



UNIVERSITAT  
POLITÈCNICA  
DE VALÈNCIA



Escola Tècnica  
Superior d'Enginyeria  
Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica  
Universitat Politècnica de València

# **Disseny i configuració de la infraestructura informàtica per a una PIME d'assessoria i consultoria**

**TREBALL FI DE GRAU**

Grau en Enginyeria Informàtica

*Autor:* Santiago Pesudo Pla

*Tutor:* Xavier Molero Prieto

Curs 2020-2021



# Resum

En aquest treball s'ha decidit analitzar les necessitats d'una empresa i dissenyar una infraestructura informàtica que s'adeqüe a la seua situació. Per fer-ho hem començat analitzant a què se dedica, quina estructura té i com és la disposició física del local on se realitza la seua activitat.

Un cop realitzada aquesta feina, hem escollit la topologia que més s'adequa a la societat. Hem triat la topologia en forma d'estel ja que permet ampliar fàcilment la infraestructura. Aquest era un dels requisits que ens havia comunicat l'empresa ja que l'esperen ampliar en un futur i disposen d'una planta baixa que actualment està arrendada però que en cas d'ampliar s'afegiria a l'activitat de l'empresa. També hem definit l'estàndard que haurà de tindre el cablejat i on es situaran cada un dels elements físics de la infraestructura.

Des de el punt de vista lògic, hem definit les diferents VLANs en les que se dividirà la xarxa, hem establert el rang d'adreces IP de cada xarxa virtual i quines IP concretes tindran alguns elements de la xarxa. Aquesta divisió de la xarxa en VLANs ens permet augmentar la seguretat de la mateixa i millorar-ne el rendiment. Posteriorment, hem comprovat la nostra proposta de manera pràctica mitjançant el programa Cisco Packet Tracer.

Un punt fonamental per a la societat és la seguretat, de manera que hem inclòs un apartat específic en el que s'explica tota una sèrie de mesures que dificulten que cap intrús pugua accedir a la xarxa i que no es perda la informació guardada en els servidors.

Finalment, hem seleccionat una sèrie de dispositius que creiem que s'ajusten bé a la infraestructura i hem elaborat un pressupost per a tindre una idea aproximada de quant costaria la seua implementació.

**Paraules clau:** Infraestructura informàtica, disseny de la xarxa, configuració de la xarxa, Cisco Packet Tracer, assessoria, consultoria.

---

# Resumen

En este trabajo se ha decidido analizar las necesidades de una empresa y diseñar una infraestructura informática que sea acorde a su situación. Para hacerlo hemos empezado analizando a qué se dedica, qué estructura tiene y cómo es la disposición física del local donde lleva a cabo su actividad.

Una vez realizadas estas tareas, hemos escogido la topología que más se adecua a la sociedad. Hemos escogido la topología en estrella ya que permite ampliar fácilmente la infraestructura. Este es uno de los requisitos que nos había comunicado la empresa dado que esperan ampliarla en un futuro y disponen de una planta baja que actualmente se encuentra alquilada, pero que en caso de tener que ampliar se añadiría a la actividad de la empresa. También hemos definido el estándar que deberá tener el cableado y dónde se situarán cada uno de los elementos físicos de la infraestructura.

Desde el punto de vista lógico, hemos definido las diferentes VLANs en las que se dividirá la red, hemos establecido el rango de direcciones IP de cada red virtual y qué IPs concretas tendrán algunos elementos de la red. Esta división de la red en VLANs nos permite aumentar la seguridad de la misma y mejorar su rendimiento. Posteriormente, hemos comprobado nuestra propuesta de manera práctica mediante el programa Cisco Packet Tracer.

Un punto fundamental para la sociedad es la seguridad, de manera que hemos incluido un apartado específico en que se explica una serie de medidas que dificultan que

ningún intruso pueda acceder a la red y que no se pierda la información guardada en los servidores.

Finalmente, hemos seleccionado una serie de dispositivos que creemos que se ajustan bien a la infraestructura y hemos elaborado un presupuesto para tener una idea aproximada de cuánto costaría su implementación.

**Palabras clave:** Infraestructura informática, diseño de la red, configuración de la red, Cisco Packet Tracer, asesoría, consultoría.

---

## Abstract

In this project, we have analysed the needs of a company and designed an IT infrastructure according to its situation. In order to do this, we started by analysing the business, its activity, its structure and the physical layout of the premises where the company carries out its activity.

After completing these tasks, we have chosen the topology that best suits the company. We have opted for the star topology as it allows the infrastructure to be easily extended. This is one of the requirements that the company had communicated to us because they hope to extend their business in the future and they have a ground floor which is currently rented, but it would be added to the company's activity in the event of growth. We have also defined the wiring standard and where every physical element of the infrastructure will be located.

On the logical level, we have defined the different VLANs into which the network will be divided, we have established the range of IP addresses of each virtual network and which specific IPs will have some elements of the network. This network division into VLANs allows us to increase the security of the network and improve its performance. Afterwards, we tested our proposal in a practical way using Cisco Packet Tracer software.

Security is a crucial point for the company, so we have included a section explaining a series of measures to ensure that no hacker can access the network and that the information stored in the servers is not lost.

Finally, we have selected a number of devices that we consider suitable for the infrastructure and we have drawn up a budget to get a rough idea of how much it would cost to implement the infrastructure.

**Key words:** IT infrastructure, network design, network settings, Cisco Packet Tracer, advisory, consulting

---

# Índex

---

<b>Índex</b>	<b>v</b>
<b>Índex de figures</b>	<b>vii</b>
<b>Índex de taules</b>	<b>viii</b>

---

<b>1 Introducció</b>	<b>1</b>
1.1 Motivació	1
1.2 Objectius	1
1.3 Estructura de la memòria	2
1.4 Ús de la bibliografia	2
1.5 Objectius de desenvolupament sostenible	3
<b>2 Descripció de l'empresa i disseny físic</b>	<b>5</b>
2.1 A què es dedica?	5
2.2 Estructura interna de l'empresa	5
2.3 Canvis que s'estan produint al sector	6
2.4 Necessitats de l'empresa	6
2.5 Estudi bàsic	7
2.6 Sala de telecomunicacions	12
2.7 Topologia utilitzada	13
2.8 Cablejat estructurat	14
2.8.1 Àrea de treball	14
2.8.2 Cablejat horitzontal	15
2.8.3 Cablejat vertical	15
2.8.4 Sala de telecomunicacions	16
2.9 Enllaços redundants	16
2.10 Mapa físic de la xarxa	17
<b>3 Disseny lògic de la xarxa</b>	<b>19</b>
3.1 Disseny de VLAN	19
3.2 Adreçament	20
3.2.1 Rang d'adreces IP	20
3.2.2 Implementació NAT	21
3.2.3 Dispositius amb adreces fixes	22
3.3 Mapa lògic de la xarxa	23
3.4 Validació de la configuració amb Packet Tracer	23
3.4.1 Cisco Packet Tracer	23
3.4.2 Peculiaritats de la simulació	24
3.4.3 Configuració dels dispositius	24
3.4.4 Simulació	28
<b>4 Connexió sense fil, servei de veu i servidors</b>	<b>33</b>
4.1 Connexió sense fil	33
4.1.1 Estàndard	33
4.1.2 Topologia	34
4.1.3 Xarxes sense fil	35

4.1.4	Adreçament	36
4.2	Servei de veu	36
4.3	Servidors	37
4.3.1	Servidor de correu	37
4.3.2	Servidor de virtualització d'equips	39
4.3.3	Servidor d'autenticació de xarxa Wi-Fi Radius	40
<b>5</b>	<b>Seguretat de la xarxa i la informació</b>	<b>43</b>
5.1	Seguretat de la xarxa	43
5.1.1	LAN	43
5.1.2	WLAN	44
5.2	Seguretat de la informació	45
<b>6</b>	<b>Pressupost del projecte i elecció de dispositius</b>	<b>49</b>
6.1	Hardware	49
6.1.1	PCs	49
6.1.2	Portàtils	50
6.1.3	Servidors	50
6.1.4	Dispositius d'emmagatzematge	50
6.1.5	Commutadors o <i>switches</i>	51
6.1.6	Encaminador	51
6.1.7	Cablejat i rossetes	51
6.1.8	Armari o <i>Rack</i>	52
6.1.9	PDU	52
6.1.10	SAI	52
6.1.11	Refrigeració	53
6.1.12	Extintors	53
6.1.13	Porta ignífuga	53
6.1.14	Punts d'accés	54
6.1.15	Tallafocs	54
6.1.16	Taula resum hardware	54
6.2	Software	54
6.2.1	Antivirus	54
6.2.2	Virtualització d'equips	55
6.2.3	Servidor de correu	55
6.2.4	Taula resum software	55
6.3	Instal·lació	56
6.4	Total	56
6.5	Manteniment	56
<b>7</b>	<b>Conclusions</b>	<b>57</b>
	<b>Bibliografia</b>	<b>59</b>

# Índex de figures

---

1.1	Llistat dels 17 objectius de desenvolupament sostenible promociats per l'ONU. . . . .	3
2.1	Plànol entresòl 1. . . . .	8
2.2	Plànol entresòl 2. . . . .	9
2.3	Plànol planta baixa. . . . .	10
2.4	Imatge d'un connector RJ-45 mascle, el qual conté vuit pins. . . . .	11
2.5	Plànol entresòl 2 amb la sala de servidors . . . . .	13
2.6	Topologia de la xarxa en forma d'estel. . . . .	14
2.7	Imatge d'una rosseta RJ-45 amb dos eixides. . . . .	15
2.8	Imatge de com és la fibra òptima multimode. . . . .	16
2.9	Esquema de la distribució física de la xarxa. . . . .	17
3.1	Distribució lògica de la xarxa amb les divisions per VLANs. . . . .	23
3.2	Imatge de la xarxa que simularem. . . . .	24
3.3	Configuració del <i>switch</i> 1. . . . .	25
3.4	Ports disponibles al commutador 1. . . . .	26
3.5	Resultat d'executar l'ordre <i>show interface trunk</i> . . . . .	27
3.6	Ordinador connectat per DHCP . . . . .	29
3.7	PING entre dos ordinadors de la VLAN 2. . . . .	30
3.8	PING entre un dispositiu de la VLAN 4 i un de la VLAN 5 . . . . .	30
3.9	PING entre un dispositiu de la VLAN 2 i un de la VLAN 4. . . . .	31
4.1	Logotip Wi-Fi. . . . .	34
4.2	Esquema de la connexió dels dispositius sense fil a la xarxa mitjançant el punt d'accés. . . . .	34
4.3	Imatge de com s'instal·laran els punts d'accés al sostre. . . . .	35
4.4	Xarxes amb connexió WiFi . . . . .	35
4.5	Imatge d'un telèfon IP. . . . .	37
4.6	Logotip del <i>software</i> Exim . . . . .	38
4.7	Imatge d'un servidor Dell PowerEdge R340. . . . .	38
4.8	Logotip del <i>Software</i> dedicat a la virtualització d'equips Citrix XenServer. . . . .	39
4.9	Servidor HPE ProLiant DL325 Gen10 P04648-B21. . . . .	40
5.1	Imatge del antivirus bitDefender . . . . .	44
5.2	Imatge d'un SAI . . . . .	45
5.3	Esquema del RAID 50 . . . . .	46
5.4	Logotip de Google Drive. . . . .	47
6.1	Imatge d'un ordinador HP Thin Client t430 . . . . .	49
6.2	Imatge d'un portàtil Innjoo Voom . . . . .	50
6.3	Imatge d'un armari HPE P9K07A. . . . .	52
6.4	Imatge d'un extintor de pols ABC de 6 kg. . . . .	53
6.5	Preu de l'antivirus. . . . .	55

## Índex de taules

---

2.1	Taula ocupació màxima d'espais. . . . .	11
2.2	Taula de connexions necessàries . . . . .	12
3.1	Taula on es mostren les VLANs en les que es dividirà la xarxa. . . . .	19
3.2	Taula on es mostren la visualització que hi haurà entre les diferents VLANs. . . . .	20
3.3	Rangs d'IPs per a cada VLAN . . . . .	21
6.1	Taula resum preu dels elements <i>hardware</i> . . . . .	54
6.2	Taula resum amb els preus finals de l'apartat del programari. . . . .	55
6.3	Resum del pressupost total . . . . .	56



---

---

# CAPÍTOL 1

## Introducció

---

En aquest primer capítol s'exposen les motivacions que m'han dut a la realització del treball fi de grau, així com els objectius que m'he proposat aconseguir. També s'explica quina estructura segueix la memòria, quin ús he fet de bibliografia i els objectius de desenvolupament sostenible que es poden veure reflectits al treball, que són l'ODS número 8 i l'ODS número 12.

### 1.1 Motivació

---

La era digital en el S. XXI ha suposat una gran revolució en tots els àmbits de l'activitat humana, millorant la qualitat de vida ja que permet estalviar temps i simplificar processos.

Així mateix en l'àmbit empresarial la informàtica ha suposat un avanç indiscutible; hui en dia, pràcticament en totes les empreses la infraestructura informàtica actua com a columna vertebral, ja que permet la optimització de tasques, rapidesa i seguretat, entre altres avantatges. Més encara, quan parlem d'empreses que treballen amb dades com és el cas de l'empresa que ens ocupa, té especial rellevància la disposició d'un sistema informàtic adequat i actualitzat a les necessitats del negoci.

Pel que fa a l'empresa per a la qual es realitza aquest treball, he de dir que és una empresa propera a mi i que es dedica a un aspecte que em resulta interessant com és el món de l'economia. Jo, junt amb el grau d'enginyeria informàtica he estudiat el grau d'Administració i Direcció d'Empreses i un màster en Direcció Financera i Fiscal, de manera que podia comprendre més fàcilment els problemes als quals s'enfronten.

M'han donat moltes facilitats per a conèixer millor l'empresa i em van mostrar interès en saber com seria i el cost associat a la infraestructura òptima per a la seua activitat actual i dels pròxims anys.

### 1.2 Objectius

---

L'objectiu principal d'aquest treball és proporcionar les directrius per a implementar una infraestructura informàtica per a una empresa concreta, dedicada a l'assessoria i consultoria en Vila-real. Per a aconseguir-ho hem de tindre en compte les necessitats de l'empresa i que la infraestructura s'adeqüe a les possibilitats econòmiques a la vegada que no quede obsoleta en període curt de temps.

Aleshores, havien de conèixer la situació actual i l'evolució que espera tindre la societat, analitzar quines expectatives d'expansió té i amb quin espai compta. De manera que

hem tractat d'obtenir una infraestructura que permetera una fàcil expansió mitjançant la topologia en forma d'estel.

Un altre dels objectius és que el pressupost siga acorde a la mida de l'empresa, de manera que triarem aquelles alternatives que ens oferisquen el millor compromís entre cost i prestacions tant, des del punt de vista del disseny com dels dispositius escollits.

Finalment, hem considerat validar la nostra proposta, de manera que mitjançant el programa Packet Tracer hem simulat una infraestructura amb les línies bàsiques de la nostra proposta per a verificar que efectivament funciona.

### **1.3 Estructura de la memòria**

---

La memòria d'aquest treball es divideix en 7 capítols en els que es detalla pas a pas des de la descripció de l'empresa per a la qual va destinada la infraestructura fins a la seua configuració i preu.

El primer capítol és una introducció en la qual se comenta la motivació que m'ha portat a realitzar aquest treball. Posteriorment, s'anomenen els objectius que hem seguit en la realització del TFG i com hem anat aconseguint-los. Després, se descriu com s'organitza la memòria i quin ús s'ha fet de la bibliografia. I finalment, s'explica què són els objectius de desenvolupant sostenible i com pot contribuir la realització d'aquest treball a aconseguir-los.

Al segon capítol es presenta l'empresa i es realitza el disseny físic de la infraestructura. S'explica a què es dedica, com s'estructura, quins canvis s'estan produint al sector i les necessitats que ha de complaure el nostre treball. Un cop presentades les necessitats s'explica, des del punt de vista físic quines decisions hem pres com ara la topologia escollida, el cablejat i on es situaran els dispositius.

El tercer capítol va destinat al disseny lògic, s'explica com s'ha fet la divisió de la xarxa en VLANs i les adreces de cada una d'aquestes. Especifica quines adreces tindran alguns dispositius amb IP fixa i es fa una simulació de la infraestructura amb el programa Cisco Packet Tracer.

A continuació, en el quart capítol, s'explica quines connexions sense fil hi hauran i a quines xarxes virtuals corresponen. Junt amb tot açò, també s'exposa quina sèrie de servidors seran necessaris, el software aparellat a aquests i els models de dispositius que es recomana seleccionar.

El capítol quint va destinat a les mesures de seguretat que tindrà la infraestructura. La seguretat és un punt molt important per a l'empresa i s'implantaran mesures per a protegir l'accés a la xarxa i per a no perdre la informació emmagatzemada als servidors.

Un dels punts importants a l'hora de presentar la infraestructura és saber el cost associat que té. En el sext capítol es detallen els costos de la seua implementació, desglossant-los per els apartats als que correspon: *hardware*, *software* i instal·lació.

Finalment, en el setè capítol s'exposen les conclusions que he tret en la realització d'aquest treball.

### **1.4 Ús de la bibliografia**

---

Per a la realització d'aquest treball fi de grau els llibres *Redes de computadoras* [12], *Estructura y diseño de computadoras* [8], *Arquitectura de computadores* [4] i *Redes de computadoras (Vol.5)* [5] han sigut la base del coneixement adquirit.



**Figura 1.1:** Llistat dels 17 objectius de desenvolupament sostenible promocionats per l'ONU.

D'altra banda, he emprat els documents "Presentació del projecte Heura als centres educatius" [2] i "Especificaciones técnicas para instalaciones de centros de la Generalitat Valenciana" [3] com una guia de com implementar les infraestructures, i m'han servit per a veure el nivell que s'exigeix als centres públics de ambdues comunitats.

