Oriol Villanova Llorens

Estudi de la infraestructura de xarxa de les escoles de primària en relació a la implantació d'una xarxa de sensors

TREBALL DE FI DE GRAU

Dirigit per Antoni Martínez Ballesté

Grau d'Enginyeria en Sistemes i Serveis de Telecomunicació

UNIVERSITAT ROVIRA I VIRGILI

Tarragona 2022

Agraïments

Aquest treball de fi de grau ha portat un gran esforç per poder realitzar-lo. He dedicat moltes hores i he hagut de fer molta recerca. M'agradaria expressar el meu agraïment al projecte ACTUA per l'oportunitat de col·laboració que m'ha ofert per a realitzar aquest estudi i especialment a l'Antoni Martínez Ballesté, director del projecte i qui em va oferir aquesta oportunitat de contribuir amb el projecte.

No hagués estat possible la realització d'aquest projecte sense el suport de la meva família, especialment dels meus pares i la meva germana, amics i companys de carrera.

Donar també les gràcies a tots els professors del grau que amb els coneixements que han ensenyat ha donat fruit a la realització de totes les assignatures de la carrera i aquest treball de fi de grau.

Resum

Aquest treball consisteix en l'estudi tècnic complet de la xarxa de dades de les escoles de primària amb l'objectiu de comprendre la seva infraestructura, el seu funcionament i els seus obstacles fent una visita en un entorn real de producció i simulant totes les variables obtingudes conjuntament amb un desenvolupament d'una aplicació per a aplicar totes les conclusions extretes.

El treball es divideix en tres parts principals. La primera part consisteix en un estudi de la infraestructura de xarxa de les escoles de primària des d'un punt de vista teòric, de producció fent una visita en un entorn real on ja estigui tota la infraestructura implementada per finalment fer les simulacions de la informació obtinguda.

La segona part es centra en l'estudi de la posició d'un kit de sensors dins de la infraestructura estudiada en la part anterior. Es fa una comparativa de les diferents zones on està connectat sempre recolzat de les simulacions realitzades.

L'última part es tracta de tancar tot el cercle de la infraestructura de xarxa on es realitza un desenvolupament d'una aplicació amb Node.js utilitzant un sistema de informació geogràfica i una verificació de funcionament dels diferents kits.

Es tracten temes sobre les xarxes de dades i internet, xarxes de sensors i desenvolupament web. Tots aquests temes són necessaris per a l'obtenció de les tres parts exemplificades anteriorment. S'apliquen en diferents etapes del procés del treball i per a objectius diferents.

Finalment es treuen conclusions del millor posicionament del kit de sensors dins de la xarxa tenint en compte totes les possibles variables obtingudes al llarg del projecte, donant peu també a la seva producció dins del projecte ACTUA per a l'extracció de dades en un entorn real.

Paraules clau: Xarxes de dades, xarxes de sensors, *IoT*, commutador, encaminador, LAN, WAN, *Cisco Packet Tracer*, *Framework*, *Python*.

Taula de contingut

Llistat de Figures

Llistat de Taules

1 Introducció i objectius

1.1 Introducció i context

Aquest estudi ve donat per la necessitat de fer el treball de final de grau per finalitzar els meus estudis. Aquesta necessitat m'ha donat l'oportunitat de veure temes més profundament en els que voldria intentar enfocar la meva carrera professional.

En aquest cas, volia enfocar el treball en la temàtica de les xarxes de dades i internet. D'aquí va sorgir la col·laboració amb el projecte ACTUA, que és un projecte per analitzar la transmissió del virus de la COVID-19 a les aules de primària, un dels 32 projectes seleccionats a la convocatòria "Pandèmies 2020". Aquest projecte necessitava conèixer a fons la xarxa que hi ha en les escoles i internet per poder desenvolupar la seva tasca.

Dins del fruit d'aquesta col·laboració, ha sortit aquest treball. En el qual he analitzat la xarxa informàtica dels centres públics d'escola primària, he fet un estudi d'implantació d'un kit de sensors per a recollir les dades i he desenvolupat un sistema per a monitoritzar l'estat de vida d'aquests kits. Mirant així tots els aspectes de xarxa possibles per a realitzar la comunicació d'aquest kit de sensors amb els servidors del projecte, hagen tingut en compte cada pas del camí des de que es recullen les dades fins que són emmagatzemades.

En el treball mostro el fruit del treball de moltes hores d'investigació i d'anàlisi de totes les possibles variables que podrien afectar en aquesta xarxa.

1.2 Missió i objectius

La missió d'aquest Treball de Fi de Grau és contribuir en el projecte ACTUA, que tracta sobre l'anàlisi del context a l'aula, per mitjà de la detecció i estudi de diferents paràmetres com ara temperatura, humitat, so, partícules, etc. En concret i, donada l'especialitat dels meus estudis de grau, em centraré en l'ús de la xarxa informàtica com a infraestructura de connexió per als nodes de sensors que necessita el projecte. En concret, el treball té aquests objectius:

- **Objectiu 1.** Estudiar la infraestructura de la xarxa d'àrea local de les escoles de primària de Catalunya. Aquestes segueixen un disseny i unes característiques descrites en el projecte Heura, del qual s'estudiarà la documentació disponible. També es farà una visita a una escola per constatar el seguiment d'aquesta arquitectura i les possibilitats reals de connexió dels nodes.
- **Objectiu 2.** Estudiar l'ús de la Raspberry Pi com a element central del kit de sensors, enfocant-me en la connectivitat d'aquest dispositiu en una aula de primària i la transmissió de dades cap a internet.
- **Objectiu 3.** Dotar al node de sensors d'un sistema per monitoritzar el funcionament d'aquests nodes mitjançant un sistema GIS[1], desenvolupant tant el *front-end* com el *back-end*, i el protocol de comunicació dels nodes cap al sensor.

[1] GIS: Sistema d'informació geogràfica

2 Antecedents

2.1 *IoT* a les aules

Des de l'aparició de les primeres eines tecnològiques s'han volgut implementar elements de gestió i control en els diferents espais on habiten les persones. Les escoles al ser centres de desenvolupament tant personal com acadèmic, són uns dels llocs en que més interès ha tingut ficar aquests tipus de tecnologies.

El terme *Internet of Things* o *IoT* com em referiré en tot aquest estudi, és un concepte que ve de l'anglès que significa internet de les coses. La seva definició és l'agrupació e interconnexió de dispositius i objectes a traves d'una xarxa de computadors, on ells puguin interactuar, ja sigui amb l'entorn (encenent un llum) o internament (emmagatzemant/enviant dades d'un sensor).

2.1.1 Història

El terme *IoT* va aparèixer per primera vegada a finals de la dècada dels 90, des de llavors ha estat una tecnologia en desenvolupament utilitzada en múltiple llocs.

En els primers anys d'aquest segle es va començar a implementar de forma massiva la tecnologia RFID, ho fa per exemple el departament de defensa del Estats Units i els magatzems de grans companyies com *Walmart*. [1]

El 2005 la ITU (*International Telecomunications Union*) publica el seu primer estudi sobre el tema fent que sigui un element d'estudi més a tractar. El mateix any neix una de les empreses més influents en aquest sector: Arduino.

Des de llavors múltiples empreses han treballat per entrar en el mercat de la IoT, algunes d'aquestes poden ser: *Cisco, Raspberry Pi, Google, Motorola*...

A dia d'avui és un àmbit que dona molt per investigar, es pot seguir desenvolupant per poder trobar noves vides d'investigació i d'actuació, però també es pot utilitzar com a eina per altres objectius com a recol·lector de dades per a diferents projectes, monitorització d'elements, etc... Al ser una tecnologia molt utilitzada en els darrers anys hi ha molta documentació disponible i una comunitat molt gran a internet de gent amb molts projectes *Open Source* que es poden utilitzar per a les diferents necessitats que es tinguin.

2.1.2 Smart Classrooms

Des de ja fa ja un temps la integració de la *IoT* a les escoles i l'aprenentatge integrant les noves tecnologies i nous mètodes d'investigació i docència estan donant lloc al terme *Smart Classroom.*

Segons l'article [2] una *smart classroom* és un espai d'aprenentatge dissenyat a partir d'un procés de codiseny que articula la dimensió pedagògica amb la dimensió ambiental i digital. Aquests espais permeten l'aprenentatge a partir del benestar de totes les persones que habiten i responen a qualsevol necessitat pedagògica.

Aquesta integració pedagògica ve donada moltes vegades per la integració de les tecnologies de la informació i la comunicació. En aquest apartat em centraré en aquestes tecnologies i com poden ajudar a l'aula.

Es poden trobar diferents explicacions del terme *smart classroom,* en l'anterior article, hi parlen de manera pedagògica i de la manera d'explicar i ensenyar. Es poden trobar altres vistes de les classes intel·ligents que afegeixen nous reptes tecnològics, i donen solucions.

En l'article [3] es defineix les *smart classroom* com espais educatius equipats amb tecnologia en diferents sentits, des de la incorporació de dispositius digitals i software d'ensenyament fins a la inclusió de xarxes de sensors que ajuden a monitoritzar els processos de la classe, recollint informació i processant-la. Actuant per oferir les millors condicions d'aprenentatge i ensenyament. En aquest mateix article es mostra en els seus diferents apartats les diferents tecnologies que es poden utilitzar per aconseguir aquest objectiu. Les més interessants sota el marc d'aquest projecte de fi de grau són:

- Un dels objectius de les *smart classrooms* es treballar sota d'un model d'educació sostenible (ESD, *Education for sostenible development*). Segons l'article es pot definir com un replanteig de l'espai físic i virtual d'ensenyament que habilita els entorns d'ensenyaments adaptatius, personalitzats i intel·ligents.
- Explica el funcionament tecnològic de les aules, parlant de dispositius per a l'ensenyament, ja siguin directament del centre o amb el concepte BYOD (*Bring your own device*) que integra dispositius dels estudiants per a l'*smart learning*. Un dels elements explicats i que pot guardar més relació amb el treball és la implementació de sensors per a monitoritzar diferents paràmetres de l'aire, d'entre ells el $C0_2$ ja que influeix directament en la capacitat d'estudi dels alumnes.

En el llibre [4] en l'apartat "*Presente y futuro de las condiciones ambientales en las smart classroom*" destaquen també la importància de les aules en el desenvolupament i rendiment dels estudiants. Destaca la creació de la aula intel·ligent que es defineix a traves de tres característiques definides per:

- La tecnològica
- La de processos
- La ambiental

En els diferents articles que s'han mostrat puc concloure que tots es fiquen d'acord amb la utilització de tecnologia per a augmentar el rendiment de les aules, sistemes per millorar els processos i rendiment de l'estudi i el control ambiental de l'aula per garantir la major comoditat dels seus ocupants i reduir les distraccions que poden arribar a produir-se en el moment de l'ensenyament.

2.2 Projecte ACTUA

En el projecte ACTUA (Anàlisis contextual dels factors de mitigació de la transmissió de la COVID-19 en l'aUIA) s'estudia la transmissió del virus de la COVID-19 en les aules de les escoles d'educació infantil i primària.

Les aules són espais tancats amb una concentració molt gran de gent. La COVID-19 és un virus de transmissió respiratòria i al concentrar-se gent de moltes unitats familiars i de nuclis diferents, les aules són un motor molt gran per a la transmissió de la malaltia.

L'objectiu del projecte és mesurar les dades de la qualitat de l'aire a les aules, com les d'humitat, temperatura i nivell de so. Ajuntant aquestes amb les dades de contagis es pot desenvolupar un model per veure la relació de transmissió amb els contagis a les escoles.

L'aplicació del projecte ACTUA dins de l'àmbit de les telecomunicacions es la implementació del kit de sensors necessari per a mesurar diferents elements de les aules de les escoles públiques de Catalunya. Com pot ser la temperatura, la humitat el CO_2 del aire...

S'ha decidit que per a la integració d'aquest kit s'utilitzarà una Raspberry Pi, explicat en l'apartat 3.1. Aquesta Raspberry Pi podrà treballar amb diferents sensors i connexions per a poder fer la tasca que ha de desenvolupar correctament. El conjunt d'aquest dispositiu i els sensors que pugui tenir connectats

l'anomenaré de diferents maneres al llarg del projecte i totes exemplifiquen el mateix: kit de sensors, Raspberry Pi, kit...

En aquest treball em centraré principalment en l'estudi i la implementació del kit de sensors dins de la xarxa d'una escola. Tenint en compte tot el procés que les dades tindran, des de que són recollides per el sensor fins a que l'investigador principal del projecte vol treballar amb elles.

Per a tenir una estructura clara de la distribució de la xarxa que formaran tots aquests kits de sensors, ens podem basar en un model a capes per treballar en els diferents aspectes del sistema. Aquestes capes es poden separar per la funció que fan:

- **Capa 1**: Capa de percepció de dades

- **Capa 2**: Capa d'intercanvi de dades

- **Capa 3**: Capa de sistemes i serveis d'informació o de software

En els següents apartats donaré context a cada capa i en la longitud del treball explicaré en detall els elements necessaris de cadascuna per a la seva implementació dins de la xarxa estudiada.

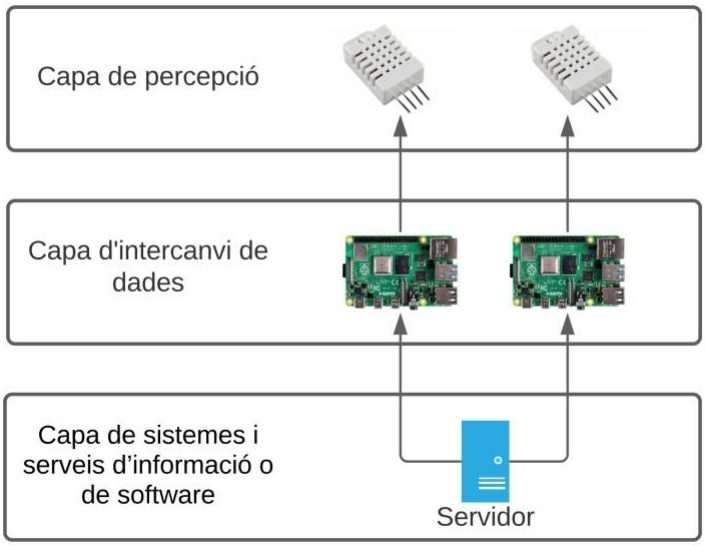

***Figura 1** - Model de tres capes*

2.2.1 Capa de percepció

La capa de percepció són tots aquells elements que envolten el recull de dades del medi físic, ja siguin els mateixos sensors, les connexions entre ells, l'alimentació dels dispositius, etc.. En aquesta capa i en el àmbit del treball només ens centrarem en els tipus de sensors en que es treballaran.

Els sensors poden ser de molts tipus i amb molts protocols de comunicació diferents, en l'apartat 3.2 es discutiran els diferents tipus de sensors i extreure conclusions per al millor tipus de sensor que s pot utilitzar dins del marc del projecte ACTUA.

2.2.2 Capa d'intercanvi de dades

Aquesta capa es pot distingir com la de xarxes i dades d'internet, en aquest cas aquest estudi es centra en el desenvolupament d'aquesta capa. Des del punt de vista de la trama Ethernet que pugui generar el

dispositiu per enviar les dades fins a la ruta que aquesta pren a través de la xarxa escolar i posteriorment a internet.

En apartats següents explico en profunditat tota la infraestructura de xarxa de les escoles públiques de Catalunya, les tecnologies que implica el funcionament d'aquestes i com implementar la connexió del kit de sensors amb aquesta xarxa estudiada.

Es pot tindre en compte les futures tendències que poden tenir aquestes xarxes, com la implementació de ipv6 o del 5G per a la seva millora i un funcionament més eficient.

2.2.3 Capa de sistemes i serveis d'informació o de software

Aquesta capa involucra tot el relacionat amb els elements de programari necessaris per a fer funcionar i mantenir el sistema. Podem distingir dos elements:

- **Producció o funcionament**: Tot el software que s'implantarà per al funcionament dels diferents sistemes, tan sigui en la recol·lecció i enviament de dades, com el processat d'aquestes.
- **De manteniment**: És el software necessari per al manteniment dels sistemes i per la revisió del seu correcte funcionament un cop estiguin implementats tots els sistemes necessaris.

En propers apartats es discutirà i s'estudiarà amb més profunditat tot els temes de les diferents capes.

3 Estudi del kit de sensors i les seves característiques

3.1 Raspberry Pi

Les Raspberry Pi són una sèrie d'ordinadors de placa reduïda o ordinadors de placa simple de baix cost desenvolupat en el Regne Unit per *Raspberry Pi Fundation* [5], amb l'objectiu de ficar en mans de les persones de tot el mon la informàtica i la creació digital.

La Raspberry Pi és la placa d'un ordinador simple compost per un SoC[2], CPU, memòria RAM, ports d'entrada i sortida, sortida d'àudio i de vídeo, un port d'alimentació, USB i entrada Ethernet amb connector RJ45. Això sí, no té interruptor d'encendre i apagar.

Darrera de tots els elements físics que pot tenir aquest dispositiu hi ha una comunitat de gent que diàriament està fent programari lliure que pot ser utilitzat per milers de persones arreu del món i fa que tot el ecosistema de la Raspberry Pi funcioni correctament.

En el cas del projecte ACTUA s'utilitzarà la Raspberry Pi 4 model B, que té les característiques més modernes i és la més versàtil a l'hora de desenvolupar les funcions necessàries pel treball. Podem fer una comparació ràpida amb totes les plaques que actualment estan a la venta:

Model	**CPU**	**RAM**	**Data**	**Preu**
Model A	700MHz ARM1176JZF-S	256MB	04/2012	25$
Model 3B	1,2GHz QUAD ARM Cortex-A53	1GB	02/2016	35$
Model 4B	1,5GHz QUAD ARM Cortex-A72	2,4 o 8GB	06/19	35$

Taula 1. *Comparació de models de Raspberry Pi. Taula simplificada de [6]*

En l'anterior taula podem veure que hi ha molts models diferents que es poden adaptar a necessitats diferents. En el cas del projecte s'està utilitzant el **model** de 2 GB de memòria RAM, ja que per a la compilació del codi necessari i les funcionalitats de xarxa que es requereixen és suficient, fent així un abaratiment del cost final d'instal·lació.

Al llarg d'aquest treball amb les diferents proves que s'han realitzat físicament he estat utilitzant el model 4B amb 2GB de memòria RAM i un emmagatzematge de 32GB.

3.1.1 Hardware

A Nivell de Hardware la Raspberry Pi [5] és un ordinador molt senzill, en el seu model més bàsic no te cap caixa i es manipula directament sobre el circuit imprès. Aquest circuit té totes les connexions necessàries per a fer ús del sistema.

Com a elements d'entrada i sortida la Raspberry té:

- 802.11 b/g/n/ac Wireless LAN
- Bluetooth 5.0 with BLE

[2] SoC: System on a chip, integració de tots els elements de computació dins d'un mateix chip

- 1x SD Card
- 2x micro-HDMI
- 2x USB2 ports • 2x USB3 ports
- 1x Gigabit Ethernet
- 1x Raspberry Pi càmera port (2-lane MIPI CSI)
- 1x Raspberry Pi display port (2-lane MIPI DSI)
- 28x GPIO pins a disposició de l'usuari

L'últim element és un dels més importants respectiu al elements d'entrada i sortida, ja que són uns pins que permeten l'entrada de dades i programació de dispositius externs com poden ser sensors, càmeres, etc.

El GPIO (*General Purpose Input Output*) és un sistema d'entrada i sortida de propòsit general, es a dir, consta d'una sèrie de pins o connexions que es poden utilitzar com entrades i sortides per a múltiples usos. Aquests pins estan inclosos en tots els models de la Raspberry pi esmentats en la **Taula 1.** Comparació de models de Raspberry Pi. Taula simplificada de [6]

Una manera de comprovar el pin en que volem treballar és consultant al *datasheet* i buscant l'esquema de pins d'entrada i sortida o bé consultant-ho dins de la mateixa Raspberry Pi des de el Terminal amb la comanda: `gpio readall` :

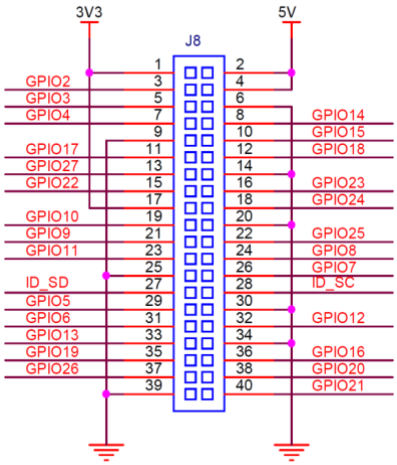

***Figura 2**. Pins GPIO Raspberry Pi 4*

3.1.2 Software

La Raspberry Pi al ser un ordinador complet amb arquitectura ARM pot carregar qualsevol sistema operatiu dissenyat per a aquesta família de processadors. El sistema operatiu s'encarrega de gestionar i assegurar els recursos del hardware del sistema i donar serveis per fer funcionar les aplicacions que l'usuari fica a executar. Els 5 sistemes operatius més importants per a la Raspberry Pi son:

- Raspberry Pi OS (Raspbian)[7]
- Windows 10 IoT Cores[8]
- LibreELEC[9]
- RetroPie[10]

En aquest projecte utilitzarem Raspbian que és el sistema operatiu oficial i esta mantingut pels propis desenvolupadors que dissenyen els ordinadors. Aquest sistema operatiu esta basat en la distribució de Linux, Debian, en aquest cas tant el sistema de fitxers com molts dels paquets necessaris funcionen de manera similar.

