Universitat de Girona
Escola Politècnica Superior

Treball final de grau

Estudi: Grau en Enginyeria Informàtica

Títol: Desenvolupament d'un sistema de monitoratge de la xarxa Wi-Fi d'una empresa

Document: Memòria

Alumne: Sergi Fernandez Rios

Tutor: Lluís Fàbrega Soler
Departament: Arquitectura i Tecnologia de Computadors
Àrea: Arquitectura i Tecnologia de Computadors

Convocatòria (mes/any): setembre 2019

Continguts

1.-Introducció

1.1.-Motivació

Comexi es una empresa fundada al 1954 enfocada a crear maquinaria per la conversió de l'envàs flexible, hi ha 2 seus una a brasil i una a Riudellots de la selva sent aquesta la principal.

Actualment hi ha sobre unes 400 persones treballant a Comexi Girona, com és normal amb una quantitat tan gran de persones el parc informàtic també és molt gran i variat hi ha des de servidors, Workstation de sobretaula o portàtils pels enginyers que necessiten un ordinador amb potència, sobretaules per personal d'oficina que no necessita mobilitat, portàtils per la gent d'oficina que sí que necessita la mobilitat sigui per anar a reunions o disposa de diferents llocs de treball, portàtils pels tècnics que puguin veure els plànols en 3 d menters estan fent el muntatge de les màquines,portàtils més lleugers perquè els comercials els puguin moure per tot el món a l'hora de fer el seu treball i també PDAs per la gent de magatzem a l'hora de rebre i gestionar tota la mercaderia que arriba.

A Comexi tenim uns 425 Ordinadors d'ells 318 són portàtils aquest número fa uns anys era molt inferior, gràcies a la mobilitat que aporta un portàtil s'ha apostat en gran mesura per una major utilització dels portàtils a diferència de sobretaules.

Actualment tenim uns 400 telèfon intel·ligent d'empresa a Comexi, la possibilitat de tenir connexió a internet, poder consultar el correu o la missatgeria instantània dintre de la mateixa empresa ha fet que siguin molt útils pel dia a dia.

Però igual que els portàtils en els últims anys hem passat de tenir telèfons fixes a petits mòbils sense connexió a internet a smartphone que utilitzen internet i es connecten al WI-FI de l'empresa.

Tot això ha millorat l'eficiència de l'empresa i la mobilitat, però té un cost actualment la xarxa WI-FI que tenim esta pensada i dissenyada fa uns anys i alguns de aquest canvis en la tecnologia no es van preveure, alguns usuaris es queixen que la xarxa Wi-Fi no tenen prou cobertura o perden la connexió temporalment.

Des de l'empresa hem decidit muntar algun sistema per fer un monitoratge de la xarxa en temps real i que ens avisi si alguna falla com per exemple un Accés Point(a partir d'ara AP) que deixa de funcionar o si hi ha molts usuaris connectats a un AP.

El que ens dedicarem en aquest treball és veure si la xarxa actual de APs té bona cobertura, quin sistema de monitoratge muntem i analitzarem les dades que puguem extreure per aplicar millores o propostes de millores sobre la xarxa de l'empresa.

1.2.-Objectius

L'objectiu és analitzar la xarxa Wi-Fi de l'empresa a fi de millorar la seva cobertura i la qualitat del seu servei (retard baix, velocitat gran, etc.), i més concretament:

1) posar en marxa una eina de monitoratge de la xarxa Wi-Fi de l'empresa que permeti saber el seu estat, detectar els problemes, analitzar el seu rendiment.

2) proposar solucions als problemes existents i millores.

2.-Viabilitat del projecte

2.1.-Viabilitat tècnica

Perquè el projecte es pugui dur a terme es necessitarà un software per fer un monitoratge d'una xarxa Wi-Fi, serà necessari instal·lar-ho en algun Servidor, per últim serà necessari disposar de APs i dispositius Wi-Fi per fer les proves si fos necessari.

2.2.-viabilitat econòmica

Per dur a terme aquest projecte es buscarà utilitzar Software gratuït i s'intentarà utilitzar tot el material del qual ja disposem a l'empresa, en cas de haver de comprar o fer alguna inversió es quedarà proposat com una inversió de millora per fer en un futur i només quedarà constància al projecte com proposta.

Per tant el cost econòmic serà mínim perquè a més del ja esmentat jo faré totes les configuracions i proves que siguin necessàries.

2.3.-Pressupost

Al ser jo l'únic que treballarà en el projecte, i l'única despesa serà les meves hores el pressupost relatiu seria el meu sou per les hores que volem dedicar al projecte.

Aproximadament es farà en unes 150 hores el projecte a un preu per hora de 5€/hora queda un pressupost com el següent:

Desglossament d'hores		Hores	Preu
	Implementació sistema monitoratge	50 Hores	250
	Proves del sistema de monitoratge	25 hores	125
	Cerca de problemes i propostes de millora	75 hores	375
Altres conceptes			
	Software de monitoratge		0
	Material per fer proves		0
Total			750 €

3.-Metodologia

Per dur a terme el projecte el que farem serà un crear un entorn de proves amb una màquina virtual on instal·larem l'eina de monitoratge i es faran totes les configuracions perquè funcioni perfectament, una vegada això sigui estable i funcioni tal com esperem es passarà a un servidor productiu.

Una vegada en productiu recollirem dades d'unes quantes setmanes per poder analitzar els problemes que poden tenir la xarxa. Amb les dades podrem revisar quins problemes hi ha a l'empresa i començarem a treballar en solucions.

Les solucions que es puguin les posarem a terme i revisarem que siguin viables i possibles, les que no serà recomanacions i aspectes a millorar que es plantejaran al cap d'informàtica per fer inversions en el futur.

4.-Planificació

El projecte ja que era una proposta feta des de l'empresa es va decidir que es faria dins del meu horari de treball i es va estimar uns 3 mesos que començaria la setmana de 18 de març, a una mitja d'una hora i mitja al dia, per veure com es faria tot es va crear una planificació inicial (veure figura 1), aquesta planificació acaba en el moment en el qual el servidor estava en productiu.