També hi ha part de la bibliografia que he consultat per a obtenir informació més puntual com és el cas del "Reial Decret 486/1997 de 14 d'abril" [1] i "l'ordenança de convivència ciutadana de Vila-real" [10] que he emprat per a conèixer la densitat màxima que poden tindre els llocs de treball i el nombre màxim de decibels permesos durant la nit a Vila-real.

Finalment, els manuals de CISCO *Cisco CCNA, routing and switching, ICND2 200-101: guia oficial para la certificación* [6], *Cisco CCENT/CCNA, ICND1 100-101: guia oficial para la certificación* [7] i *Redes Cisco: curso práctico de formación para la certificación CCNA* [9] els he emprat per a la configuració dels elements en el Packet Tracer.

## 1.5 Objectius de desenvolupament sostenible

Els objectius de desenvolupament sostenible (ODS) son una sèrie de 17 objectius adoptats per els països membre de la Organització de les Nacions Unides (ONU) en 2015, que pretenen posar fi a la pobresa, protegir el medi ambient i garantir que totes les persones puguem gaudir de pau i prosperitat per a 2030. Podem veure tot el llistat en la Figura 1.1.

En aquest treball considere que en podem veure reflectits dos, l'objectiu número 8: Treball decent i creixement econòmic; i el número 12: Producció i consum responsables.

La infraestructura informàtica pot considerar-se la base per a una empresa que dedicada a treballar amb dades, de manera que és imprescindible per a poder desenvolupar-se i augmentar la seua mida, creant nous llocs de treball qualificat que és una de les manques que sovint té Espanya.

D'altra banda, considere que s'aplica l'objectiu 12 perquè a l'hora d'establir la infraestructura hem pres decisions que ens permetran reduir els residus tecnològics. Un exemple és el cas d'utilitzar clients lleugers que tenen una vida més llarga que els clients pesats ja que, com necessiten poca capacitat de còmput per a funcionar, no queden tant obsolets conforme augmenta l'exigència de les aplicacions. A més, el consum energètic d'aquestos és considerablement menor.



---

---

## CAPÍTOL 2

# Descripció de l'empresa i disseny físic

---

En aquest capítol es fa una introducció a l'empresa per a la qual dissenyarem la infraestructura. Explicarem quin és el seu model de negoci, la disposició física de l'empresa i les necessitats que té promogudes per els canvis que es produeixen al sector.

Posteriorment, veurem la distribució física de la infraestructura, analitzarem a fons les oficines on se situa l'empresa, també veurem la topologia més beneficiosa per a l'organització i mostrarem quin és el cablejat i nombre de rossetes necessari.

### 2.1 A què es dedica?

---

L'empresa en qüestió se situa a Vila-real i es defineix com "Un despatx professional integrat per economistes i graduats socials amb una àmplia experiència i coneixements en l'àmbit de l'assessorament i les seues diferents àrees. Creada en 1994, ofereix al seus clients, persones físiques, autònoms, PIMES i grans empreses, un servei de consultoria i assessorament integral, directe i personalitzat en tots aquells camps que afecten a la gestió econòmica de l'empresa." <sup>1</sup>. D'entre aquestos destaquem les àrees de serveis fiscals, mercantils, financers, comptables, laborals, auditories, concursals i peritacions.

### 2.2 Estructura interna de l'empresa

---

En l'empresa no hi ha una marcada divisió per departaments però sí que podem distingir tres departaments diferents: l'àrea de laboral, l'àrea d'administració i una altra àrea en la que s'engloben la resta de serveis.

Cada treballador té assignades una sèrie d'empreses i per a certes feines més crítiques, el treball una vegada es realitza és supervisat per un altre membre de l'empresa amb la finalitat d'assegurar una qualitat òptima.

En l'actualitat hi treballen un total de 9 persones: dos en el departament de laboral, dos en administració i cinc que tenen un rol més general encara que dintre d'estes cinc persones hi ha d'algunes més especialitzades en algunes funcions com ara l'auditoria o les finances.

Actualment l'empresa ocupa dos entresòls, l'un al costat de l'altre. En el principal es troben tres despatxos individuals, un despatx doble on es troba l'àrea de laboral, una

---

<sup>1</sup>Informació extreta de la pàgina web de l'empresa.

sala de treball amb 5 llocs de treball i una cafeteria. A l'altre entresòl trobem una sala de reunions amb una taula allargada amb capacitat per a 8 persones, així com un arxiu amb documents emmagatzemats.

Encara que pel moment no es contemple, l'empresa també és propietària de la planta baixa situada al davall del segon entresòl i, com que volem que el treball realitzat en aquest TFG tinga validesa en cas d'una ampliació, tindrem en compte la facilitat d'incloure aquest espai en la xarxa de l'empresa per si en un futur s'hagués d'utilitzar. Més avall es fa una descripció més profunda de l'espai físic i s'adjunten els plànols.

## 2.3 Canvis que s'estan produint al sector

---

Des de la creació de l'empresa a principis de la dècada del 90 s'han emprat els ordinadors com ajuda per a dur a terme la feina, encara que l'arribada d'Internet ha suposat un salt important en quant a l'optimització de la feina.

Abans els clients s'encarregaven de dur els documents com ara factures, rebuts, escriptures, etc. presencialment a l'empresa, la qual s'encarregava de processar tota la informació. Aquest procés d'intercanvi presencial de dades dificultava l'expansió geogràfica de la societat.

Actualment els clients solen enviar tota la informació escanejada, reduint el temps necessari per a realitzar les tasques. A més, per algunes tasques com ara la comptabilitat, si el client envia la informació en fulls de càlcul, seguint una estructura concreta, el programa que utilitzen és capaç d'introduir-la sola, quedant sols la feina corresponent a la revisió.

Tot apunta a que en un futur les tasques mecàniques com ara la comptabilitat acabaran desapareixent i cobrarà més importància l'anàlisi de les dades reflectides per aquesta. De manera que els programes seran capaços en sols escanejar una factura comptabilitzar-la correctament.

## 2.4 Necessitats de l'empresa

---

Hem preguntat a la direcció de l'empresa quines son les necessitats que creuen més rellevants per a la infraestructura de l'empresa. En la resposta rebuda sobretot s'ha posat l'accent en la seguretat de la xarxa ja que es tracten dades de certa rellevància, valor i confidencialitat. És per això que haurem de considerar la replicació de dades en llocs geogràfics diferents, així com seguretat en els diferents *routers* i *switches* de la xarxa.

El COVID-19 ha tingut un gran impacte en la societat i de fet ha provocat noves necessitats a l'empresa. Fins ara el teletreball era una cosa anecdòtica a les empreses, moltes desconfiaven de la productivitat d'aquesta manera de treballar però després de vores forçats a implantar-lo les empreses s'han adonat que aquesta reducció de la productivitat no té perquè produir-se. A la nostra empresa, encara que la seua activitat fora considerada essencial i tingueren permès acudir als llocs de treball (tenien que tramitar ERTES, acomiadaments, gestió d'altres empreses amb treballs essencials i demès) creuen que és una bona alternativa i que en alguns casos es pot utilitzar per exemple per a facilitar la conciliació de vida laboral i familiar.

Finalment, també ens han comunicat que tenen una alarma amb sistema de videovigilància per a tindre-ho en compte a l'hora del disseny lògic.

## 2.5 Estudi bàsic

---

Per a començar, estudiarem minuciosament el lloc físic on es troba situada l'empresa.

L'espai consta de dos entresòls, el primer que es mostra en la Figura 2.1, consta de 207 metres quadrats i és on es desenvolupa l'activitat general de l'empresa. En ell podem observar una zona d'espera al costat de l'entrada on hi ha un sofà i dos butaques. Tot seguit, a l'esquerra trobem un primer despatx, corresponent a un dels dos responsables de l'empresa. A continuació, també a l'esquerra, se situa un segon despatx que ocupa el segon responsable de l'empresa, aquest es una mica més gran i té una taula rodona que pot utilitzar-se per atendre clients.

Avançant, a la dreta, trobem la sala de treball amb cinc taules corresponents a cinc llocs de treball, precedida per un mostrador per a atendre els clients. A la dreta comença un passadís d'uns deu metres en el qual trobem un tercer despatx utilitzat actualment per a atendre clients en un àmbit més privat, una cafeteria on els treballadors poden prendre alguna cosa, i a la fi del passadís es distingeixen dos banys (el de dones i el d'homes) i un arxiu on es guarden documents en paper.

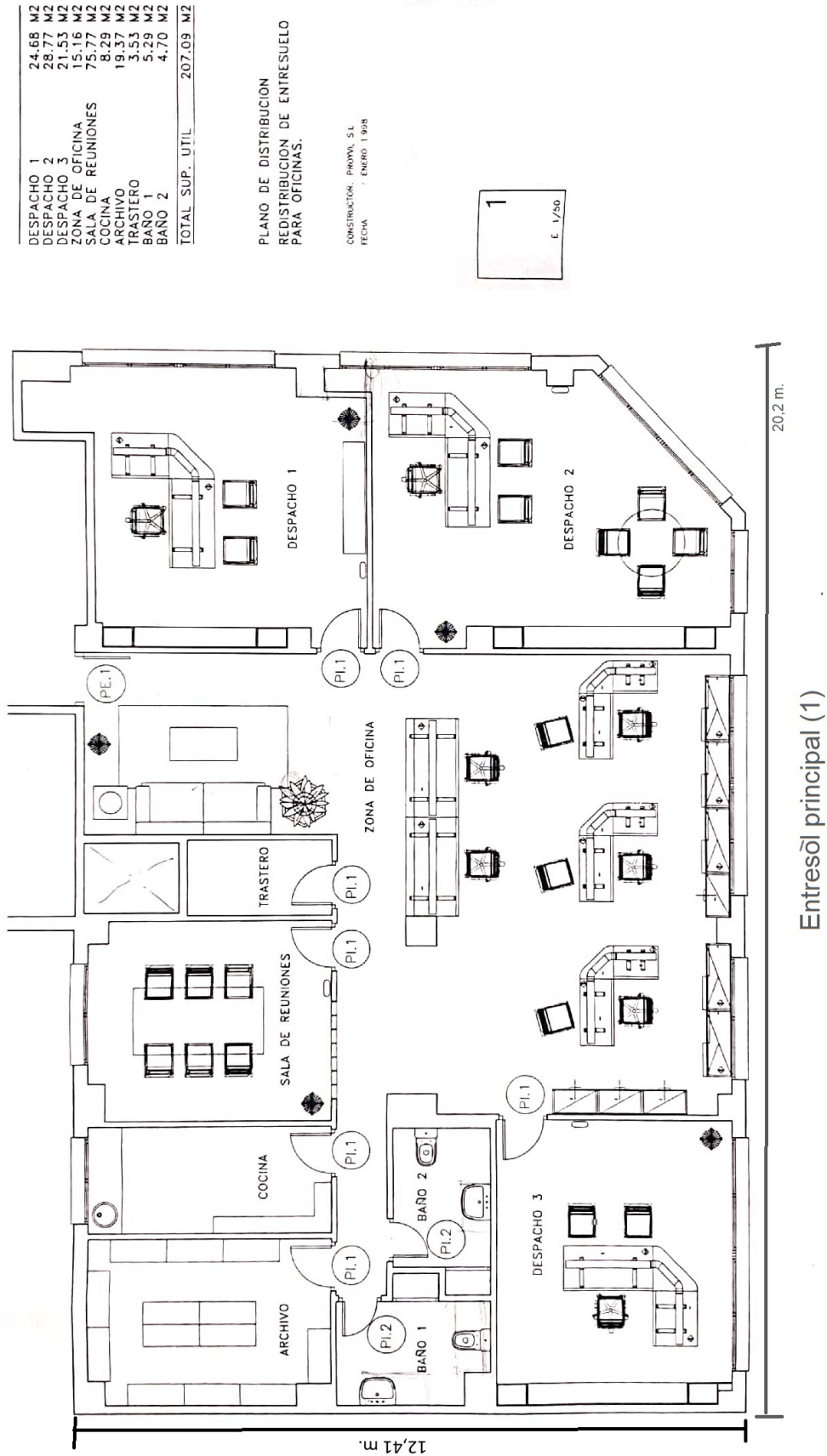
El segon entresòl se mostra en la Figura 2.2 i és un poc més menut, d'uns 100 metres quadrats. En ell trobem en entrar a l'esquerra els banys, a la dreta una sala de reunions amb una taula allargada per a reunir-se diverses persones, i al fons a l'esquerra un altre arxiu on també se guarden documents.

A part, l'empresa també té en propietat la planta baixa situada al davall del segon entresòl, que podem veure en la Figura 2.3. En l'actualitat s'ha suprimit l'escala que la unia amb el segon entresòl i l'immoble està arrendat, però si l'empresa ho considerara necessari podria tornar a posar-se l'escala i utilitzar-lo, de manera que tindrem en compte la facilitat d'ampliació de la xarxa de l'empresa per si més avant es decidira incorporar aquest espai a la seua activitat.

En la Taula 2.1 podem veure l'estimació de l'ocupació màxima de cada espai. Per calcular-la, hem partit del que s'anomena en el *Reial Decret 486/1997, del 14 d'abril* [1] el qual estableix les disposicions mínimes de seguretat i salut als llocs de treball. En concret, a l'annex 1, apartat A), subapartat 2, podem llegir el següent: «Les dimensions dels locals de treball hauran de permetre que els treballadors realitzen el seu treball sense riscos per a la seua seguretat i salut i en condicions ergonòmiques acceptables. Les seues dimensions mínimes seran les següents: a) 3 metres d'alçada des del sòl fins al sostre. No obstant, en locals comercials, de serveis, oficines i despatxos, l'altura podrà reduir-se fins als 2,5 metres d'alçada. b) 2 metres quadrats de superfície lliure per treballador. c) 10 metres cúbics, no ocupats, per treballador.»

Però, després de parlar-ho amb l'empresa ens han dit que pel tipus de treball que realitzen, en el qual utilitzen una gran quantitat de papers i documents, no consideren viable establir aquesta xifra de 2 metres quadrats com a referència i creuen que com a mínim es necessitarien 3 metres quadrats per a poder treballar correctament. De manera que finalment hem considerat aquesta xifra de 3 metres quadrats per treballador per a totes aquelles zones susceptibles de convertir-se en espais de treball, es a dir, ho aplicarem als despatxos i a la sala de treball però també ho farem en la sala de reunions i a la planta baixa ja que encara que en l'actualitat no hi haja gent treballant de manera fixa en un futur podria canviar la distribució i posar-s'hi taules de treball.

Per a la sala d'espera entenem que és més fiable l'estimació que ens donen des de l'empresa, els quals ens diuen que no recorden cap moment en el que s'hagen ocupat simultàniament els cinc seients destinats a aquest fi.



**Figura 2.1:** Plànol entresòl 1.

El encaminador d'aquest entresòl es situaria en la sala anomenada "trastero" de manera que estaria prou centrada respecte els llocs de treball. Hi ha una xicoteta errada en la llegenda del plànol ja que la superfície indicada per a la sala de reunions i la zona de treball estan intercanviades.





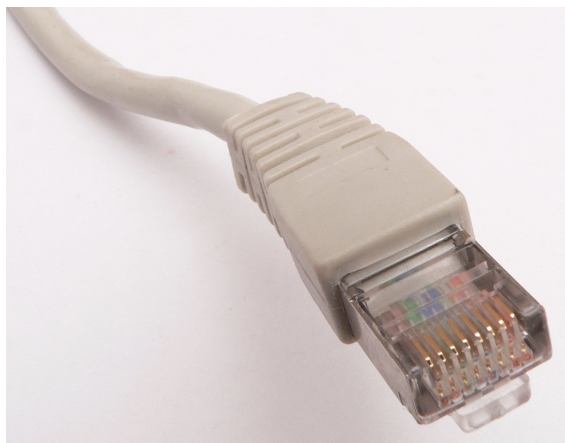
**Figura 2.2:** Plànol entresòl 2.

Destaquem la sala de reunions que haurà de admetre la connexió de molts ordinadors de manera segura ja que es poden connectar tant ordinadors de l'empresa com de clients.



**Figura 2.3:** Plànol planta baixa.

Té uns 100 metres quadrats de superfície i actualment esta arrendada però un creixement de l'empresa plantejaria incloure-la de manera activa en la activitat de l'assessoria.



**Figura 2.4:** Imatge d'un connector RJ-45 mascle, el qual conté vuit pins. Aquestes connexions son molt populars per a connexions de xarxa Ethernet i gairebé qualsevol ordinador compta amb almenys un port RJ-45.

Per a veure-ho de manera més clara mostrarem el càlcul realitzat per al despatx 1. Com que té 24,68 metres quadrats i com a màxim podria treballar 1 empleat per cada 3 metres quadrats, hem establert l'ocupació màxima en 8 persones.

Estància	Metres quadrats	Ocupació màxima
Sala d'espera	15,38	5
Despatx 1	24,68	8
Despatx 2	28,77	9
Despatx 3	21,53	7
Sala de reunions de l'entresòl 1	15,16	5
Zona d'oficina	60,39	25
Arxiu de l'entresòl 1	19,37	6
Traster	3,53	1
Cafeteria	8,29	5
Sala de reunions de l'entresòl 2	51,21	17
Arxiu de l'entresòl 2	13,33	3
Planta baixa	108,81	30

**Taula 2.1:** Taula ocupació màxima d'espais.

Prenent com a referència el nombre de 3 persones per metre quadrat en els llocs susceptibles de ser utilitzats com a llocs de treball i una estimació contrastada amb l'empresa de l'ocupació màxima puntual en les zones que no son de treball. Les superfícies de cada zona han sigut extretes a partir dels plànols.

A partir d'aquesta Taula 2.1 hem elaborat la Taula 2.2 de connexions que haurà de tindre cada estància, considerant que hi ha estàncies que no son de treball i per tant no requeriran tantes connexions com l'ocupació màxima que hem assignat. Les connexions es duran a terme mitjançant l'estàndard RJ-45, que és el més emprat per a connectar xarxes de cablejat estructurat, podem observar una imatge d'aquest tipus de connexions en la Figura 2.4.

