending mail to alonso.diaz@berenguela.es , with subject : Notas
Examen Ordinario... Mail Server: 200.0.1.10
Send Success.
```

Figura 5.5: Envío de mail por parte del profesor a alumno

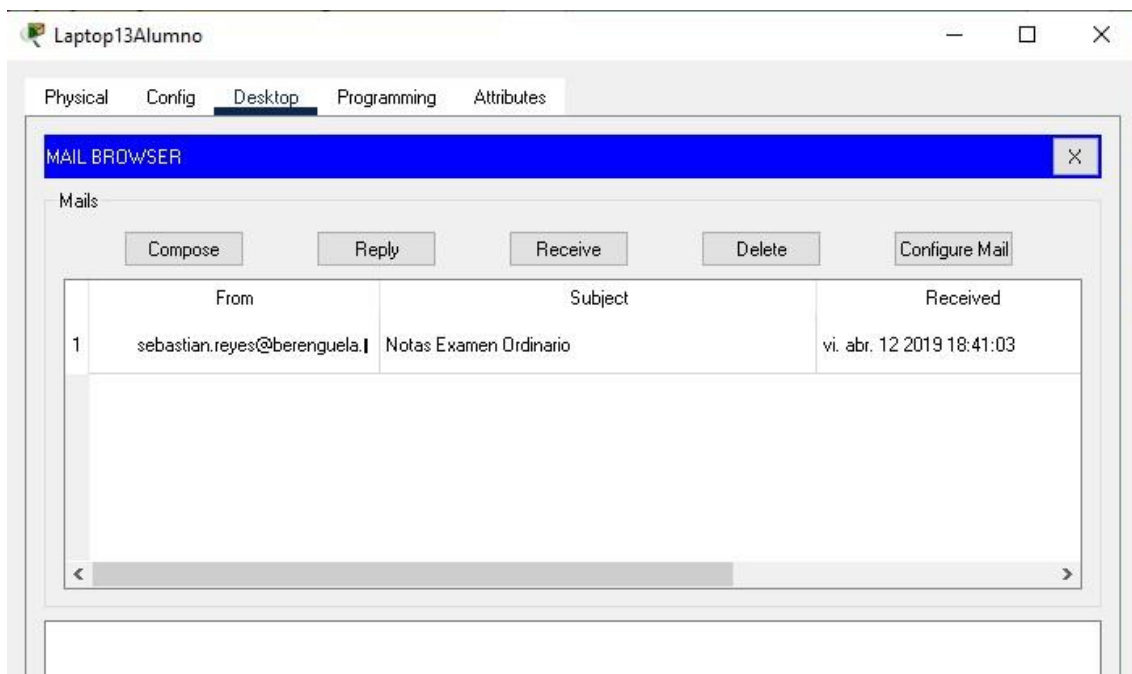


Figura 5.6: Recepción de mail por parte del alumno

5.2.3. Servidor web

El **objetivo** marcado para el servidor web consiste en probar si cumple con el servicio establecido inicialmente, mediante la descarga de la página www.berenguela.es en cualquier ordenador del instituto. A la misma vez, estaremos probando el funcionamiento del DNS, que nos proporciona el ISP.

El **criterio de aceptación** que vamos a utilizar, por tanto, es que un ordenador debe de poder acceder al sitio web citado anteriormente que como hemos dicho este alojado en el servidor 200.0.1.14. Para poder traducir el nombre de domino por la IP, debe conectarse con el DNS.

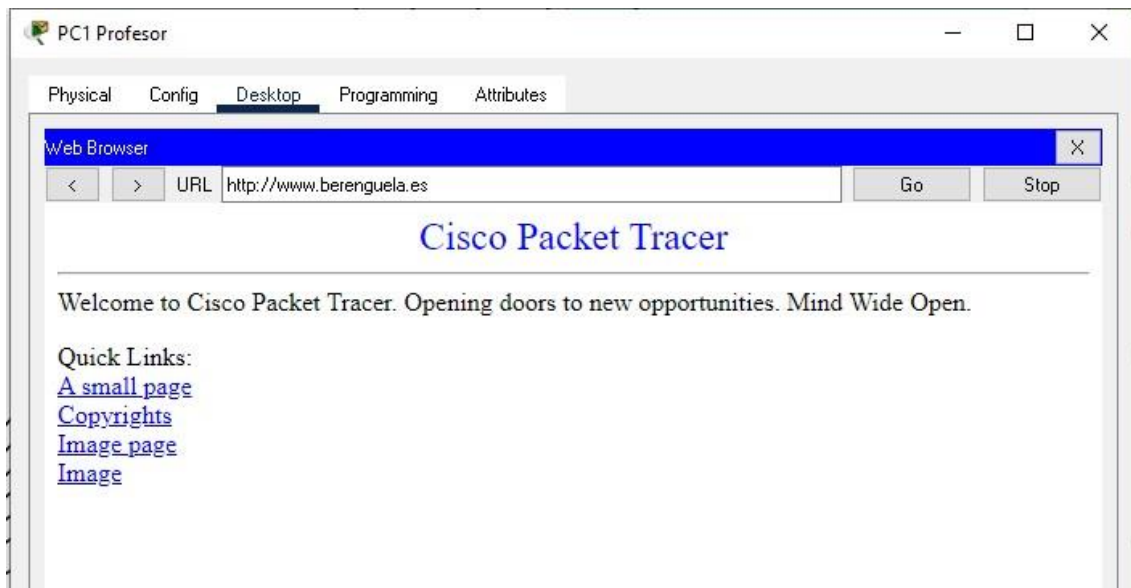


Figura 5.7: Página oficial del instituto

APÉNDICE A PRESUPUESTO

G-PLES

Dirección: Paseo de la Universidad, 4, 13071 Ciudad Real, Cdad. Real Telf.: +34 630 47 73 68

Correo electrónico: gplescompany@gmail.com

Ciudad Real, Ciudad Real, 13001

Fax: +34 630 47 73 68

Sitio web: www.sites.google.com/view/g-ples/home