Aquesta distribució està optimitzada per funcionar en equips que es basen en processadors d'arquitectura ARM[3]. Raspbian inclous varis paquets i programes de manera nativa, com pot ser la interfície gràfica que utilitza la PIXEL[4]. D'aquest sistema operatiu hi ha tres versions:

- **Completa**: És la que inclou la interfície gràfica PIXEL i diferents programes ja instal·lats per a fer diferents tasques com programar, navegar per internet... Degut a tot el software addicional que conté, aquesta versió pesa sobre uns 3GB.
- **Estàndard**. Segueix tenint l'escriptori PIXEL i els programes bàsics. En aquesta versió s'ha eliminat el software opcional, tot s'ha d'instal·lar manualment. Pesa al voltant d'1GB.
- **Lite**: En aquest cas només disposem d'una línia de comandes en la que podem interactuar amb la distribució. És la versió més petita ja que només pesa 400MB.

Per al projecte ACTUA s'utilitza la versió completa, tot i que el seu funcionament un cop configurat tot el software necessari, no varia entre les versions i per tant les simulacions o les integracions de sensors no afecten segons la versió del programari que s'utilitzi.

A banda del sistema operatiu, la Raspberry és un dispositiu dissenyat majoritàriament per a crear programari i fer funcions que un ordinador normal seria capaç però que per cost i volum no tindria sentit. Unes de les eines més importants que es poden fer servir són les llibreries especialitzades per poder treballar amb qualsevol llenguatge (Java, python, C) i poder-se comunicar amb els pins GPIO de la placa. En l'apartat 3.3 discutiré més a fons sobre el tipus de software que ens trobem en la Raspberry i com utilitzar-lo.

3.2 Sensors utilitzats

Per a escollir un sensor primer s'ha de categoritzar els elements que hi ha disponibles avui en dia en el mercat i com els podem adaptar al projecte.

Hem de trobar el sensor que més ens convingui per utilitzar dins del marc del projecte. Aquests tipus de sensors han de ser fàcils de muntar, amb un manteniment baix i amb una connexió fiable ja que geogràficament poden estar en molts llocs diferents. Podem distingir tres tipus de sensors diferents:

- **Categoria 1**: Sensors analògics digitals amb connectivitat directa. Aquest sensors van connectats directament a la placa. Nosaltres treballarem amb Raspberry pi i en un entorn controlat on haurem de repetir moltes vegades el kit de sensors que s'instal·larà en les escoles.

[3] ARM: Advanced RISC Machine, és una arquitectura RISC (Reduced Instruction Set Computer) de 32 i 64 bits. Són processadors simples de baixa potencia ideals per a funcions IoT.

[4] PIXEL: Pi Improved X-Window Enviornment Lightweight. Escriptori minimalista utilitzat en la distribució de Raspbian.

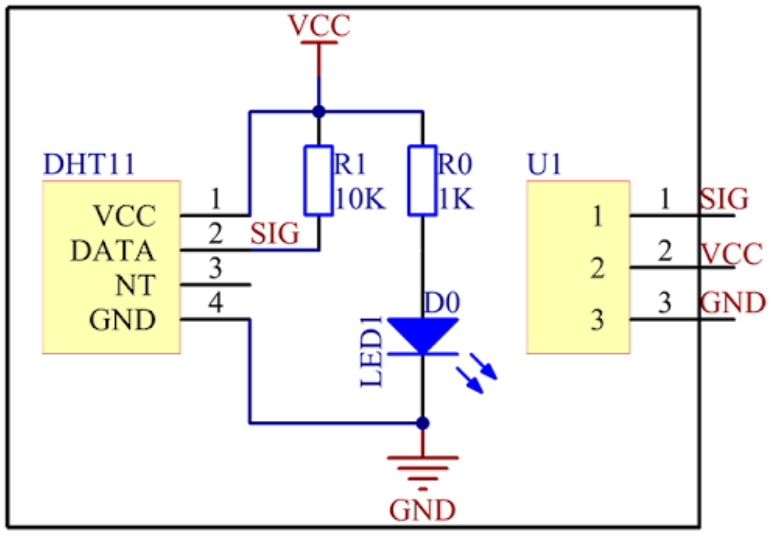

Figura 3. Composició sensor DHT11 [11]

- **Categoria 2**: Sensors de baix cost amb connectivitat Bluetooth. Tenen una connexió sense fils mitjançant aquest protocol que a vegades depenent del entorn en que es fiquin i de les interferències del espectre electromagnètic en aquell espai pot funcionar a poc rendiment, avui en dia generalment van connectades directament a una aplicació mòbil.

- **Categoria 3**: Sensors que tenen connectivitat TCP/IP capaços de muntar i enviar paquets de xarxa per a fer un enviament de les dades a internet, generalment al núvol de cada companyia fabricadora d'aquests sensors.

En el projecte ACTUA **el millor tipus de sensors són els de categoria 1**, ja que són els més robusts, els més manipulables i els que tenen un cost més baix. Aquesta conclusió s'extreu a partir de de la taula d'avantatges i inconvenients dels 3 sensors:

	Avantatges	**Inconvenients**
CAT 1	- Baix cost - Connexió fiable (sobretot si es pot arribar a soldar) - Solen ser petits i amb molta documentació per treballar amb RBPI4 - Consumeix pocs recursos	- Si es trenquen s'han de canviar manualment - Difícil de detectar un error (sobretot en el pla del projecte on hi ha molts en remot)
CAT 2	- Pots tenir altres formes de treballar amb aquest sensor (aplicació al telèfon) - No han d'estar físicament juntes amb la RBPI4	- Val més diners - Entorn generalment més tancat. - Difícils de mantenir si deixa d'haver suport del fabricant

CAT 3	- Per a un ús domèstic o amb pocs sensors pot funcionar correctament	- Un cost molt elevat per el que ofereixen - Solen estar vinculats al suport que els hi dona la companyia que els produeix

***Taula 2**. Comparació de les diferents categories de sensors*

3.3 Programari

Per a fer possible la utilització dels sensors esmentats es necessita un programari que ens permeti modificar el comportament d'aquests, rebre i enviar dades.

Aquestes feines les podem desenvolupar programant el software necessari amb un llenguatge de programació. Actualment el més popular envers la Raspberry Pi és *Python*, tot i que es pot utilitzar qualsevol altre llenguatge que pugui ser compilable en l'arquitectura del processador.

Un **IDE** és un **entorn de desenvolupament integrat** ("*Integrated Development Enviroment*"). És l'escenari digital utilitzat en programació per desenvolupar l'aplicació. Aquests poden anar-hi des de simple editors de text amb un compilador de codi, com a programes amb eines de pausa de codi, simulació de dispositius i altres elements. En el cas de la Raspberry Pi el IDE que ve instal·lat per defecte en el sistema operatiu amb més característiques és el *Thonny* [12] IDE, el qual ens permet treballar amb *Python* i executar el seu codi.

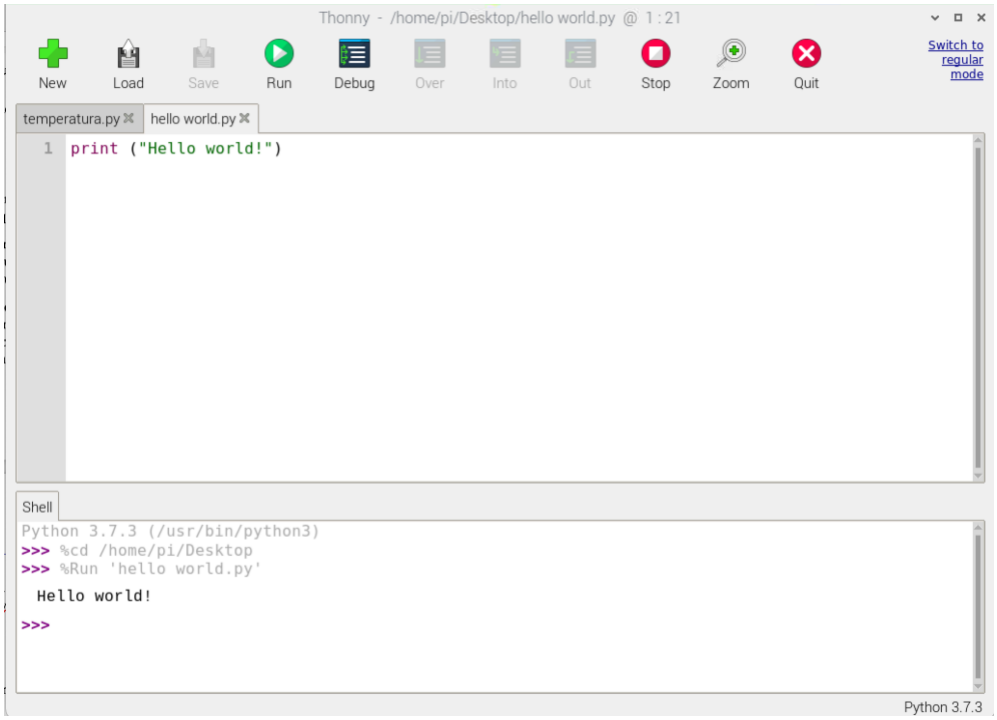

***Figura 4**. Interfície gràfica Thonny*

En aquest cas es pot veure un espai gran on es pot escriure tot el codi necessari per a fer les funcionalitats necessàries. Eines per treballar amb el codi a la part superior i una consola de comandes en la part inferior.

Al Raspbian OS al ser de programari lliure es pot treballar amb molts altres desenvolupadors de codi.

3.4 Manteniment del kit de sensors

El manteniment d'aquest sensors és un punt molt important dins del seu correcte funcionament, ja que te molts elements que en algun moment o altre puguin anar malament. S'ha de tenir en compte però que per a fer el manteniment d'aquest kit s'ha de fer de la manera més segura possible (parlant des del punt de vista informàtic) i respectant totes les normatives de protecció de dades que hi ha vigents.

Segons la llei de protecció de dades BOE-A-2018-16673 [13] s'ha de anar amb cura a l'hora de tractar les dades. Aquestes han de viatjar per la xarxa d'una manera encriptada i que no pugui desvelar autories ni alguna informació del centre escolar en la que es treballa. Donades totes aquestes dades i com es veurà en l'apartat 4 d'aquest treball la tasca de manteniment creix una mica, ja que per configuracions del centre no podem accedir remotament al kit de sensors, ja que s'hauria de tenir un forat obert en la xarxa per a treballar remotament deixant una vulnerabilitat oberta en la xarxa fent possible un atac que vulneri tota la protecció de dades existent.

Hi ha certs tipus de programes que poden treballar amb la gestió remota de dispositius, de fet, un dels plantejaments inicials d'aquest treball era utilitzar un d'aquests. Podem fer una comparació ràpida entre alguns que hi ha al mercat.

	Avantatges	**Inconvenients**
Remoteit [14]	- Escalable en Raspberry pi - Treball sense conèixer la IP i amb molts protocols - Pot tenir links amb dominis	- Amb molts elements té una subscripció de pagament - Analitzat poc
DWService [15]	- Escalable en Raspberry i dispositius infinits - Treballa sense conèixer la IP - Treball des de navegador	- Servei al núvol i no es sap del cert quina informació utilitzen.
TeamViewer [16]	- Mes generalitzat - Molts usuaris	- S'ha de tenir Ubuntu instal·lat a la Raspberry

***Taula 3**. Comparació programes de manteniment*

A priori sembla una gran opció i que es podria fer un manteniment correcte sense infringir cap llei respecte a la protecció de dades i tindríem un lloc segur per a les dades de viatge. El problema però es que aquests programes necessiten de la validació d'un servidor extern per a poder treballar amb aquest servei de connexió remota. Aquest servidor no està controlat per el projecte ACTUA i per tant, no es sap com o que emmagatzema quan es fa la connexió remota amb els diferents nodes o kits de sensors. Per tant, aquesta opció és descartada.

El projecte ACTUA planteja fer un curs de formació a les escoles per a que hi hagi un encarregat del manteniment d'aquest kit de sensors i que al ser possible sigui aquesta persona capaç de resoldre

qualsevol inconvenient que pugui sorgir a l'hora de fer funcionar aquest kit. Aquesta persona podrà estar en contacte amb els tècnics del projecte per a qualsevol problema que pugui sorgir i que no estigui en les seves capacitats ser reparat. El projecte es planteja l'ús de les respostes HTTP dels mètodes POST per a enviar certes comandes per a modificar ítems de la configuració de la Raspberry sense tenir que accedir remotament en aquesta.

3.5 Seguretat i vulnerabilitats en el kit de sensors

En el món digital en el que vivim cada vegada més es necessita una seguretat major en els dispositius connectats a la xarxa que puguem arribar a utilitzar. Per tant, al saber que el kit de sensors està connectat a internet s'han de tenir en compte certes mesures que s'han de seguir per protegir aquest kit de possibles amenaces. En aquest apartat ens centrarem en la seguretat i vulnerabilitats que es puguin ocasionar dins del kit de sensors, a base del maquinari de la Raspberry pi i del sistema operatiu que aquesta pugui estar fent servir.

Segons l'article [17] ens poden trobar alguns problemes de seguretat tant en hardware com en software. Alguns d'aquests problemes són fàcilment adreçables i d'altres no tenen solució si no es canvia algun component físicament.

Si parlem de hardware i segons l'article tenim els següents problemes:

- **Alimentar** la Raspberry per **USB**. En certes aplicacions cal alimentar dispositius externs amb el bus USB de la Raspberry. Aquest, pot ser alimentat al reves, és a dir, que des de un alimentar USB extern estem donant corrent al dispositiu. Aquest, no te protecció USB, per tant, si es dona una corrent molt alta pot destruir el processador sencer.
- **Augmentar** la **freqüència** de rellotge del processador. Aquesta és un tècnica que s'utilitza sovint, el problema és que la Raspberry quan arriba als 85ºC la pujada de freqüència s'atura. Es poden canviar els valors que es queden dintre del chip i fer que aquest llindar no es compleixi, trencant així el dispositiu.
- **Pins GPIO:** Els pins en que es poden connectar els sensors de la Raspberry tenen una corrent màxima de 3.3V, si s'alimenten amb una corrent superior poden danyar el bloc controlador d'aquests pins.

Poden haver-hi altres vulnerabilitats o debilitats depenent del model de la Raspberry que s'estigui fent funcionar.

Parlant de software i tornant a referenciar l'article, podem trobar diversos problemes. Com s'ha discutit en el apartat 3.1.2 hi ha molts tipus de sistemes operatius, dels mes important són el *Raspbian* i el Windows IoT:

- **Raspbian:** La gran facilitat d'instal·lació d'aquest sistema operatiu es un dels seus majors problemes ja que aquesta instal·lació proporciona un usuari i contrasenya comuns a totes que després es pot canviar dins del sistema operatiu. Segons l'article, fent un estudi amb l'eina *nmap* es pot trobar un port obert (22) amb el servei *ssh*, amb les versions més noves i sense cap vulnerabilitat.
- **Windows IoT:** Aquest sistema operatiu també dona una contrasenya i usuari d'administrador per defecte, fent-lo en aquest cas similar al cas del sistema oficial. La instal·lació estàndard d'aquest sistema operatiu deixa oberts els ports 21(FTP), 22(SSH), 135(RPC), 445(Samba), 4020(remote debug), 5985 (remote management), 8080(servei web), 9955(AllJoyn) i

47001(WinRM). El mes perillós es el servei FTP[5] ja que es un servei anònim i que dona permís de lectura i d'escriptura a la Raspberry, fent que qualsevol persona tingui accés al dispositiu i pugui modificar qualsevol configuració si amb anterioritat no s'ha marcat una contrasenya per aquest servei.

[5] FTP: File Transfer Protocol: Protocol de transferència de fitxers a través de la xarxa que s'usa normalment per a baixar i pujar fitxers de dispositius remots.

4 Estudi de la infraestructura de xarxa d'una escola

Un dels punts més importants en el desenvolupament del projecte ACTUA i el motiu principal d'aquest treball de fi de grau és la connexió del kit de sensors en qualsevol de les xarxes escolars en les que es pot treballar.

L'objectiu d'aquest apartat és descobrir les topologies d'aquestes xarxes, estudiar-les i trobar el millor punt de connexió del kit de sensors per a fer les funcionalitats que es requereixen. Es treballarà amb xarxes només d'escoles públiques, les quals venen regulades per la generalitat de Catalunya i el Departament d'Educació, per tant, i donada la similitud, en fer l'estudi de la documentació disposada obtindrem la informació de la configuració de xarxa de totes les escoles públiques de Catalunya.

El projecte HEURA [18] completa la disposició de les infraestructures de cablatge estructurat i Wi-Fi a tots els centres docents i serveis educatius dependents del Departament d'Educació. L'objectiu de l'actuació és subministrar les infraestructures necessàries per a fer arribar la banda ampla a tots els espais docents dels centres considerats. Aquest projecte té com a objecte la explicació tècnica de:

- **La cobertura Wi-Fi**. Tant la infraestructura física com la lògica. L'accés a la xarxa sense fils es farà a través de punts d'accés (AP), que s'integraran adequadament al sistema de cablatge general. Estarà basat en autenticació amb clau compartida (WPA-PSK), xarxa local del centre i en WPA amb validació *Radius* en qualsevol servidor de la xarxa *eduroam*.
- **El cablatge estructurat**. Passant per les connexions físiques RJ45, com amb els elements de xarxa generals que la conformen (Encaminadors, commutadors...).
- **La xarxa elèctrica**: Instal·lació elèctrica independent al cablatge estructurat i que fa funcionar tota la maquinària de xarxa.

En aquest apartat em centraré en els dos primers aspectes esmentats, valorant totes les seves configuracions i accés a internet que ens poden aportar si connectem la Raspberry Pi directament a qualsevol d'aquests punts. Es tindrà en compte però l'últim punt ja que si la infraestructura de xarxa no disposa de dispositius *PoE*[6], s'haurà de buscar un endoll per poder alimentar elèctricament el kit de sensors.

4.1 Projecte HEURA

El projecte HEURA [18] te com a objectiu donar les eines per a que estudiants i docents puguin tenir una connexió a internet amb una garantia, seguretat i fiabilitat adequades. Aquest projecte contempla diferents tecnologies per a realitzar la comunicació i diferents escenaris com el de les escoles rurals amb poca infraestructura fins a elles, escoles grans i petites.

El projecte posa a disposició d'alumnes i docents varies maneres de connectar-se. Ja sigui per una xarxa sense fils o directament a la xarxa amb fils. Per a saber les característiques de cada una hem de mirar el protocol que composen cadascun d'aquestes formes de connexió d'una manera tècnica i detallada.

- La connexió pel protocol **Wi-Fi** (IEEE 802.11)
- La connexió per parell trenat **Ethernet** (IEEE 802.3)

[6] PoE: Power over Ethernet: És una tecnologia que incorpora l'alimentació elèctrica a una infraestructura LAN estàndard

4.1.1 Wi-Fi (IEEE 802.11) a la xarxa sense fils

El protocol IEEE 802.11ac, és un estàndard que permet la interconnexió sense fils de dispositius electrònics. Els dispositius habilitats amb Wi-Fi (ordinadors, tauletes educatives, projectors, etc...) poden connectar-se a una LAN i a internet a traves d'un punt d'accés (AP).

Wi-Fi és una marca de la *Wi-Fi Alliance*, l'organització comercial que compleix amb els estàndards 802.11 relacionats amb la WLAN[7]. L'última versió en la que s'està treballant és la Wi-Fi 6 (802.11ax).

Les xarxes Wi-Fi utilitzen dos bandes de freqüència diferents, una compresa entre 2400 a 2483,5MHz, a la que denominem banda 2.4GHz i una altra compresa entre els 5150 a 5725 MHz, a la que denominem banda 5GHz.

La banda de 2.4GHz té compresos un total de 13 canals de 20 MHz d'ample de banda que es solapen entre ells. És per això que es sol dir que d'aquests 13 canals nomes podem utilitzar 3, ja que és la única distribució de canals que no es solapen entre ells com es pot veure en la següent figura:

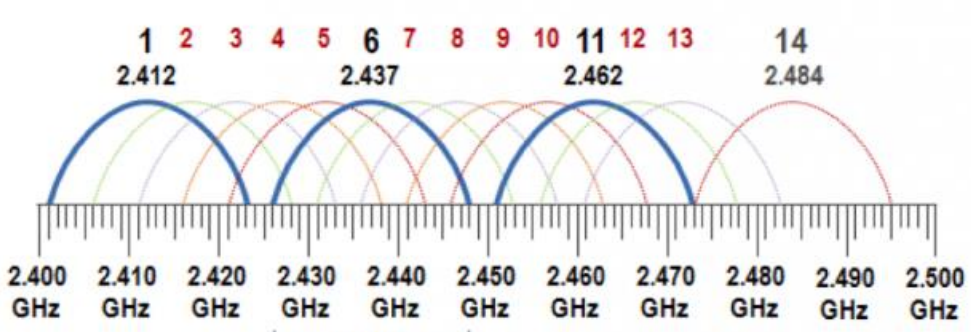

***Figura 5**. Canals Wi-FI banda 2.4GHz [19]*

La banda de 5 GHz compren un total de 19 canals de 20MHz de ample de banda i que no es solapen entre ells. Això ens permet l'ús de tots en la nostra xarxa Wi-Fi.