A la cafeteria hem establert el nombre de connexions en tres, dos es situaran al davant dels dos tamborets que hi ha i una tercera al costat de la cafetera pensat en el IOT i la possibilitat d'incloure algun electrodomèstic intel·ligent.

## 2.6 Sala de telecomunicacions

Després d'analitzar la distribució física de l'empresa s'ha decidit que el millor lloc per a situar els servidors és en una part de l'arxiu del segon entresòl. Actualment està ocupat per prestatgeries plenes de documents però hi ha molts que ja han prescrit i es poden destruir i d'altres que es poden escanejar i guardar en format digital.

Situariem el *rack* o armari en una sala que construiríem al fons del arxiu, fent una paret que separe físicament els dos espais, com se mostra en color roig a la Figura 2.5. La sala tindria una forma una mica irregular, mesurant la paret més curta 2,59 metres i la més llarga 4,06 metres, de manera que compliria les mesures mínimes recomanades per la Generalitat Valenciana en el document "Especificaciones técnicas para instalaciones de centros de la Generalitat Valenciana" [3] que especifica una superfície mínima de 2,2 x 3 metres. A més, ben justet, però també mesura 2,60 metres d'alçada, que és una altra de les recomanacions citades en el anterior document.

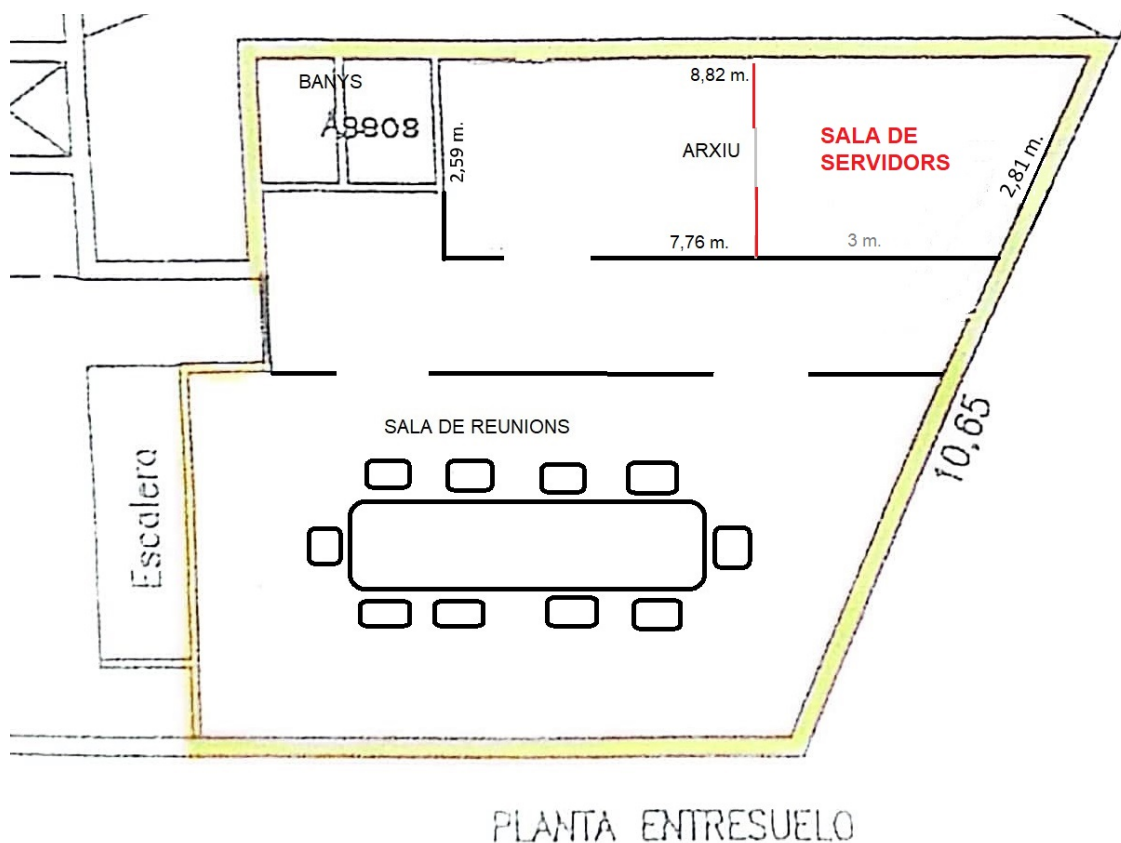
Per a aconseguir que l'armari es trobe segur, les parets i el sostre se pintaran per la part interior amb pintura ignífuga i antiestàtica. La porta també serà de material ignífug i mesurarà 1 metre d'amplada per 2,13 metres d'alçada, tancada amb clau de seguretat i tancant l'habitació el més hermèticament possible per a evitar l'entrada de pols.

D'altra banda, com que l'alçada del sostre és la mínima recomanada per la GVA, en lloc d'instal·lar-hi sòl tècnic, s'opta per conduir els cables a través de reixetes situades en el sostre. La refrigeració se durà a terme mitjançant un aparell d'aire condicionat que, per mitjà d'una sèrie de sensors s'encarregarà de mantindre la sala a una temperatura constant d'entre 20 i 25 graus centígrads durant tot el dia. Hem de tindre en compte que la sala se situa en un entresòl i que al damunt hi viu gent, de manera que a l'hora d'escollir la refrigeració hem de posar l'accent en la sonoritat de l'aparell. L'ordenança municipal de Vila-real, en allò relatiu al nivell de soroll màxim que se pot emetre sols diu: «no han de transcendir a la via pública ni a la comunitat veïnal» [10], però no especifica un nombre límit de decibels. Altres ciutats que si ho fan solen especificar-lo entre els 25 db i 35 db depenent de quina estància de l'habitatge veïnal siga l'afectada. Si verem que el servidor i el sistema de refrigeració emeten un nivell de soroll massa elevat, aïllariem sonorament la sala.

Estància	Connexions necessàries
Sala d'espera	1
Despatx 1	8
Despatx 2	9
Despatx 3	7
Sala de reunions de l'entresòl 1	5
Zona d'oficina	25
Arxiu de l'entresòl 1	6
Traster	1
Cafeteria	3
Sala de reunions de l'entresòl 2	17
Arxiu de l'entresòl 2	1
Planta baixa	30

**Taula 2.2:** Taula de connexions necessàries

Ha estat extreta a partir de la taula d'ocupació màxima tenint en compte les necessitats.



**Figura 2.5:** Plànol entresòl 2 amb la sala de servidors  
Podem distingir en color roig la sala de servidors amb la entrada de color gris.

## 2.7 Topologia utilitzada

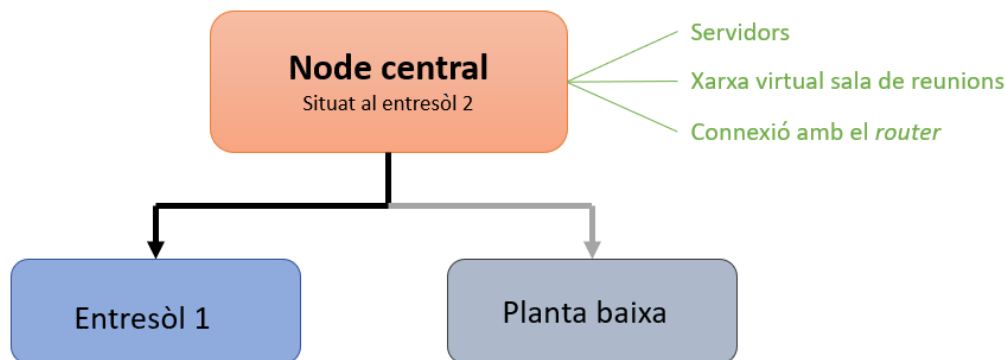
La topologia fa referència al tipus de connexió existent entre els nodes d'una xarxa. En aquest cas tindrem un node central al qual se connecten la resta de nodes, és l'anomenada "xarxa en estrella" o topologia en forma d'estel.

Dintre d'aquesta topologia trobem el *Main Distribution Frame* (MDF) o instal·lació de distribució principal, que és l'armari en el qual se situen els equips de comunicacions principals del centre com ara servidors, tallafocs, encaminador, SAI principal, commutador principal i el panel de connexions on es connectaran els diferents IDF.

D'altra banda, i com hem introduït en el paràgraf anterior, també trobem els *Intermediate Distribution Frame* (IDF) o instal·lacions de distribució intermèdia, que fa referència als *racks* secundaris que s'instal·laran en cada un dels edificis, en aquest cas correspondria un al entresòl 1 i la possibilitat de connectar un altre per a la planta baixa ja que com es tracta d'una instal·lació reduïda, per a estalviar costos, el mateix MDF donarà servei a l'entresòl 2.

El *switch* IDF de l'entresòl 1 se situarà en la sala anomenada com "traster" en el plànol. En l'actualitat s'utilitza com a magatzem de material d'oficina i en ell també es troba el sistema de música però encara queda lloc per a posar-hi el commutador en un armari xicotet. D'altra banda, el *switch* de l'entresòl 2, que a banda també farà la funció de MDF, se situarà en la mateixa sala de servidors, dintre de l'armari.

Un dels punts forts d'escollir esta topologia és la facilitat de dimensionament de la xarxa que ofereix. D'altra banda té l'inconvenient de que una fallada en el node central inhabilita la xarxa completa, però com que en el node central trobarem els servidors i es



**Figura 2.6:** Topologia de la xarxa en forma d'estel.

Veiem un node central del qual ixen les connexions als encaminadors de cada edifici de treball. Veiem que la planta baixa apareix en color gris ja que aquest node no s'implementarà en un primer moment però en el document sí que es contempla la seua incorporació en un futur.

treballarà amb clients lleugers, una fallada en el node central seria igualment crítica per la infraestructura.

Un cop escollida i descrita la topologia a utilitzar, podem observar l'esquema final en la Figura 2.6.

## 2.8 Cablejat estructurat

Se coneix com cablejat estructurat el sistema de cables, connectors, canalitzacions i dispositius que permeten establir una infraestructura de telecomunicacions.

En aquest projecte podem distingir 4 àrees físiques de cablejat: d'una banda l'àrea de treball, d'altra el cablejat horitzontal o de distribució, el cablejat vertical o *backbone* i finalment la sala de telecomunicacions.

### 2.8.1. Àrea de treball

El cablejat de l'àrea de treball és el que uneix els ordinadors dels treballadors amb les rosetes situades a la paret. Per a dur a terme aquesta funció s'empraria cablejat de coure UTP amb connectors RJ-45, com és habitual en aquest tipus de connexions i baix l'estàndard T568B. S'empraran uns amb categoria 6 ja que aquestos ens asseguruen evitar l'efecte conegut com *crosstalk* i el soroll, i ofereixen una velocitat de fins a 1 Gbps. En aquest cas no podran superar una longitud màxima de 3 metres.

El *crosstalk* o diafonia es dona quan una part dels senyals presents en un circuit apareix en un altre, generalment degut a acoblaments magnètics. Per altra banda, quan parlem de soroll en telecomunicacions en referim a perturbacions de la senyal produïdes per múltiples causes que empobreixen la qualitat d'aquesta.

Per a la instal·lació tindriem en compte el nombre màxim de connexions per cada estància que hem indicat abans en la Taula 2.2.



**Figura 2.7:** Imatge d'una rosseta RJ-45 amb dos eixides. Aquestes seran les rossetes que s'instal·laran en l'àrea de treball i a les quals es connectaran els ordinadors de l'oficina.

### 2.8.2. Cablejat horitzontal

Per cablejat horitzontal ens referim a l'estructura que uneix els *switches* dels entresòls amb les rossetes situades en les àrees de treball.

Per a fer-ho també emprarem cablejat UTP de categoria 6 com a mínim, amb connectors RJ-45 baix l'estàndard T568B. Una de les limitacions d'aquest cablejat és la longitud màxima, que se situa en els 90 metres però en el nostre cas no suposa cap problema ja que l'entresòl més gran mesura 20 metres x 12 metres, de manera que encara que redirigim el cablejat en regletes per les parets en cap cas superarem els 90 metres de longitud que pot assolir aquest tipus de cablejat.

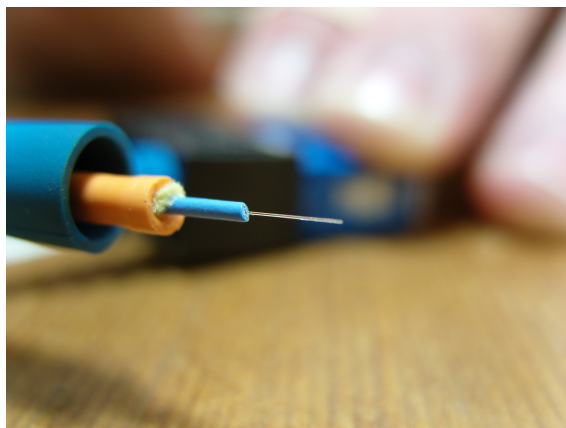
En canvi, sí que podríem tindre problemes amb la longitud mínima ja que per a evitar els efectes de l'energia reflectida s'estableix en 15 metres. El que podem fer en aquest cas és afegir cablejat extra fins arribar a aquesta xifra. El fenomen de l'energia reflectida se dona quan la senyal enviada per un canal, en aquest cas un cable, rebota i torna cap a l'emissor.

### 2.8.3. Cablejat vertical

El cablejat vertical és l'encarregat d'unir el commutador principal amb els commutadors secundaris situats en cada entresòl. Se tracta d'unes connexions que hauran de tindre una elevada amplada de banda, és per això que tenim dos opcions, bé realitzem estes connexions amb fibra òptica o les realitzem per mitjà de múltiples connexions amb cables UTP, el que se coneix com un *Etherchannel*. La connexió mitjançant fibra ens permet unes longituds majors però com que l'espai on se situarà la infraestructura no és massa gran tampoc tindrem cap problema amb la limitació de longitud.

Finalment, per qüestions d'estalvi econòmic hem decidit optar per posar un *Etherchannel*, ja que l'ús d'una o altra modalitat té influència en altres elements com els commutadors.





**Figura 2.8:** Imatge de com és la fibra òptica multimode.

Observem les diferents capes que componen el cablejat i l'aïllen de possibles distorsions.

Autor: De Hhedeshian - Trabajo propio, CC BY 3.0,

<https://commons.wikimedia.org/w/index.php?curid=4328378>

#### 2.8.4. Sala de telecomunicacions

Ja havíem dit que la sala de telecomunicacions se situarà dins de l'arxiu del segon entre-sòl, formant un recinte de 9,14 metres quadrats, però a continuació especificarem quins elements trobarem dintre d'aquest recinte.

D'una banda trobarem el *rack* que és l'armari d'unes mesures estàndards on es posen servidors, *switch* i resta d'aparells de forma senzilla i organitzada. La seua unitat de mesura d'alçada es la U, que equival a 1,75 polzades o 4,445 centímetres; en canvi la seua amplada és de 60 centímetres i la seua profunditat pot variar entre 60 i 120 centímetres.

D'altra banda, dintre de l'armari trobarem per un costat els servidors de l'empresa, i per altre l'encaminador corresponent a l'entresòl 2. A més, també instal·larem un SAI, que s'encarregaria de proporcionar electricitat a l'armari en cas de caiguda de la xarxa elèctrica per tal de guardar les tasques en curs i no perdre informació.

## 2.9 Enllaços redundants

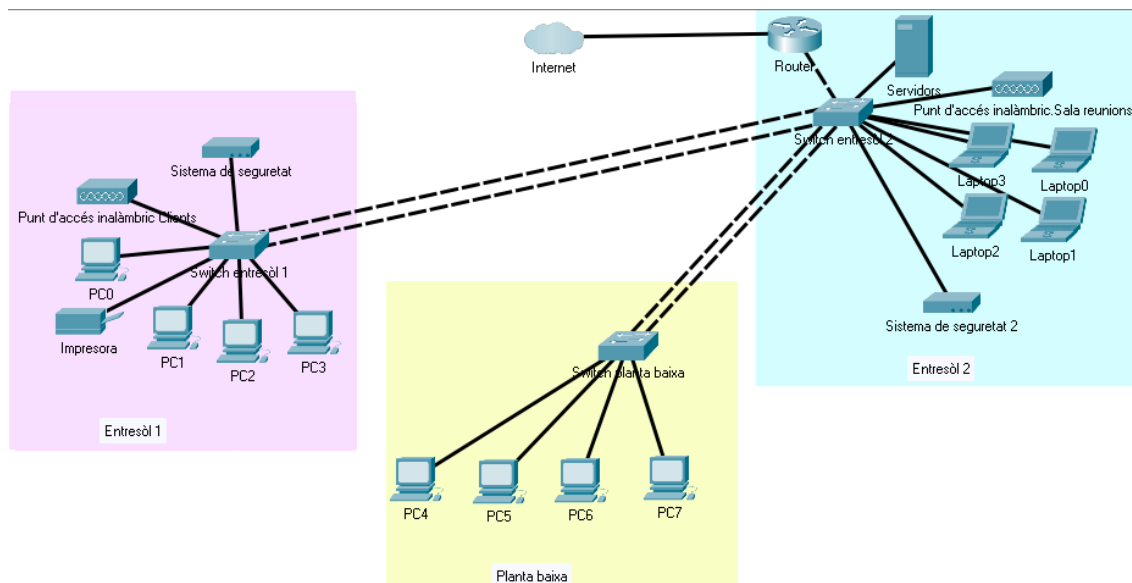
---

Els *switches* IDF estan connectats amb el commutador principal per un *Etherchannel* la qual cosa suposa que la connexió discorre per més d'un cable de manera que, en cas d'haver un problema en algun, no s'interrompia la connexió sinó que disminuiria l'amplada de banda.