Factura para: IES BERENGUELA DE CASTILLA

Teléfono: 926872909

N.º de factura: 12366

Dirección: Calle Teófila Sánchez, 14. 13260, Bolaños de Calatrava (Ciudad Real)

Fax: 926872830

Fecha: 26/05/2021

Correo electrónico: 13004778.ies@edu.jccm.es

Factura para:

N.º de artículo	Descripción	Cant.	Precio por unidad	Descuento	Precio
1232	Cisco WS-C2960 – 24pc-s - Switch de capa 2	9	900,00 €	50,00 €	8.050,00 €
1233	Ubiquiti Networks UAP-ACLR - Punto de Acceso Inalámbrico	15	143,45 €		2.151,75 €
6534	Cisco Catalyst WS-C3850-24T-S - Switch de capa 3 o multicapa	1	2.230,00 €		2.230,00 €
3464	Fibra multimodo 50/125 OM2 LSZH 12 fibras 1m	30	1,31 €		39,30 €
4564	Bobina Cable UTP Cat6 1m	350	0,27 €		94,50 €
4564	ASA5516-FPWR-K9 ASA 5516-X with FirePOWER services, 8GE	1	1.990,56 €		1.990,56 €
4443	HPE ML350 Gen10 51182P 32G	1	5.500,45 €		5.500,45 €
					- €
					- €
					- €
					- €
					- €
				Subtotal de la factura	20.056,56 €
				Tipo impositivo	
				Impuesto sobre las ventas	- €
				Otros	
				Depósito recibido	
				TOTAL	20.056,56 €

Hacer que todos los cheques se extiendan a nombre de G-PLES.

Total a pagar en 200 días. Cuentas vencidas sujetas a un cargo por servicios de 5% al mes.