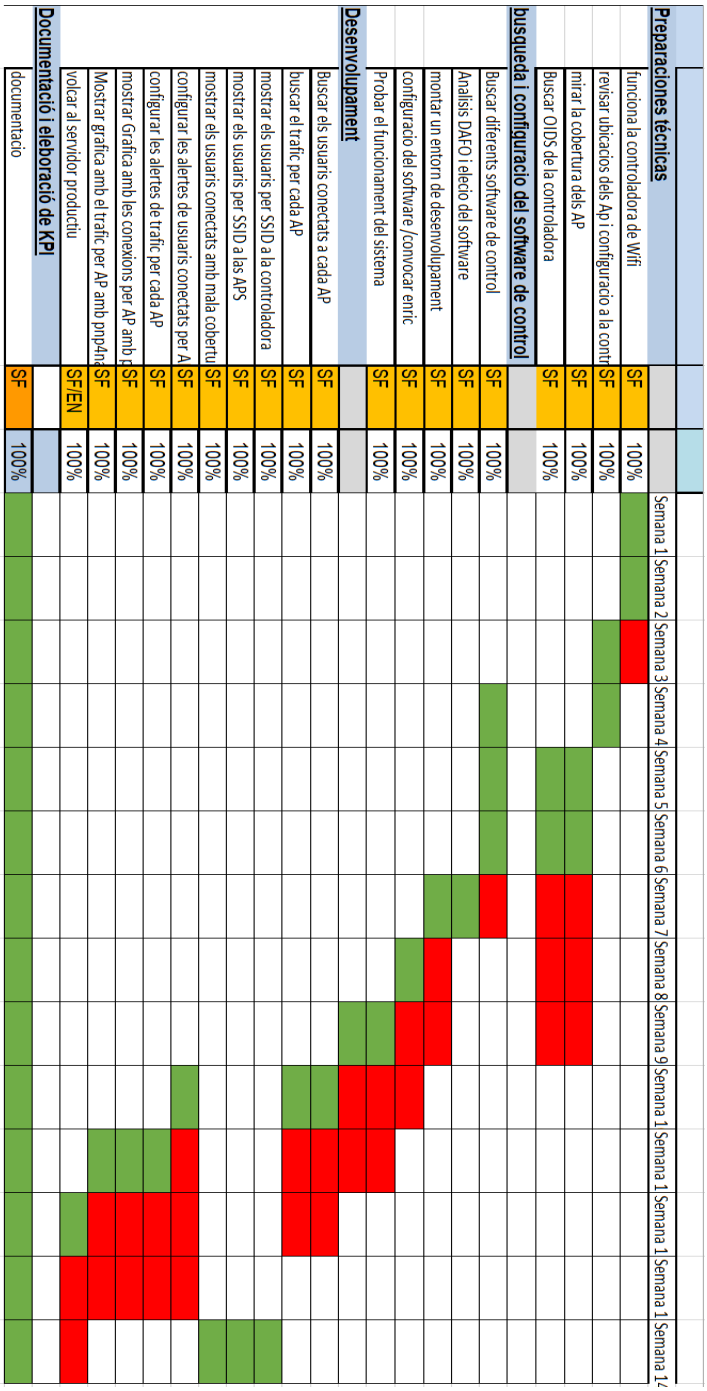


Figura 1 Planificació

En la figura es pot veure que en verd el temps previst inicialment i en vermell el retràs sobre el temps previst, la suma dels dos és el total de el qual ha costat fer cada part planificada.

Encara que es va acabar a mb una mica de retràs aquesta part, inicialment estava pensada per durar 12 setmanes i no 14 però per la carregà de treball i que el projecte va començar amb una setmana de retràs el total va ser dues setmanes extra en aquest apartat.

Per la segona part del projecte recopilació de dades, cerca de problemes i possibles solucions hem dedicat un mes i mig(veure figura 2) a partir de la finalització del fet que el sistema estigues en productiu, les tres primeres setmanes per recopilar les dades, una per buscar el problema i dos més per veure possibles solucions i provar si és possible les solucions.

	Setmana 15	Setmana 16	Setmana 17	Setmana 18	Setmana 19	Setmana 20
Recopilació de dades						
Anàlisis de les dades						
Cerca de solucions i proves						

Figura 2 Planificació de la segona part

5.Conceptes bàsics de la tecnologia de xarxa Wi-Fi

5.1.-Xarxa Wi-Fi

La xarxa Wi-Fi es basa en l'estàndard IEEE 802.11 [1],[2] , utilitza la ràdio freqüència per poder transmetre dades a través de l'aire, Per això es necessita que els dispositius que vulguin utilitzar aquesta tecnologia tinguin una antena per poder emetre les ondes de ràdio.

Els elements que formen part una xarxa Wi-Fi:

- Access point: són els dispositius que fan de pont entre la xarxa Cablejada i la xarxa sense fils.
- Dispositius sense fils: són els elements que emeten i reben la informació que circula per la xarxa, per exemple Portàtils, smartphones ,tables o PDA
- Router: Fa la funció de Access point, switch ethernet i de enrutador, és l'encarregat de fer de pont entre diferents xarxes i el canvi de medi entre la xarxa sense fils i la xarxa cablejada.

Els estàndards més comuns són 802.11b,802.11g,802.11n que emeten en una banda de 2.4GHz i a una velocitat de 11 ,54 i 300 mbits/s, que són acceptats universalment i són els més implementats.

Des del 2013 existeix l'estàndard 802.11ac que opera en la banda de 5GHz,degut que la banda de 2,4 hi ha més tecnologies que la utilitzant com per exemple el Bluetooth.

Per evitar que els dispositius tinguin interferències la banda de 2,4GHz i de 5GHz[3] estan dividits en canals per exemple la banda de 2,4GHz té els canals 1,2,3,4,5,6,7,8,9,10,11,12,13,14 , cada dispositiu està associat a un canal per el qual emet per evitar interferències, encara que els canals se superposen amb els canals que estan contigus (veure figura 3).