En cas d'incorporar la planta baixa a la infraestructura, amb el seu corresponent *switch*, també podem afegir una connexió entre els dos commutadors secundaris de manera que en cas de caiguda del *Etherchannel* la informació seguiria tenint un camí per arribar al MDF. Per a poder dur a terme aquesta idea s'implementarà l'*Spanning Tree Protocol*, el qual evitarà l'aparició de bucles desactivant l'enllaç.

L'*Spanning Tree Protocol* (STP) és un protocol de capa 2 que té com a objectiu evitar l'aparició de bucles, a la vegada que garanteix la presència d'enllaços redundants que entraran en funcionament en cas que un enllaç falle. Per tal d'aconseguir-ho activa i desactiva enllaços de connexió de manera que sempre existeix un únic camí que poden prendre les trames i aquest canvia depenent del estat dels enllaços.





**Figura 2.9:** Esquema de la distribució física de la xarxa.

Observem con el *switch* del entresòl 2 té una funció mixta ja que treballa com a MDF per a donar servei al entresòl 1 i a la planta baixa, però al mateix temps actua com a IDF per a la xarxa del entresòl 2.

## 2.10 Mapa físic de la xarxa

En la Figura 2.9 podem observar un esquema de la distribució de la xarxa.

Primer de tot, trobem la distinció dels diferents edificis per colors, en color rosa s'agrupa la sèrie d'elements que correspondran al entresòl 1, en color blau els elements corresponents al entresòl 2 i en color groc els elements que es disposarien en la planta baixa.

El *router* que proporcionarà accés a Internet se situa en el entresòl 2, dintre del *rack* situat a la sala de telecomunicacions. En el mateix armari també hi estan els servidors i el *switch* del entresòl 2. Aquest *switch* té funcions com a MDF, ja que proporciona accés als servidors i connecta l'entresòl 1 i la planta baixa a la xarxa, però també té funcions pròpies d'un IDF perquè la xarxa del entresòl 2 està directament associada a aquest dispositiu. D'aquesta manera podem abaratir el cost de la infraestructura.

L'entresòl 1 se connecta a la xarxa mitjançant un *Etherchannel* entre el *switch* del entresòl 2 i el del entresòl 1, d'aquesta forma obtenim una major amplada de banda i en cas de produir-se una avaria en una de les connexions no se perdria la connexió amb el MDF. A aquest *switch* del entresòl 1 se connectaran la resta de dispositius com els ordinadors de treball, la impressora i el sistema de seguretat. El *switch* del entresòl 1 se situarà en el traster, dintre d'un armari xicotet.

Finalment, també trobem representat les connexions de la planta baixa encara que, per ara, no se duran a terme ja que no se necessita aquest espai i actualment està llogat. L'estructura seria similar a la del entresòl 1, amb un *Etherchannel* que unisca el *switch* del entresòl 2 i el de la planta baixa per a tindre una major amplada de banda i millorar la fiabilitat. La resta de dispositius de la planta baixa estarien connectats al *switch* situat en aquest edifici.



# Disseny lògic de la xarxa

---

En aquest capítol comentarem la estructura lògica de la xarxa. Presentarem les divisions en les diferents VLAN, les seues adreces IP i mostrarem un mapa de com queda dividida la xarxa des del punt de vista lògic.

Per disseny lògic entenem com se comuniquen els dispositius en la xarxa, amb independència del disseny físic d'aquesta. Per a facilitar el disseny la xarxa es dividirà en VLANs la qual cosa en suposarà una sèrie de avantatges que veurem a continuació.

### 3.1 Disseny de VLAN

---

Una VLAN (*Virtual Local Area Network* o xarxa d'àrea local virtual) és un mètode aplicat en la capa d'enllaç per a crear xarxes lògicament independents d'una mateixa xarxa física, que pot comprendre diferents segments de la xarxa. Cada VLAN funciona com una LAN (xarxa d'àrea local) individual i diverses VLAN poden coexistir en un o diversos *switches*.

Els beneficis d'implementar VLANs són diversos, entre els més destacats trobem:

- Reducció de la latència i càrrega del tràfic de la xarxa i els dispositius, estalviant recursos i millorant l'eficàcia del sistema. Ja que se limita el tràfic de *broadcast* i *multicast*.
- Major seguretat. Els dispositius vinculats a una xarxa virtual no tenen accés directe a dispositius d'altres xarxes, la qual cosa reforça la confidencialitat.
- Més facilitat per a expandir la xarxa.

Després d'analitzar l'estructura i les necessitats de l'empresa s'ha decidit dividir la xarxa en 5 xarxes virtuals que es mostren en la Taula 3.1.

VLAN	Nom
2	Xarxa de treball
3	Clients
4	Sala de reunions
5	Servidors
6	Seguretat

**Taula 3.1:** Taula on es mostren les VLANs en les que es dividirà la xarxa.

La VLAN 2 serà a la qual es connectaran els ordinadors de treball de l'empresa. És a dir, tots els treballadors tindran el seu ordinador de taula en esta xarxa.

La VLAN 3 està destinada a la connexió dels dispositius personals dels clients amb la finalitat de poder oferir un servei de connexió a Internet quan, per exemple, estan esperant a ser atesos. També serà a la qual podran connectar-se els dispositius personals dels treballadors, com ara telèfons mòbils, si desitgen tindre un accés a Internet sense utilitzar les dades mòbils.

La VLAN 4 està destinada a la connexió dels ordinadors en la sala de reunions. Hem de tindre en compte que a aquesta àrea poden connectar-se ordinadors de la empresa però també d'altres empreses i per aquest motiu se separa en una xarxa diferent a la del àrea de treball.

La VLAN 5 serà a la qual se connecten els servidors de l'empresa. S'ha optat per aquesta solució per a millorar la seguretat de la xarxa, ja que qualsevol connexió amb els servidors haurà de passar primer per l'encaminador.

L'empresa té un sistema de seguretat que inclou càmeres de seguretat i el qual utilitza la connexió a la xarxa per a retransmetre les imatges. No ens haurem d'encarregar de la gestió i l'emmagatzemament de la informació perquè és el propi proveïdor de l'alarma el que ho fa però sí que destinarem la VLAN 6 per a la retransmissió de les dades d'una manera més segura.

De forma predeterminada la VLAN nativa (VLAN 1) serà des de la qual l'administrador de la xarxa podrà configurar els encaminadors de manera remota. A més, s'emprarà per a intercanviar el tràfic del protocol d'enllaç troncal (VTP) amb altres dispositius de la xarxa.

Les visualitzacions entre les VLANs quedaran de la forma que s'indica en la Taula 3.2:

	VLAN 2	VLAN 3	VLAN 4	VLAN 5	VLAN 6	Router
VLAN 2	No	No	No	No	No	Sí
VLAN 3	No	No	No	No	No	Sí
VLAN 4	No	No	No	No	No	Sí
VLAN 5	No	No	No	No	No	Sí
VLAN 6	No	No	No	No	No	Sí

**Taula 3.2:** Taula on es mostren la visualització que hi haurà entre les diferents VLANs. Com veiem les diferents VLANs sols tenen visibilitat amb el *router* de manera que per a comunicar-se entre les diferents VLANS haurà de ser mitjançant aquest dispositiu.

Emprarem el protocol 802.1Q per a etiquetar les VLANs, de manera que les diferents xarxes virtuals se podran comunicar utilitzant un *switch* de capa 3 sense problemes d'interferències (l'anomenat *trunking*, que fa referència a quan per un enllaç transcorren més d'una VLAN identificades per etiquetes).

Les diferents xarxes virtuals se crearan assignant de manera manual (estàtica) els ports de commutador a les diferents VLANs. És una forma senzilla però té l'inconvenient que en cas de canviar el port de connexió d'entrada al commutador, s'ha de configurar manualment la connexió.

## 3.2 Adreçament

### 3.2.1. Rang d'adreces IP

L'adreçament de l'empresa es durà a terme mitjançant direccions privades, la qual cosa ens aporta una sèrie d'avantatges com ara:

- Que un nombre elevat d'usuaris tinguin accés a Internet des d'un nombre de direccions públiques molt reduït, disminuint el cost associat a la compra d'aquestes adreces.
- Proporciona major seguretat ja que els dispositius configurats amb adreces internes no són visibles per a usuaris d'altres xarxes locals o externes.

Cada VLAN se configurarà com una subxarxa diferent de tipus C. Els rangs d'adreces IP que se configuraran en els dispositius de la xarxa de l'empresa son els que es mostren a la Taula 3.3.

VLAN 2 - Xarxa de treball	192.168.1.0
VLAN 3 - Clients	192.168.32.0
VLAN 4 - Sala de reunions	192.168.64.0
VLAN 5 - Servidors	192.168.96.0
VLAN 6 - Seguretat	192.168.128.0

**Taula 3.3:** Rangs d'IPs per a cada VLAN

Les portes d'enllaç o *Gateway* de cada VLAN son:

- VLAN 2: 192.168.1.254
- VLAN 3: 192.168.32.254
- VLAN 4: 192.168.64.254
- VLAN 5: 192.168.96.254
- VLAN 6: 192.168.128.254

La màscara de subxarxa que se configurarà en totes les VLANs serà la 255.255.255.0 i el *router* que donarà connexió a Internet tindrà la seua interfície dividida en diverses subinterfícies lògiques, una per cada VLAN.

L'electrònica principal se dividirà en dos commutadors, un situat a l'armari de la sala de servidors i l'altre ubicat en l'armari de l'entresòl. Del primer commutador eixiran connexions a les VLANs servidors, sala de reunions i seguretat; mentre que del segon eixiran connexions a les VLANs xarxa de treball, clients i seguretat.

### 3.2.2. Implementació NAT

L'electrònica i equips de l'empresa se configuraran en rangs d'IPs privades, amb la qual cosa s'ha d'habilitar en l'encaminador la traducció de direccions de xarxa (NAT) per a permetre que les xarxes privades s'encaminin a través d'Internet.

Els principals avantatges que proporciona l'ús de NAT són:

- Direccions IP reutilitzables.
- Diversos equips d'una xarxa poden compartir una direcció IP única.
- Funciona de manera transparent i protegirà els usuaris de la xarxa privada de l'empresa de l'accés des de el domini públic.
- Impedeix a usuaris externs a la xarxa de l'empresa accedir a equips del negoci.

No tot són avantatges, també hem de tindre en compte alguns inconvenients que pot suposar el seu ús:

- Si se vol permetre l'accés a un usuari extern se requerirà de configuracions addicionals.
- El fet d'haver de traduir les adreces suposa una major càrrega per el *router*.

Implementarem la NAT dinàmica, de manera que el *router* tindrà una llista amb les adreces públiques i les assignarà als dispositius interns quan aquestos requereixen d'accés a Internet.

### 3.2.3. Dispositius amb adreces fixes

Hi ha diversos elements que estaran configurats amb una adreça IP interna fixa, és el cas dels ordinadors de treball, servidors, impressora, càmeres de seguretat i commutadors.

Emprarem un servidor proxy-cache per a augmentar la seguretat a la vegada que se reduirà el temps de resposta. L'assignarem a la VLAN 3, que com hem dit abans serà l'assignada per als servidors. La seua adreça IP serà 192.168.96.3. Per la seua part, el servidor de virtualització d'equips se situarà en la IP 192.168.96.4 i el de correu en la IP 192.168.3.5.

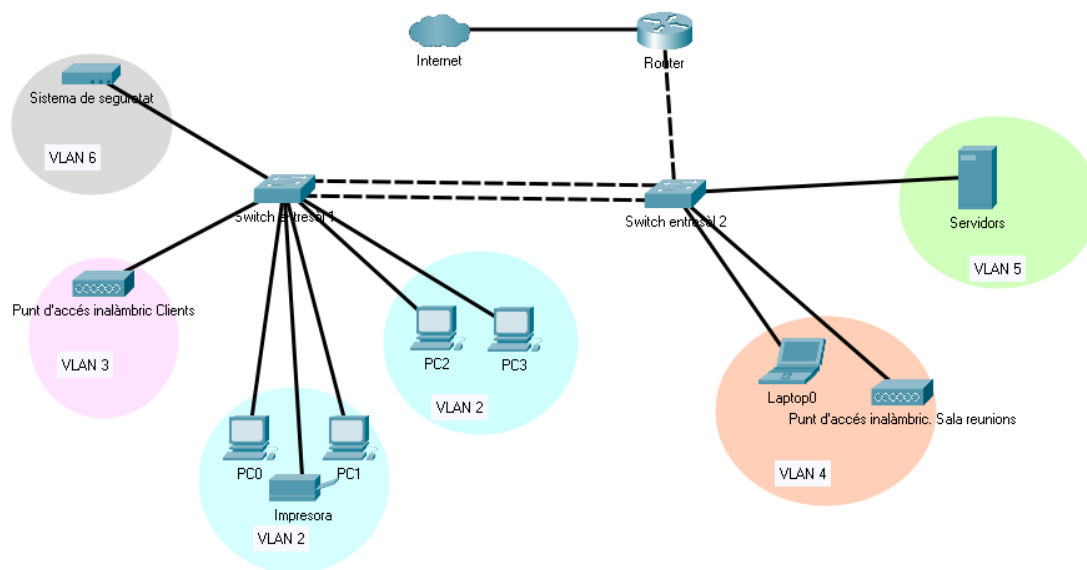
Hem de tindre en compte l'existència d'una impressora de grans dimensions situada a l'entresòl 1 que dona servei a tota la zona de treball, la qual estarà connectada a la VLAN 2 amb l'adreça fixa 192.168.1.3.

Els ordinadors de treball (clients lleugers) se reparteixen en 4 zones diferents, aquesta és la seua distribució i les adreces IPs que tindran assignades:

- Despatx 1: 1 ordinador
  - IP: 192.168.1.4
- Despatx 2: 1 ordinador
  - IP: 192.168.1.5
- Despatx 3: 2 ordinadors
  - IP: 192.168.1.6
  - IP: 192.168.1.7
- Sala treball / zona oficina: 5 ordinadors
  - IP: 192.168.1.8
  - IP: 192.168.1.9
  - IP: 192.168.1.10
  - IP: 192.168.1.11
  - IP: 192.168.1.12

Hi haurà 3 càmeres de seguretat, dos a l'entresòl 1 i una a l'entresòl 2, configurades en la VLAN 6 amb les adreces IP 192.168.128.2, 192.168.128.3 i 192.168.128.4.

Quant a les connexions sense fil, tant la de la xarxa de clients com la de la xarxa de la sala de reunions, se configuraran les IPs mitjançant un servidor DHCP amb un *pool*



**Figura 3.1:** Distribució lògica de la xarxa amb les divisions per VLANs.

Els dos *switches* encara que en el dibuix apareixen de manera separada actuaran com un únic dispositiu.

d'adreces que comprendrà, en el cas de la xarxa de clients, des de l'adreça 192.168.32.1 fins la 192.168.32.253. En el cas de la xarxa de la sala de reunions com tindrem rossetes i connexió sense fil, el *pool* d'adreces disponibles per al servidor DHCP comprendrà des de la direcció 192.168.64.1 fins la 192.168.64.253.

### 3.3 Mapa lògic de la xarxa

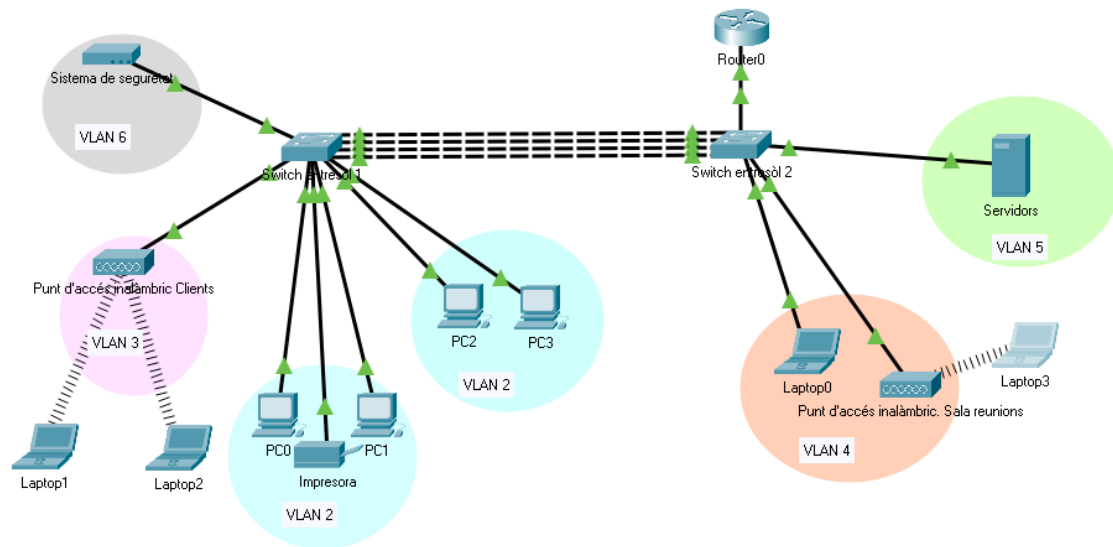
Finalment, en la Figura 3.1 observem un esquema lògic de la xarxa amb la separació per VLANs descrita en els apartats anteriors.

### 3.4 Validació de la configuració amb Packet Tracer

Per acabar amb el disseny lògic comprovarem la configuració escollida amb el programa de Cisco Packet Tracer per a la qual cosa configurarem els dispositius i realitzarem simulacions.

#### 3.4.1. Cisco Packet Tracer

Cisco Packet Tracer és un programa desenvolupat per l'empresa Cisco Systems que permet dissenyar, configurar i simular xarxes mitjançant equips virtuals i connexions simulades. Aquest programa va sorgir com una ferramenta destinada a l'ensenyança per a poder practicar sense haver de costejar els commutadors i encaminadors que tenen un preu elevat. És per això que no estan tots els models de dispositius de Cisco i algunes funcionalitats que podem esperar en dispositius punters no podem configurar-les.