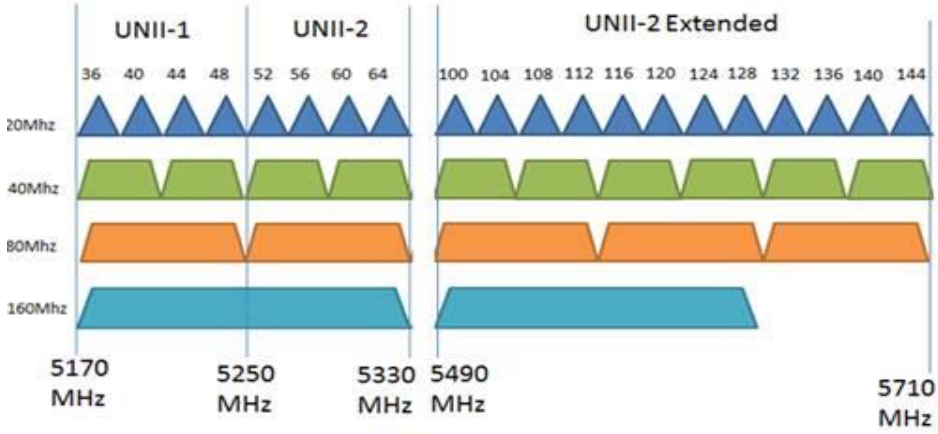

***Figura 6**. Canals Wi-FI banda 5GHz [19]*

[7] WLAN: Wireless Local Area Network, xarxa d'area local sense fils

Si agrupem dos o més canals en un canal de més capacitat, estem creant un *bonding channel*. Aquesta agrupació de canals ens permet aconseguir velocitats més altes.

Sabent que el protocol de Wi-Fi 6 està encara en poques aplicacions, podem fer una comparativa dels dos protocols:

	Wi-Fi 5 (802.11ac)	**Wi-Fi 6 (802.11ax)**
Bandes de treball	2.4GHz i 5GHz	2.4GHz i 5GHz
Banda ampla del canal	20, 40, 80, i 160 MHz	20, 40, 80, i 160 MHz
Modulació més alta	256QAM	1024QAM
Velocitat de transmissió	433 Mbps (80MHz) amb una màxima de 7000 Mbps	600 Mbps (80MHz) amb una màxima de 10000 Mbps

Taula 4. *Comparació Wi-Fi 5 i 6*

Sabent així que en el cas del projecte on hi hauria la connectivitat optima seria en punts d'accés que treballessin amb el protocol 80.11ac en la banda del 5 GHz trobant una major velocitat de dades, una major fiabilitat i menys col·lisions en els canals que retransmeten la informació.

4.1.2 Ethernet (IEEE 802.3) xarxa cablejada

Ethernet és l'estàndard de xarxes d'àrea local (LAN) o una xarxa de llarg abast (WAN). La versió mes actual d'aquest estàndard és la 802.3an tot i que hi ha d'altres que estan en desenvolupament. Aquesta tecnologia descriu com els dispositius de xarxa poden empaquetar les dades i enviar-les, passant des de de el nivell físic al nivell d'enllaç de dades.

En una xarxa Ethernet cada dispositiu se li assigna una direcció pròpia MAC de 48 bits[20]. Els membres de la xarxa poden transmetre missatges amb alta freqüència. La comunicació mútua entre els elements s'utilitza l'algorisme CSMA/CD. Tot i que avui en dia amb aquest algorisme ja s'eviten totes les col·lisions que puguin haver-hi de trames dins del medi, inicialment el fonament en que es basava en el següent procés per enviar una trama dins del medi.

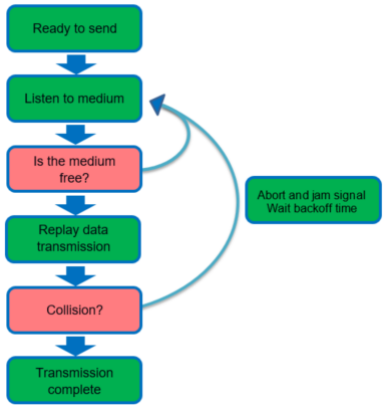

Figura 7*. Enviament trama Ethernet [17]*

Aquesta tecnologia al treballar al nivell físic i al nivell d'enllaç té moltes característiques úniques. Si parlem de l'aspecte físic s'ha de parlar del cable. Generalment s'ha utilitzat cable de coure trenat amb

connectors RJ45 per a fer les connexions d'aquestes xarxes tot i que la fibra òptica també pot utilitzar aquest protocol. L'estàndard Ethernet ha anat evolucionant durant els anys fent que tingui més característiques tant de longitud de cable com velocitat de transmissió, en la següent taula podem veure la comparativa.

Estàndard	Denominació	Velocitat de transmissió	Cablejat	Any de publicació
802.3	10 Base5	10 MB/s	Coaxial	1983
802.3a	10 Base2	10 MB/s	Coaxial	1988
802.3i	10 Base-T	10 MB/s	Parell trenat	1990
802.3j	10 Base-FL	10 MB/s	Fibra òptica	1992
802.3u	100 Base-TX FX i SX	100 MB/s	Parell trenat i F.O	1995
802.3z	1000 Base-SX i LX	1 GB/s	Fibra òptica	1998
802.3ab	1000Base-T	1 GB/s	Parell trenat	1999
802.3ae	10 Base-SR, SW, LR, LW, ER, EW, LX4	10 GB/s	Fibra òptica	2002
802.3an	10G Base-T	10 GB/s	Parell trenat	2006

Taula 5. *Comparativa protocols Ethernet. Taula extreta de [17]*

Actualment es treballa amb l'últim estàndard 802.3an el qual ens proporciona una longitud de cable de 100m.

A nivell de la capa d'enllaç es pot parlar sobre la trama de dades que s'envia. Aquesta trama te una longitud mínima de 72 bytes i una màxima de 1526 bytes.

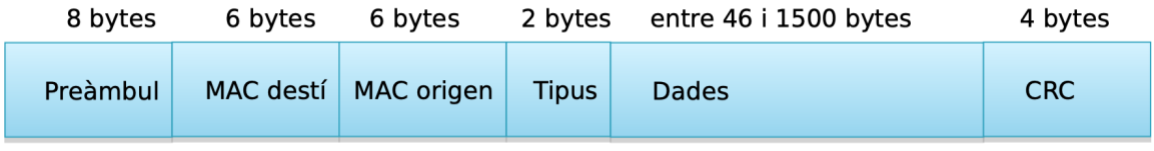

Figura 8*. Trama Ethernet [21]*

Depenent del protocol poden haver variacions de la trama, i com s'explicarà en el apartat 5.1.1 del projecte hi ha tecnologies que poden modificar aquesta trama per a oferir certs serveis o configuracions addicionals com poden ser les xarxes d'àrea local virtuals.

Un cop revisats els diferents protocols i tecnologies per les quals ens podrem connectar, podem començar a parlar de la infraestructura de xarxa. Aquesta conté tots els elements de la xarxa necessaris per a poder treballar. En els següents apartats s'explicarà en profunditat els dos aspectes que hem de tenir en compte d'una xarxa de computadors connectada a internet:

- **La topologia física**: Que engloba tots els elements físics de xarxa (ordinadors, encaminadors, encaminadors, etc...)
- **La topologia lògica**: Que engloba les configuracions de tots els elements físics, les configuracions de les VLANs i les rutes que poden fer els paquets per comunicar les diferents màquines.

4.1.3 Topologia física

Els elements tangibles que conformen la xarxa són una part essencial d'aquesta. S'han de buscar elements robusts, amb una eficiència energètica acceptable i que siguin capaços de gestionar el tràfic de xarxa corresponent dins de les necessitats de cada instal·lació.

Les xarxes es dissenyen seguint un model jeràrquic amb l'estructura de maquinari, el projecte HEURA esta dissenyat sota un model així. Ens podem basar en el model jeràrquic *Cisco* [22] per a saber les diferents capes d'actuació:

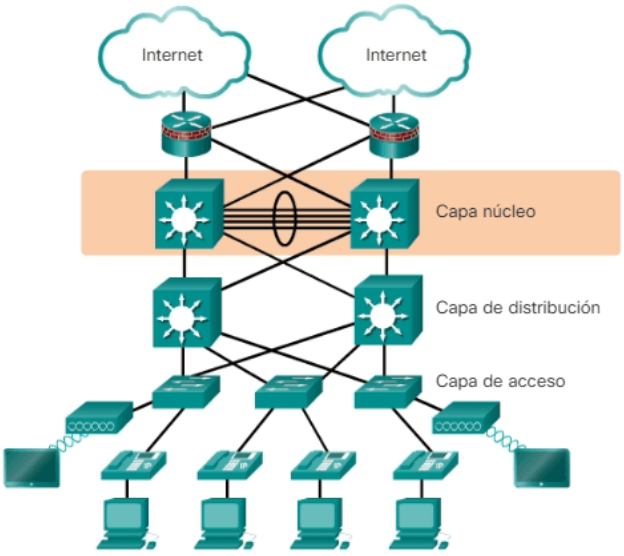

Figura 9. *Model per capes Cisco [22]*

- La capa **nucli** també es coneix com a "*backbone de xarxa*". La capa nucli consta de dispositius de xarxa d'alta velocitat. Aquests estan dissenyats per commutar paquets el més ràpid possible. Com es mostra en la figura, la capa nucli es fonamental per la connectivitat interna de els dispositius de la capa de distribució. Alguns aspectes fonamentals de la capa nucli poden ser els següents:

    - Proporcionar commutació d'alta velocitat
    - Proporcionar confiabilitat i tolerància a les fallades
    - Ha de ser escalable mitjançant equips més ràpids

- S'ha d'evitar la manipulació de paquets que impliquin una gran exigència per la CPU a causa de la seguretat, la inspecció i el QoS[8]

En el projecte HEURA i al estar tractant amb xarxes relativament petites aquesta capa nucli es tracta del encaminador que pugui haver-hi en cada escola donat per un proveïdor de serveis d'internet. Depenent de la xarxa i de la mida de l'escola es pot donar que hi hagi una redundància física amb una altra connexió. A nivell de encaminament de paquets i com indicaré en el següent apartat, no implica cap canvi que hi hagi un, dos o mes dispositius en aquesta capa.

Per tant, tot i ser de les capes més importants, al estar tractant amb una xarxa simple no cal fer un sistema redundant molt gran, així podent reduir costos de la instal·lació.

- La **capa de distribució** agrega totes les dades rebudes dels commutadors de la capa d'accés abans que es transmetin a la capa nucli per el encaminament cap al destí final. La capa de distribució es la frontera entre els paquets del nivell 2 i del nivell 3 de la capa OSI. Aquesta capa s'utilitza un commutador multinivell, en aquest cas el projecte HEURA contempla aquest tipus de hardware, en la nomenclatura del projecte es considera com a **commutador principal**. La capa de distribució ha de proporcionar els següents serveis:

  - Agregació d'enllaços LAN o WAN
  - Seguretat basada en polítiques en forma de llistes d'accés (ACL) i filtrat.
  - Serveis de Routing entre xarxes LAN i VLAN i entre dominis de Routing.
  - Redundància i balanceig de càrrega
  - Control en el domini de *broadcast* o difusió, aquesta capa no envia una difusió a tots els elements connectats a ella.

Dins del projecte HEURA s'utilitza nomes un sol commutador multicapa de nivell 3, aquest permet la interconnexió de les diferents VLANs i l'encaminament del tràfic correcte cap a la capa nucli i posteriorment cap a internet. El projecte recomana un equipament específic per a fer les funcionalitats requerides. El model DLINK DGS-3627 switch de 24 ports de nivell 3.

***Figura 10**. DLINK DGS-3627 24p*

Aquest equip farà les funcions d'encaminament dels paquets de totes les subxarxes del centre amb l'equip extern d'encaminament de la capa nucli.

- La **capa d'accés** en un entorn LAN, aquesta atorga accés a la xarxa per els dispositius finals (PCs, tauletes, etc.) Aquesta incorpora commutadors de nivell 2 i punts d'accés que proporcionen

[8] QoS: Quality of service: És el rendiment mig d'una xarxa de dades

connectivitat entre les estacions de treball i els servidors. La capa d'accés compleix varies funcions, incloses les següents:

- Commutació a nivell 2
- Alta disponibilitat
- Seguretat del port
- Classificació i marcació de QoS
- Inspecció del protocol ARP
- PoE i VLAN auxiliars.

Els elements d'aquesta capa dins del projecte HEURA són els que podem anomenar com a commutadors secundaris. Aquests tenen configurades totes les VLAN i s'encarregaren de retransmetre els paquets de nivell 2. El projecte recomana una sèrie de dispositius per a aquest ús també de la marca DLINK. Els seus models respectius son:

- **DES-3526**: (**Figura 11**) De 24 ports 10/100 + 2 ports 10/100/1000. Fa la funció de commutador dels paquets de tots els usuaris repartits per les subxarxes que gestiona la capa de distribució amb el commutador de nivell 3.

Figura 11. DES-3526 24p

- **DES-3026**. 24 ports 10/100 Nivell 2.

Figura 12. DLINK DES-3026 24p

Hi ha altres marques disponibles per a fer les diferents funcionalitats requerides, aquestes poden ser 3COM, ALLIED, ZYXELL... es important però que tots els elements de les diferents capes siguin del mateix fabricant, per evitar problemes i fallades inesperades.

Dins de la capa d'accés també podem trobar el punts d'accessos sense fils, aquests treballaran amb el protocol 802.11ac explicat en l'apartat anterior i amb encriptació WPA/PSK personal. Seguint amb la Marca DLINK, el projecte recomana el model **DWL-2200AP**.

Figura 13. DLINK DWL-2200AP

Aquests equip fa les funcions de punt d'accés a la xarxa dels paquets dels usuaris repartits per les subxarxes de connectivitat sense fils. Aquest dispositiu està alimentat per PoE i suporta velocitats de xarxa sense fil de fins a 108 Mbps i ofereix una interoperabilitat sense problemes amb els equips sense fils.

Distribució de ports

El projecte marca unes directives dels ports en els que s'han de fer les connexions pertinents. Aquests ports estan configurats segons les xarxes virtuals corresponents, explicades en l'apartat 4.1.4. Tenim llavors una disposició de ports diferents per als elements de la capa de distribució i per els elements de la capa d'accés:

Per a la capa de distribució on tenim el commutador multicapa de nivell 3 ha d'haver-hi una configuració de ports que pugui distribuir tot el tràfic en les diferents VLANs. La distribució queda com la següent figura:

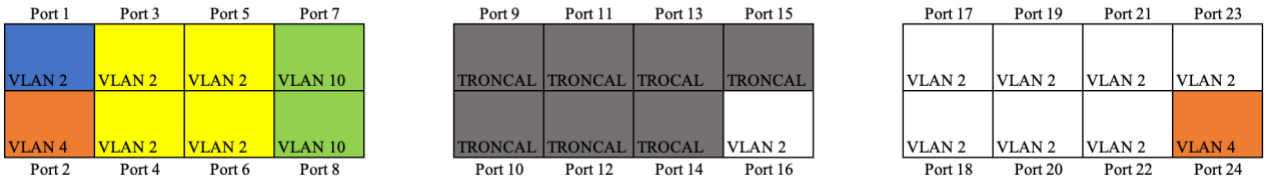

Figura 14. Distribució ports commutador principal

La distribució de colors són ports especials:

- En el **port 1** de color blau hi va la connexió al **encaminador** de la capa nucli
- El **port 2** de color taronja esta destinat a una connexió directa per a fer la **gestió** de tots aquests elements de xarxa.
- Els **ports 3-6** de color groc estan destinats a la connexió amb diferents **servidors** del centre els quals si que poden anar connectats directament a aquest commutador.
- Els **ports 7-8** de color verd estan configurats per als **administradors** de la xarxa.
- Els **ports 9-15** de color gris són els que efectuaran la connexió amb tots els altres **dispositius** de la capa d'accés.
- El **port 24** de color taronja esta destinat a la connexió amb el **SAI**.

- Els ports no esmentats o de qualsevol altre commutador que no s'utilitzin s'han de deixar per defecte en la VLAN 2.

Per a la capa d'accés la distribució de ports és diferents, ja que aquí la funció principal és donar connectivitat als usuaris finals. La distribució queda com la següent figura

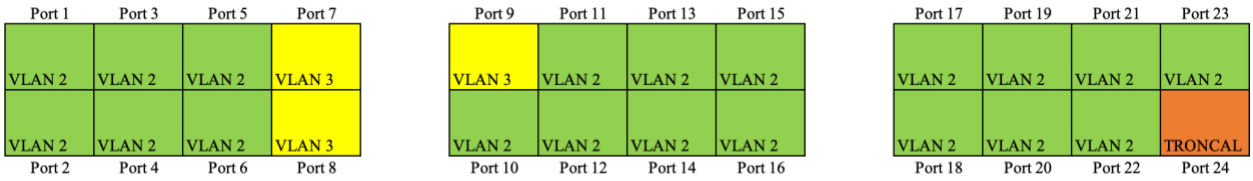

Figura 15. *Distribució ports commutador/s secundari/s*

- Els ports marcats en color **verd** estan connectats els elements de la **VLAN 2** directament.
- Els **ports 7-9** de color groc són els destinats a tenir una connexió directa amb els **punts d'accés** per a la connexió a la xarxa sense fils.
- El **port 24** (o últim port en cada model de commutador) es destinarà a la **connexió troncal** amb el commutador de distribució.

Disposició dins de l'armari de comunicacions

La posició que ocupa cada element dins d'un armari de comunicacions ve donada també pel projecte HEURA[18], seguit amb un etiquetatge. Aquest procés es però purament organitzatiu i no te cap efecte en el rendiment de la xarxa, o en la decisió final de on es col·locarà la Raspberry Pi.

Aquest etiquetatge treballa de la següent manera:

- Els racks o armaris es marquen amb una R i un numero, sent el primer R0.
- Els commutadors dins del armari (rack) es marquen amb la mateixa nomenclatura del armari afegint SS si és secundari o SC si és el primari. Per tant podria quedar com R0SC1
- El nivell o altura que es marca amb una P, si comença a dalt de tot és P1

Poden haver-hi més elements de marcatge depenent de la instal·lació de la forma en que es pot separar el hardware.

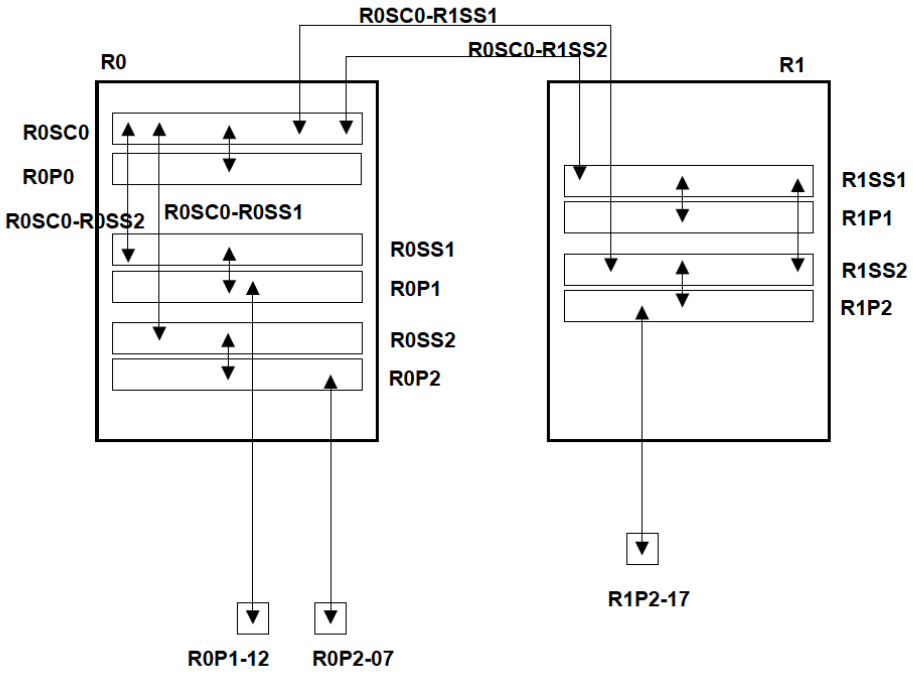

Figura 16. Distribució física projecte HEURA dins del armari [18]

Esquema de la topologia física

La topologia explicada anterior en la seva forma més bàsica es pot simplificar en un esquema de la topologia física general com segueix:

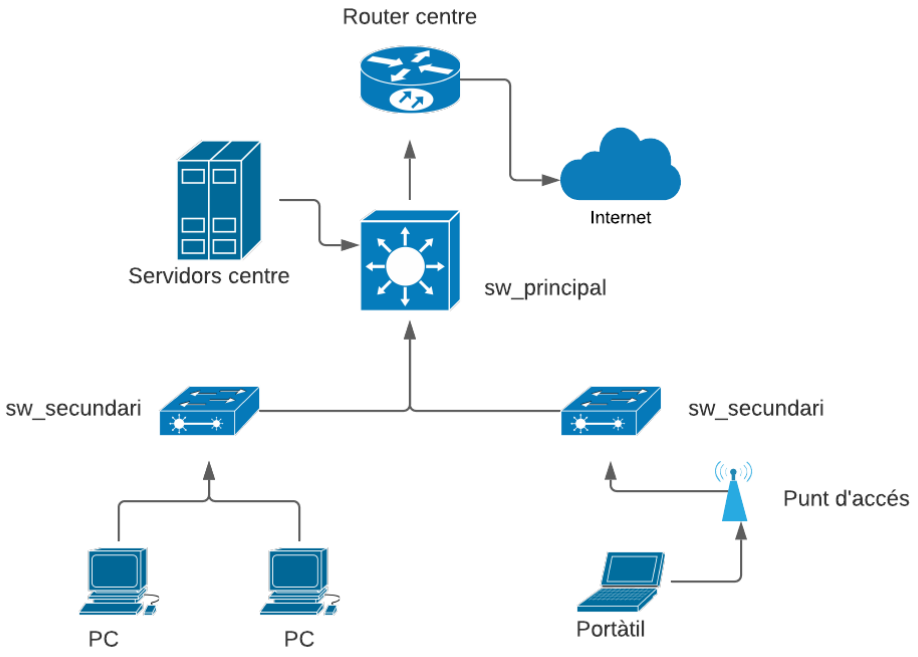

Figura 17 - Topologia bàsica plantejada pel projecte HEURA

Per a la representació de la topologia anterior s'ha tingut en comte la configuració dels ports de cada commutador i les indicacions de la documentació del projecte.