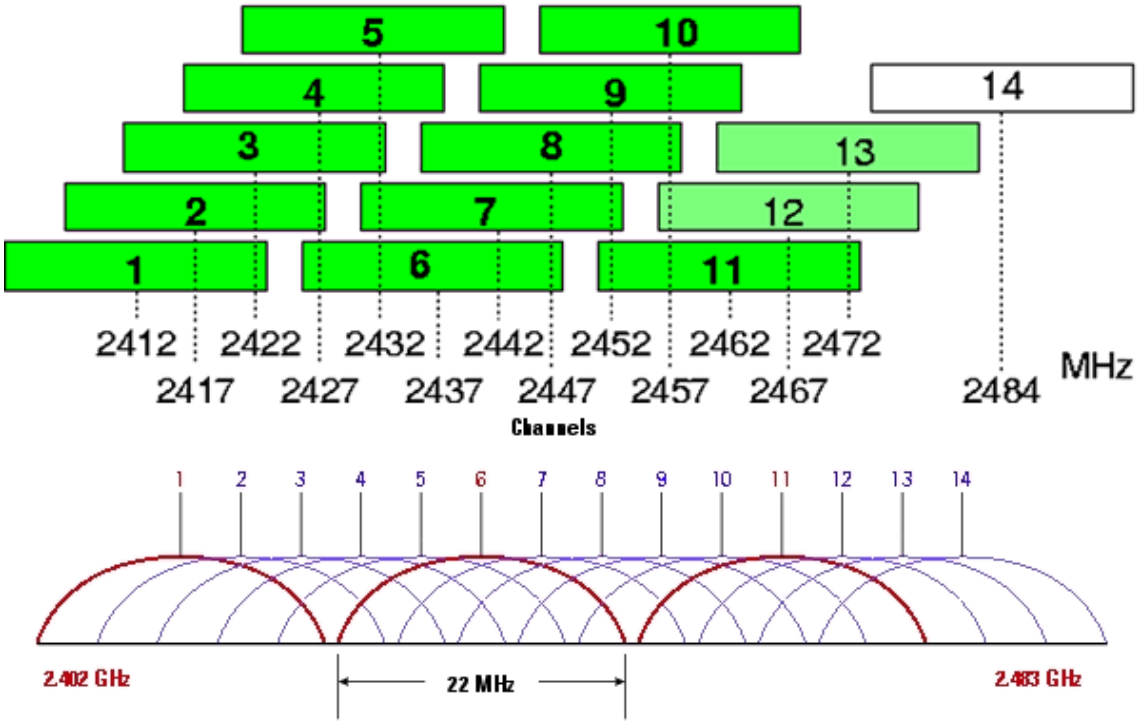


Figura 3 Distribucio de canals en la banda de 2,4GHz

Quan Un dispositiu connectat per Wi-Fi envia informació la informació es codifica en ones que en viatjar per aire arriben a tots els dispositius que estan al seu abast on tots els dispositius estan escoltant i si ells són els destinataris descodifiquen el paquet i el processen, en cas que el destinatari no estigui a l'abast el router és l'encarregat de redirigir el paquet sigui per Wi-Fi o per la xarxa cablejada.

5.3.-Diferencies Banda 2.4GHz i 5GHz

Com ja hem comentat i hi ha dos tipus de bandes de Wi-Fi una a 2,4GHz i l'altra a 5GHz a continuació veure quines són les diferències entre les dues bandes[4]:

- La banda de 2.4GHz com ja hem contactat té 14 canals i la de 5GHz té 25 canals en els dos casos els canals contigus poden presentar un superposició en a la freqüència però al haver molt més canals un medi té menys interferències.
- La velocitat de connexió de la xarxa Wi-Fi de 2,4GHz està entre 50 i 60 Mbps i la de Wi-Fi 5GHz pot arribar a 867 Mbps, la xarxa de 5GHz pot arribar a més altes velocitats podent aprofitar millor la velocitat d'una xarxa moderna.
- En contrapartida de la velocitat la xarxa 5GHz en ser més rapida no té tant d'abast com la de 2,4 que és més lenta però pot arribar més lluny, a més el Wi-Fi de 2,4GHz pot travessar millors parets i obstacles que la xarxa de 5GHz.

Si el que es vol és una xarxa amb menys interferències i més velocitat és té que buscar que tots els dispositius possibles estiguin a 5GHz i si el que es vol és una millor cobertura es haurà d'utilitzar la de 2,4Ghz.

5.2.-Access points i controladora Wi-Fi

Una controladora[5] Wi-Fi té tota la informació i configuració sobre la xarxa Wi-Fi i els AP, en comptes de com funciona el router domèstic ,la configuració de cada AP està centralitzada a la controladora el que fa que els AP siguin més ràpids i necessitin menys lògica interna per poder treballar.

Per poder fer això s'utilitza un protocol anomenat WAPCAP[6], Control And Provisioning of Wireless Access Points) basat en LWAPP(Lightweight Access Point Protocol) que aporta una millora que el que afegeix seguretat en la comunicació de la informació.

Aquest protocol utilitza el port UDP 5246 pel control i el port UDP 5247 per les dades.

En fer canvis sobre la controladora, gràcies al protocol WAPCAP s'envien els canvis a cada AP i es configura de manera rapida i senzilla.

6.-Estudi de la situació inicial de la xarxa Wi-Fi de l'empresa

D'entrada a l'empresa tenim 3 xarxes WI-FI:

- **CXG**: xarxa IP 192.168.220.0/22 amb interval de adreces IP de 192.168.220.0 fins a 192.168.223.255 on estan ubicats totes els portàtils, tablets i pda. És una xarxa filtrada pel Firewall que bloqueja l'accés algunes pàgines d'internet (pornografia, jocs,etc.) però té accés total a tota la xarxa interna de Comexi (servidors i serveis interns).
- **CXGMobil**: xarxa 192.168.180.0/22 amb un interval de adreces IP 192.168.180.0 a 192.168.183.255, aquesta xarxa esta pensada per ubicar únicament als Smartphones, en la que es pot accedir als servidors de i serveis de comexi i també a internet amb alguna restriccions (jocs, radio, pornografía).
- **Visites**: Xarxa 192.168.230.0/24 aquesta xarxa esta pensada per les visites de persones externes a l'empresa, aquesta xarxa té navegació lliure per internet, en aquest cas el Firewall no filtra res, el que no té accés és a la xarxa interna, els servidors i serveis de Comexi.

Una vegada sabem com funcionen les xarxes Wi-Fi, es va buscar com funcionen els APs, en el cas de l'empresa tenim un número indeterminat de AP controlat per una controladora Wi-Fi.