**Figura 3.2:** Imatge de la xarxa que simularem.  
Hem simplificat el nombre de dispositius en cada VLAN.

### 3.4.2. Peculiaritats de la simulació

Com apuntàvem, al programa sols estan disponibles alguns dispositius de la marca, de manera que a continuació indicarem quins hem seleccionat per a fer la nostra simulació i altres mesures que hem hagut de prendre per a poder implementar la infraestructura en el programa.

- Hem reduït el nombre d'ordinadors en les VLANs.
- No hem implantat el tallafocs.
- Per als dos commutadors hem escollit el model Catalyst 2960 de capa 2, ja que les funcions de capa 3 són limitades.
- L'encaminador que s'utilitza és el model Cisco 2811.
- Per als portàtils hem afegit el mòdul de connexió sense fil.
- Els punts d'accés són el model PT-AP.
- L'encaminador serà qui s'encarregarà de canviar els missatges d'una VLAN a una altra.

Amb tot açò, l'esquema de la infraestructura que configurarem és el que observem a la Figura 3.2.

### 3.4.3. Configuració dels dispositius

#### Commutadors

Primer que tot cal definir les VLANs als dos *switches*, per fer-ho escriurem les següents instruccions al CLI de cada *switch*:



```
Switch#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
2 xarxa_treball	active	Fa0/1, Fa0/2, Fa0/5, Fa0/6 Fa0/7
3 clients	active	Fa0/3, Fa0/4
4 sala_de_reunions	active	
5 servidors	active	
6 seguretat	active	Fa0/8
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

**Figura 3.3:** Configuració del *switch 1*.

Aquest és el resultat de l'ordre *show vlan brief* en el commutador 1.

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 2
Switch(config-vlan)# name xarxa_treball
Switch(config-vlan)# vlan 3
Switch(config-vlan)# name clients
Switch(config-vlan)# vlan 4
Switch(config-vlan)# name sala_de_reunions
Switch(config-vlan)# vlan 5
Switch(config-vlan)# name servidors
Switch(config-vlan)# vlan 6
Switch(config-vlan)# name seguretat
```

Un cop definides les VLANs, cal assignar cada port del commutador a la VLAN corresponent. A continuació, a mode d'exemple se mostra com s'ha assignat el port fastEthernet 0/8 del *switch 1* a la VLAN 6 (seguretat).

```
Switch# configure terminal
Switch(config)# interface fastEthernet 0/8
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 6
Switch(config-if-range)# exit
```

Per a comprovar que s'ha configurat tot correctament podem executar l'ordre:

```
Switch# show vlan brief
```

que com podem veure a la Figura 3.3 ens mostrarà un llistat de les VLANs existents en el commutador així com el llistat dels ports i a quina VLAN està assignat cada un.

Per a millorar la seguretat, s'ha de desactivar els ports que no s'utilitzen, per exemple per al *switch 1* desactivarem els ports fastEthernet del 13 al 24:

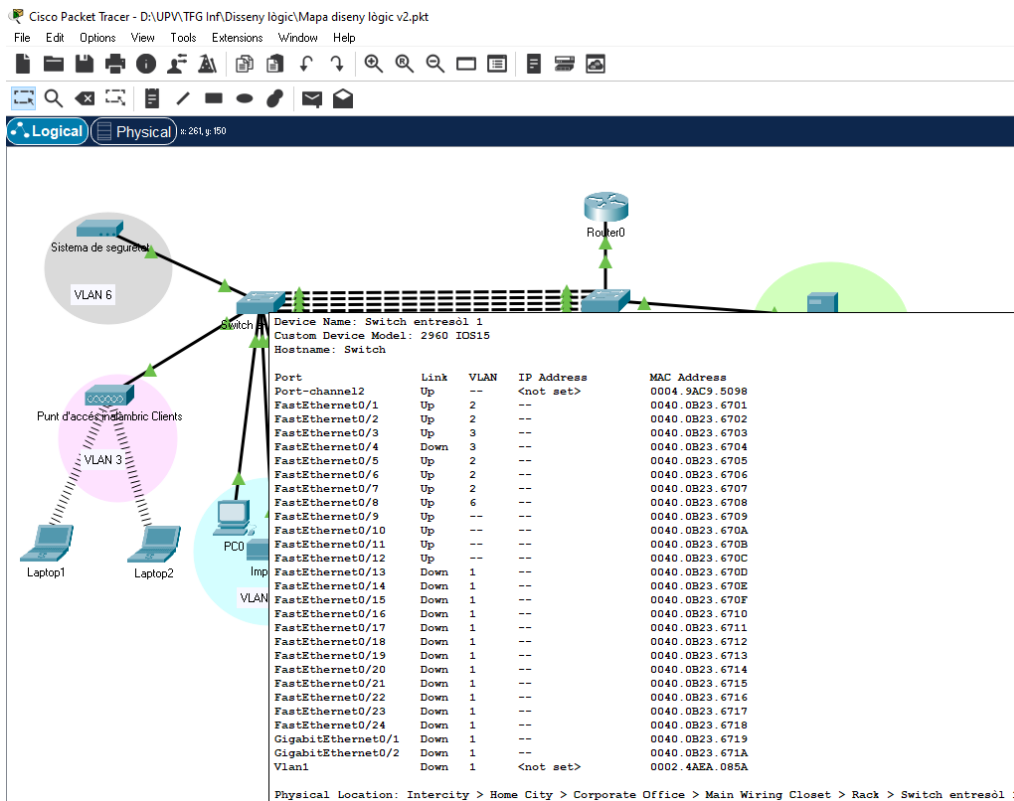


Figura 3.4: Ports disponibles al commutador 1.

```
Switch# configure terminal
Switch(config)# interface range FastEthernet 0/13-24
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address
sticky
Switch(config-if)# switchport port-security violation
restrict
```

La connexió entre els dos commutadors se farà mitjançant un *Etherchannel* de manera que tenim més amplada de banda i més fiabilitat. Per configurar-lo hem d'introduir aquestes instruccions:

```
Switch# configure terminal
Switch(config)# interface range FastEthernet 0/9-12
Switch(config-if-range)# channel-group 2 mode on
Switch(config-if)# exit
```

Amb este codi hem assignat els ports fa0/9, fa0/10, fa0/11 i fa0/12 al port-channel 2. Haurem de repetir el procés en el CLI del commutador 2 per que el canal quede configurat, indicant els ports del *switch 1*. Observem que l'*Etherchannel* s'ha creat correctament perquè al situar el cursor damunt del commutador ens apareix, a part dels ports físics que té, un altre anomenat *port-channel2* com es veu a la Figura 3.4.

Finalment, establim algunes connexions en mode *trunk* per a permetre que per un mateix enllaç físic pugui transcórrer tràfic de diferents VLANs. Serà el cas de les conne-

```
Switch#show interfaces trunk
Port      Mode          Encapsulation  Status        Native vlan
Po2       on            802.1q         trunking      1

Port      Vlans allowed on trunk
Po2       2-6

Port      Vlans allowed and active in management domain
Po2       2,3,4,5,6

Port      Vlans in spanning tree forwarding state and not pruned
Po2       2,3,4,5,6
```

**Figura 3.5:** Resultat d'executar l'ordre *show interface trunk*.

xions que uneixen els dos commutadors i el commutador principal amb l'encaminador. Podem configurar-ho de la següent manera:

```
Switch# configure terminal
Switch(config)# interface Port-channel2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport mode trunk allowed
vlan 2,3,4,5,6
Switch(config-if)# exit
```

També se pot comprovar si s'ha executat correctament l'ordre amb la instrucció:

```
Switch# show interface trunk
```

que ens mostra el resultat de la Figura 3.5.

## Encaminador

Una vegada configurats els commutadors anem a configurar l'encaminador. En aquest cas ens caldrà preparar les funcions de ROAS (*Router on a stick*) per a que el tràfic pugui viatjar entre les diferents VLANs i la funció de DHCP.

Per a configurar el ROAS hem de subdividir la interfície que uneix el encaminador i el commutador en subinterfícies virtuals, una per cada VLAN. Assignarem a cada subinterfície una adreça IP i una màscara de xarxa vàlida per a la VLAN que li correspon i les configurarem per a que treballen amb el protocol d'etiquetat de trames IEEE 802.1Q. Els equips de cada xarxa virtual utilitzaran com a porta d'enllaç l'adreça IP de la subinterfície virtual encarregada del seu encaminament.

```
Router# configure terminal
Router(config)# interface fastEthernet 0/0.2
Router(config-subif)# encapsulation dot1q 2
Router(config-subif)# ip address 192.168.1.254
255.255.255.0
Router(config-subif)# exit
Router(config)# interface fastEthernet 0/0.3
Router(config-subif)# encapsulation dot1q 3
```

```
Router(config-subif)# ip address 192.168.32.254
255.255.255.0
Router(config-subif)# exit
Router(config)# interface fastEthernet 0/0.4
Router(config-subif)# encapsulation dot1q 4
Router(config-subif)# ip address 192.168.64.254
255.255.255.0
Router(config-subif)# exit
Router(config)# interface fastEthernet 0/0.5
Router(config-subif)# encapsulation dot1q 5
Router(config-subif)# ip address 192.168.96.254
255.255.255.0
Router(config-subif)# exit
Router(config)# interface fastEthernet 0/0.6
Router(config-subif)# encapsulation dot1q 6
Router(config-subif)# ip address 192.168.128.254
255.255.255.0
Router(config-subif)# exit
Router(config)# interface fastEthernet 0/0
Router(config-if)# no shutdown
```

El servei de DHCP permet assignar adreces IP dinàmicament. Aquesta funció s'implementarà sols per les VLANs 3 i 4 ja que per a les demés els dispositius connectats seran fixos i no necessitem eixa facilitat de configuració.

Haurem d'executar els següents comandaments en el terminal del *router*:

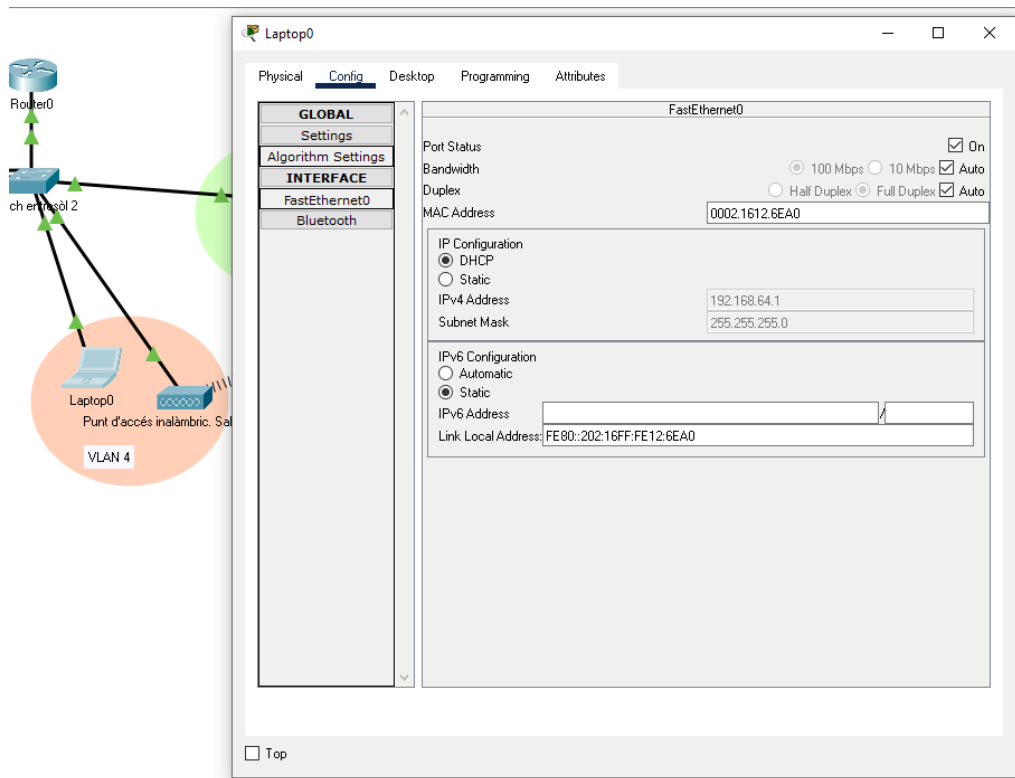
```
Router# configure terminal
Router(config)# ip dhcp pool clients
Router(config-dhcp)# network 192.168.32.0 255.255.255.0
Router(config-dhcp)# default-router 192.168.32.254
Router(config-dhcp)# exit
Router(config)# ip dhcp pool sala_de_reunions
Router(config-dhcp)# network 192.168.64.0 255.255.255.0
Router(config-dhcp)# default-router 192.168.64.254
Router(config-dhcp)# exit
```

## Dispositius finals

Per últim, sols ens queda configurar els dispositius finals: La impressora, els PCs, sistema de seguretat i els portàtils. Les VLANs 2, 5 i 6 no tenen configurat el DHCP de manera que haurem d'assignar les adreces IP que havíem dit a l'apartat 3.2.3 de manera manual; i per als dispositius connectats a les VLANs 3 i 4 la configuració de l'adreça IP es realitzarà de forma automàtica, com veiem en la Figura 3.6.

### 3.4.4. Simulació

Per a comprovar que la infraestructura dissenyada funciona correctament enviarem diversos «pings» entre els dispositius. Primer ho provarem entre els de la mateixa VLAN, després provarem entre diferents VLANs i finalment realitzarem la prova entre diferents VLANs connectades cada una a un commutador.



**Figura 3.6:** Ordinador connectat per DHCP

. Es tracta del portàtil anomenat *Laptop0* en la simulació, connectat a la VLAN 4 mitjançant cable i configurat de manera automàtica per el sistema DHCP.

### Connexió entre la mateixa VLAN

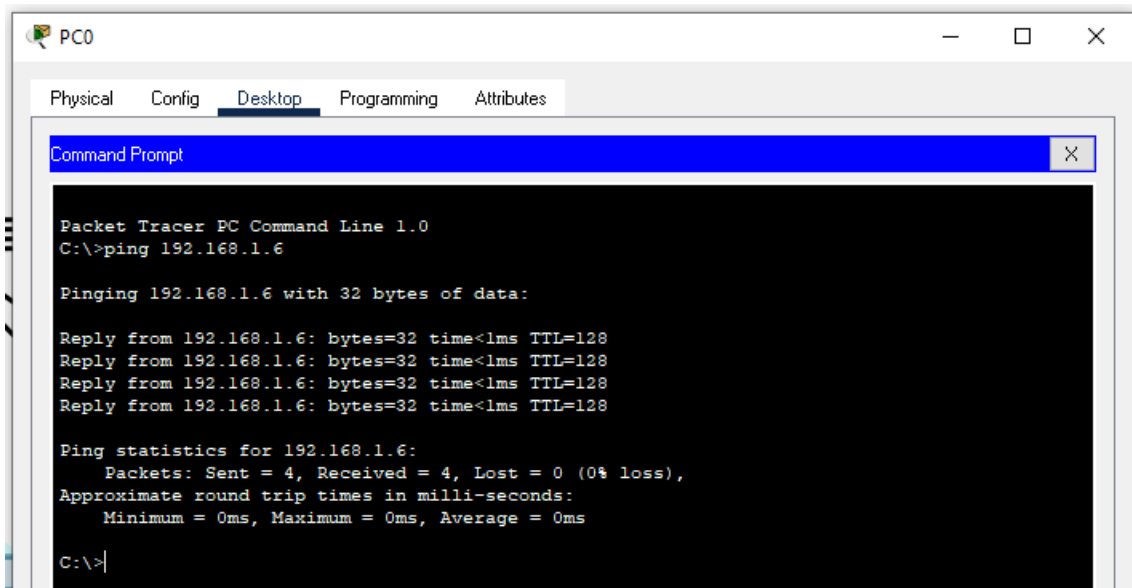
Per a confirmar que els missatges s'envien correctament dintre de la mateixa VLAN enviarem un «PING» entre l'ordinador PC0 (ip: 192.168.1.8) i el PC2 (ip: 192.168.1.6), ambdós situats en la VLAN 2 (xarxa de treball), com se mostra en la Figura 3.7.

### Connexió entre VLANs diferents en el mateix commutador

A continuació comprovarem que hi ha connexió entre elements de diferents VLANs, és a dir si el *router* està funcionant correctament. Ho farem amb un missatge entre el *Laptop3*, configurat en la VLAN 4 i el servidor, configurat en la VLAN 5; com se mostra a la Figura 3.8.

### Connexió entre diferents VLANs passant per el *Etherchannel*

Per últim, queda comprovar si el *Etherchannel* ha estat configurat correctament, de manera que enviarem un missatge entre un ordinador de la VLAN 2, com per exemple el *Laptop1* que té l'adreça IP 192.168.32.2 i el l'ordinador de la VLAN 4 amb l'adreça 192.168.64.2, com se mostra en la Figura 3.9.