4.1.4 Topologia lògica

Per a saber on podem connectar el nostre kit de sensors hem de valorar les configuracions lògiques del port que trobem disponible. A l'apartat anterior he discutit la distribució del ports en la xarxa física. Ara s'ha de tenir en compte la configuració d'aquest port per a veure si es pot ficar el dispositiu.

Xarxes d'àrea local virtuals (VLANs)

En les xarxes modernes hi ha connectats tot tipus de dispositius i cada un d'ells te una funcionalitat diferent. Per a gestionar tots aquests dispositius s'implementa l'ús de les xarxes d'àrea local virtuals (VLANs). En el cas del projecte Heura diferència varies VLANs per als diferents tipus de tràfic i usuaris que puguin estar utilitzant la xarxa.

Les VLAN és una tecnologia de xarxes que ens permet crear xarxes lògiques independents entre si dins de la mateixa infraestructura física. És a dir, una infraestructura física conforma una LAN, al implementar VLAN podem tenir l'equivalent de 2 o més xarxes dins del mateix hardware. Aquestes xarxes virtuals ens ofereixen una sèrie de avantatges que fa que sigui la millor manera de gestionar i muntar una xarxa. [23]

- **Seguretat**: Les xarxes virtuals queden totalment independitzades i tot i que en el mateix hardware hi hagi dues de configurades no es poden veure entre elles ni travessar paquets, excepte en el cas que un encaminador tingui en la seva taula de rutes les IP de cada una de les xarxes virtuals.
- **Segmentació**: Ens permeten separar els equips de les mateixes xarxes. Poden organitzar el tràfic de diferents maneres. (Estudiants/professors, en departaments...)
- **Flexibilitat**: Ens dona l'opció de modificar les diferents xarxes sense tenir que fer cap canvi físic i col·locar equips nous. És un sistema fàcilment escalable i que nomes requereix de software per a fer-lo servir correctament.
- **Optimització de la xarxa**: Al separar tot el tràfic fa que la càrrega en els dispositius sigui més petita, ja que si nomes prové molt tràfic d'una xarxa virtual, només s'ha de processar aquesta.

Segons el model Cisco de les VLAN i com està estructurat al projecte Heura tenim que cada VLAN és una xarxa que correspon a una xarxa IP. Per tant al dissenyar-les o al implementar-les s'ha de tenir en compte la implementació d'un esquema de direccionalment de xarxa jeràrquic. El direccionalment jeràrquic de la xarxa significa que els bits de la xarxa IP s'apliquin a les diferents VLANs de forma ordenada com es pot veure en la **Figura 18**. Es a dir, si treballem amb la VLAN 10 utilitzarem el direccionalment 192.168.10.0/24, la VLAN 20 192.168.20.0/24 etc.

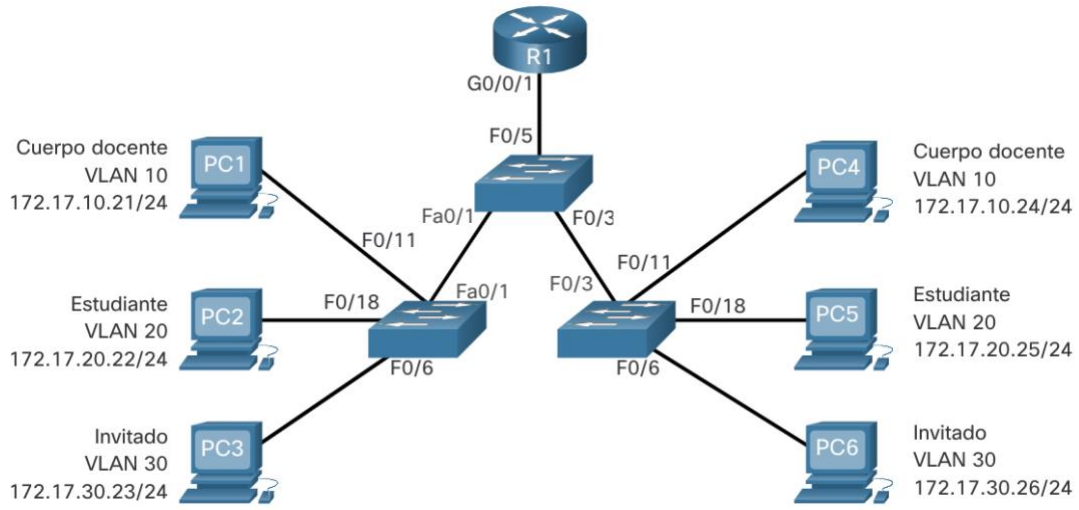

***Figura 18**. Direccionament jeràrquic VLANs [23]*

Dins del projecte HEURA s'estructuren les VLANs d'aquesta manera, seguin un ordre de construcció jeràrquic. Les escoles es separen en 6 VLANs diferents que tenen diferents funcionalitats.

VLAN	RANG IP
VLAN 2 – Educativa cable docent	192.168.0.0/24 * Pot avançar amb 192.168.1.0... 192.168.2.0...
VLAN 3 – Educativa sense fils docent	192.168.130.0/24
VLAN 4 – Gestió de commutadors i punts d'accés	192.168.140.0/24
VLAN 5 – Convidats sense fils eduroam	192.168.150.0/24
VLAN 6 – Futura vídeo – telefonia IP	192.168.160.0/24
VLAN 10 – Gestió – administració	192.168.110.0/24

***Taula 6.** Rang IP diferents VLANs projecte HEURA[18]*

El commutador principal multicapa ha d'estar configurat en totes les VLAN amb l'adreça 192.168.X.1.

Es pot fer una breu explicació de l'aplicació de cada VLAN i la visibilitat que tindran entre elles. Les visibilitats de les VLAN venen configurades dins del commutador principal de capa 3. En el apartat de simulacions del projecte s'entrarà en detall com es fa aquesta configuració.

La VLAN 2 és la que dona servei per cable a els usuaris de l'escola, ja sigui ordinadors de les aules com de professors, aquesta serà visible amb la VLAN 3 i la 4.

La VLAN 3 fa la mateixa funcionalitat que la VLAN 2 però de manera sense fils. Aquesta com ja he esmentat te visibilitat amb la VLAN 2 i la VLAN 4.

La VLAN 4 és la que ens permet gestionar el hardware remotament, les adreces d'aqueta VLAN se lis assigna al maquinari de la xarxa, com els commutadors o els punts d'accés sense fils, ja que aquests moltes vegades tenen l'opció de ser controlats remotament mitjançant el protocol ssh[9] o Telnet[10].

La VLAN 5 no és visualitzarà des de cap altra xarxa virtual, aquesta nomes tindrà connexió a internet amb la connexió establerta. Aquesta xarxa per connectar-se es necessita una validació a un servidor *Radius*[11] de la *Xtec*.

La VLAN 6 no es visualitzarà des de cap altra xarxa virtual, i permetrà l'accés a internet amb connexió establerta.

La VLAN 10 tampoc tindrà visualització des de cap altra xarxa virtual i permetrà l'accés a internet amb connexió establerta.

Les adreces que s'assignaran a cada equipament de gestió i les adreces finals a cada dispositiu es dona a configurar a cada instal·lador de la xarxa de cada escola, per tant, podem esperar que estiguin dins del rang establert però pot haver-hi variacions en cada escola. L'únic es que el encaminador se li assignarà l'adreça 192.168.140.1 dins de la VLAN de gestió. Un cop fetes aquestes consideracions, es pot mostrar l'esquema de xarxa amb les VLAN activades.

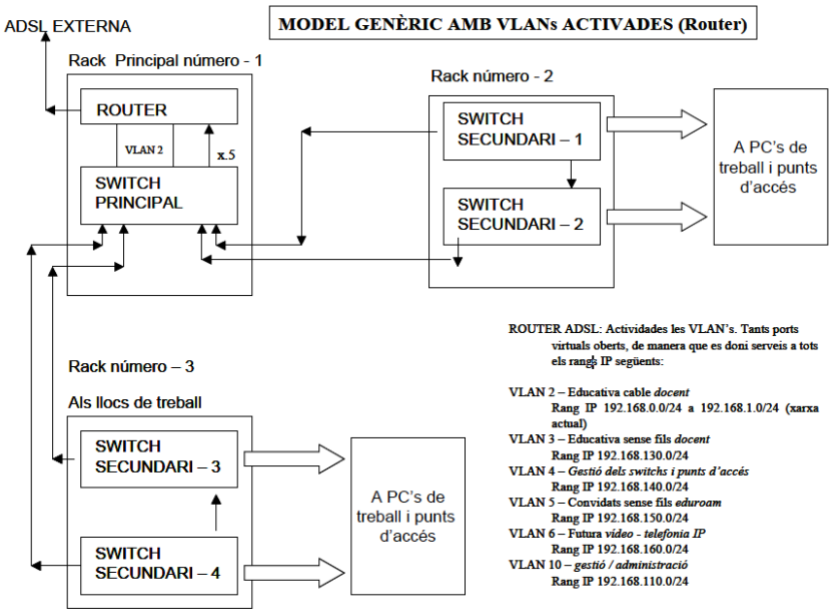

***Figura 19**. Model genèric amb VLANs activades [18]*

Com a consideració final s'ha de comentar que les adreces dels diferents dispositius que es connectin a les VLAN 2 i VLAN 3 obtindran una adreça mitjançant el protocol DHCP, aquesta adreça la proporcionarà el servidor DHCP de l'escola, pot estar configurat exteriorment o internament dins del encaminador.

[9] ssh: Secure Shell és el nom d'un protocol que la seva funció és l'accés a remot a un servidor mitjançant un canal segur.

[10] Telnet: Teletype Network és el nom d'un protocol que ens permet accedir a una altra màquina remotament. Normalment utilitzat per a gestionar maquinari de xarxa.

[11] Servidor Radius: Servidor d'autentificació d'usuaris centralitzat.

4.2 Xarxa de l'escola La Vitxeta de Reus

Per acabar l'estudi de la xarxa de l'escola, he anat presencialment a una escola per tal de fer les comprovacions necessàries per a saber si el projecte HEURA implementat en aquestes es segueix de manera correcta o pot ser el cas de que hi hagin diferències referents a la implementació feta a cada centre escolar.

El dia 25 de novembre del 2021 vaig anar a l'escola La Vitxeta de Reus per a realitzar aquestes proves. Vaig realitzar proves de connexió i una petita revisió de la infraestructura física que tenen. Les proves realitzades de connexió s'han realitzat de dues maneres: Amb una connexió cablejada i una sense fils. Corresponents a la VLAN 2 i la VLAN 3. En aquest apartat em centraré a corroborar la utilització del projecte HEURA dins de l'escola. Cal destacar que per temes de administratius i de privacitat no he pogut accedir a les VLANs de gestió i administració.

La primera prova realitzada ha estat de manera cablejada. L'escola te habituades algunes aules de reforç i amb tot l'equipament necessari per a fer classe. He connectat el meu equip portàtil a una presa de xarxa d'una d'aquestes aules a una altura d'uns 1,5m aproximadament que hi ha una caixa amb dues connexions Ethernet i 6 connexions elèctriques. Una d'aquestes remarcada en color vermell que indica que te una connexió al SAI[12] de l'escola. En aquest cas és indiferent quina connexió agafar, jo he connectat el meu cable a la superior perquè em venia més a mà.

***Figura 20**. Presa RJ-45 i de connexió La Vitxeta*

Un cop feta la connexió per cable, he pogut realitzar les probes pertinents per a comprovar la connexió. Aquestes proves les he realitzat amb el Terminal de un sistema operatiu MacOS i els "ping" venen recomanats per el projecte HEURA i la seva implementació. Les proves han estat les següents:

[12] SAI: Sistema d'alimentació ininterrompuda: Quan la connexió elèctrica es perd aquest dispositiu subministra electricitat que te emmagatzemada.

Proves a realitzar	Si	No
Hi ha connectivitat?	✖	
Adreçament dins del rang de la VLAN 2?	✖	
Ping Router (192.168.0.1/24)	✖	
Ping Yahoo	✖	
Ping Google	✖	
Ping Gencat	✖	
Connexions disponibles a les aules?	✖	
Switch connectats?	✖	
Segueix la infraestructura Heura?	✖	

Taula 7. Proves realitzades amb cable La Vitxeta

Adreçament IP obtingut: **192.168.3.164**

Velocitat de baixada: **735 Mbps**

Velocitat de pujada: **441 Mbps**

Les proves realitzades han sortit exitoses, la IP està dins d'un rang de la VLAN 2 donada per el projecte HEURA, tenim una velocitat de connexió més que decent i segueix tota la infraestructura que s'havia estudiat en apartats anteriors.

D'altra banda, he realitzat proves a la xarxa sense fils Docent del centre. Al realitzar les proves, la directora del centre m'ha comentat que aquesta xarxa està per desaparèixer i que s'està integrant una nova xarxa que malauradament no em podia donar accés perquè és una xarxa de proves i que encara no esta implementada. Per tant, és possible que en un futur proper la xarxa docent no estigui en funcionament. Tot i així actualment és la xarxa sense fils que més s'utilitza dins del centre i la que està dins del projecte HEURA. Les proves realitzades són molt similars a les realitzades anteriorment ja que el principal és buscar la connectivitat que té l'escola i demostrar que te sortida a internet.

Aspectes a mirar	Si	No
Hi ha connectivitat?	✖	
Adreçament dins del rang de la VLAN 3?		✖
Ping Router (192.168.130.1/24)	✖	
Ping Yahoo	✖	

Ping Google	✖	
Ping Gencat	✖	
Acces point dins de aules? Fer foto	✖	
Switchs connectats i *acces point* funcionant?	✖	

***Taula 8**. Proves realitzades sense fils La Vitxeta*

Adreçament IP obtingut: **192.168.3.167**

Velocitat de baixada: **320 Mbps**

Velocitat de pujada: **215 Mbps**

En aquest cas, al connectar-me a la xarxa sense fils, l'adreçament obtingut no és l'especificat per el projecte HEURA, esta dins del mateix rang que el trobat en la connexió per cable. És probable que al estar fent proves amb la nova xarxa sense fils estiguin usant adreçaments de la VLAN 3.

Les proves dins del marc de la connexió han tingut bon resultat i de moment segueixen les directius del projecte HEURA i no tenen cap problema per sortir a l'exterior per internet. A l'escola La Vitxeta tenen la infraestructura física segons estableix el projecte. Aquesta infraestructura consta d'un encaminador que te com a proveïdor de servei *Movistar*, el commutador de nivell 3 Cisco i commutadors de nivell 2 Cisco. En la **Figura 21** es pot veure l'armari central de comunicacions amb els seus diferents elements senyalats sobre aquesta.

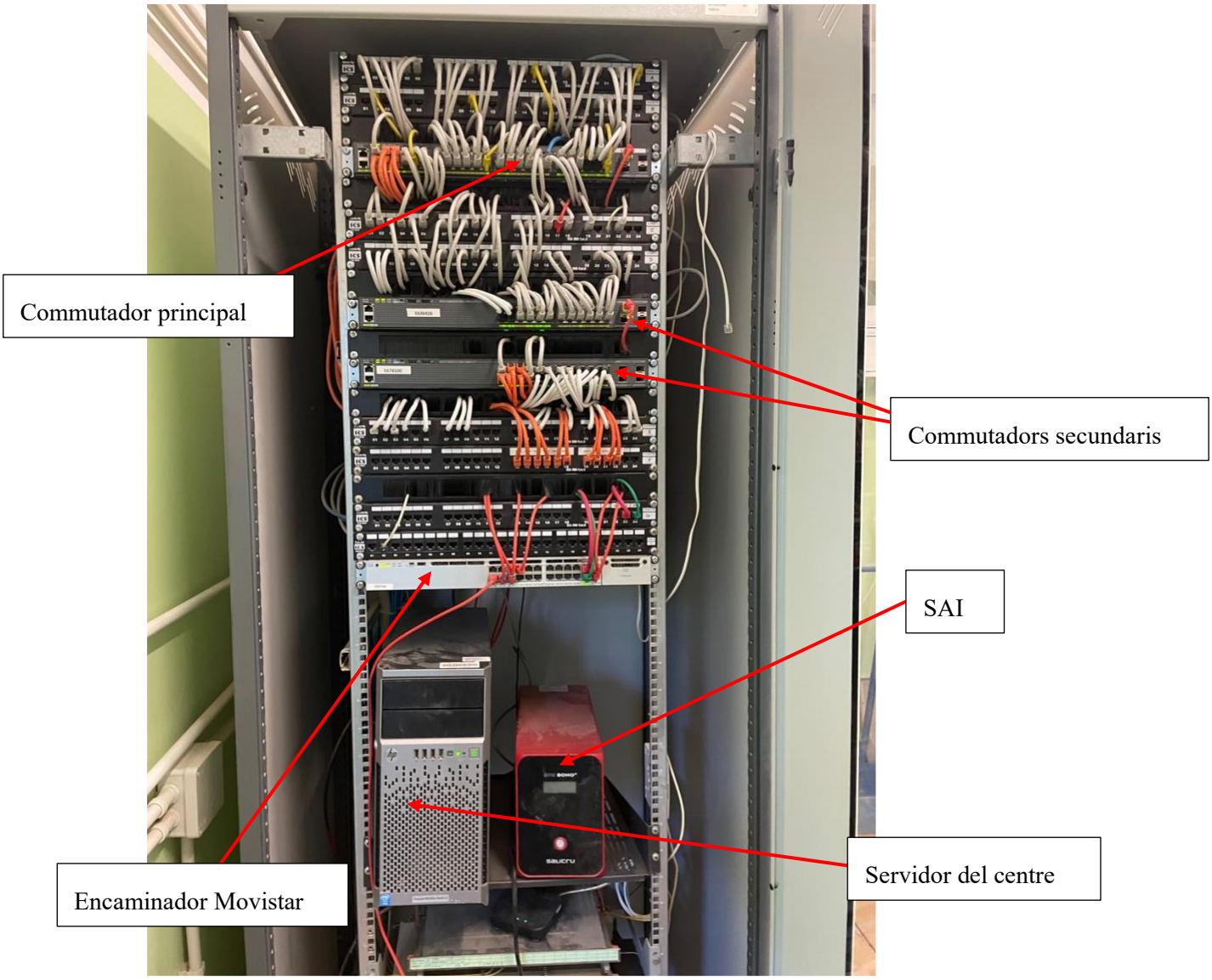

***Figura 21**. Armari principal La Vitxeta*

El centre escolar te una altre armari de comunicacions en la segona planta, aquest donava servei a una antiga aula d'informàtica que m'han dit que amb la recent implementació de tauletes i dispositius mòbils no utilitzen i els ordinadors estan retirats. En aquest cas, l'armari estava tancat sota clau però hi ha connectat un commutador de nivell 2 que dona connexió als ports de l'aula en concret com es pot veure en la **Figura 22**.

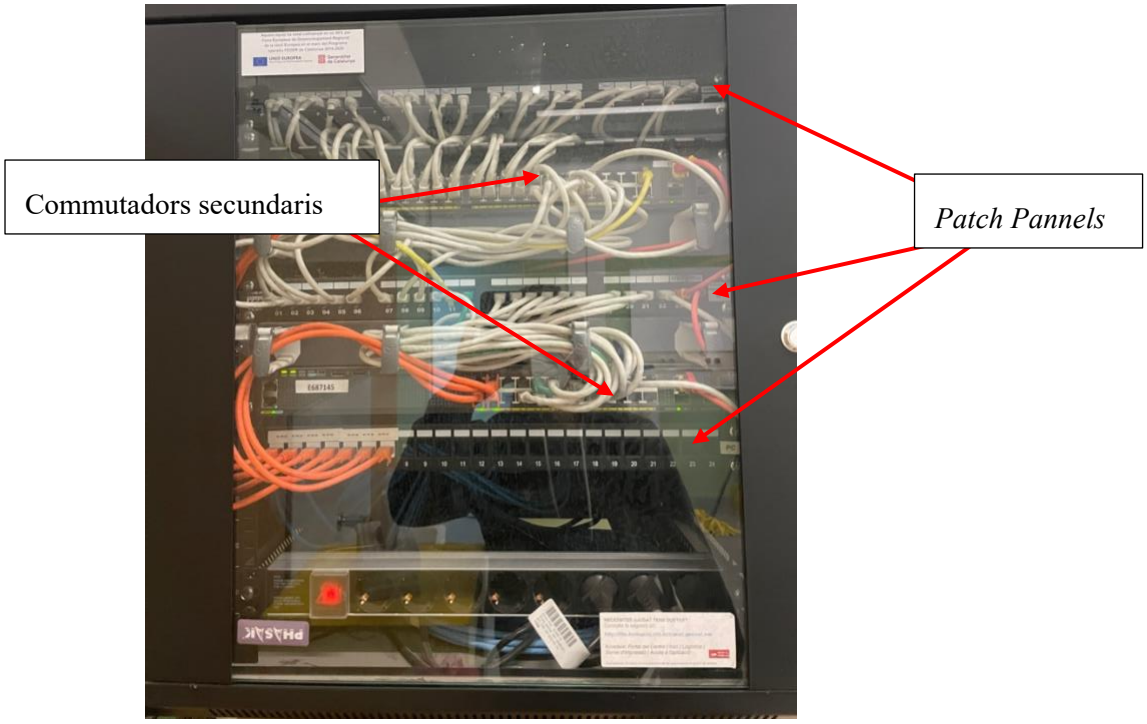

***Figura 22**. Armari secundari La Vitxeta*

El cablejat no s'ha pogut seguir des de l'armari de telecomunicacions principal i el secundari, tot i que la connexió va del commutador principal als secundaris. Tampoc he pogut comprovar la correcte configuració dels ports com marca el projecte HEURA degut a que no he tingut les claus d'accés dels diferents commutadors. En tot cas per al marc del projecte ACTUA i la realització d'aquest treball de final de grau no afecta en el desenvolupament o en les simulacions que es poden realitzar. Probablement tot i que les escoles estiguin sota unes directrius de disseny de xarxa probablement hi hagi variacions depenent del maquinari usat i de la empresa que hagi fet la instal·lació i que hagi configurat l'equipament.