El que necessitem saber es el número d'APs i on estan ubicats , perquè a l'empresa no hi ha cap registre per escrit de tot això, també seria bo saber la cobertura de cada AP, ja que tampoc hi ha dades al respecte.

El que buscarem i seria necessari per portar a terme el projecte seria saber la quantitat d'usuaris a cada AP, quants usuaris estan connectats a cada xarxa Wi-Fi, seria bo saber també si els usuaris connectats tenen o no una bona senyal amb el AP connectat, el percentatge d'utilització de la CPU per enviar o rebre paquets del AP i per últim com esta de carregat el canal per el qual emet el AP

6.1Localització dels AP

Com ja hem comentat no es tenien registres físics de la ubicació de cada AP , el primer que farem és anar a la controladora on esta la informació de tots els AP (figura 3) i revisar si hi ha informació respecte a la ubicació (figura 4)

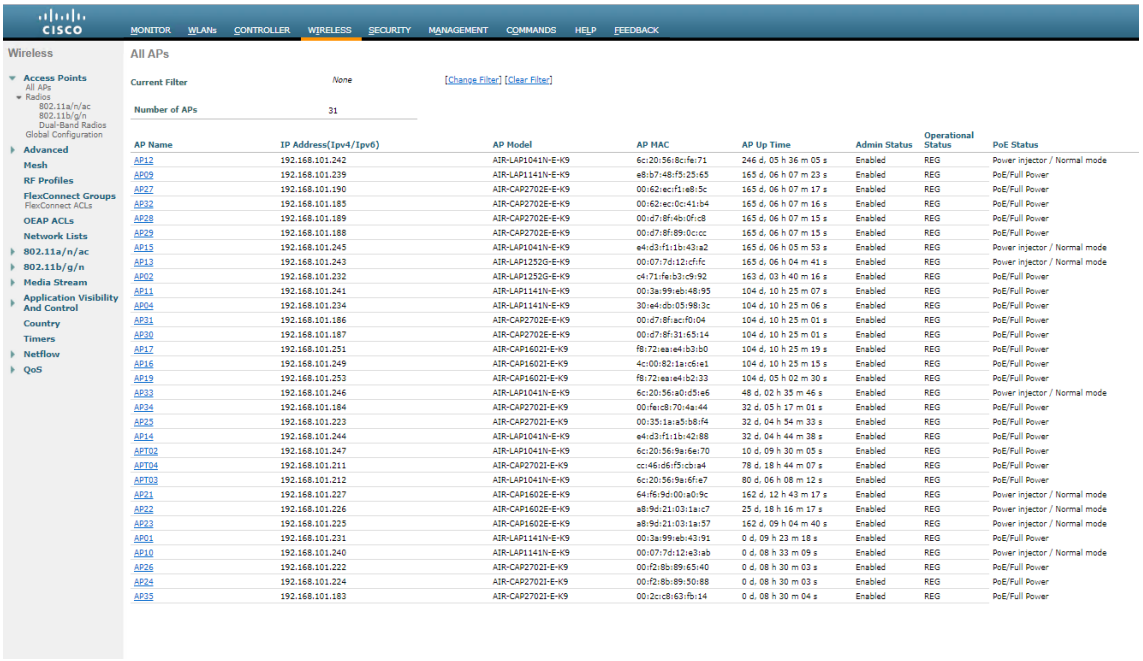


Figura 4 panell APs controladora Wi-Fi

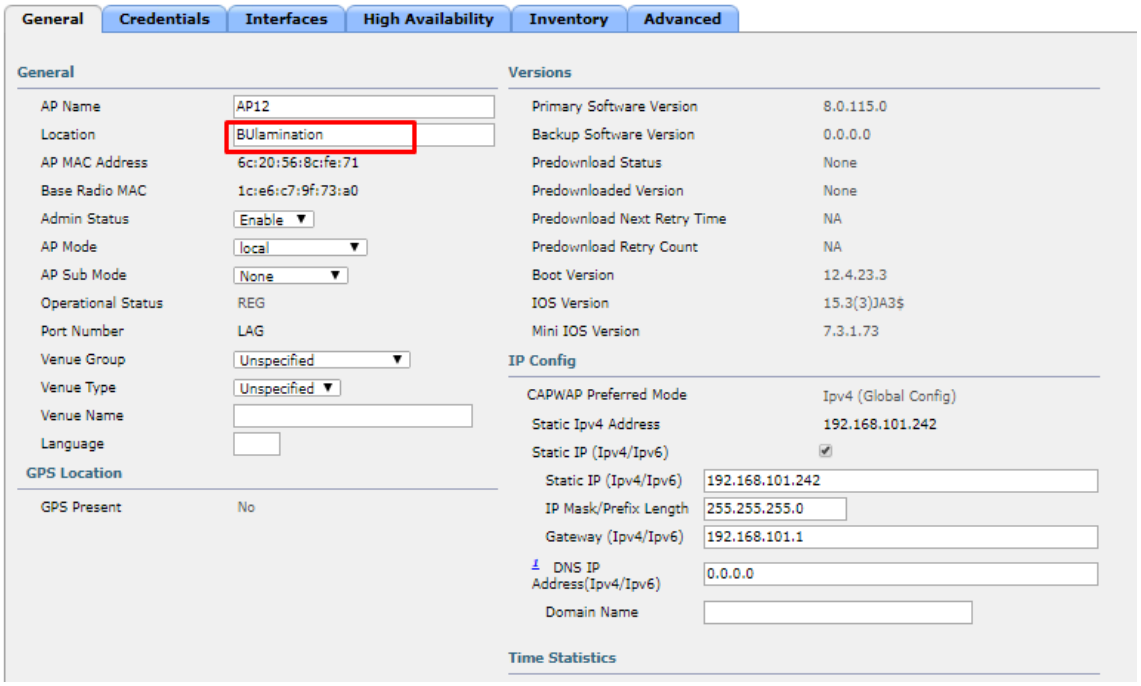


Figura 5 panell configuracio d'un AP

Encara que alguns APs sí que tenen bé la ubicació la majoria no, per això ens vam dedicar a aconseguir els plànols de tota l'empresa per ubicar tots i cada un dels APs.

Per fer això utilitzem un mètode des de la controladora que és indicar a un AP que faci llum intermitent i així poder el podrem localitzar.