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

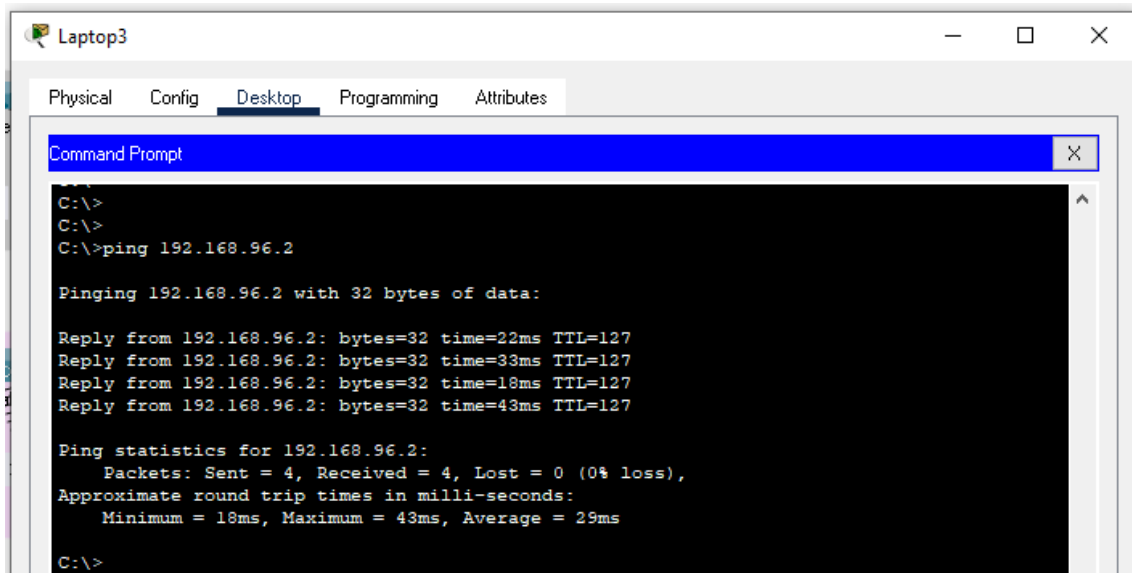
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

**Figura 3.7:** PING entre dos ordinadors de la VLAN 2.

Hem enviat un missatge PING entre l'ordinador amb l'adreça IP 192.168.1.8 i un en l'adreça 192.168.1.6 ambdues configurades manualment i el missatge ha arribat sense cap problema.



```
Laptop3
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>ping 192.168.96.2

Pinging 192.168.96.2 with 32 bytes of data:

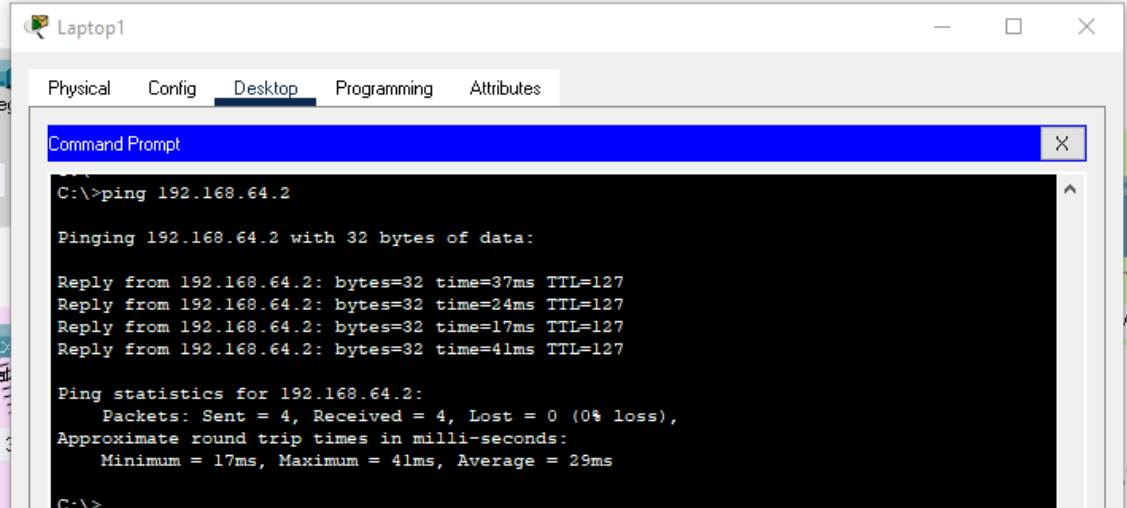
Reply from 192.168.96.2: bytes=32 time=22ms TTL=127
Reply from 192.168.96.2: bytes=32 time=33ms TTL=127
Reply from 192.168.96.2: bytes=32 time=18ms TTL=127
Reply from 192.168.96.2: bytes=32 time=43ms TTL=127

Ping statistics for 192.168.96.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 43ms, Average = 29ms

C:\>
```

**Figura 3.8:** PING entre un dispositiu de la VLAN 4 i un de la VLAN 5

. Hem enviat un missatge PING entre l'ordinador amb l'adreça IP 192.168.64.2 configurada mitjançant DHCP i un servidor en l'adreça 192.168.96.2 configurada manualment i el missatge ha arribat sense cap problema.



The image shows a Packet Tracer interface with a 'Laptop1' window. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the execution of a ping command to the IP address 192.168.64.2. The output indicates that four packets were successfully received with 0% loss, and the round trip times are within acceptable ranges (17ms to 41ms).

```
C:\>ping 192.168.64.2

Pinging 192.168.64.2 with 32 bytes of data:

Reply from 192.168.64.2: bytes=32 time=37ms TTL=127
Reply from 192.168.64.2: bytes=32 time=24ms TTL=127
Reply from 192.168.64.2: bytes=32 time=17ms TTL=127
Reply from 192.168.64.2: bytes=32 time=41ms TTL=127

Ping statistics for 192.168.64.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 17ms, Maximum = 41ms, Average = 29ms

C:\>
```

**Figura 3.9:** PING entre un dispositiu de la VLAN 2 i un de la VLAN 4. El missatge ha travessat el etherchannel i ha arribat sense cap problema.





# Connexió sense fil, servei de veu i servidors

---

La majoria de les connexions de l'empresa seran amb fil ja que se tracta de dispositius amb una ubicació física fixa i el fet de connectar-los mitjançant cablejat augmenta la velocitat i la seguretat de la connexió. Però hi ha casos en els que una connexió sense fil facilita molt el procés de configuració, com és el cas dels dispositius mòbils, ordinadors portàtils i d'altres per als que no hi ha una ubicació fixa prevista. En la primera part d'aquest capítol veurem quines xarxes tindran connexions sense fil, i quina serà la seua configuració.

D'altra banda, per al correcte funcionament del sistema informàtic de l'empresa se necessiten una sèrie de servidors. El fet de necessitar servidors que ens aporten funcionalitats diferents no implica que físicament hi haja d'haver tants equips com servidors, sinó que podem agrupar diferents funcions en una mateixa màquina física. Al final del capítol explicarem quins servidors necessitem, els seus requisits i l'elecció de dispositius que hem fet.

## 4.1 Connexió sense fil

---

### 4.1.1. Estàndard

L'estàndard que se seguirà per al model de connexió sense fil serà el 802.11g, especificat per l'IEEE. Les seues característiques són les següents:

- Alta amplada de banda, amb un rendiment màxim de 54 Mbps.
- El radi d'arribada de la senyal és de 27 metres en ambients tancats i fins a 75 en ambients oberts.
- Un únic punt d'accés pot donar servei fins a 50 usuaris.
- El rang de freqüència és de 2,4 GHz.

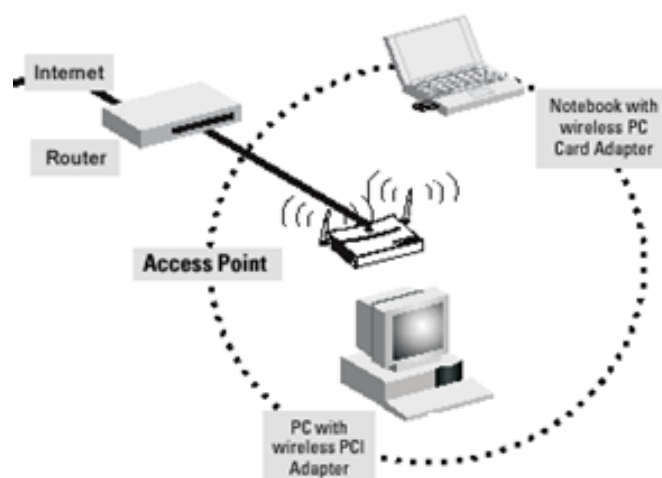
Wi-Fi Alliance és una altra organització encarregada de comprovar els dispositius LAN de diversos fabricants. Si un dispositiu té el logotip Wi-Fi significa que ha superat tots els estàndards i que pot comunicar-se amb altres dispositius amb el mateix estàndard. Podem observar la imatge del logotip Wi-Fi en la Figura 4.1.

La freqüència lliure que compren la banda de 2,4 GHz està subdividida en 14 canals separats per 5 MHz entre ells. Donat que amb 802.11g una antena empra 22 MHz per



**Figura 4.1:** Logotip Wi-Fi.

Aquesta icona s'assigna a un dispositiu una vegada l'organització Wi-Fi Alliance s'ha assegurat que compleix tots els estàndards corresponents i que certifica que és capaç de comunicar-se amb altres aparells amb el mateix estàndard.



**Figura 4.2:** Esquema de la connexió dels dispositius sense fil a la xarxa mitjançant el punt d'accés. El punt d'accés va connectat al encaminador o commutador i cal que els dispositius finals tinguin una targeta de xarxa que suporti aquest tipus de connexions sense fil.

a transmetre dades, els canals adjacents se superposen i s'interfereixen entre sí. És per aquest motiu que per a planificar la xarxa sense fil de l'empresa s'empraran els canals 1, 7 i 13 que no se solapen entre sí i aleshores no provoquen interferències.

Emprarem el mètode d'accés múltiple per detecció de portadora amb prevenció de col·lisions (CSMA/CA) amb el qual se crea una reserva en el canal per a que s'utilitze per una conversació específica. Quan un canal està reservat cap altre dispositiu podrà transmetre per aquest, de tal manera que s'eviten possibles connexions.

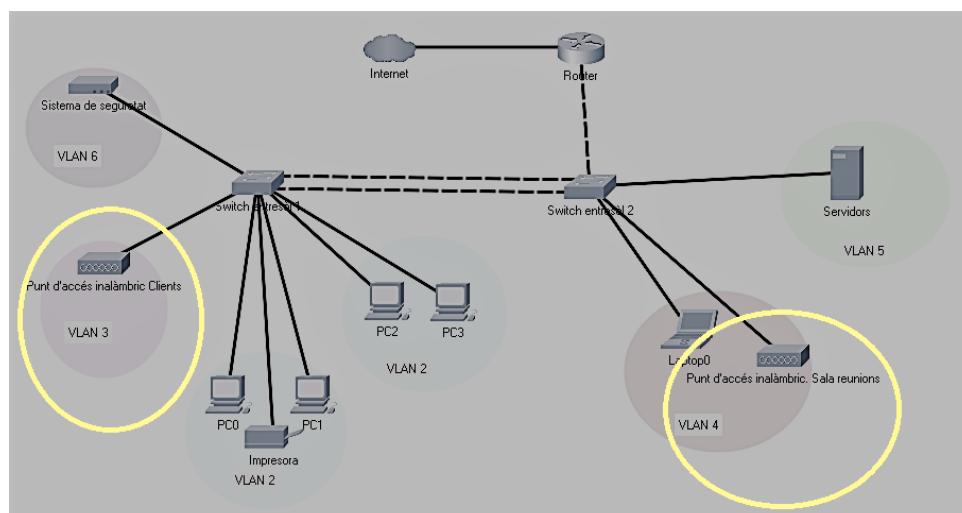
#### 4.1.2. Topologia

La topologia de la xarxa sense fil que s'implementarà és el mode d'infraestructura en la que cada dispositiu deu de comunicar-se amb un punt d'accés per a obtenir un permís que li permeti connectar-se a la xarxa. L'*Acces Point* controla totes les comunicacions i garanteix que tots els equips tinguin igual accés al medi. Veiem un esquema d'esta connexió en la Figura 4.2.

Com que les àrees que ha de cobrir cada xarxa WiFi són relativament menudes, sols ens caldrà un punt d'accés per a cada VLAN amb WiFi, ja que amb una freqüència de 2,4 GHz l'abast de la senyal se situa al voltant dels 45 metres en interiors.



**Figura 4.3:** Imatge de cómo s'instal·laran els punts d'accés al sostre. D'aquesta manera evitem molts dels obstacles que redueixen l'abast de la senyal i a més, tenim més llibertat per a poder situar el dispositiu en el punt que considerem més adequat.



**Figura 4.4:** Xarxes amb connexió WiFi

Instal·larem punts d'accés omnidireccionals, i el punt més òptim per tal d'evitar obstacles que empitjoren la qualitat de la senyal, és el sostre, tal i com s'observa en la Figura 4.3. Haurem de tindre en compte evitar posar-lo en mig de la sala per a evitar que la senyal rebote de manera simètrica en les parets i s'anul·li.

#### 4.1.3. Xarxes sense fil

En la xarxa de la empresa hi han dos xarxes sense fil, Figura 4.4, amb funcions diferenciades que són xarxa clients i sala de reunions.

##### Clients

A la xarxa clients se connectaran els clients que desitgen tindre una connexió a Internet quan estan en la empresa, per exemple, esperant a ser atesos. Però també s'espera que siga emprada per els treballadors per a connectar els seus dispositius personals, com

ara el telèfon mòbil, mentre estan a l'oficina. Ja que actualment hi han unes 10 persones treballant a l'empresa i volem tindre capacitat d'expansió col·locarem un punt d'accés que pugui suportar fins a 30 usuaris. Per l'extensió de la empresa, amb un sol punt d'accés situat a l'entresòl 1, deuria d'haver-hi prou per a donar servei a tota l'oficina, ja que aquesta xarxa, per ara, sols té sentit instal·lar-la a l'entresòl 1.

L'accés a aquesta xarxa haurà de ser prou dinàmic, no se pot atendre individualment cada una de les peticions de connexió, i com que no se connectaran dispositius amb informació sensible a aquesta xarxa hem decidit que no comptarà amb autenticació.

### **Sala de reunions**

La xarxa sala de reunions tindrà tant connexions cablejades com sense fil. La finalitat d'aquesta xarxa és proporcionar accés a Internet tant a dispositius de l'empresa com de clients quan estiguen a la sala de reunions. S'ha decidit separar-la de la xarxa de clients perquè poden connectar-se ordinadors amb informació sensible. No s'espera que tinga tantes sol·licituds de connexió com la xarxa sense fil de clients, de manera que amb una capacitat de 20 usuaris hi hauria prou. Com que sols ha de proporcionar accés a una sala, amb un sol punt d'accés situat a la mateixa tindrem prou per a cobrir tota l'àrea.

Com se tracta d'una VLAN a la qual se connectaran dispositius amb informació sensible, hi afegirem un procediment d'autenticació per el qual, una vegada connectat a la xarxa Wi-Fi es redirigirà a una pàgina web que ens sol·licitarà unes credencials. Aquestes credencials seran emeses per un dels ordinadors del despatx i tindran una caducitat de 3 hores ja que les reunions no solen superar aquesta duració.

#### **4.1.4. Adreçament**

Com ja s'ha comentat en el capítol anterior, cada xarxa sense fil va associada a una VLAN diferent amb un rang d'IPs diferent. D'una banda, els punts d'accés de la xarxa de clients, configurats en la VLAN 3, assignaran IPs mitjançant el servei DHCP amb el *pool* d'adreces 192.168.32.1 - 192.168.32.253. D'altra banda, els punts d'accés de la xarxa de la sala de reunions també se configurarà amb el servidor DHCP però amb un *pool* corresponent a les adreces de la VLAN 4 que abastarà les adreces IP 192.168.64.1 - 192.168.64.253.

## **4.2 Servei de veu**

---

Entre les necessitats de l'empresa s'inclou la possibilitat de comunicar-se entre el personal a través del telèfon, la qual cosa agilitza el procés de fer consultes puntuals als companys de treball. També és essencial que quan entra una telefonada a l'empresa aquesta se pugui adreçar fàcilment a la persona concreta a la qual va dirigida.

L'empresa ens ha comunicat que en aquest moment tenen aquest sistema i està proporcionat per la mateixa companyia que ofereix el servei telefònic. Estan contents i no contempen canviar-ho per una implementació pròpia. En la Figura 4.5 observem un exemple de telèfon IP que són els que s'empren per a aquest tipus de comunicacions.



Figura 4.5: Imatge d'un telèfon IP.

Observem com compta amb tecles de marcació ràpida per a poder comunicar-se amb els números prefixats, habitualment companys de la mateixa àrea de l'empresa.

## 4.3 Servidors

---

Per les necessitats de l'empresa, arribem a la conclusió que necessitarem implementar serveis de correu, de virtualització d'equips i serveis per a l'autenticació sense fil (servidor Radius).

### 4.3.1. Servidor de correu

Aquest servidor s'encarregarà de controlar tots els comptes de correu del personal de l'empresa. Serà on s'emmagatzemen els correus rebuts i enviats, de manera que s'haurà de fer còpies de seguretat amb una freqüència elevada i la informació que puga contindre serà molt valuosa.

Actualment el format dels correus de l'empresa es *usuari@nomEmpresa.com* i tenim previst que aquest format se mantinga ja que és senzill i fàcil de recordar per als clients.

#### Requisits mínims de *hardware*

L'equip haurà de tindre els següents requisits mínims per a un correcte funcionament:

- Processador amb una freqüència mínima de 1.5 GHz.
- Memòria RAM de 32 GB com a mínim.
- Memòria secundària igual o superior a 250 GB ja siga en format magnètic o flash.

#### *Software* necessari

En el servidor de correu instal·larem el *software* de Exim, Figura 4.6. Es tracta d'un servidor de correu per a la transferència de missatges desenvolupat a la Universitat de Cam-



**Figura 4.6:** Logotip del *software* Exim



**Figura 4.7:** Imatge d'un servidor Dell PowerEdge R340.

L'empresa americana Dell. Es tracta d'un dispositiu pensat per a PIMES que ofereix una bona relació entre característiques i preu.

bridge destinat a utilitzar-lo en sistemes Unix. Rep actualitzacions freqüents i té una alta capacitat de personalització i configuració. <sup>1</sup>

### Equip seleccionat

Per tal d'estalviar en el consum elèctric, i com que, per les dimensions de l'empresa, no se necessita una gran capacitat per als diferents servidors, hem decidit que tant el servidor de correu com els servidors Radius i proxy compartiran un mateix dispositiu físic; de manera que l'equip seleccionat haurà de complir amb els requeriments que tots tres necessiten.