Es pot concloure que La Vitxeta segueix el projecte HEURA casi en la seva totalitat, podent extraure d'aquí que dins d'un cert marge en totes les aules que es vulgui instal·lar un kit de sensors es podrà fer sense cap problema.

5 Implementació del kit dins de la xarxa i explicació del seu funcionament

Com he explicat en la introducció del projecte, l'estudi de la xarxa de dades de les escoles públiques de Catalunya ve donat per la necessitat del projecte ACTUA de ficar-hi una sèrie de kits de sensors per a poder recopilar dades de la qualitat d'aire.

En aquest apartat del projecte estudiaré en la xarxa exemplificada anteriorment els millors punts on podem fer la connexió de la Raspberry Pi, les complicacions que podem trobar i els avantatges que podem tenir en vers connectar-ho en una part o en una altra. Els diferents entorns que estudiaré són:

- **Per la xarxa cablejada docent**. Donada la seva gran robustes i la velocitat que he obtingut en la proba de connexió de l'escola La Vitxeta. Estudiaré els avantatges d'aquest punt de connexió, els seus desavantatges i si finalment es pot fer una connexió estable.
- **Per la xarxa Wi-Fi educativa**. Ens dona una major flexibilitat de col·locació del dispositiu, així com una velocitat de connexió més que acceptable. Estudiaré també els avantatges e inconvenients d'aquest punt de connexió per concloure finalment si es pot realitzar la connexió a través d'aquest medi.

Un cop realitzat aquesta comparativa i havent extret conclusions explicaré tot el recorregut de la xarxa restant (des de el encaminador de l'escola fins al servidor ACTUA), discutiré l'arquitectura implementada per a fer aquest camí i he implementat una aplicació web per a fer possible aquest últim tram.

Per acabar l'apartat he simulat les diferents opcions discutides per a valorar d'una manera més cartera les conclusions extretes i veure que el plantejament fet és correcte.

A més donaré alguna informació extra útil per a la implementació d'aquest dispositiu. Com poden ser temes de seguretat.

5.1 Estudi de la posició de la Raspberry pi

Per a tenir clar on podem connectar el kit de sensors hem de fer una reflexió a doble banda. Quin és el punt físic que puc connectar el kit i en aquest punt físic quina configuració hi ha aplicada.

Des del punt de vista del entorn físic s'ha de connectar directament en la capa d'accés, en un punt d'accés o bé en un commutador secundari. Per a fer la connexió en aquests dos punts i seguint la **Figura 15** només es pot mitjançant la VLAN 2 (Educativa cablejat) o la VLAN 3 (Educativa sense fils).

Parlant de la configuració s'involucren moltes més variables que poden afectar en la connexió i/o en el rendiment i funcionament de la Raspberry. S'ha de suposar que l'assignació DHCP i que l'obtenció de l'adreça dins del rang disponible ha de ser correcte, i que la taula d'adreçament ha de ser també correcte. Per tant el problema central que ens pot presentar és que la configuració del port on connectem el dispositiu.

Aquest problema del DHCP, quan vaig visitar l'escola La Vitxeta, es va realitzar una proba de connexió. Vaig connectar el meu portàtil per a comprovar l'assignació DHCP, en les probes que es poden veure en l'apartat anterior, l'adreçament s'agafa correctament i s'assigna una IP sense cap problema.

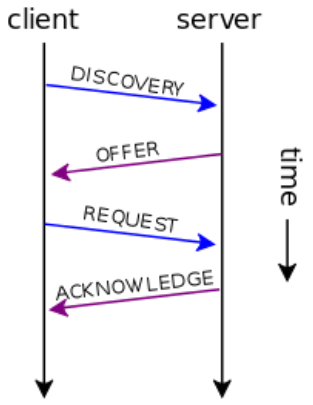

Figura 23. Assignació DHCP [24]

5.1.1 Etiquetatge de xarxes d'àrea local virtuals

El problema més important que ens podem trobar dins de la configuració d'un port d'un commutador és la manera en que es transmet la informació de la capa 2.

Depenent del fabricant del hardware i de com funcioni la xarxa, es poden canviar les trames Ethernet per a contenir informació de la VLAN amb la que es treballa, se li afegeix una etiqueta a la trama exemplificat en la **Figura 24**. Com s'ha explicat en el apartat Estudi de la infraestructura de xarxa d'una escola referent a l'estàndard Ethernet i al seu mètode de funcionament.

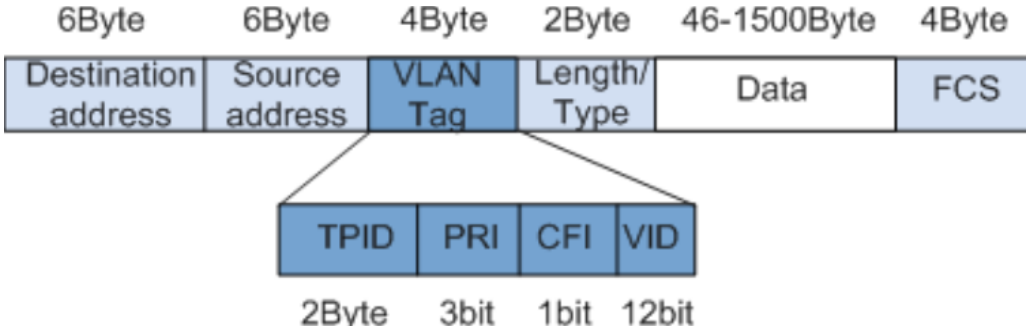

Figura 24. Trama Ethernet amb VLAN Tagging [25]

Aquesta etiqueta d'identificació pot ser agregada o eliminada per un host, un encaminador o un commutador. Dins de la xarxa i dins de cada aparell es pot configurar per a que treballi amb aquest format. Els ports es poden configurar de tres maneres:

- **Sense etiquetar:** En la nomenclatura *Cisco* en que he basat explicació d'aquest treball s'anomena nativa. Aquesta opció s'utilitza per a connexions directes amb els dispositius finals, ja que en un ordinador, el NIC no pot treballar amb aquestes trames. També es pot utilitzar quan es connecten dos commutadors entre si per restringir la comunicació de VLANs entre els dos, tot i que generalment la connexió entre dos commutadors es fa en mode *trunk*.
- **Etiquetats:** En aquest cas hi ha elements de la xarxa que per funcionar envien un paquet etiquetat amb la seva VLAN, com per exemple els telèfons IP, aquests dispositius s'ubiquen entre l'ordinador i la toma del commutador i necessiten saber quin tràfic va dirigit cap a ells.

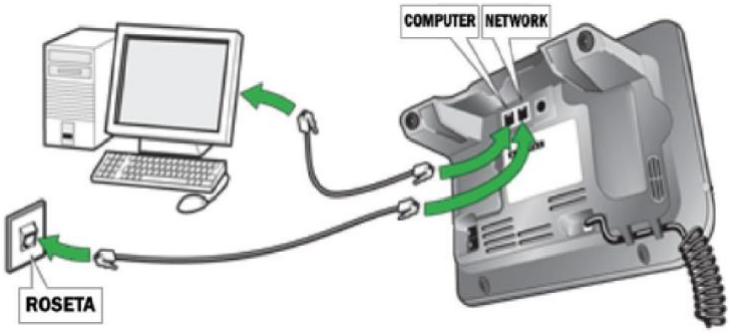

Figura 25. Telèfon IP funcionament amb VLAN tagging [26]

- **Port en mode *trunk*:** Aquests ports poden estar també denominats com a troncals. Són ports configurats per a passar la informació de moltes VLAN. Aquest port acceptarà i retransmetrà el tràfic de totes les que tingui configurades amb etiqueta, tot i que es pot configurar una VLAN per a que el seu tràfic passi de forma no etiquetat. Aquesta VLAN s'anomena la VLAN nativa.

La Raspberry pi que s'utilitza per a aquest projecte no és capaç de llegir el tràfic etiquetat, per tant l'hem de connectar en un port que ens deixi treballar sense aquest etiquetatge. En aquest cas ens valdran els ports del **commutador secundari** del rang **1-6 10-23**. D'altra banda hi ha el tràfic no etiquetat que treballen en els punts d'accés. En aquests punts d'accés també podem fer la connexió sense fils amb el kit de sensors, s'ha de tenir en compte però que els punts d'accessos tenen menys fiabilitat i que depenent del model tenen una limitació d'usuaris que es poden connectar a ell.

Resumint podem veure que podem fer la connexió amb la **VLAN 2** mitjançant un port especificat en un **commutador secundari**. O bé en un **punt d'accés Wi-Fi** a la **VLAN 3** i que va directament també a aquest commutador.

5.1.2 Connectar a la VLAN 2 per Ethernet

Com s'ha exposat en l'apartat anterior el lloc ideal per a realitzar la connexió de la Raspberry Pi és mitjançant un cable de coure trenat utilitzant el protocol Ethernet dins de la VLAN 2. En aquest cas la VLAN 2 proporciona connexió directa a internet i esta aïllada de les altres xarxes, fent que en cap moment es pogués accedir a la VLAN de gestió de cap servidor administratiu del centre escolar.

Per a fer la connexió en aquesta VLAN s'ha de connectar el kit de sensors en una roseta d'una classe, aquest kit ha de poder tenir al seu abast corrent elèctrica (si el commutador no disposa de *PoE*) i de la presa RJ45 per a fer la connexió amb el commutador. Depenent de l'escola i l'equipament que tingui cadascuna, es possible que s'hagi d'habilitar una nova toma o que s'hagi d'utilitzar un petit *hub* per a tenir diverses connexions.

El medi físic està compartit per els equips escolars que hi hagin, com poden ser els ordinadors dels professors a cada classe, i els estudiants o dispositius que estiguin connectats també per cable. En aquest cas la Raspberry ha d'estar enviant dades cada x temps al servidor, aquestes dades però seran per comprovar el seu estat, mentre que les dades dels sensors s'enviaran en una hora de baixa activitat en el centre.

En aquest apartant exposaré els avantatges i desavantatges de connectar el kit de sensors en aquesta VLAN.

Avantatges

Aquesta connexió al ser realitzada per cable i utilitzant la tecnologia Ethernet i com s'ha explicat en el apartat 4 aquest protocol i mètode connexió aporta una estabilitat molt gran a la connexió, aportant segons la **Taula 5**.

Fora dels aspectes tècnics i de robustesa tenim que mitjançant aquest mètode de connexió la possibilitat de que s'alimenti mitjançant *PoE* fent que només s'hagi d'utilitzar un cable per a connectar el kit de sensors, evitant així possibles fallades de la corrent elèctrica i amb seguretat que el commutador al qual està connectada aquesta Raspberry Pi te una connexió al sistema d'alimentació Ininterrompuda i encara que la llum marxi podrà seguir funcionant.

També ens aporta una seguretat física, ja que per a la gent que estigui en la aula podrà veure en tot moment que el kit de sensors està connectat i es pot detectar alguna fallada comuna. Com a més distanciament amb els usuaris, ja que al ficar el kit de sensors en escoles esta subjecte a que hi haurà nens de primària a prop del maquinari, es possible que aquest sofreixi alguns danys físics. Pel vist en l'apartat Xarxa de l'escola La Vitxeta de Reus les preses RJ45 i les tomes elèctriques solen estar a una alçada d'1,5m i generalment en zones on treballen els professors.

Desavantatges

Tot i que sobre el paper connectar el kit de sensors amb aquesta tecnologia sembla la millor idea també hi ha un seguit de desavantatges que no s'han de deixar passar per extreure les conclusions ja que són igual d'importants.

Per el que a equipament es refereix, aquest mètode de connexió és més car ja que necessita un cable extra (si no es te *PoE* als commutadors) per a fer la connexió i depenent del lloc d'instal·lació la mida d'aquest pot canviar o ser insuficient o massa llarg en alguns casos. Aquest cable es pot trencar o li pot passar qualsevol problema físic que no estigui al control dels tècnics.

Per a preparar el kit de sensors s'ha de tenir en compte el forat per a fer entrar aquest cable dins del contingut de la caixa on estigui tota la maquinària.

Conclusions

Valorant els avantatges i desavantatges d'aquesta connexió i donada la finalitat de perquè s'instal·la el kit de sensors en les escoles, és una opció molt bona ja que ofereix fiabilitat, tenim un entorn que ens ofereix seguretat (com discutiré en l'apartat Seguretat de la xarxa) i una connexió relativament barata i que no s'ha de fer cap modificació en la xarxa de l'escola per poder treballar amb aquesta.

5.1.3 Connectar a la VLAN 3 per Wi-Fi

En els apartats anteriors s'han exposat els diferents punts on es pot fer la connexió del kit de sensors dins de la xarxa de l'escola proposada per el projecte HEURA. Un dels dos punts en que es pot fer la connexió es mitjançant la xarxa sense fils docent ja que com s'ha comprovat en el apartat Xarxa de l'escola La Vitxeta de Reus, és una xarxa prou robusta i amb una connectivitat correcte cap a l'exterior.

El protocol Wi-Fi exemplificat en l'apartat Projecte HEURA es pot demostrar que és un protocol prou fiable amb una velocitat de transmissió decent i que actualment amb la implementació del IEEE 802.11ac la connexió és correcta (**Taula 4.** *Comparació Wi-Fi 5 i 6*).

Depenent de l'escola i de la seva infraestructura però pot ser que en determinat punt del dia (si els alumnes estan utilitzant tauletes, ordinadors, etc.) els punts d'accés no tinguin la capacitat de servir a suficients usuaris, fent que es pugui arribar a perdre la connexió en determinats moments.

Avantatges

En vers a la connexió per cable no podem afegir cap avantatge que estigui relacionat amb la fiabilitat i la robustesa de la connexió ja que en aquest aspecte guanya l'altre protocol.

Amb aquesta connexió sense fils es pot destacar la versatilitat que dona en fer la instal·lació del kit de sensors en qualsevol part del aula on hi hagi senyal de connexió amb la xarxa sense fils docent. Això fa que sigui possible la instal·lació de la Raspberry Pi en llocs molt poc accessibles per els alumnes però que es puguin detectar totes les variables que es volen representar dins del projecte ACTUA. Tot i que amb aquesta flexibilitat queda tot depenent d'on hi hagi una presa elèctrica dins de l'aula perquè sinó el dispositiu no pot funcionar.

Es pot destacar que respecte a la connexió Ethernet aquesta no necessita de cap cable opcional i que per tant la connexió es fa d'una manera més econòmica ja que la Raspberry pi ja te incorporat el chip per a establir connexions sense fils, cosa que fa que no s'hagi de comprar cap element addicional per a fer la connexió.

Es pot fer un kit de sensors més estanc ja que no s'ha de deixar cap forat per a fer pas al cable de connexió, si es munta tot dins d'una caixa només s'hauria de deixar un forat visible per a fer la connexió elèctrica.

Desavantatges

En aquest aspecte en podem destacar la possible fallada del medi de connexió, ja que al ser l'aire el medi compartir pot estar saturat per altres senyals com els de connexions Wi-Fi properes o per a que al punt d'accés en el que esta connectat el kit de sensors tingui ja molts usuaris transmeten i rebent dades fent que depenent del model d'AP no es pugui garantir l'enviament de les dades.

El protocol IEEE 802.11ac normalment és te la costum que si en algun moment no funciona o va massa "lent" a ulls dels usuaris es tendeix a reiniciar els dispositius fent que hi hagi una possible assignació de DHCP, que no ha d'afectar en cap cas al funcionament del kit, però que pot causar un tall de la connexió i una possible pèrdua de dades.

Conclusions

Com a conclusió podem extreure que es un mitjà de connexió totalment vàlid que es pot fer servir sense cap tipus de problema. Pot haver-hi alguna tallada puntual del servei però avui en dia no es solen produir ja que hi ha molts sistemes de reforç i es un medi molt treballat.

Es pot fer la connexió independentment del medi i per tant les dues alternatives es poden utilitzar depenent de com està distribuïda l'escola i dels elements que hi ha en cada classe. Donant així més possibilitats del muntatge i més opcions per a fer la connexió. He provat les dues connexions en un entorn virtual fent una representació emulada d'una escola fent proves de connexió entre elles. Ho mostraré en l'apartat Simulacions. I es pot utilitzar les dues maneres de manera alterna o com millor convingui en cada escola.

5.2 Lectura de les dades

Tots els elements de xarxa no tindrien sentit si no es fes una lectura correcta de les dades, ja que són aquestes les que finalment han de ser enviades per internet i les que s'hauran de treballar per obtenir resultats. L'objectiu d'aquest treball no és la recol·lecció de dades, i de moment el projecte ACTUA no esta definit quines dades i com es recol·lectaran. Tot i així val la pena parlar una mica sobre aquest tema per tenir una mica de context per poder ficar el conjunt del projecte sobre la taula.

La lectura de les dades es fa a través de sensors, amb el propòsit de mostrar un element físic de la infraestructura, he muntat una Raspberry Pi connectada amb un sensor de temperatura i humitat DHT22 per a recol·lectar aquestes dades.

5.2.1 Python

Aquest apartat té poca representació dins del marc d'aquest treball de final de grau. Tot i així com he comentat amb anterioritat i per donar context a l'estudi realitzat en aquest. Donaré una mica de context en la programació d'aquesta part realitzada al projecte ACTUA, ja que, finalment la primera manipulació de les dades es fa en aquest apartat. He treballat plenament amb el llenguatge de programació *Python* [27].

En aquest apartat es vol aconseguir un programa amb un nivell d'autonomia molt elevat i que sigui escalable per la quantitat de sensors que vulguem implementar. Per a poder aconseguir aquests objectius s'han implementat dins de la Raspberry dos processos. Un principal que s'anomena

`sensor_manager.py` i una de secundaria que li dona nom cadascun dels sensors que s'hagin d'implementar. Per a seguir aquesta explicació, és recomanable anar mirant la figura **Figura 26**

El *sensor manager* és l'encarregat de gestionar tots els processos dels sensors, l'enviament de dades al servidor i la comunicació de comandes amb el servidor. Aquest programa és l'encarregat també de generar la base de dades en la que els sensors ficaran la informació i que posteriorment s'enviarà a través del protocol FTP cap al servidor. El *sensor manager* haurà d'enviar periòdicament uns "batecs" cap al servidor per a comprovar de que esta funcionant, aquesta funcionalitat que cap dins del objectiu del projecte i de l'estudi de xarxa s'implementarà en els apartats posteriors d'aquest treball.

Els sensors són els diferents processos que gestionaran la recollida de dades dels diferents sensors que es vulguin implementar en el projecte. En aquest cas aquests processos han de poder emmagatzemar les dades dins d'una base de dades compartida i han d'estar escoltant un port UDP per a poder rebre instruccions del sensor manager.

L'arquitectura plantejada en el moment de la presentació d'aquest treball està en procés de desenvolupament i per tant no disposa de la seva funcionalitat completa. Aquesta es pot trobar en el repositori del *Github* [28] on es va actualitzant.

Finalment dins d'aquesta arquitectura cal destacar com he dit al començament d'aquest apartat que te poca cosa a veure amb la connexió de xarxa, tot i que hi ha parts desenvolupades de l'enviament de les dades per FTP i com es veurà en apartats posteriors, l'enviament de batecs cap al servidor per a la comprovació dels kits de sensors.

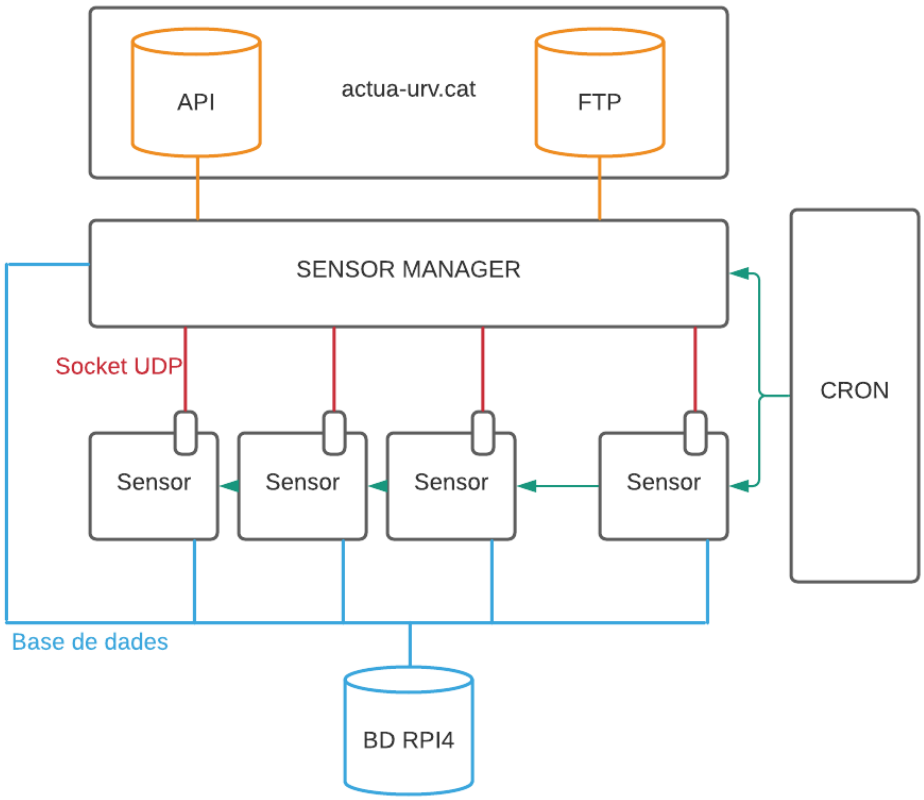

***Figura 26** - Arquitectura kit de sensors a instal·lar*

5.3 Enviament i processament de les dades

L'enviament de les dades és la finalitat del projecte ACTUA i la seva arribada al servidor, per tant, després de la infraestructura de xarxa de l'escola tots els llocs per els quals passin les dades són de vital importància i cal fer també un estudi d'aquests medis i una implementació pràctica d'aquests, La finalitat d'aquest apartat és definir el recorregut que fan les dades un cop estan recollides per el kit de sensors i desenvolupar un prototipat dels components per tal de tenir un sistema funcional.