Els plànols de l'empresa amb la ubicació es troben a annexos (Vegeu annexes Plànols AP)

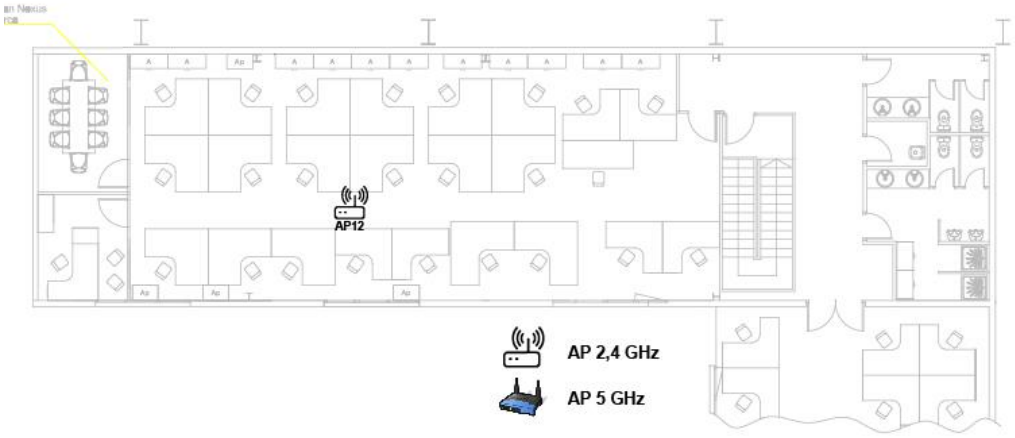


Figura 6 Mapa Ubicacio Ap BU Lamination

Una de les coses que vam veure en revisar la controladora és que principalment hi ha dos tipus de APs uns que emeten a 2.4GHz i un altre que poden transmeti la senial a 2,4 o a 5 GHz.

Després de fer tot això el que hem aconseguit és la següent taula (Figura 6) on es pot veure el nom de cada AP el model, la seva ubicació i el tipus d'AP que és.

ap	Model	ubicació	Tipus
AP01	AIR-LAP1141N-E-K9	DESPATX TIC	2,4GZ
AP02	AIR-LAP1252G-E-K9	Nau B sobre mag. eines	2,4GZ
AP04	AIR-LAP1141N-E-K9	Nau 6-CPD	2,4GZ
AP09	AIR-LAP1141N-E-K9	cova	2,4GZ
AP10	AIR-LAP1141N-E-K9	montserrat	2,4GZ
AP11	AIR-LAP1141N-E-K9	lamination	2,4GZ
AP12	AIR-LAP1041N-E-K9	recepcio Materials	2,4GZ
AP13	AIR-LAP1252G-E-K9	procurement	2,4GZ
AP14	AIR-LAP1041N-E-K9	offset	2,4GZ
AP15	AIR-LAP1041N-E-K9	gerencia	2,4GZ
AP16	AIR-CAP1602I-E-K9	comercial	5GZ
AP17	AIR-CAP1602I-E-K9	Nau 10 MIG	5GZ
AP19	AIR-CAP1602I-E-K9	Nau 10 armari B4	5GZ

AP21	AIR-CAP1602E-E-K9	Nau 10 fondo	5GZ
AP22	AIR-CAP1602E-E-K9	Nau A p2 Xifra	5GZ
AP23	AIR-CAP1602E-E-K9	Nau A p2 Auditori	5GZ
AP24	AIR-CAP2702I-E-K9	Nau A p2 agudes	5GZ
AP25	AIR-CAP2702I-E-K9	NAU A	5GZ
AP26	AIR-CAP2702I-E-K9	NAU A	5GZ
AP27	AIR-CAP2702E-E-K9	NAU A	5GZ
AP28	AIR-CAP2702E-E-K9	NAU A	5GZ
AP29	AIR-CAP2702E-E-K9	NAU A	5GZ
AP30	AIR-CAP2702E-E-K9	Nau A	5GZ
AP31	AIR-CAP2702E-E-K9	Nau A	5GZ
AP32	AIR-CAP2702E-E-K9	Nau A	5GZ
AP33	AIR-LAP1041N-E-K9	sala polivalent	2,4GZ
AP34	AIR-CAP2702I-E-K9	Bu service	5GZ
AP35	AIR-CAP2702I-E-K9	Flexo	5GZ
APT02	AIR-LAP1041N-E-K9	entrada Mas joals	2,4GZ
APT03	AIR-LAP1041N-E-K9	mig Mas Joals	2,4GZ
APT04	AIR-CAP2702I-E-K9	Mas Joals oficines	5GZ

Figura 7 Ubicacio de cada AP

6.2Revisar la cobertura de la xarxa

Una vegada tenim a tots els APs localitzats el que es va fer és buscar la cobertura dels APs a totes les zones, per fer això ens vam baixar un programa anomenat visiwave site survey[7], en el que carregarem el mapa de la zona que volem fer l'anàlisi de la cobertura i amb un portàtil anem marcant punt per punt zones sobre el pla en el qual el programa analitza el senyal dels Wi-Fis que rep i al final crea un mapa de calor amb la intensitat d'una Wi-Fi.

Amb aquest programa es pot fer una anàlisi per la cobertura total dels APs per una xarxa en concret (Figura 8) o per una xarxa i un sol AP (Figura 9).