Una bona opció és el servidor PowerEdge R340 Server (Figura 4.7), de la marca Dell. Es tracta d'un servidor en format de Rack (ocupa 1 U) amb les següents característiques entre altres:

- Capacitat d'instal·lar fins a 64 GB de memòria RAM
- Compatibilitat amb la funció Hot-Plug
- 8 ranures per a discs durs de 2,5"
- 4 ranures per a discs durs de 3,5"

<sup>1</sup>Informació extreta de <https://dade2.net/es/los-7-mejores-servidores-de-correo-en-linux/>



**Figura 4.8:** Logotip del *Software* dedicat a la virtualització d'equips Citrix Xenserver. La imatge correspon a la versió 7.3 encara que actualment ja està disponible fins la versió 8.2.

### 4.3.2. Servidor de virtualització d'equips

Considerem que la millor forma de treballar és amb clients lleugers, de manera que els ordinadors sols transmetran la imatge i les interaccions dels usuaris i serà al servidor on es duran a terme totes les operacions. Aquest mètode facilita la incorporació de noves aplicacions als ordinadors i els procediments d'actualització ja que tots els programes i la informació s'emmagatzemen de manera centralitzada en el servidor. A més, els clients lleugers tenen de manera general una vida útil més elevada ja que la càrrega que han de suportar és baixa i no depèn de la complexitat de les aplicacions. A més, aquest sistema facilita la implementació d'un dels requisits que ens ha demanat l'empresa i és la facilitat de teletreballar.

#### Requisits mínims de *hardware*

Per a poder utilitzar esta estructura necessitem un servidor capaç de virtualitzar tots els equips i amb memòria suficient per a poder emmagatzemar tota la informació, de manera que buscarem un equip que complisca els següents requisits:

- Processador amb una freqüència mínima de 1.5 GHz.
- Memòria RAM de 64 GB com a mínim.
- Memòria secundària igual o superior a 10 TB en format magnètic.

#### *Software* necessari

Per a implantar el servei de virtualització d'equips tenim diverses opcions de programari, d'entre totes elles nosaltres apostem per un *software* anomenat Citrix Xenserver (Figura 4.8). Es tracta d'un programari que pot operar sobre Windows o Linux i que té tant una versió lliure com de pagament.

#### Equip seleccionat

Hem seleccionat com a dispositiu més adequat el servidor HPE ProLiant DL325 Gen10 P04648-B21. Se pot observar una imatge del servidor en la Figura 4.9 i entre les seues característiques destaquem:





**Figura 4.9:** Servidor HPE ProLiant DL325 Gen10 P04648-B21.

Es tracta d'un servidor en format Rack de la marca Hewlett Packard Enterprise (HP).

- Processador AMD Epic 7401P amb 24 nuclis a 2 GHz i memòria cau de 64 MB, el que suposa que té una gran capacitat per a execucions i accessos concurrents.
- Memòria interna DDR4-SDRAM amb 32 GB. Compta amb 16 *slots*, ampliable fins a 512 GB, de manera que assegura un gran rendiment i flexibilitat a l'hora de realitzar ampliacions.
- Capacitat d'emmagatzematge de fins a 20 TB amb 8 ranures i possibilitat d'implantar un RAID 10, 50 i 60. Aporta escalabilitat i la possibilitat d'obtenir una millor gestió de l'emmagatzematge.
- Compatibilitat amb la funció Hot-Plug, la qual cosa millora la disponibilitat.
- Certificat Energy Star, de manera que té un ús eficient de l'energia.
- Duplicat de la refrigeració, ports Ethernet i bateria, la qual cosa assegura una major disponibilitat davant d'una fallada de *hardware*.

### 4.3.3. Servidor d'autenticació de xarxa Wi-Fi Radius

Com hem dit ja anteriorment, la xarxa de l'empresa compta amb dos punts d'accés sense fil, un destinat a donar connexió als clients que desitgen tindre un accés a Internet en la sala d'espera o per a connectar els dispositius personals dels treballadors i l'altre destinat a proveir d'Internet a equips que es troben a la sala de reunions. Considerem que a la xarxa de clients no cal afegir autenticació de xarxa, hi hauria prou amb una contrasenya que s'indicaria en la oficina. Però per a la sala de reunions, com es tracta d'una VLAN que a la qual se connectaran dispositius amb informació delicada, hi afegirem un procediment d'autenticació mitjançant un servidor Radius.

Aquest servidor utilitzarà l'autenticació EAP amb PEAP. Els noms d'usuari i les contrasenyes les generarà un ordinador de manera aleatòria i tindran una validesa de 3 hores. També s'aconseguirà que la informació viatge de manera segura mitjançant l'encriptació de dades amb el sistema WEP.

#### Requisits mínims de *hardware*

Els requisits mínims que ha de complir l'equip per a muntar un servidor Radius sobre Linux són els següents:

- Processador a 1.5 GHz (Pentium 4 o superior)
- 256 MB de memòria RAM
- 10 GB de memòria en disc dur.



**Software necessari**

El dispositiu ha de comptar amb Debian GNU/Linux, i s'ha d'instal·lar el programa de codi obert FreeRadius, actualment l'última versió és la 3.0.23, i configurar-lo per a controlar l'accés a la xarxa sense fil.

**Equip seleccionat**

Com ja hem dit abans, per a millorar el consum energètic i com que els serveis d'autenticació i proxy no requereixen de gran capacitat de còmput, hem decidit agrupar aquestos serveis amb el servei de correu en un únic dispositiu físic. Com apuntàvem se tracta del servidor Dell PowerEdge R340 i les seues característiques se descriuen en el apartat anterior de servidor de correu.



# Seguretat de la xarxa i la informació

---

Com ja hem dit en aquest treball, la seguretat es un punt fonamental per a l'empresa per el tipus de dades que se tracten, de manera que s'implementaran tanques de diferents tipus per a garantir-la. Distingim dos tipus diferents de seguretat, un des del punt de vista de la confidencialitat de la informació, on intentarem evitar que persones no autoritzades puguem accedir a la informació, i l'altre des del punt de vista de la fiabilitat per tal de no perdre informació.

## 5.1 Seguretat de la xarxa

---

Si ens centrem en les mesures per a evitar que persones no autoritzades accedeixen a la informació trobem les que s'implementen en la LAN i en la WLAN

### 5.1.1. LAN

- Elements i aplicacions.

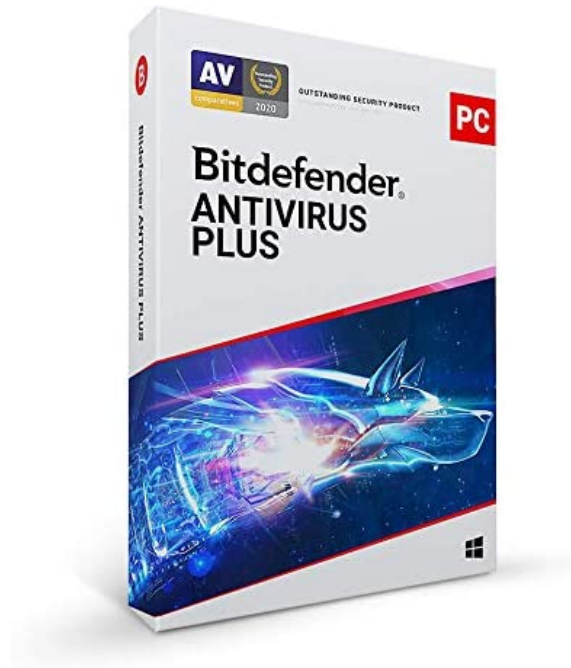
Per a protegir la xarxa és fonamental el paper de les aplicacions, qualsevol aplicació és susceptible de tindre falles de seguretat permetent que la informació quede exposada.

Quan se detecten les vulnerabilitats, l'equip de suport de les aplicacions treuen noves actualitzacions per a resoldre-ho de manera que és essencial que tots els equips tinguem les aplicacions actualitzades per tal d'evitar falles de seguretat d'aquestes.

A més, tots els dispositius hauran de contar amb un antivirus per tal de detectar i eliminar possibles amenaces. En aquest cas considerem que un bon antivirus seria l'anomenat BitDefender (Figura 5.1), que desenvolupat per l'empresa romana del mateix nom, és considerat un del millors antivirus en la actualitat. Per suposat, és essencial tindre tant l'aplicació de l'antivirus com la seua base de dades actualitzada.

- *Firewall* o tallafocs

És un sistema de seguretat per a bloquejar accessos no autoritzats a un ordinador mentre que se segueix permeten la comunicació de l'ordinador amb altres serveis autoritzats. Poden ser tallafocs *hardware* o *software*. En el nostre cas optem per un dispositiu físic que es connectarà al *switch* principal situat a l'entresòl 2 i s'encarre-



**Figura 5.1:** Imatge del antivirus bitDefender

garà de filtrar els paquets que entren a la xarxa. També detectarà i evitarà possibles atacs DoS (denegació de servei) que podrien tornar la xarxa durant un temps.

- Proxy

Un proxy és un equip informàtic que actua d'intermediari entre les connexions d'un client i un servidor de destí, filtrant tots els paquets entre els dos.

El servidor proxy és un element que fa una doble funció ja que d'una banda millora la velocitat dels accessos a Internet i d'altra és una barrera més de seguretat front a amenaces.

- Llistes de control d'accés (ACL)

Les llistes de control d'accés són una forma de determinar els permisos d'accés apropiats a un usuari. Poden configurar-se generalment per a controlar el tràfic entrant i eixint.

### 5.1.2. WLAN

- Canviar configuracions predeterminades

És important canviar la configuració predeterminada d'elements com els punts d'accés, ja que aquests solen tindre per defecte una configuració amb SSID (nom inclòs en tots els paquets d'una xarxa per a indentificar-los com a part d'aquesta), de manera que se pot facilitar la identificació d'una xarxa per a un atacant. Haurem de canviar-la i desactivar la difusió SSID.

- Habilitar autenticació.

La xarxa sense fil sala de reunions realitzarà la validació mitjançant el protocol d'autenticació extensible (EAP), que proporciona autenticació de dos vies mitjançant el servidor Radius. Aquest servidor funciona de manera independent als punts d'accés i manté la base de dades d'usuaris vàlids que poden tindre accés a la xarxa.



Figura 5.2: Imatge d'un SAI

Quan un usuari es connecta ha de proporcionar un nom d'usuari i una contrasenya, aquests se comparen en la base de dades del servidor i si coincideix s'obté l'autenticació.

- Encriptació

La xarxa sense fil clients s'encriptarà mitjançant el sistema WPA, i la xarxa anomenada sala de reunions ho farà mitjançant WPA2. El sistema WPA genera claus d'encriptació dinàmiques de 64 a 256 bits cada cop que un client estableix una connexió amb el punt d'accés. La diferència entre les dos versions d'aquest sistema és que la WPA2 canvia la clau cada pocs minuts, encara que se tracta de la mateixa connexió, de manera que augmenta la seguretat.

## 5.2 Seguretat de la informació

---

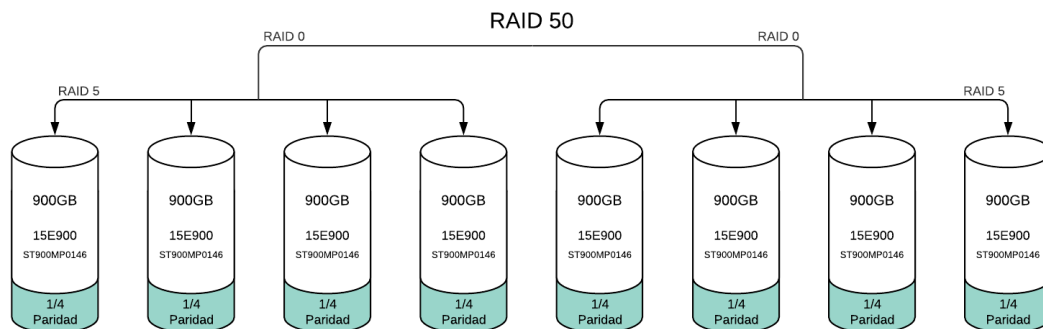
Hem vist elements que impedeixen que terceres persones puguin accedir sense consentiment a la informació de la xarxa, però també hem de tindre en compte que la informació no se perdi per falles en la xarxa. Per a evitar esta situació implantarem les següents mesures:

- SAI

Per tal d'evitar la pèrdua d'informació a causa d'una aturada del subministrament d'electricitat, posarem SAIs (sistema d'alimentació ininterrompuda) connectats a tots els dispositius. De manera que davant d'una interrupció del subministre elèctric els dispositius tindrien energia durant el temps suficient per a guardar totes les tasques en curs i no perdre informació. Podem veure un exemple en la Figura 5.2.

- RAID

Un RAID, acrònim de les paraules matriu redundat de discs independents en anglès, és un conjunt d'unitats de memòria que el sistema operatiu percep com a una sola unitat lògica. La diferència entre configurar RAIDs o no és fonamentalment la tolerància a errors. Hi ha diferents nivells de RAID i depenent de l'escollit s'obté una major o menor tolerància a errors.



**Figura 5.3:** Esquema del RAID 50  
El RAID 50 suposa una combinació del RAID 5 i el RAID 0.

En aquest cas, per als nostres servidors implementarem RAIDs 50, el que significa una combinació del RAID 5 i RAID 0, com s'aprecia en la Figura 5.3.

El RAID 0 associa dos o més discs com a un sol, de manera que la informació se divideix entre tots els discs, permetent una major velocitat d'escriptura i lectura ja que es pot escriure i llegir la informació simultàniament en els diferents discs, però no proporciona seguretat davant errors ja que no hi ha replicació de la informació.

El RAID 5 necessita com a mínim 3 discs, encara que de memòria efectiva sempre hi haurà un menys dels instal·lats, ja que cada disc haurà d'emmagatzemar  $1/n$  de dades per a la paritat. Aquestes dades s'utilitzaran en cas de fallada d'un disc per a recuperar el contingut d'aquest de manera que el sistema és capaç de suportar la fallada d'un disc. A més de la capacitat de recuperar-se de la fallada d'un disc, el RAID 5 se caracteritza per velocitats de lectura elevades, mentre que les de escriptura són un poc més lentes ja que s'ha de calcular la paritat. En general podem dir que el RAID 5 combina seguretat i rendiment.

La combinació dels dos tipus de RAID suposa un excel·lent rendiment en quant a la velocitat i la seguretat, ja que pot suportar con a mínim la fallada d'un disc, podent arribar fins a dos si els discs que fallen pertanyen a elements diferents del RAID 0.

- Control de temperatura

En la sala de servidors és important que la temperatura estiga controlada en cada moment per a evitar que els dispositius treballen fora de les condicions òptimes i puguin fallar o acurtar la seua vida útil. Aquest sistema anirà aparellat al sistema de refrigeració de la sala, de manera que serà capaç de regular automàticament la temperatura.

- Còpia de seguretat en el núvol

És molt important tindre còpies de seguretat i que aquestes se situen en llocs geogràfics diferents per tal d'evitar elements que puguin afectar a tota una zona geogràfica. Per a guardar la informació, des de l'empresa ens han dit que prefereixen un sistema automàtic i no haver de emportar-se discs durs a casa o fer còpies de seguretat a propòsit, de manera que la millor solució és la realització de còpies de seguretat automàtiques en el núvol.

Hi ha moltes companyies que ofereixen serveis d'emmagatzematge en el núvol com ara Google, Amazon, Microsoft, etcètera. En aquest cas proposem utilitzar els serveis de Google Drive (Figura 5.4).

- Impediment físic d'accedir als servidors i dispositius de la xarxa.



**Figura 5.4:** Logotip de Google Drive.

Aquest punt és aplicable tant a assegurar la fiabilitat de les dades com a evitar que terceres persones accedeixen a la xarxa. Se tracta d'evitar per mitjans físics l'accés al servidors i *switches* de l'organització.

Per aconseguir-ho instal·larem armaris amb clau tant en l'entresòl 1 com en l'entresòl 2 i també controlarem l'accés a la sala de servidors mitjançant un pany a la porta.





# Pressupost del projecte i elecció de dispositius

---

UN vegada explicada la infraestructura en aquest capítol veurem quin és el cost monetari que suposa la seua implantació, per fer-ho especificarem els elements concrets escollits per a cada dispositiu i el seu preu. Cal dir que la informació dels preus d'alguns models no és massa clara ja que pot variar molt depenent del nombre de dispositius que compra una organització i no hi ha publicat un preu unitari; en eixos casos intentarem donar un preu orientatiu.

## 6.1 Hardware

---

Quan parlem de pressupost, el preu del *hardware* i demés elements físics és el primer que ens ve a la ment però no és l'única cosa a tindre en compte. Ací es mostren els elements que hem de considerar:

### 6.1.1. PCs

Com ja hem anomenat anteriorment, el PCs que utilitzarem seran clients lleugers de manera que tindran un cost més reduït i una vida útil més llarga. Hem escollit el model Thin Client HP t430 de la marca Hewlett-Packard (Figura 6.1) que té un preu unitari al voltant de 290€. Per a la infraestructura necessitarem 9 dispositius i adquirirem un més a mode de respot, de manera que el cost total serà de 2 900€.



Figura 6.1: Imatge d'un ordinador HP Thin Client t430



**Figura 6.2:** Imatge d'un portàtil Innjoo Voom

### 6.1.2. Portàtils

Necessitarem portàtils per a les reunions que se duguen a terme en la sala de reunions i en el cas de que s'hagen de dur a alguna empresa per a explicar alguna cosa. També se tractarà de dispositius lleugers de manera que no necessitaran gran capacitat de càlcul.

Els dispositius escollits són el model Innjoo Voom amb el processador Intel Celeron (Figura 6.2) que tenen un preu unitari d'uns 200€, la qual cosa suposaria un total de 400€.