Un cop les dades hagin arribat el destí passen al procés del processament. Aquest és el punt final de les dades en el seu procés de recol·lecció, transport i processat. Les dades venen donades en molts formats diferents, idealment emmagatzemades dins d'una base de dades o en un fitxer en format JSON[13]. Aquestes estan enviades a traves del protocol FTP al servidor en un fitxer en format *.csv* i són emmagatzemades en una base de dades que posteriorment pot fer les transformacions necessàries.

Aquestes dades es poden processar de moltes maneres diferents per aconseguir els objectius marcats. Tot i així una part fonamental de com es processen les dades, és la manera de representar-les. Aquestes dades han d'estar representades d'una manera clara per a poder entendre-les, l'objectiu d'aquesta representació es obtenir una imatge que ajudi a interpretar les dades de manera concisa i és important el poder de comunicació i interpretació que s'aconsegueix amb aquestes. Aquest processament s'efectua en la part del servidor.

Aquest enviament i processat de les dades es pot explicar en dos punts diferents, explicaré la infraestructura necessària per a fer aquest enviament de les dades un cop surten del encaminador de l'escola i un cop arribin al seu destí final explicaré el desenvolupament fet en software per a gestionar aquestes dades, ja que és un pas molt important dintre del estudi de la infraestructura de la xarxa en general.

5.3.1 Infraestructura de xarxa

La infraestructura de xarxa que s'utilitza per a fer aquest enviament de les dades és molt més gran que la simple xarxa estudiada d'una escola. A part d'aquesta, un cop els paquets han sortit del encaminador han de travessar la infraestructura que tingui muntada cada ISP. Aquesta infraestructura és el que vulgarment s'anomena com a "internet" te una gran quantitat de nodes i és casi impossible saber que passa per aquí dins, ho discutiré una mica més en l'apartat Internet.

Un cop el paquet ha arribat al destí final que és el servidor del projecte ACTUA les dades es tracten de varies maneres, al ser el final del recorregut d'aquestes i per tant també és un extrem de la infraestructura de xarxa val la pena fer un prototip del software que hi funcioni correctament i que es pugui implementar dins del projecte ACTUA com a prototip. En aquest aspecte i amb el prototip de software realitzat em centraré en l'apartat Servidor.

Aquesta infraestructura de xarxa es pot visualitzar d'una manera més correcte a la **Figura 27** en la qual es pot representar el transport de les dades per la infraestructura del ISP com un núvol.

[13] JSON: JavaScript Object Notation. Format de variables amb JavaScript que s'ha convertit en estàndard

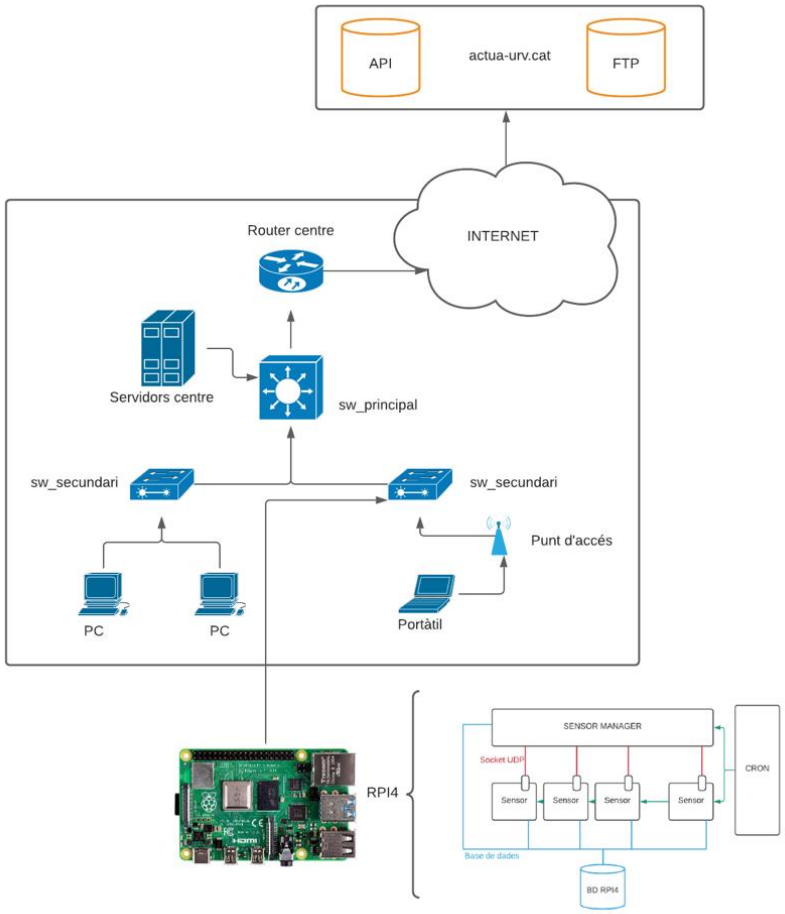

Figura 27 - Infraestructura al complet

5.3.2 Internet

L'enviament de les dades es farà a través d'internet amb xarxes privades dels proveïdors de servei d'internet que hi pugui haver a Catalunya. Aquest aspecte es totalment ocult però s'assegura que les dades arribaran d'un punt a l'altre sense cap pèrdua i d'una manera correcte.

Hi ha algunes maneres de trobar el camí que segueix un paquet o els salts que fa dins de la xarxa del proveïdors de servei d'internet però és molt difícil d'exemplificar o d'acabar de descobrir com és físicament aquesta infraestructura. En aquest apartat no es pot aprofundir tant en aquest tema per aquesta mancança de poder conèixer la xarxa física.

Aquesta impossibilitat de conèixer exactament el camí que segueixen els paquets amb les dades ve donat per la naturalesa de configuració dels encaminadors que hi ha pel camí. Hi ha una quantitat molt gran de protocols que defineixen rutes i miren quina es la millor per arribar a un destí en concret que donarien per a fer un treball de final de grau en ells mateixos. En aquest cas com es pot veure en l'article [29] els camins que agafa un paquet per arribar al destí poden ser varis i poden tenir grans variacions depenent de molts factors diferents. Hi ha articles com el [30] que mostren una manera de reduir aquests camins i fer-los d'una manera que es puguin registrar per saber per on passa el paquet en cada moment del seu viatge.

En aquest projecte i com s'ha mostrat en la **Figura 27** podem veure tot aquest procés de camins i de salts de manera simplificada com a una connexió directa entre l'encaminador de l'escola i el servidor. Tot i aquest aspecte he trobat oportú la realització d'aquest apartat i la recerca d'alguns documents que

tractessin sobre aquest tema. El destí final dels paquets a través d'internet es el servidor i es en el que em vull centrar.

Servidor

El servidor com he anat comentat al llarg del treball de final de grau és el destí final del trajecte de les dades. Aquest esta allotjat per una companyia externa i físicament no tenim accés, es pot configurar tot remotament i ficar tota classe de programari a dins per a que desenvolupi les funcions necessàries.

Aquest servidor ha de desenvolupar diverses funcions. Primer de tot ha d'actuar com a node central de tot el sistema del kit de sensors, per tant, aquest servidor ha de ser capaç de suportar moltes peticions a la vegada i ha d'estar actiu les 24 hores del dia els 7 dies de la setmana. Ha de tenir un sistema d'emmagatzematge suficientment ràpid com per a poder emmagatzemar les dades que li arriben des de les diferents Raspberry Pi i per llegir les dades en cas que es demanin des d'un servei extern. Per últim, aquest servidor ha de poder tenir un accés web en el que el públic en general i els membres del projecte ACTUA puguin visitar. Aquesta pot tenir moltes variacions i una web és un procés que sempre es poden afegir i treure coses. En trets generals aquesta web hauria de tenir un mapa interactiu amb tots els nodes que hi ha connectats al sistema amb una representació gràfica de si estan o no actius.

Tots aquests serveis que ha de suportar el servidor es poden categoritzar en dos parts depenent de la tasca que desenvolupin i la funció que tinguin. En aquest cas ja s'està començant a entrar en el mon del desenvolupament web i per tant aquestes dos característiques mencionades són les que marquen aquest desenvolupament.

- **Backend**: Segons l'article [31] el *backend* és la capa d'accés a dades d'un software o de qualsevol dispositiu que no és directament accessible per als usuaris. Aquesta conté la lògica de l'aplicació que mou aquestes dades. Es pot programar en molts tipus de llenguatge de programació i *frameworks* diferents el qual discutir-los tots no es adequat en aquest treball. L'aplicació de mostra que he fet està programada amb Node.js[14]
- **Frontend:** En el mateix article [31] es defineix el *frontend* com a la part d'un programa (en aquest cas el programari que mou el servidor web) a la que l'usuari pot accedir directament. Són totes les tecnologies de disseny i desenvolupament web que són executades generalment en el navegador i que s'encarreguen d'interactuar amb els usuaris. La part desenvolupada en aquest treball per tancar la infraestructura de xarxa completa està explicada.

5.4 Implementació del sistema de comprovació d'estat de la Raspberry Pi

En aquest apartat implementaré el sistema de comprovació d'estat de la Raspberry Pi, el qual s'encarregarà d'enviar "batecs" al servidor per a que aquest pugui comprovar que el dispositiu està funcionant correctament. Aquets missatges s'enviaran a través d'un mètode HTTP POST a una API que emmagatzemarà les dades. En aquest apartat parlaré i implementaré els termes de *frontend* i *backend* explicats en l'apartat anterior exemplificats amb el codi desenvolupat per a fer aquesta presentació.

En el cas d'aquesta arquitectura el que primer s'ha de fer és fer una organització general del que s'ha de fer i com plantejar-ho. La idea és que la Raspberry Pi enviï en el moment de connectar-se, les seves dades corresponents a longitud, latitud per a tindré la localització geogràfica del dispositiu, el nom i

[14] Node.js: Entorn de temps d'execució de JavaScript

l'hora. Un cop enviades aquestes dades inicials, cada un cert temps torni a fer una connexió al servidor indicant l'hora.

Per la part del servidor anirà rebent l'hora dels diferents dispositius que anirà actualitzant en la seva persistència de dades que s'explicarà en aquest apartat més endavant. Amb aquesta hora actualitzada, es podrà comprovar que la Raspberry ha donat senyals de vida en els últims minuts i per tant, el sistema esta funcionant. Tota aquesta informació s'arreplega dins d'una plana web on mostra un mapa amb els diferents punts de latitud i longitud de les ubicacions dels kits i el seu estat, indicat amb color verd si està actiu o vermell si està caigut.

Per a poder realitzar aquestes tasques i desenvolupar el codi corresponent s'ha utilitzat el *framework*[15] Node.js [32] en la part del servidor, que permet realitzar una aplicació web configurant tant el *backend* amb la seva API i el *frontend* amb el seu visualitzador de mapa i la seva visualització de les dades. Mentre que per la Raspberry Pi he desenvolupat un petit codi de python de mostra (sense seguir l'arquitectura del projecte ACTUA per a simplificar aquest apartat) que envia dades al servidor i batecs conforme està actiu.

- Part del servidor: Aquest apartat es pot separar en els dos elements que s'han comentat en els apartats anteriors, el *backend* i el *frontend.*

  Com a implementació del *backend* al servidor en el desenvolupament del programa realitzat s'ha implementat una API (fitxer *my_api.js[33]).* Aquesta s'encarrega de vàries funcions:
  - Es poden enviar dades del programa de la Raspberry (que simularà les dades del sensor) i les emmagatzemarà en persistència de dades.
  - Gestiona els enviaments dels kits de sensors dels paquets avisant de que estan funcionant, es a dir, dels batecs. Aquesta es la part essencial en que s'ha centrar principalment el desenvolupament del codi. Aquest emmagatzema les dades a persistència i pot fer modificacions cada vegada que rep un batec.
- Part de la Raspberry Pi: En aquest cas per a simular la infraestructura de xarxa no seguiré la implementació que segueix el projecte ACTUA, ja que aquesta esta pensada per un entorn de producció i escalable. He desenvolupat un petit codi en *Python* que fa les crides necessàries a la api per poder autentificar-se de manera correcta i encriptada, i l'enviament dels batecs. Aquest codi queda en segon pla en el marc d'aquest treball de fi de grau i es implementat purament per a que el sistema funcioni. Es pot trobar en el repositori de codi[34].

En el següent apartat em centraré en l'explicació del codi i del funcionament de la part del servidor i de l'enviament de batecs.

5.4.1 Explicació codi implementat sistema de confirmació de funcionament

En aquesta part em referiré al codi implementat en el repositori [33] o del fitxer *myapi.js* i *myclient.js* que són els més importants en el desenvolupament d'aquesta aplicació.

EL fitxer myapi.js està escrit en *javascript*, aquest conté tota la lògica de la API. Una *Aplication Programming Interfaces* es tracta d'un conjunt de definicions i protocols que s'utilitzen per desenvolupar el software de les aplicacions, permetent la comunicació entre dues o més aplicacions a través d'un conjunt de regles [35]. Em centraré en l'explicació de les regles necessàries per aconseguir els objectius marcats del projecte, les regles que siguin necessàries per el correcte ús del programa s'han desenvolupat de tota manera.

[15] Framework: És un esquema de treball per a realitzar projectes de desenvolupament de software.

Per a poder gestionar la API, s'han de marcar uns *endpoints* que són les URLs d'una API que responen a una petició HTTP [36]. Aquests *endpoints* seran els encarregats de carregar la informació a la persistència de dades.

- **/api/setup/encriptat**: Es el primer *endpoint* que es fa servir i dona tota la informació de la Raspberry en format JSON indicant els valors mostrats en la **Figura 28** i es farà servir la primera vegada que s'executa el codi de *Python* i envia tota la seva informació. Tota la informació que s'envia per aquest *endpoint* va encriptada mitjançant un mètode d'encriptació que explicaré més endavant,

```
{
    "Lat": 41.119722,
    "Lon": 42.119832,
    "Data": "2021-12-20",
    "Hora": "09:10:26",
    "Nom": "Nom_Escola"
}
```

***Figura 28** - JSON a enviar a la API*

- **/api/up**: S'utilitza periòdicament per enviar l'estat de la Raspberry. El format es el mateix que en la **Figura 28** i teòricament només ha de modificar l'hora. El *frontend* de la Raspberry serà l'encarregat de mostrar si està actiu o caigut.
- **/api/enviar**: S'envien les dades del sensor per a guardar-les a la persistència de dades de l'aplicació. Les dades s'envien també en format JSON com es pot veure en la **Figura 29** seguint un format semblant als enviats anteriorment.

```
{
    "Temperatura": 12.0,
    "Humitat": 0,
    "Data": "10/06/1999",
    "Hora": "09:15:26"
}
```

***Figura 29** - JSON a enviar a la API*

Dels *endpoints* anteriors he de fer algunes consideracions. He esmentat al llarg d'aquest apartat i l'apartat anterior el concepte de persistència de dades, en aquest cas es tracta de l'escriptura d'un fitxer JSON, idealment s'hauria de treballar amb una base de dades per evitar problemes d'accés al fitxer però amb el poc volum de dades en que es treballa amb aquest desenvolupament de software es millor seguir amb la dinàmica d'aquest fitxer. Per altra banda, cal comentar també que les dades quan s'envien estan encriptades amb una clau compartida entre el client i el servidor.

Tota la part desenvolupada dels "batecs" no tindria cap sentit si no es pot visualitzar de cap manera. En el mateix repositori [33] parlant dels fitxers *myclient.js*, *index.html* e *index.css* composen el *frontend* de la pàgina. La part més important i la que te pes dins de l'estudi plantejat i per la qual s'ha desenvolupat aquest codi es el fitxer *myclient.js* un fitxer també escrit en *Javascript* que te com a objectiu veure si en els últims 5 minuts hi ha hagut actualitzacions enviades per el kit de sensors i mostrar-les a una plana web en un mapa. D'aquí podem destacar dos parts importants:

- La part del mapa que mostra la pàgina web està feta amb *Open Street Map* [37] que es un projecte dirigit a crear i oferir dades geogràfiques lliures al mon. Aquest eina te llibreries implementades per a fer un mapa personalitzat amb marcadors i elements propis. En aquest cas i com a proves d'exemple, he utilitzat ubicacions de la URV per a representar-les en el mapa i

fer les simulacions de que allí hi ha un kit de sensors. Es mostra d'una manera similar a la de la **Figura 30**

***Figura 30** - Implementació mapa Open Street Map*

- Com a segona part es te el fitxer *myclient.js[33]* que te la configuració lògica dels elements. Aquest codi genera els punters al mapa, els hi dona color depenent del estat en que es troba la Raspberry (Verd si fa menys de 5 min que ha actualitzat l'estat i vermell si fa més de 5 minuts que no ha actualitzat l'estat). A part d'inserir també els valors de la temperatura i humitat en format text dins de la pàgina web.

He realitzat una explicació del codi en format vídeo per a completar tota la informació representada en aquest apartat i per a fer una petita prova. Aquesta representació es pot trobar en el enllaç [38]. El codi del projecte, com he anat referenciant al llarg del apartat es pot trobar en el seu corresponent repositori[33].

5.5 Seguretat de la xarxa

Per a parlar de la seguretat de la xarxa de les escoles del projecte HEURA hem de parlar una mica d'aspectes generals de seguretat en xarxes, el camí que es pot duu a terme de cara d'un atacant per a realitzar un atac a la xarxa i de les mesures que cal prendre per evitar que pugui entrar dins de la xarxa o del dispositiu final usuaris no desitjats.

Les xarxes de computadors estan formades per la interconnexió de milers d'ordinadors. Per tant, a nivell molt bàsic hem de poder definir la seguretat d'un ordinador i aquesta es pot extrapolar al conjunt de la xarxa. En el llibre *Computer Security Handbook* [39] defineix el concepte com la protecció oferta a un sistema d'informació autònom per aconseguir els principals objectius de preservar la **integritat**, la **disponibilitat** i la **confidencialitat** d'aquests sistemes d'informació, ja sigui en el camp del hardware, software, firmware o en l'àmbit de les comunicacions.

Segons el llibre *Network Security Essencials* [40] podem donar una definició als termes per aconseguir els objectius d'aquesta seguretat.

- **Integritat**: Vigilar contra les modificacions d'informació o destrucció de manera inapropiada, assegurant el no-repudi i l'autenticitat d'aquesta. Una pèrdua d'integritat en un sistema es quan uns d'aquests punts anteriors es perd.

- **Disponibilitat**: Assegurar un accés fiable i ràpid per al us de la informació. Es pot perdre aquest aspecte quan dissenyem un sistema de seguretat que no ens permeti realitzar aquests objectius, per tant, aquests sistemes haurien de ser transparents a l'usuari i no haurien de poder apreciar-se.
- **Confidencialitat**: Preservar les autoritzacions i les restriccions a la informació, incloent informació personal i propietària.

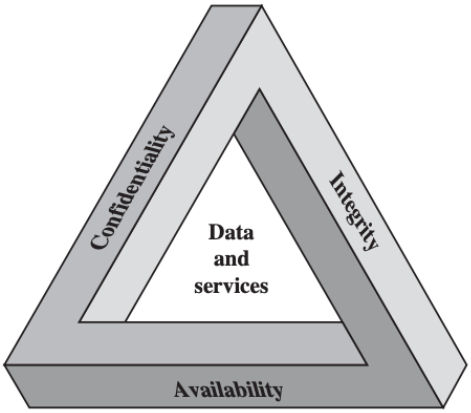

Figura 31. *3 Parts de les dades per a assegurar la seguretat [26]*

Un aspecte molt important de la seguretat i que normalment no es sol parlar gaire es el físic. L'accés físic a una infraestructura o un xarxa d'ordinadors es un aspecte preocupant i que no hi ha prou consciència. En la meva visita a l'escola La Vitxeta descrita en l'apartat Xarxa de l'escola La Vitxeta de Reus, només havent contactat per correu electrònic amb aquesta escola vaig anar i vaig tenir total accés de manera autònoma. En aquest cas un atacant pot enviar un correu de *phishing* fent-se passar per un estudiant realitzant el seu TFG i tindria total accés a la xarxa de l'escola per poder fer qualsevol atac. Aquest fenomen entre d'altres exemples es coneix com a atac d'enginyeria social, el qual es basa en fer una relació humana ja sigui de negoci o personal de manera falsa ocultant la teva identitat per a tenir accés a sistemes informàtics que d'una altra manera només personal autoritzat podria tenir.

En empreses més grans on els seus CPD[16] tenen informació confidencial solen tenir accés biomètric per entrar i només el personal autoritzat per la empresa pot entrar, i si per algun motiu hi ha un visitant al centre ve acompanyat de un guarda de seguretat per evitar possibles atacs d'aquest tipus.

5.5.1 Pentesting a la Raspberry

En el marc d'aquest projecte i en la decisió anterior de la col·locació s'han tingut en compte els tres aspectes anteriors. Moltes vegades els mateixos protocols de xarxa ja ho ofereixen directament. Tot i així es una bona pràctica fer un seguit de proves per a saber que no hi ha cap vulnerabilitat oberta dins d'aquests elements.