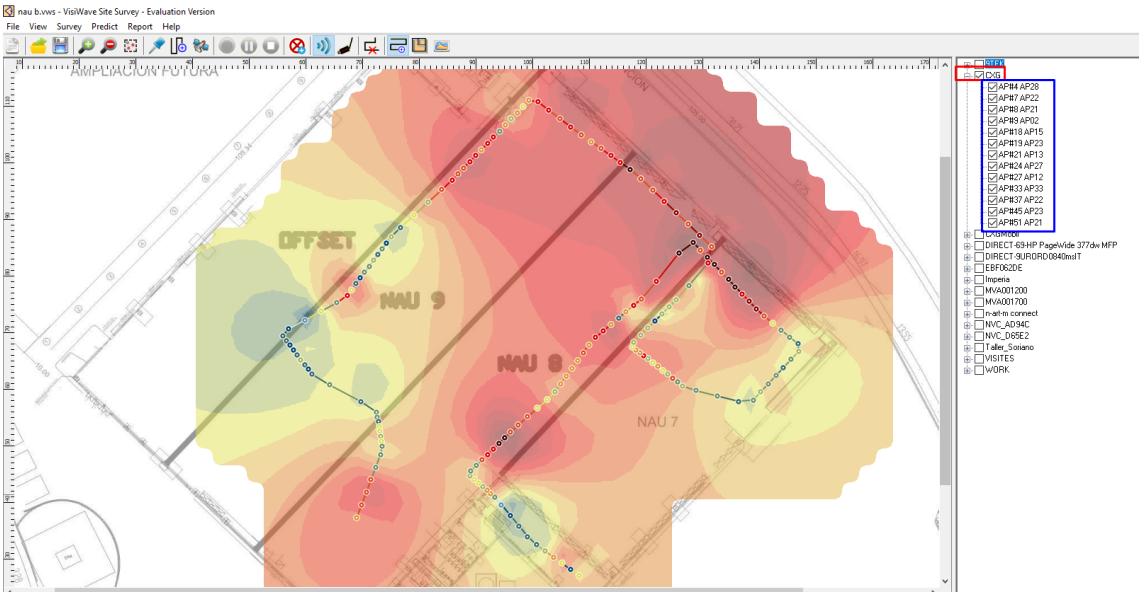


Figura 8 Programa visiwave site survey

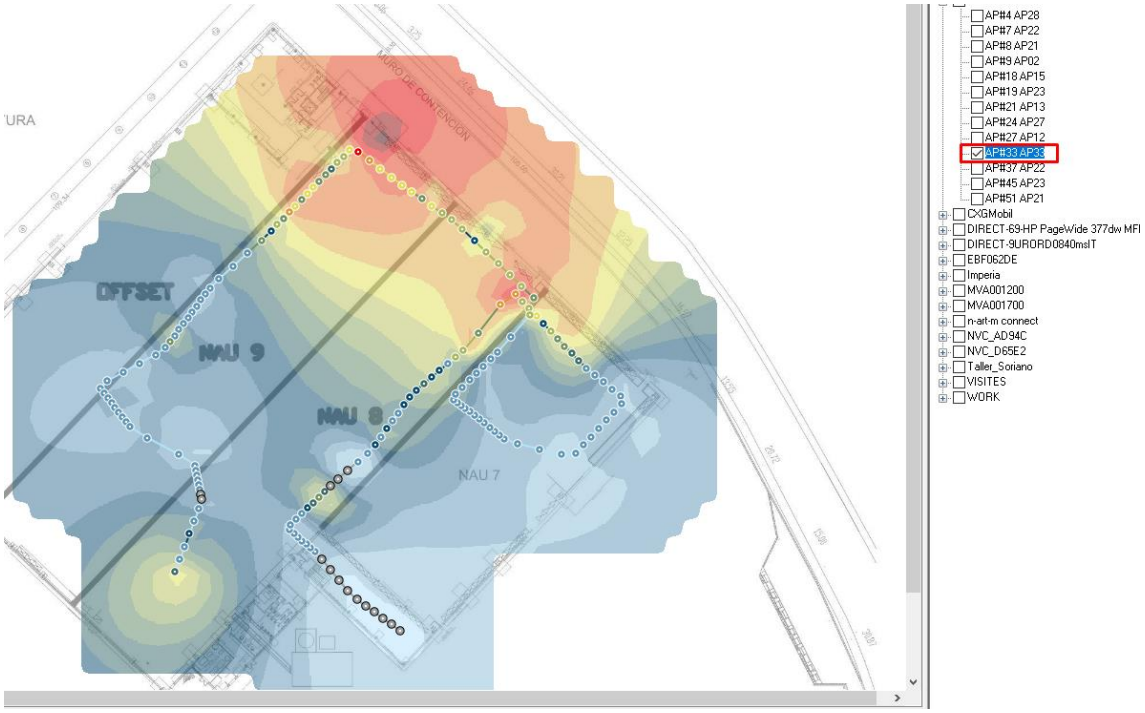


Figura 9 Cobertura per un sol AP

Com es pot veure a les figures abans mostrades la cobertura que està mostrada en decibels amb una escala de colors des d'un blau que indica que hi ha poca cobertura a un vermell més intens que és que la cobertura és excel·lent.

Aquí podem veure (figura 10) com queda un plànol amb la llegenda per veure els colors i la ubicació dels APs sobre el planol

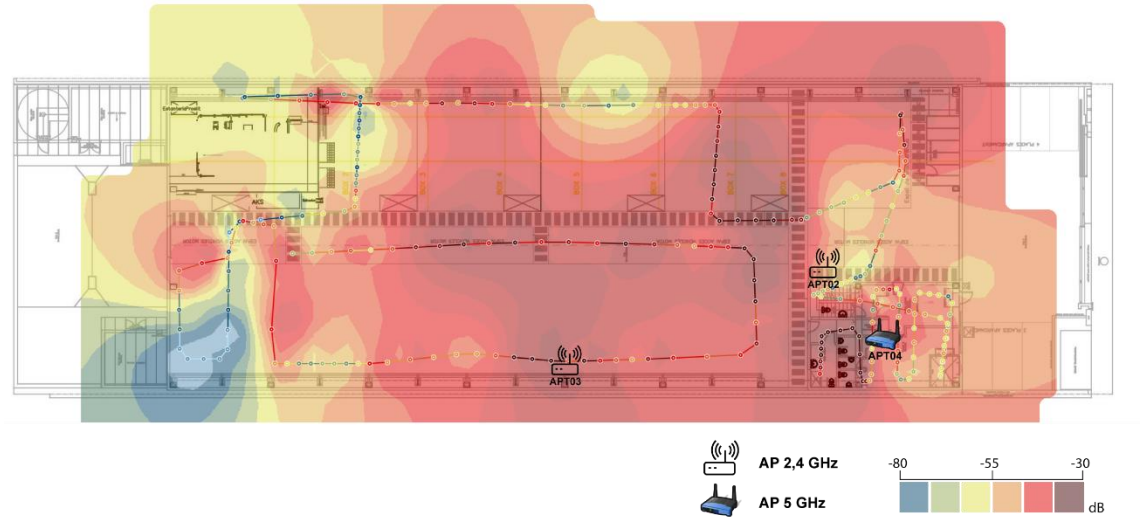


Figura 10 Planol de cobertura i Ubicacio de APs

A la secció Cobertura Ap del anexe es pot veure la resta

7.-Implantació d'una eina de monitoratge de la xarxa Wi-Fi

7.1.-anàlisis de software per portar a terme el monitoratge

Després de donar un primer cop d'ull hem vist molt software que poden ser d'utilitat aquí podem veure uns exemples:

- Nagios [8]
- Cacti [9]
- Graphite[10]
- Prometheus[11]

7.1.1.-NAGIOS

Hi ha dues versions la primera de pagament i una segona gratuïta, la que hem tingut en compte a l'hora de veure que ens aporta és la gratuïta.