### 6.1.3. Servidors

En la secció de servidors ja hem dit quins dispositius adquirirem per la infraestructura, se tracta del servidor Dell PowerEdge R340 per al servidor de correu i Radius, i del servidor HPE ProLiant DL325 Gen10 P04648-B21 per a la virtualització d'equips.

El primer té un preu aproximat de 3 800€ i el segon 2 100€ el que suposa un total de 5 900€

### 6.1.4. Dispositius d'emmagatzematge

Junt amb els servidor hem de tindre en compte la memòria secundària que acompanyara a aquestos. Hem dit que volem instal·lar un RAID 50, la qual cosa suposa que tindrem de memòria efectiva dos discs menys dels instal·lats i que necessitarem elements de recanvi per si algun falla per a fer ús de la funció *hot-plug* dels servidors i tornar a disposar de la capacitat de recuperació de la informació.

Quan tenim un RAID, té especial importància que tots els discs durs siguin iguals ja que de no ser-ho la memòria de tots els discs quedarà limitada a la del element de menor capacitat, amb la despesa de recursos que això suposa. Com que no sabem la disponibilitat de discs del mateix model que hi haurà en un futur és recomanable tindre una gran quantitat de discs de recanvi de manera que comprem un 50% més dels discs que necessitem en un principi.

En aquest punt hem arribat a un dilema, d'una banda volíem tindre emmagatzematge suficient per a una futura ampliació de la infraestructura però d'altra banda el preu de la memòria és cada vegada més econòmic de manera que hem de filar prim i aconseguir un bon balanç.

Utilitzarem dos models diferents per als dos servidors, ja que el servidor encarregat de virtualitzar els equips té una necessitat major de memòria secundària. Per al servidor dedicat al correu i Radius utilitzarem el model Seagate EXOS 15E900, que té una capacitat unitària de 600GB, com el servidor té una capacitat de 8 ranures comprarem 12 discs durs. El seu preu individual és de 250€, de manera que el preu total serà de 3 000€.

Per al servidor de virtualització d'equips necessitarem més memòria, és per això que emprarem discs de 2TB de la marca HPE, model SAS III 2TB (765466-B21). Tenen un preu unitari de 325€i comprarem 12 unitats de manera que el preu final serà de 3 900€.

### 6.1.5. Commutadors o *switches*

Per al commutador principal optarem per una marca més *premium* com ho és Cisco, ja que és una peça clau per a tota la infraestructura. Hem escollit el commutador Cisco 2960-24TT que té un preu de 405.74€.

En el cas del commutador secundari hem escollit la sèrie D-Link DGS-1210 ja que és econòmica i fiable (ofereix garantia de per vida) de manera que té una molt bona relació qualitat-preu. Escollirem el de 48 boques amb un preu de 330€.

### 6.1.6. Encaminador

La companyia que ofereix el serveis d'Internet sol proporcionar un *router* però les seues funcions solen ser prou limitades de forma que instal·larem un dispositiu propi que ens permeti una major configuració. En aquest cas hem escollit el dispositiu DGS-1210-12TS/ME de la marca D-Link que ofereix a part de les funcions típiques d'un *router* l'administració de punts d'accés. Té un preu de 380€.

### 6.1.7. Cablejat i rossetes

Dintre d'aquest apartat distingim per una banda els cables Ethernet que connectaran tota la infraestructura i d'altra les rossetes que se situaran en les diferents habitacions.

#### Cablejat ethernet

Per al cablejat Ethernet ja hem indicat que utilitzarem cablejat UTP de categoria 6, que se sol vendre en bobines de 300 metres i és econòmic. Per a tota la infraestructura hem estimat que necessitarem uns 3 000 metres, com cada bobina costa uns 70€ haurem d'afegir un total de 700€ al pressupost.

#### Rossetes

Tenint en compte la ocupació màxima dels espais i que cal almenys una rosseta per cada lloc de treball, hem estimat el nombre necessari de rossetes en 116, encara que comprarem 130 per a tindre'n de recanvi. Cada unitat té un preu de 2€ per la qual cosa suposa un total de 260€.



**Figura 6.3:** Imatge d'un armari HPE P9K07A.

Observem com té a la cara frontal i posterior una reixeta que permet el pas de l'aire i per tant una millor refrigeració.

#### 6.1.8. Armari o Rack

Per a la nostra instal·lació necessitarem dos armaris, un gran que anirà a la sala de servidors (entresòl 2) i un altre menut que anirà en el traster del entre-sòl 1. L'armari gran serà el RACK HPE P9K07A (Figura 6.3) que té un preu de 660€. Per al menut hem escollit el Digitus Mural, un armari molt més senzill, de 7U amb un preu de 90€, de manera que el preu total dels armaris serà de 750€.

#### 6.1.9. PDU

Per a subministrar energia als dispositius es requereix d'una PDU (*Power Distribution Unit*). Aquest aparell permet multiplicar i distribuir l'alimentació elèctrica de manera intel·ligent i és important que aquest dispositiu permeti controlar l'encesa i apagat dels dispositius de manera progressiva i controlada per a evitar sobrecàrregues en el sistema elèctric.

Hem escollit el model P9S11A de HPE amb un voltatge nominal d'entrada de 100-240V, rang que supera en ambdós sentits el requerit per els dispositius. Necessitarem dos unitats i el seu preu unitari és de 665€, de manera que el preu total serà de 1 330€.

#### 6.1.10. SAI

Com ja hem vist anteriorment el SAI és un dispositiu que ens aporta fiabilitat a la infraestructura ja que és capaç de proporcionar electricitat en cas de caiguda de la xarxa elèctrica durant temps suficient per a guardar les tasques en curs.

Necessitarem dos dispositius que instal·larem en l'entresòl 1 i 2 respectivament, al igual que els PDU. Hem escollit el model HPE J2R03A que té un preu unitari de 770€ la qual cosa suposa un total de 1 540€.



**Figura 6.4:** Imatge d'un extintor de pols ABC de 6 kg.

S'ha de tindre en compte que per a que els equips electrònics estiguen protegits s'ha d'enfocar a la flama des d'una distància superior a 2 metres.

#### 6.1.11. Refrigeració

La refrigeració dels servidors és fonamental per al bon funcionament del sistema. Hi ha sistemes específics per a centres de processament de dades però en aquest cas hem optat per una opció més econòmica i adequada a les necessitats de l'empresa instal·lant un aire condicionat convencional que regularà la temperatura de la sala de manera intel·ligent. Després de sondejar els dispositius i preus podem concloure que el preu aproximat és d'uns 500€.

#### 6.1.12. Extintors

En cas d'incendi, per a evitar danyar els aparells electrònics, s'han d'utilitzar uns extintors especials. Es tracta d'extintors per a focs de classe C (elèctrics) i els situarem a l'entrada de les sales on es troben els dos *racks* tant en l'entresòl 1 com a l'entresòl 2. Aquests extintors seran de 6 kg de pols ABC (Figura 6.4) i tenen un preu cadascú de 25€, és a dir en total 50€.

#### 6.1.13. Porta ignífuga

Aquesta porta es situarà a l'entrada de la sala de servidors i permet que, en cas de produir-se un incendi, siga més difícil que aquest afecte als servidors de l'empresa. El seu preu és de 150€.

Element	Nombre	Preu total
PCs	10	2 900 €
Portàtils	2	400 €
Servidors	2	5 900 €
Discs durs	24	6 900 €
Commutadors	2	735 €
Encaminador	1	380€
Cablejat i rossetes	3 000 m, 130	960 €
Armaris	2	750 €
PDU	2	1 330 €
SAI	2	1 540 €
Refrigeració	1	500 €
Extintors	2	50 €
Porta ignífuga	1	150 €
Punts d'accés	2	480 €
Tallafocs	1	900 €
<b>TOTAL</b>		<b>23 875 €</b>

**Taula 6.1:** Taula resum preu dels elements *hardware*

#### 6.1.14. Punts d'accés

Anteriorment ja hem introduït per a que serveixen els punts d'accés i on tenim pensat posar-los. En aquest cas hem seleccionat el model C9105AXI-x de la sèrie Cisco Catalyst 9100 Series Access Points, ja que són dispositius populars per als que hi ha multitud de suports compatibles. A més, compta amb antena de 2.4 GHz i 5 GHz omnidireccional de manera que per als dispositius més propers oferiria una velocitat major de connexió. El seu preu unitari es de 240€, com en necessitem dos, el preu final serà de 480€.

#### 6.1.15. Tallafocs

Per al tallafocs o *firewall* físic hem seleccionat el model FotiGate 80F de la marca Fortinet que és una de les més reconegudes en la fabricació de tallafocs físics per a petites i mitjanes empreses. El preu del dispositiu és de 900€.

#### 6.1.16. Taula resum hardware

En la Taula 6.1 observem un resum de tots els dispositius, el nombre de unitats que comprarem i el preu total.

## 6.2 Software

### 6.2.1. Antivirus

Com hem nomenat anteriorment la solució adoptada per a l'antivirus és el software de BitDefender. A la seua pàgina web podem calcular el preu anual depenent del nombre de dispositius, si seleccionem 14 dispositius (9 PCs, 2 portàtils i 3 servidors) el preu és de 328.99€ en un descompte del 30%. Si no, el preu normal es de 469.99€ com observem a la Figura 6.5.

**Bitdefender GravityZone Business Security**

Millor protecció, millor rendiment

GravityZone està constantment classificat com a número 1 en proves de seguretat independents, proporcionant seguretat de confiança a empreses de totes les mides.

**Trieu el vostre pla ara amb 30% descompte**

Dispositius:  - 14 +

Introduïu el nombre total de dispositius (portàtils, ordinadors de sobretaula, servidors de fitxers) que vulgueu protegir de 3 a 100.

Podeu cobrir fins a 5 servidors. Els servidors representen fins al 30% del total de dispositius.

1 any  2 anys  3 anys

**30% descompte**

~~469,99 €~~  
**328,99 €**  
Impostos no inclosos

**COMPRA ARA**

[Comprar assistit amb un soci](#)

**Figura 6.5:** Preu de l'antivirus.

Es tracta d'una captura extreta de la pàgina web de l'empresa del antivirus on podem calcular el preu en funció dels dispositius. Com s'observa per a 12 dispositius podem cobrir fins a 4 servidors.

Software	Preu x unitat	Duració	Nombre	Total (anual)
Antivirus	(Preu no lineal)	Anual	14	329 €
Virtualització	2 €	1 mes	11	264 €
Sistema operatiu	12 €	Sense limit	11	132 €
<b>TOTAL</b>				<b>725 €</b>

**Taula 6.2:** Taula resum amb els preus finals de l'apartat del programari.

### 6.2.2. Virtualització d'equips

En aquest punt hem de separar dos tipus de software diferents, d'una banda el que propicia la virtualització, que com hem dit abans serà el Citrix XenServer i d'altra el sistema operatiu dels usuaris. El software de Citrix té un preu associat de 2€ per usuari i mes, de manera que si contem 11 usuaris (9 PCs i 2 portàtils) tindria un cost anual de 264€.

Per al SO escollirem Windows 10 ja que a l'empresa estan acostumats a treballar amb aquest sistema i així ens assegurem que tot els programes que utilitzen segueixen sent compatibles. Cada llicència de Windows 10 té un preu de 12€ de manera que serà un total de 132€.

### 6.2.3. Servidor de correu

El software que utilitzarem és el de Exim que és de codi obert per la qual cosa no té un cost associat.

### 6.2.4. Taula resum software

A la Taula 6.2 veiem un resum dels preus dels elements de programari.

Element	Preu
Hardware	23 875 €
Software	725 €
Instal·lació	7 500 €
<b>TOTAL</b>	<b>32 101 €</b>

Taula 6.3: Resum del pressupost total

### 6.3 Instal·lació

---

Per a valorar el preu de la instal·lació hem contactat amb una empresa de Vila-real dedicada a aquest tipus de tasques. Degut a que és un projecte per un TFG no ens han elaborat un pressupost al detall però després d'explicar com seria la instal·lació ens han donat un preu aproximat de 7 500€.

### 6.4 Total

---

Finalment, en la Taula 6.3 tenim el pressupost final del projecte, diferenciat per els elements *hardware*, *software* i la instal·lació.

### 6.5 Manteniment

---

Fins ara hem vist el que seria el pagament inicial per a tindre la infraestructura, però a banda hi haurà una serie de despeses que es repetiran cada any per a tindre el sistema funcionant.

Primer que tot hem de considerar que els elements físics poden trencar-se i haver-los de substituir, encara que no podem quantificar aquest cost. Després, en l'apartat del *software* tant l'antivirus com el programa de virtualització tenen un cost continu de 329 € i 264 € anuals respectivament.

Amb tot açò podem afirmar que la infraestructura tindrà un cost de manteniment mínim de 593 € segons els preus actuals dels programes. Si augmenta el nombre de treballadors s'ha de tindre en compte que també augmentaran els costos de manteniment de l'estructura i també ocorrerà si se trenca algun dispositiu.



---

---

## CAPÍTOL 7

# Conclusions

---

En aquest TFG s'ha elaborat el disseny de la infraestructura informàtica per a una empresa d'assessoria i consultoria, adequant el projecte i atenent a les necessitats comunicades per la empresa en qüestió.

Primer que tot vam parlar en un directiu per a que ens informara de les necessitats principals que té l'organització i conèixer millor quina forma tenen de treballar i la infraestructura amb la que compten en l'actualitat. Cal dir que l'empresa no té informàtics propis sinó que és una empresa externa la que s'encarrega de tot el sistema informàtic.

Parlant amb aquest responsable de l'empresa ha quedat palès que una de les principals preocupacions és un atac informàtic que revelara informació dels clients o bloquejara els ordinadors deixant a l'assessoria en una situació molt compromesa. A més, també hem apreciat una convicció de que el futur del negoci passa per tindre un sistema informàtic punter que permeta facilitar a l'hora d'implantar nous programes i funcionalitats.

Partint d'aquestes premisses hem dissenyat una infraestructura on sobretot destaca la seguretat de les dades i amb clients lleugers que permeten una major velocitat a l'hora de d'implantar actualitzacions i funcionalitats. Hi ha una minuciosa divisió de la xarxa en xarxes virtuals (VLANs), s'ha optat per elements *hardware* de seguretat com ara tallafocs per a millorar la seguretat i inclús hem proposat canviar la distribució física del local on es troba la empresa per a poder construir una sala de servidors amb tots els requeriments que aquesta necessita.

El punt que he trobat més difícil ha sigut la realització del disseny lògic i la implementació d'aquest en Packet Tracer per a realitzar les posteriors simulacions. Probablement el fet de realitzar el treball més d'un any després de finalitzar les classes del grau haja influït en no recordar bé com funcionava aquest *software* i com es configurava el *hardware*.

Amb tot açò hem realitzat un projecte seriós, amb el seu pressupost aparellat que sóc conscient, pot ser una inversió elevada depenent de la PIME però que de bon segur proporcionarà una infraestructura sòlida per a treballar amb capacitat d'acompanyar l'organització en el seu creixement sense quedar-se obsoleta o menuda en el curt o mig temps.

Pel que em consta l'empresa volia saber com seria i quant costaria tindre una infraestructura puntera però de moment no va a instal·lar-la, si canviara de parèixer i volguera implementar-la caldria revisar sobretot els preus dels diferents elements ja que com apuntàvem en l'apartat del pressupost poden variar molt depenent d'on es consulten els preus i sovint depèn molt del nombre de dispositius que s'espera comprar. També caldria aclarir quin nivell d'elements *hardware* es vol adquirir; en el projecte es contempla un nivell mig ja que pense que no té sentit planificar una infraestructura a llarg termini si després

utilitzem uns dispositius de gama baixa que podrien donar-nos problemes amb el pas del temps i l'augment de les exigències.

Per a finalitzar dir que, encara que crec que el meu futur laboral no discorrerà íntimament lligat al mon de la enginyeria informàtica sí que m'ha resultat útil per a recordar molts dels conceptes vist en el grau i aprendre'n de nous més enllà del que veiem estrictament en classe. Sóc conscient de que la informàtica és útil per a qualsevol eixida laboral i cada vegada va a créixer més aquesta importància, de manera que crec que és un enorme valor afegit al grau i màster d'ADE que he cursat.

# Bibliografia

---

- [1] Butlletí Oficial de l'Estat "Reial Decret 486/1997 de 14 d'abril" Ministeri de Treball, 1997.
- [2] Centre de Telecomunicacions i tecnologies de la Informació "Presentació del projecte Heura als centres educatius". Generalitat de Catalunya, 2007.
- [3] Direcció General de Tecnologies de la Informació i les Comunicacions. "Especificacions tècniques para instalaciones de centros de la Generalitat Valenciana". Generalitat Valenciana, 2020.
- [4] Hennessy, J. L., Patterson, D. A. *Arquitectura de computadores. Un enfoque cuantitativo*. McGraw-Hill, 2003.
- [5] Kurose, J., Ross, K. W. *Redes de computadoras (Vol. 5)*. Pearson education, 2010.
- [6] Odom, W. *Cisco CCNA, routing and switchting, ICND2 200-101: guia oficial para la certificación*. Pearson Educación, 2014.
- [7] Odom, W. *Cisco CCENT/CCNA, ICND1 100-101: guia oficial para la certificación*. Pearson Educación, 2014.
- [8] Patterson, D. A., Hennessy, J. L. *Estructura y diseño de computadores*. Reverté, 2018.
- [9] Pérez Torres, D. *Redes Cisco: curso práctico de formación para la certificación CCNA*. RC Libros, 2018.
- [10] Seu electrònica Vila-real "Ordenança de convivència ciutadana de Vila-real". Ajuntament de Vila-real, 2012.
- [11] Stallings W., Vargas A. C., Espinosa A. P. *Organización y arquitectura de computadores*. Pearson Educación, 2006.
- [12] Tanenbaum, A. S. *Redes de computadoras*. Pearson Educación, 2003.