Es poden fer algunes proves en la topologia de xarxa exemplificada i amb la Raspberry Pi per veure si el sistema es segur. Aquesta tasca la podríem definir com a *pentesting* [41] que es una pràctica en el mon de la *cyber* seguretat que consisteix en atacar diferents entorns o sistemes amb la finalitat de trobar i prevenir possibles fallades en aquest. Per a fer aquest test de penetració he muntat un sistema de dos

[16] CPD: Centre de processament de dades. Normalment hi solen haver servidors, equipament de xarxa i sistemes d'alimentació ininterrompuda

Raspberry pi una utilitzant Raspbian i l'altre a mb una distribució de Linux especialitzada en aquestes tasques anomenada *Kali Linux*. He utilitzat el mateix adreçament IP que l'usat en la VLAN 2 del projecte HEURA.

He utilitzat la eina *nmap* [42] fent un escaneig dels ports més rellevants que generalment s'utilitzen, de manera segura (-s). La comanda es la següent:

nmap -sV -p 20,21,22,23,25,53,79,80,110,143 192.168.0.0-255

```
┌──(kali㉿kalipi)-[~]
└─$ nmap -sV -p 20,21,22,23,25,53,79,80,110,143 192.168.0.0-255
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-22 13:18 UTC
Nmap scan report for 192.168.0.1
Host is up (0.0033s latency).
```

***Figura 32**. Codi per a escanejar ports de la xarxa*

```
Nmap scan report for 192.168.0.124
Host is up (0.0034s latency).

PORT    STATE  SERVICE  VERSION
20/tcp  closed ftp-data
21/tcp  closed ftp
22/tcp  open   ssh      OpenSSH 7.9p1 Raspbian 10+deb10u2+rpt1 (protocol 2.0)
23/tcp  closed telnet
25/tcp  closed smtp
53/tcp  closed domain
79/tcp  closed finger
80/tcp  open   http     nginx 1.14.2
110/tcp closed pop3
143/tcp closed imap
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

***Figura 33**. Resultat de l'escaneig de ports*

En la sortida de la comanda podem veure els escanejos de tots els hosts que hi ha, dona tots els hosts que troba dins de la xarxa, en la proba han sortit altres elements connectats a la LAN però ens centrarem en la IP 192.168.0.124 ja que es la que correspon a la Raspberry que te Raspbian.

En la sortida de la comanda del *nmap* mostra de tots els ports indicats a dalt els serveis del qual correspon i si està obert. En aquest cas ens ha mostrat que tenim el port **22** amb el servei **OpenSSH** 7.9 obert i un servei **web** al **80** obert també.

Un cop fet aquest escaneig és el moment de fer recerca i trobar possibles vulnerabilitats que siguin compatibles amb els protocols i els ports que hem trobat oberts. A internet hi ha molts cercadors de vulnerabilitats que podem utilitzar per trobar quina es la millor manera d'atacar aquest port. La millor eina és la web CVE*Details* [43] on podem filtrar vulnerabilitats trobades per versió i protocol, com enllaços externs on hi trobarem molta més informació i possiblement algun executable que s'aprofita de la vulnerabilitat. Al buscar una vulnerabilitat per la versió de *openssl* podem trobar la següent vulnerabilitat descoberta per aquesta versió. Explicada tècnicament dins del document [44]

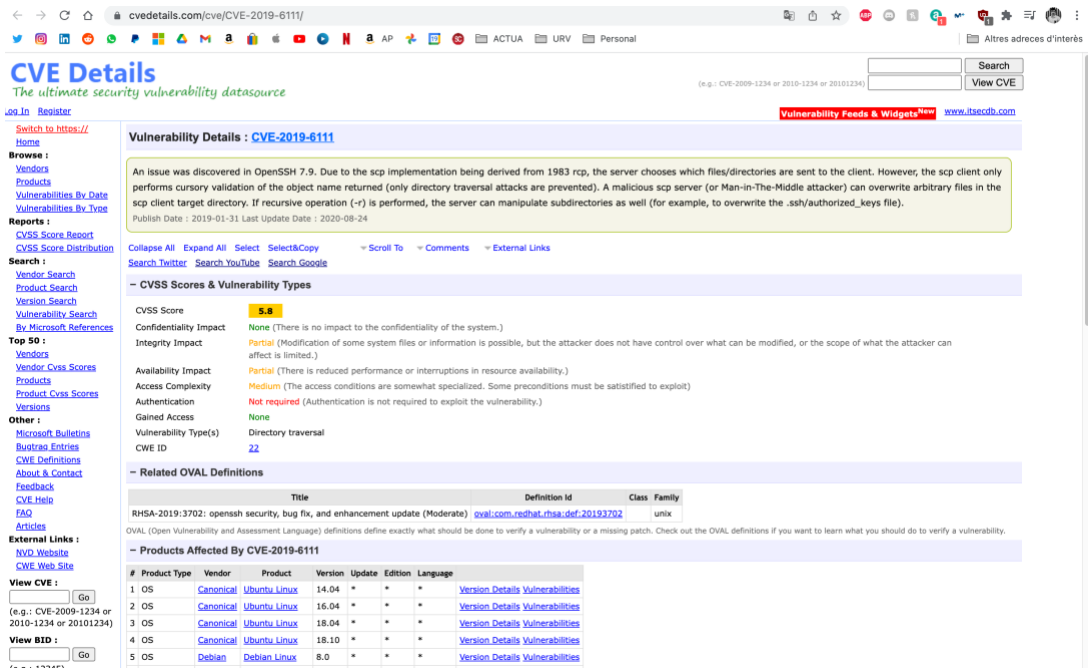

***Figura 34**. CVE Details per a buscar vulnerabilitats [43]*

Es poden trobar moltes altres vulnerabilitats per aquest protocol i depenent de la versió. La mateixa pàgina web ens proporciona estadístiques de les vulnerabilitats que hi ha hagut del protocol al llarg dels anys i quin tipus d'atacs s'han efectuat com es mostra en la **Figura 35**. Vulnerabilitats per any i per tipus

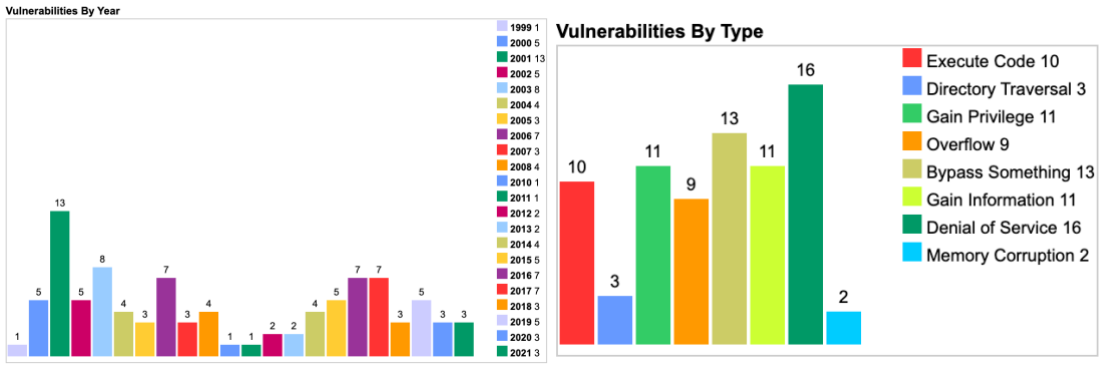

***Figura 35**. Vulnerabilitats per any i per tipus [43]*

En el model de la Raspberry pi i amb la vulnerabilitat descoberta, de moment no s'ha fet cap atac que hagi sortit exitós i no es pot representar. Tot i així amb els coneixements necessaris sobre aquesta vulnerabilitat, hi hauria un punt d'entrada possible al sistema i un possible atac. Com s'ha mostrat en la **Figura 33** també es podrien realitzar les mateixes passes per detectar una vulnerabilitat i intentar atacar el sistema amb el port **80**.

5.6 Simulacions

Una de les parts més importants i en la que s'ha sustentat aquest estudi es la realització de simulacions basant-nos en el entorn real que s'ha plantejat. Aquestes simulacions corroboren el funcionament plantejat i s'han fet conjuntament amb l'estudi del marc teòric per tal de ajudar a la presa de decisions que s'han anat fent al llarg del treball.

La simulació es una eina que ens permet veure el que passa en un entorn real en el que es molt complicat accedir-hi o no es pot aconseguir econòmicament. En aquest apartat m'he centrat en simular la xarxa de les escoles presentades per el projecte HEURA, fent les proves pertinents i efectuant enviament de paquets de dades per a comprovar tota la connectivitat.

Les simulacions estan feta sota les directrius del projecte HEURA, per tant, han de ser similars a totes les infraestructures dels col·legis públics de Catalunya però les simulacions en si no representen cap escola en concret.

S'ha simulat la xarxa amb més elements i amb més camins a realitzar, per tant, infraestructures presentades pel projecte HEURA d'escoles rurals amb una VLAN no s'ha simulat ja que es el mateix concepte molt més simplificat.

5.6.1 Programari a utilitzar

Per a realitzar aquestes simulacions s'ha d'escollir el programari que millor ens convingui. Cal buscar un programa que sigui fàcil d'utilitzar, que doni la màxima versatilitat en l'entorn de xarxa i que les simulacions siguin el més realistes possible.

En el món de les xarxes hi ha varis programes de simulació on cadascun ofereix alternatives diferents i amb valoracions a tenir en compte a l'hora de realitzar les simulacions:

- **Cisco packet tracer**: Es una eina de la companyia Cisco [45] amb la que es possible dissenyar xarxes i realitzar simulacions del seu ús i tràfic. Es una aplicació de descàrrega gratuïta però que s'ha de tenir llicència o conta de Cisco per poder utilitzar-la. Disposa d'una interfície d'usuari intuïtiva que facilita la seva utilització a l'hora d'afegir element de la xarxa. Podem configurar els elements de xarxa de moltes maneres diferents i simulen els sistemes operatius de Cisco i les seves comandes de IOS [46]
- **NetSim**: En un software de xarxes per a modelat i simulació de protocols, investigació i desenvolupament de xarxes i aplicacions de defensa. Permet analitzar sistemes informàtic a fons. [47]. Es un programa que s'utilitza per a estudiar certificacions Cisco. Te una versió disponible de prova i una amb llicència.
- **GNS3**: Segons la seva pagina web [48] es un software per construir dissenyar i testejar una xarxa en un entorn lliure de riscs. Es un entorn de simulació a temps real amb funcions per a fer tests abans de la distribució als elements físics. La xarxa es pot provar amb molts productes de fabricants diferents. Una característica que el fa especial es que el pots connectar directament a una xarxa real fent servir elements físics i de simulació en el programa.

Aquests simuladors són els principals en el món de l'educació i la investigació, n'hi ha d'altres específics en certs aspectes de les xarxes i que busquen altres objectius. Per a la simulació d'una escola pública de Catalunya un simulador amb capacitats de simular una LAN i que calculi be les rutes es necessari.

En **aquest projecte** he escollit el simulador **Cisco Packet Tracer** per a treballar. Es un programa que ja he fet servir en anterioritat i el llenguatge de comandes Cisco el conec (ja que per cada fabricant les comandes poden variar les unes de les altres), es un software que a través de la universitat tinc accés i es un dels més potents del món i que més es recomanen per les simulacions. L'única limitació que te es que els elements de xarxa que es poden simular només poden ser de la marca *Cisco*, cosa que fa que no s'hagin pogut utilitzar els models exactes d'elements de xarxa que el projecte HEURA recomana tot i que això en cap cas afecta la funcionalitat ni altera els resultats obtinguts de les simulacions.

5.6.2 Simulació connexió VLAN 2

Com he comentat en els apartats anterior hi ha dos maneres per a connectar la Raspberry Pi, el més fiable i amb una robustesa més gran donada la tecnologia discutida en l'apartat 4.1 es connectar-lo per cable a la VLAN 2. Aquesta primera simulació es centra en aquest aspecte, tenint en compte tots els elements de configuració de xarxa presentats en els apartats anteriors. L'esquema general de la simulació ve donada per el següent esquema:

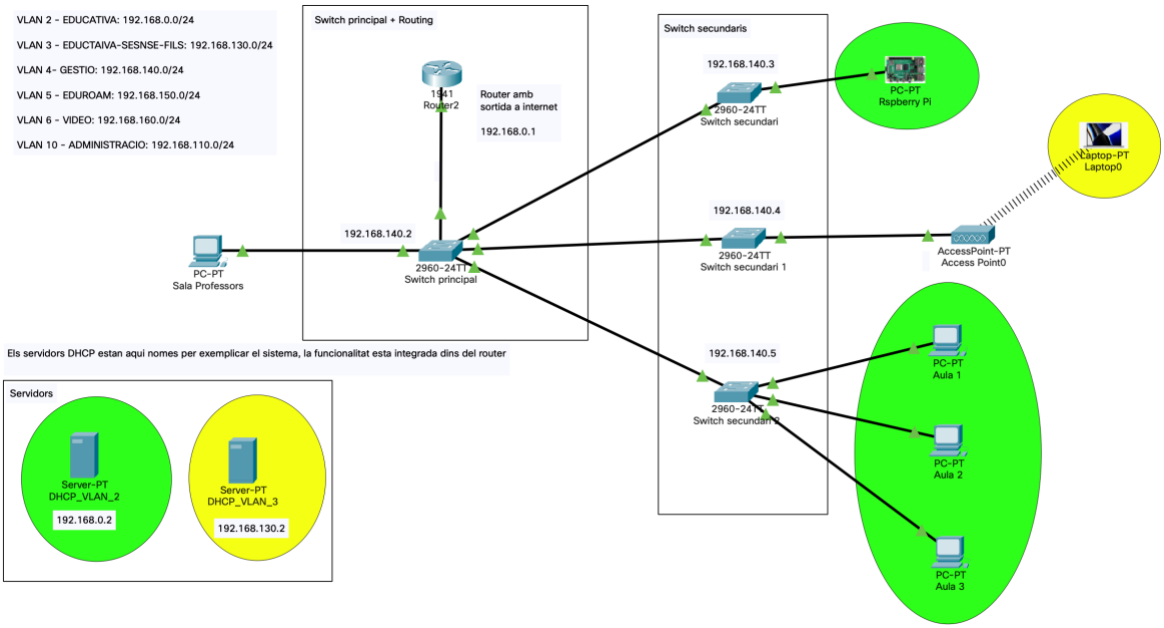

Figura 36. Simulació integració Kit de sensors VLAN 2

En aquesta simulació podem veure la Raspberry Pi connectada en un dels commutadors secundaris els quals tenen ports disponibles en la VLAN 2. Les adreces venen gestionades per DHCP per el commutador principal configurades al Annex show running-config commutador principal, he ficat físicament dos servidors DHCP per a representar-ho gràficament a la simulació i veure els diferents dominis d'actuació. En cap cas modifiquen aquests el comportament de la xarxa o de l'obtenció de les adreces IP. Es pot comprovar aquest adreçament entrant a la línia de comandes de la Raspberry com es pot veure en la següent figura (**Figura 37**):

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::20B:BEFF:FE4E:2651
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.0.2
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.0.1
```

Figura 37. IP Raspberry Pi dins del rang VLAN 2

Tots els paquets de la Raspberry pi passen per el commutador secundari en el que estigui connectada, aquest també te configurades les VLAN necessàries per a fer les distinció d'aquestes xarxes virtuals d'àrea local privades. Aquests commutadors a part de tenir les VLAN configurades per a que puguin travesser els diferents ports i que puguin donar connexió als dispositius connectats als ports configurats

com he discutit en la **Figura 15.** Distribució ports commutador/s secundari/s han de tenir una adreça de gestió que pugui ser accessible per a un ordinador amb la IP de gestió corresponent. Aquesta adreça de gestió està a la VLAN 4 i es necessària per a connectar-se remotament al commutador amb el protocol ssh o Telnet per a fer tasques de manteniment i de configuració per l'administrador de la xarxa. Aquesta VLAN com s'ha explicat en l'apartat 4 del treball no es pot veure des de les altres VLAN, per tant a ulls de la Raspberry pi no s'hi pot connectar i tampoc arriben els *ping* en el cas de realitzar-ne un. En aquest cas la adreça assignada ha d'estar dins del rang i per tant no afecta a l'ús de la xarxa quin numero de host fiquem. En el cas d'aquesta simulació he ficat al commutador que esta directament al kit de sensors l'adreça 192.168.140.3 amb màscara 255.255.255.0. Això es pot comprovar amb la comanda: `show running-config` dins del commutador [**Figura 38**] la configuració sencera en forma de comandes IOS de cisco està en el Annex show running-config commutador secundari.

```
interface Vlan1
 no ip address
 shutdown
!
interface Vlan4
 ip address 192.168.140.3 255.255.255.0
```

***Figura 38**. IP de gestió*

Per a provar l'ús d'aquesta xarxa es pot fer una sèrie de simulacions de tràfic de xarxa per a demostrar que funciona. Les proves realitzades venen resumides en la següent taula.

Prova	**Origen**	**Destí**	**Estat**
Ping	Raspberry Pi 4	Laptop	OK
Ping	Raspberry Pi 4	Aula 1 (mateixa VLAN)	OK
Ping	Raspberry Pi 4	Encaminador	OK

***Taula 9**. Proves de connexió simulades VLAN 2*

Totes aquestes proves es poden corroborar en la resposta del programa en la **Figura 39** en aquest cas totes les proves han estat efectuades correctament assegurant la connectivitat de les connexions estudiades.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	Rspberry Pi	Laptop0	ICMP		0.000	N	0
	Successful	Rspberry Pi	Aula 1	ICMP		0.000	N	1
	Successful	Rspberry Pi	Router2	ICMP		0.000	N	2

***Figura 39**. Proves correctes al Packet Tracer*

5.6.3 Simulació connexió VLAN 3

La simulació de la connexió a la VLAN 3 es molt similar a la feta en l'apartat anterior ja que les bases d'aquesta són les mateixes i per tant les probes i les configuracions realitzades són molt similars.

En aquest cas efectuem el canvi de la Raspberry Pi de la xarxa cablejada a la de sense fils, es passa a treballar dins del domini de la VLAN 3 amb el seu adreçament IP corresponent marcat en la **Taula 6.**

Rang IP diferents VLANs projecte HEURA. En aquest cas la topologia general ve donada de la següent manera:

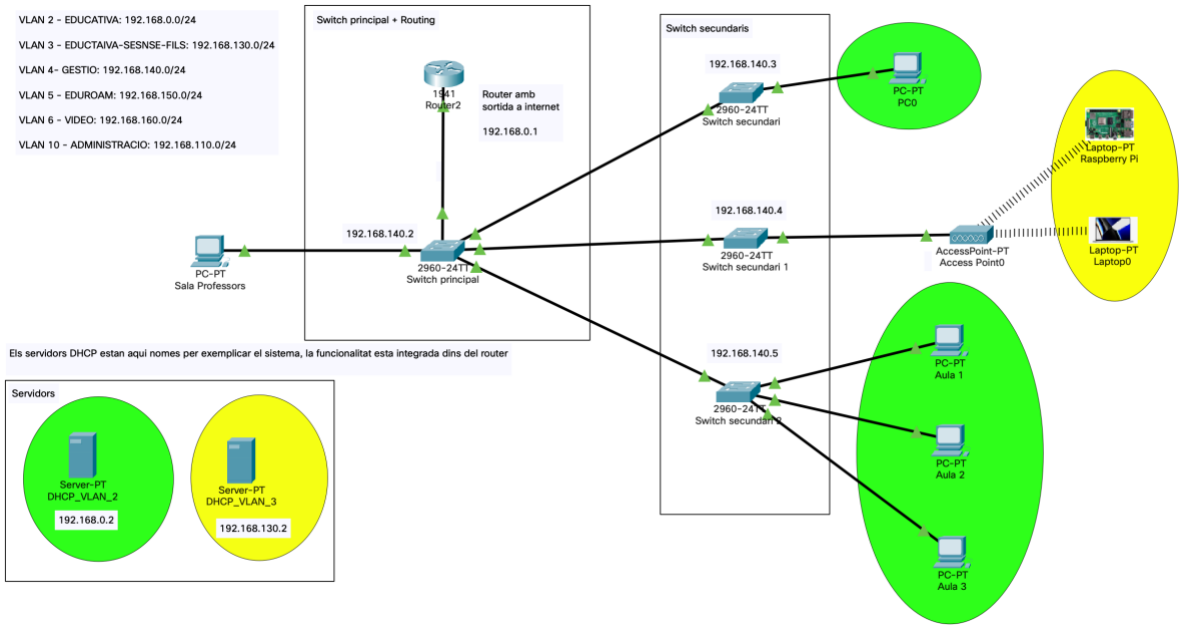

***Figura 40**. Topologia de xarxa amb Raspberry connectada a la VLAN 3*

En aquesta topologia mantenim les configuracions del commutador principal trobades en el apartat Annex show running-config commutador principal i les del commutador secundari trobades en el apartat Annex show running-config commutador secundari. Tot i així per a fer la connexió s'ha hagut de configurar el punt d'accés sense fils per poder transmetre un SSID[17] de l'escola i configurar la Raspberry Pi per a que es pugui connectar a aquesta xarxa.

Per part del punt d'accés sense fils te molt poca configuració, és el model genèric de Cisco i radia a 2,4GHz, amb un autentificació WPA2-PSK i encriptació AES. Com a clau d'accés i per a fer aquestes proves he ficat la clau 12345678, cosa que no es recomana mai fer ja que és una falta de seguretat molt gran.