```

!
interface GigabitEthernet1/0/1
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
 no cdp enable
!
interface GigabitEthernet1/0/2
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
 no cdp enable
!
interface GigabitEthernet1/0/3
 switchport access vlan 20
 switchport mode access
 switchport nonegotiate
 no cdp enable
!
interface GigabitEthernet1/0/4
 switchport access vlan 20
 switchport mode access
 switchport nonegotiate
 no cdp enable
!
interface GigabitEthernet1/0/5
 switchport access vlan 20
 switchport mode access
 switchport nonegotiate
 no cdp enable
!
interface GigabitEthernet1/0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
 switchport access vlan 30
 switchport mode access
 switchport nonegotiate
 no cdp enable
!
interface GigabitEthernet1/0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
!

```

```

interface GigabitEthernet1/1/1
  no switchport
  ip address 200.0.1.1 255.255.255.252
!
interface GigabitEthernet1/1/2
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface GigabitEthernet1/1/3
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface GigabitEthernet1/1/4
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan10
  mac-address 00e0.f9c1.0401
  ip address 172.16.7.254 255.255.248.0
  ip access-group 1 in
  ip access-group 1 out
!
interface Vlan20
  mac-address 00e0.f9c1.0402
  ip address 172.16.8.254 255.255.255.0
  ip access-group 2 in
  ip access-group 2 out
!
interface Vlan30
  mac-address 00e0.f9c1.0403
  ip address 172.16.9.62 255.255.255.192
  ip access-group 3 in
  ip access-group 3 out
!
interface Vlan40
  mac-address 00e0.f9c1.0404
  ip address 172.16.9.78 255.255.255.240
  ip access-group 4 in
  ip access-group 4 out
!
router rip
  version 2
  network 172.16.0.0
  network 200.0.1.0
  no auto-summary
!
ip classless
!
ip flow-export version 9
!
!
access-list 1 deny 172.16.9.64 0.0.0.15
access-list 1 permit any
access-list 2 deny 172.16.9.64 0.0.0.15
access-list 2 permit any
!

```


Configuración de los switch capa 2

```

version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface GigabitEthernet0/1
 switchport mode trunk
!
interface GigabitEthernet1/1
 switchport access vlan 10
 switchport mode access
 no cdp enable
!
interface GigabitEthernet2/1
 switchport access vlan 20
 switchport mode access
 no cdp enable
!
interface GigabitEthernet3/1
 switchport access vlan 10
 switchport mode access
 no cdp enable
!
interface GigabitEthernet4/1
 switchport access vlan 20
 switchport mode access
 no cdp enable
!
interface GigabitEthernet5/1
 switchport access vlan 10
 switchport mode access
 no cdp enable
!
interface GigabitEthernet6/1
 switchport access vlan 20
 switchport mode access
 no cdp enable
!
interface GigabitEthernet7/1
!
interface GigabitEthernet8/1
!
interface GigabitEthernet9/1
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0

```

BIBLIOGRAFÍA

FUENTES NO ONLINE

1. CISCO. «Campus. Resumen de Diseño». En: (2013).
2. CISCO. «Cisco Product Quick Reference Guide». En: ().
3. Cisco Validated design. «Campus LAN and Wireless LAN Design Guide». En: (2018).
4. Marcos Huerta. «Metodología de Diseño de Red TOP-DOWN». En: ().
5. A Jesin. *Packet Tracer network simulator*. Packt Publishing Ltd, 2014.
6. Priscilla Oppenheimer. *Top-down network design*. Cisco Press, 2010.
7. B. Piper. *Learn Cisco Network Administration in a Month of Lunches*. Manning Publications Company, 2017. isbn: 9781617293634.

FUENTES ONLINE

1. Ernesto Aringanello. *Proceso de configuración de ACL*. 2006. url: <http://aprenderedes.com/2006/11/proceso-de-configuracion-de-acl/>.
2. Hewlett Packard Enterprise. *HPE ProLiant ML350 Gen10 Server*. 2017. url: <https://content.etalize.com/Manufacturer-Brochure/1041986461.pdf>.
3. Ubiquiti Networks. *UniFi UAP/UAP-LR Punta de acceso Guía De Inicio Rápido*. url: https://dl.ubnt.com/guides/UniFi/ES/UAP_UAP-LR_QSG_ES.pdf.
4. UCLM. *Normativa de Política de Seguridad de la Red de Comunicaciones*. 2006. url: <https://e.uclm.es/servicios/doc/?id=UCLMDOCID-12-193>.
5. Alex Walton. *Diseño Jerárquico de Redes*. url: <https://ccnadesdecero.es/disenio-jerarquico-de-redes/>.