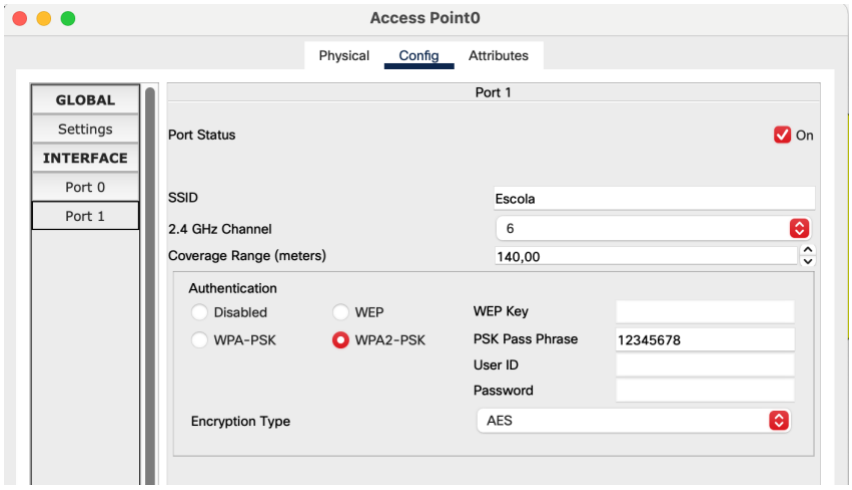

***Figura 41**. Configuració punt d'accés Cisco*

[17] SSID: *Service Set Identifier*. Es podria definir vulgarment com el "nom del Wi-Fi"

En aquesta configuració no cal fer cap modificació ni indicar en quina VLAN és treballa ja que aquesta tasca la desenvolupa el commutador al qual està connectat el punt d'accés. Per tant, un cop aquestes configuracions han estat realitzades i la Raspberry connectada al punt d'accés, es pot observar l'assignació DHCP que li ha donat el sistema. En aquest cas com ja he indicat en l'apartat anterior s'ha exemplificat l'ús dels servidors DHCP amb una màquina física però aquesta funcionalitat està integrada en el commutador de nivell 3.

A nivell de la Raspberry podem obtindré la seva IP des de la consola de comandes. La configuració realitzada és correcte i s'assigna una adreça dins del rang esperat com es pot veure en la **Figura 42**.

```
C:\>ipconfig

Wireless0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::290:CFF:FEAC:5DA4
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.130.3
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.130.1
```

***Figura 42**. IP de la Raspberry Pi en la VLAN 3 sense fils*

Per a comprovar que les configuracions fetes s'han realitzat de manera correcte podem fer unes petites probes per a veure si la connexió funciona be. Podem esperar el mateix resultat que hem obtingut amb la connexió per cable, ja que sota la capa de configuració el funcionament de les dos tecnologies és el mateix en quan a tractament de trames i formació de paquets. Si seguim les proves de l'apartat anterior per a tenir una consistència major podem extreure que:

Prova	**Origen**	**Destí**	**Estat**
Ping	Raspberry Pi 4	Laptop (mateixa VLAN)	OK
Ping	Raspberry Pi 4	Aula 2	OK
Ping	Raspberry Pi 4	Encaminador	OK

***Taula 10.** Proves de connexió simulades VLAN 3*

Aquesta taula és pot corroborar amb la sortida del programa quan es simula la xarxa. En aquest cas totes les proves han estat realitzades amb èxit dins de la simulació, com es pot comprovar en la **Figura 43**

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Raspberry Pi	Laptop0	ICMP		0.000	N	0	(edit)	(delete)
	Successful	Raspberry Pi	Aula 2	ICMP		0.000	N	1	(edit)	(delete)
	Successful	Raspberry Pi	Router2	ICMP		0.000	N	2	(edit)	(delete)

***Figura 43**. Resultat proves VLAN 3 Packet Tracer*

Amb aquests resultats i els de l'apartat anterior he pogut demostrar que els dos mètodes estudiats per a realitzar la connexió de la Raspberry Pi funcionen correctament i que per tant dins del marc del estudi del projecte, el kit de sensors es pot situar sense cap problema en **qualsevol dels dos llocs** garantint la

connexió dins de la xarxa amb altres dispositius i la connexió cap a internet, de manera que les dades poden fer el seu camí satisfactòriament a través d'internet.

Durant la simulació lògica de la xarxa m'he trobat amb el problema que amb el commutador de nivell 3 que proporciona el *Packet Tracer* no es pot configurar la xarxa amb un ús correcte. Per tant, he hagut de simular el commutador de nivell 3 amb un de nivell 2 i un *router on a stick.*

5.6.4 Simulació física

El programari *Cisco Packet Tracer* te l'opció de distribuir la xarxa d'una manera física i ens permet veure el rang de cobertura dels punts d'accés que estiguin implementats en la xarxa. Per tant en les simulacions dels apartats anterior he fet una petita distribució física sobre un plànol d'una escola que ja ofereix el mateix programari. En aquest apartat el que vull fer èmfasi és la distribució de l'equipament dins dels armaris per reforçar el descobert en la distribució en l'escola de La Vitxeta i la distribució que demana el projecte HEURA.

El primer a tenir en compte en aquesta distribució és la mida de l'escola en la que es treballa, en aquest cas, el mapa que proporciona el programa és relativament petit. Un cop així podem distribuir els elements per les diferents aules.

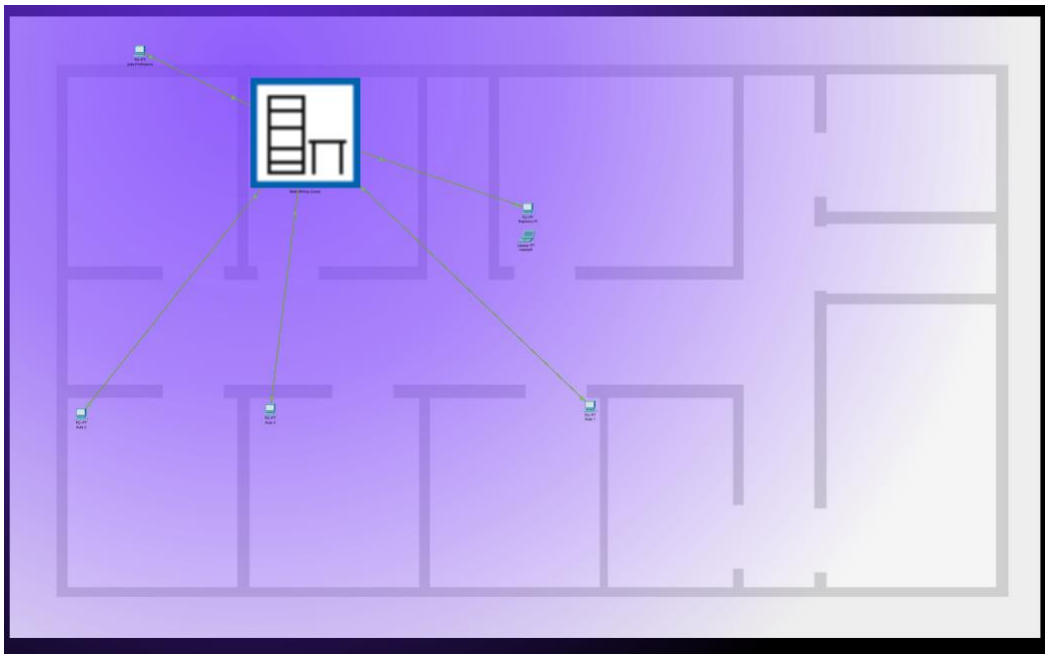

***Figura 44**. Distribució física dels elements*

Com es pot veure en la **Figura 44** la gamma de colors lila representa la cobertura del punt d'accés que es troba dins l'armari de comunicacions. Dins d'aquest es pot trobar tot l'equipament de xarxa. En aquest cas i per la mida de l'escola he optat per ficar-ho tot dins de la mateixa sala però seguint la distribució vista en la escola La Vitxeta com es pot veure en la **Figura 21** i en la **Figura 22**. Obtenint així els diferents armaris:

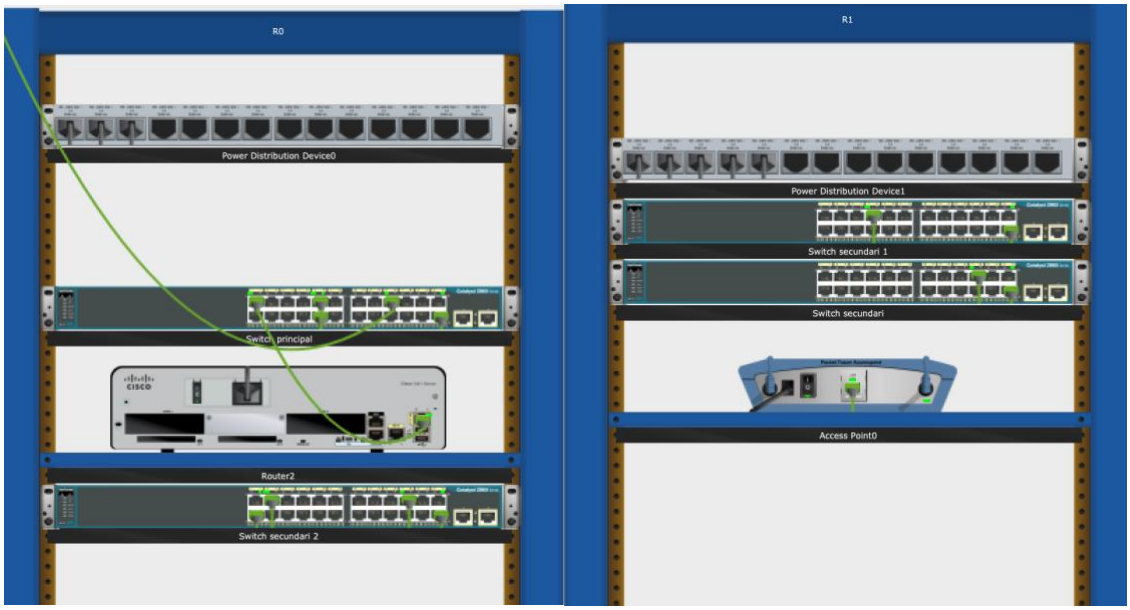

***Figura 45**. Armari primari R0 i secundari R1*

Tenint en el armari R0 o principal el encaminador que dona accés a internet, el commutador principal i un commutador secundari. I en el armari R1 com està implementat en l'escola visitada, hi ha un parell de commutadors secundaris i un punt d'accés tot i que aquest últim hauria d'estar idealment distribuït per les diferents zones de l'aula, com que en aquesta simulació dona bona cobertura a tota la planta, es pot deixar en aquest armari per estalviar cablejat i espai.

Com a conclusió de la simulació física i amb retrospectiva amb les simulacions fetes respectives als dos mètodes de connexió, puc concloure en que la viabilitat de connexió de les dues formes com s'ha descobert amb l'estudi de la infraestructura del projecte HEURA [18] és totalment bona i que en qualsevol dels dos llocs de connexió tenim bona velocitat de xarxa i visió cap a internet. De part de la simulació física he descobert que és viable la manera en què esta configurada en l'escola La Vitxeta i com està representada en el projecte HEURA.

6 Conclusions i línies futures

6.1 Conclusions

Per a concloure m'agradaria fer algunes petites consideracions dels resultats obtinguts com l'esforç que m'ha suposat.

El treball al començament sembla una muntanya que no saps per on pujar-la, et vas plantejant petits objectius i segmentant el treball per tal de poder fer-lo de la millor manera possible, sempre donant peu a possibles replantejos, apartats que no porten a cap lloc i s'han de refer. Tot i tenir tots aquests reptes, els objectius expressats en l'índex del treball s'han desenvolupat de manera satisfactòria.

L'estudi de la xarxa d'àrea local de les escoles de primària de Catalunya ha estat un èxit, gràcies en part per la bona documentació que hi ha per part de la Generalitat, com per la possibilitat que he tingut de visitar un centre i fer probes de connexió en un entorn real.

L'estudi de l'ús de la Raspberry i la implementació d'un sistema de monitorització han estat la part central del projecte amb més dificultats tècniques ja hagin estat per el desconeixement inicial de les eines a utilitzar o dels processos a seguir.

A nivell personal el treball m'ha aportat una gran quantitat de coneixements que no hagués adquirit sinó hagués tingut l'oportunitat de realitzar aquest treball ni de col·laborar amb el projecte ACTUA.

6.2 Línies Futures

Un projecte d'aquesta mida sempre té petites millores que fer i es podria dir que és inacabable, tot i així hi ha coses que es podrien afegir o millorar en una futura revisió del projecte o en una posada en producció d'aquest.

El sistema de monitorització del kit de sensors es pot desenvolupar d'una manera més ordenada i preparada per a la producció, ja que en aquest treball m'he centrat en el seu funcionament i el programa pot tenir alguns *bugs* no desitjats.

La finalitat d'aquest treball és ajudar al projecte ACTUA a completar el seu objectiu i tenir un major coneixement de la xarxa. A l'entrega d'aquest treball estic col·laborant laboralment amb el projecte i espero que les coses que s'han mencionat en aquest treball i els seus elements puguin estar implementats d'una manera correcta en un entorn de producció. Tota aquesta informació s'anirà actualitzant en la pàgina web del projecte.

Els processos de xarxes de sensors com aquestes i de connexions similars dona peu a moltes alternatives i moltes línies d'investigació que en un futur es pot fer ús d'elles. Ja que cada vegada més la tendència de les xarxes de sensors, el internet de les coses i la monitorització d'ambients va en augment i sempre s'ha de garantir el bon funcionament d'aquests elements i la protecció de dades del individu.

Segur que en l'amplada de tot el treball hi ha alguna línia més que seguir, tot i així crec que s'ha dut a terme de la millor manera possible complint els objectius marcats inicialment i d'una manera satisfactòria.

7 Referències i recursos web

[1]Deloitte. “IoT- Internet Of Things”. [Accés: 16/10/21] URL: https://www2.deloitte.com/es/es/pages/technology/articles/IoT-internet-of-things.html

[2] Smart classroom projecte. “¿Que es una Smart Classroom?” [Accés: 17/11/21] URL: https://smartclassroomproject.com/que-es-una-smart-classroom/

[3] Cebrián, G.; Palau, R.; Mogas, J. “The Smart Classroom as a Means to the Development of ESD Methodologies”. [Accés 31/12/21] URL: https://doi.org/10.3390/su12073010

[4]Mogas, J.;Márquez Ruiz, M; Palau, R. “Presente y futuro de las condiciones ambientales en las Smart classroom” llibre INNOVAGOGIA 2020 [Accés: 1/12/22] URL: https://www.innovagogia.es/innovagogia-2020/

[5] Raspberry Pi fundation. “Raspberry Pi” [Accés 16/10/21] URL: https://www.raspberrypi.org/

[6]Comohacer.eu, “Comparativa Raspberry Pi” [Accés: 3/12/21] URL: https://www.comohacer.eu/comparativa-y-analisis-raspberry-pi-vs-competencia/

[7] Raspberry Pi fundation. “Raspbian ” [Accés: 18/10/21] URL: https://www.raspbian.org/

[8] Microsoft. “Windows IoT Core” [Accés: 18/10/21] URL: https://docs.microsoft.com/es-es/windows/iot-core/windows-iot

[9] LibreELEC “LibreELEC” [Accés: 18/10/21] URL: https://libreelec.tv/

[10] Retropie. “Retropie” [Accés: 18/10/21] URL: https://retropie.org.uk/

[11]Sunfounder. “Humidity sensor module” [Accés: 2/11/21] URL: http://wiki.sunfounder.cc/index.php?title=Humiture_Sensor_Module

[12] Thonny org. “Thonny IDE” [Accés: 12/10/21] URL: https://thonny.org/

[13]Gobierno de España “BOE-A-2018-16673” [Accés: 24/10/21] URL https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

[14] RemoteIt [Accés: 2/11/2021] URL: https://remote.it/

[15] DWService [Accés: 2/11/2021] URL: https://www.dwservice.net/

[16] Teamviewer [Accés: 2/11/2021] URL: https://www.teamviewer.com/es/

[17] Sainz Raso, Jorge & Martín, Sergio & Diaz, Gabriel & Castro, Manuel. (2019). Security Vulnerabilities in Raspberry Pi–Analysis of the System Weaknesses. IEEE Consumer Electronics Magazine. 8. 47-52. 10.1109/MCE.2019.2941347.

[18]Generalitat de Catalunya. “Projecte HEURA” [Accés: 8/11/21] URL: http://xtec.gencat.cat/ca/at_usuari/guies/projecteheura/

[19] Lliure Ferré “Conceptos generales de Wi-Fi” [Accés: 12/8/21] Arxiu

[20]Ionos. “¿Qué es el Ethernet?” [Accés: 18/11/21] URL: https://www.ionos.es/digitalguide/servidores/know-how/ethernet-ieee-8023/

[21] Dr. Agustí Solanas “Disseny de Xarxes, Xarxes d’alta velocitat i troncal”. [Accés: 2/11/21]

[22] Cisco “Estructura de capes” [Accés: 21/10/21] Document dins del curs CCNA network essentials.

[23] Cisco “Switching, Routing, y Wireless Essentials” [Accés: 21/10/21] Document dins del curs CCNA network essentials.

[24]Servidores DHCP [Accés: 12/11/21] URL: https://www.sites.google.com/site/redeslocalesyglobales/5-redes-mixtas-integradas/5-servicios-en-red/servidores-dhcp

[25] Programmer click. “Formato de trama de datos VLAN encapsulada 802.1Q” [Accés: 3/11/21] URL: https://programmerclick.com/article/4011728695/

[26] UCM “Telefonia fija” [Accés: 3/11/21] URL: https://www.uc3m.es/sdic/servicios/telefonia-ip-fija

[27] Santander. “Qué es python y porque deberiamos aprender a usarlo” [Accés: 28/11/21] URL: https://www.becas-santander.com/es/blog/python-que-es.html

[28]Batista, E.; Villanova, O. “Codi Python projecte ACTUA” [Accés: 7/1/22] URL: https://github.com/edgarbdf/urv-actua

[29] Renata Teixeira, Keith Marzullo, Stefan Savage, and Geoffrey M. Voelker. 2003. In search of path diversity in ISP networks [Accés: 1/12/21] URL: https://doi.org/10.1145/948205.948247

[30] Neil Spring, Ratul Mahajan, and David Wetherall. 2002. Measuring ISP topologies with rocketfuel. [Accés: 1/2/21].URL: https://doi.org/10.1145/964725.633039

[31]Platzi, “Cual es la diferencia entre frontend i backend” [Accés: 3/12/21] URL: https://platzi.com/blog/que-es-frontend-y-backend/

[32]Node.js [Accés: 13/11/21] URL: https://nodejs.org/es/

[33]Villanova, O. “Codi desenvolupat TFG” [Desenvolupat al llarg del treball] URL: *https://github.com/oriol-v-ll/WEB_API*

[34]Villanova, O. “Python desenvolupat TFG” [Desenvolupat al llarg del treball] URL: *https://github.com/oriol-v-ll/WEB_API/tree/master/nodePythonApp*

[35]Xataka, “API: Que es y para que sirve” [Accés: 27/12/21] URL: https://www.xataka.com/basics/api-que-sirve

[36]Stack Overflow, “¿Que es un entry point i un end point?” [Accés: 14/12/21] URL: https://es.stackoverflow.com/questions/51758/qu%C3%A9-es-un-entry-point-y-un-end-point/51764

[37]Open Street Map [Accés: 12/12/21] URL: https://wiki.openstreetmap.org/wiki/ES:P%C3%A1gina_principal

[38]Villanova, O “Vídeo explicatiu del codi” URL: https://www.youtube.com/watch?v=8NuSJp6pHKw

[39]Seymour Bosworth, Michel E.Kabay, Eric Whyne. “Computer security handbook” [Accés: 20/11/21] Llibre

[40]William Stallings "Network security essentials:*applications and standards* fourth edition" [Accés: 25/11/21] Llibre

[41]Campus ciber seguridad [Accés: 25/11/21] URL: https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting#:~:text=El%20Pentesting%20es%20una%20abreviatura,posibles%20fallos%20en%20el%20mismo.

[42] nmap.org. "nmap" [Accés: 26/11/21] URL: https://nmap.org/

[43] CVEDetails [Accés: 26/11/21] URL: https://www.cvedetails.com/

[44] scp client multiple vulnerabilities [Accés: 29/11/21] URL: https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt

[45] Cisco "Cisco Packet Tracer" [Accés: 11/11/21] URL: https://www.netacad.com/es/courses/packet-tracer

[46] Cisco "IOS Cisco" [Accés: 30/11/21] URL: https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-software-releases-listing.html

[47] Boson. "Network Simulator" [Accés: 24/11/21] URL: https://www.boson.com/netsim-cisco-network-simulator

[48] GNS3 [Accés: 24/11/21] URL: https://www.gns3.com/software

8 Annexos

8.1 Annex show running-config commutador secundari

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/2
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/5
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 3
switchport mode access
!
interface FastEthernet0/8
switchport access vlan 3
switchport mode access
!
interface FastEthernet0/9
switchport access vlan 3
switchport mode access
!
interface FastEthernet0/10
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/11
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/12
switchport access vlan 2
switchport mode access
```

```
!
interface FastEthernet0/13
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/14
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/15
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/16
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/17
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/18
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/19
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/20
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/21
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/22
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/23
switchport mode trunk
!
interface FastEthernet0/24
switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
interface Vlan4
ip      address      192.168.140.3
255.255.255.0
!
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
```

8.2 Annex show running-config commutador principal

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname switch_principal
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/2
switchport access vlan 4
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 3
switchport mode access
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
switchport mode trunk
!
interface FastEthernet0/10
switchport mode trunk
!
interface FastEthernet0/11
switchport mode trunk
!
interface FastEthernet0/12
switchport mode trunk
!
interface FastEthernet0/13
switchport mode trunk
!
interface FastEthernet0/14
switchport mode trunk
!
interface FastEthernet0/15
switchport mode trunk
!
interface FastEthernet0/16
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/17
switchport access vlan 2
```

```
switchport mode access
!
interface FastEthernet0/18
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/19
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/20
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/21
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/22
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/23
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
interface Vlan4
ip address 192.168.140.2
255.255.255.0
!
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
end
```