Nagios o nagios core com també es coneix és un software llicenciat com a GNU que serveix per monitorar xarxes i equips, a més d'oferir un sistema d'avisos.

Nagios pot monitorar serveis en xarxa com ICMP,HTTPS,SNMP,FTTP o SSH.

És un software molt personalitzable, amb una gran comunitat que sempre està fent plugins o complements per poder afegir funcionalitats al sistema.

Té un sistema de visualització senzill, i és fàcil veure quins sistemes dels monitorats estan fallant o donen problemes.

Nagios està disponible per distribucions Windows com per Linux, funciona amb un servidor web apache i s'accedeix a través de navegador.

7.1.2.-Cacti

Un software basat en tecnologia RRDtool que pot guardar tota mena d'informació i tractar-la per mostrar gràfica, Està programat sobre PHP i JavaScript, funciona totes les plataformes però per funcionar necessita MySQL,PHP RRDTool ,net-snmp i apache o IIS.

Cacti funciona amb una llicència GPL i és gratuït.

Utilitza el protocol SNMP per poder fer consultes a dispositius en xarxa dels quals obtindrà les dades per poder fer gràfiques i generar els informes que es vulguin configurar

RRDtool

Un sistema RRDtool[12] és com una base de dades limitada en espai, quan arriba a l'espai màxim sobreescriu les dades més velles que es tenen, és té que pensar com si fos un cercle.

Aquest tipus de sistemes són útils per mirar a curt termini però no poden tenir un històric molt gran.

7.1.3.-Elecció

En un principi es va plantejar l'opció d'utilitzar cacti, però al final com a l'empresa ja disposem d'un servidor de nagios que actualment ja fa el monitoratge dels servidors i es vol ampliar perquè faci el monitoratge de les impressores de l'empresa, ens va semblar millor opció centralitzar-ho tot en un sol servidor on tindríem tota la informació i a la llarga serà més simple de mantenir i .

7.2.-SNMP

SNMP (Simple Network Management Protocol)[13],[14] és un protocol d'Internet (de la capa d'aplicació) per a la gestió de xarxa. En la seva arquitectura hi ha estacions de gestió i elements de xarxa gestionats, com estacions, routers, switches, i altres. A les estacions de gestió s'executen "aplicacions de gestió" que permeten tant monitorar els elements de xarxa (obtenir informació del seu funcionament) com controlar-los (canviar el seu comportament). Als elements de xarxa hi ha "agents de gestió" responsables de realitzar les tasques que les estacions de gestió els demanin. Les aplicacions de gestió i els agents de gestió es comuniquen fent servir el protocol SNMP.

Actualment disposa de 3 versions sent la 3 la primera que aporta seguretat a les a la informació que circula per la xarxa.

7.2.1.-Com funciona?

Disposa principalment de dues funcions la de llegir dades d'un dispositiu o modificar alguna variable d'un dispositiu, també hi ha una menys important que és la possibilitat de notificació a través de snmp quan alguna variable a un sistema canvia.

El que utilitza el protocol per preguntar per una variable o una altra està en una taula anomenada MIB (Management Information Base) és un arbre que a cada una de les fulles és un OID (Object Identifiers)[15], [16]

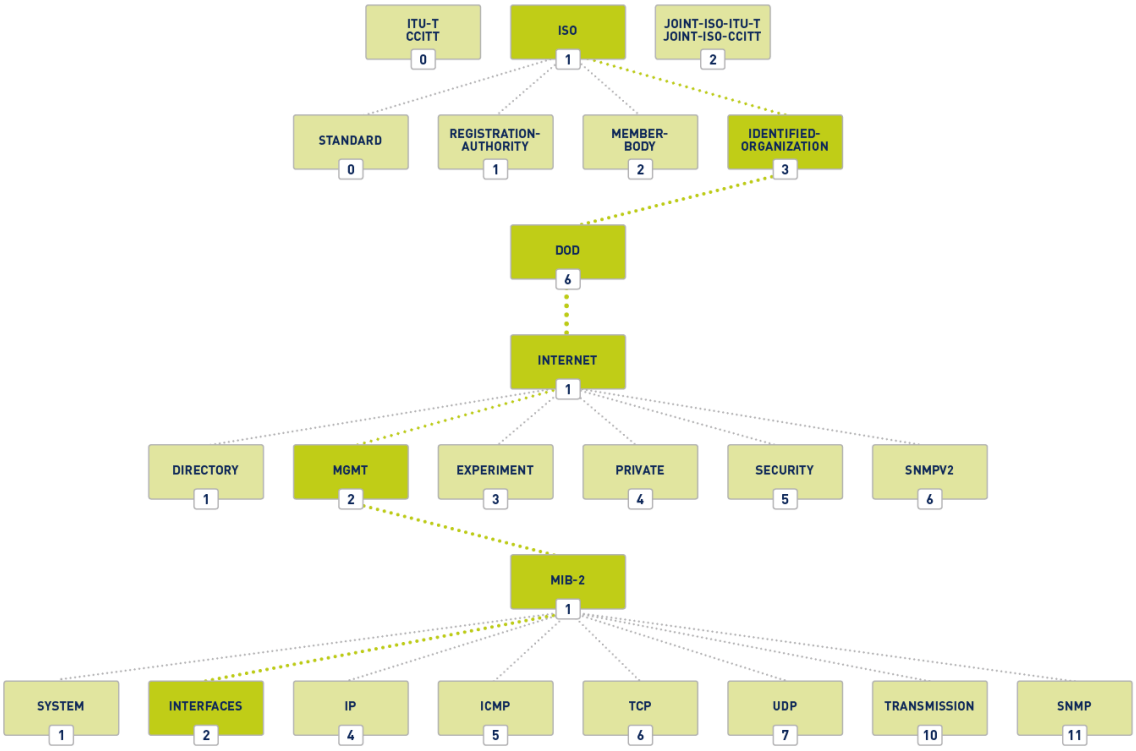


Figura 11 Arbre organització MIB

Llavors el que es fa és preguntar sobre l'arbre aquest: per exemple si volem saber com és el nostre cas alguna cosa sobre els APS de cisco haguérem de fer:

1.(ISO) 3.(Identifica ORGANIZATION) 6.(DOD) 1.(INTERNET) 4.(PRIVATE) 1.(ENTERPRISE) 14179.(Airespace, Inc) 2.(BSNWIRELESS) O si està abreviat queda 1.3.6.1.4.14179.2

Cada fabricant té una branca de la taula dedicada als seus dispositius on es poden preguntar totes les variables que es poden donar.

Per poder consultar a través d'un paquet SNMP una vegada s'obté la ruta del OID que es vol consultar o modificar s'utilitzarà un GetRequest si es vol aconseguir informació ,un SetRequest si el que necessitem és modificar alguna variable O trap si es vol generar notificacions quan canvia alguna cosa de la variable.

Aquest paquet tenen tots la mateixa estructura

versió	Comunitat	SNMP PDU

Figura 12 Estructura SNMP

Primer s'indica la versió del protocol que s'utilitza sigui la versió 1 ,2 o la 3. A la part del bytes que va la comunitat es descriu si és públic o privat, per últim a la part SNMP PDU és el lloc on s'indicarà si és un GetRequest, un SetRequest o un Trap.

Per enviar aquest tipus de paquets per xarxa normalment s'utilitza algun programa per ajudar en la sintaxi del missatge.

7.2.2.-Versions

Com ja hem explicat hi ha 3 versions[17]:

La primera versió va néixer al 1988, va ser bastant criticat per la falta de seguretat però funcionava bé.

La segona versió molt més completa i amb un gran nivell de seguretat era tota una millora del primer però no va agradar per complexitat de la seguretat i la gent va acabant fent ús d'una modificació que es va començar a dir 2c (c de comunity) on el que es feia era eliminar la seguretat per deixar-la com a la v1.

Per la gran diferencia entre la v1 i la v2 no eren compatibles els paquets.

La V3 afegeix seguretat criptogràfica als paquets i millora alguna de les deficiències que té la versió 2, però el gran salt és que la seguretat no és tan complexa com abans.

7.3.-configuració Nagios

Com hem indicat abans el Protocol SNMP necessita una aplicació de gestió i d'un agent de gestió, en el cas de l'agent de gestió el que farà aquesta feina serà els APs de l'empresa i la controladora Wi-Fi als que no és té que instal·lar o configurar l'agent de gestio, ja que per defecte ja ve configurat, el que farem en aquesta secció serà configurar i instal·lar l'aplicació de gestió per portar a terme el projecte.

Hem fet la instal·lació de nagios sobre una màquina virtual REDHAD 7.6

Per fer la instal·lació hem seguit la guia des de la mateixa documentació que indica Nagios[18], l'única configuració que és té que fer és afegir un usuari i contrasenya pel Nagios.

Una vegada la instal·lació està acabada per provar si funciona mirarem si podem utilitzar la comanda de snmpwalk. Snmpwalk és una aplicació d'un paquet anomenat NET-snmp [Bibliografia] que farà d'aplicació de gestió per posar-se en contacte amb les agents de gestió snmp dels quals obtindrem les dades perquè pugui funcionar nagios, ja que la majoria de les dades les obtindrem de preguntar a la controladora.

```
[root@localhost ~]# snmpwalk -c public 192.168.101.230  -v 2c 1.3.6.1.4.1.14179.2.1.1.1.2
SNMPv2-SMI::enterprises.14179.2.1.1.1.2.1 = STRING: "CXG"
SNMPv2-SMI::enterprises.14179.2.1.1.1.2.2 = STRING: "VISITES"
SNMPv2-SMI::enterprises.14179.2.1.1.1.2.3 = STRING: "CXGWMA"
SNMPv2-SMI::enterprises.14179.2.1.1.1.2.4 = STRING: "CXG2"
SNMPv2-SMI::enterprises.14179.2.1.1.1.2.5 = STRING: "CXGMobil"
[root@localhost ~]#
```

Figura 13 prova SNMP

Per exemple aquesta consulta 1.3.6.1.4.1.14179.2.1.1.1.2 (vegeu figura 13) pregunta a la controladora WIFI quins Suid estan configurats, podem veure que hi ha més dels que hem explicat inicialment això és perquè alguns estan des que habilitats.

```
[root@localhost ~]# snmpwalk -c public 192.168.101.230  -v 2c 1.3.6.1.4.1.14179.2.1.1.1.6
SNMPv2-SMI::enterprises.14179.2.1.1.1.6.1 = INTEGER: 1
SNMPv2-SMI::enterprises.14179.2.1.1.1.6.2 = INTEGER: 1
SNMPv2-SMI::enterprises.14179.2.1.1.1.6.3 = INTEGER: 0
SNMPv2-SMI::enterprises.14179.2.1.1.1.6.4 = INTEGER: 0
SNMPv2-SMI::enterprises.14179.2.1.1.1.6.5 = INTEGER: 1
[root@localhost ~]#
```

Figura 14 Consulta amb SNMP sobre les xarxes Wi-Fi

Si preguntem amb el OID 1.3.6.1.4.1.14179.2.1.1.1.6 (vegeu figura 14) ens indica amb un 1 els que estan habilitats i amb un 0 els que no.

Ara que ja està funcionant mirarem quines dades són las que volem, despres de buscar tota la informació que pot proporcionar la controladora sobre els AP hem decidit que volem aquestes dades:

- **Comprovar connectivitat dels AP i controladora**: per fer això es farà fent constantment pings als dispositius i mesurant el temps de resposta si el temps és molt gran o directament no hi ha resposta pot ser un indicatiu que no estan funcionant o que hi ha algun problema a la xarxa.
- **Usuaris connectats al AP**: volem saber quants dispositius estan connectats a cada AP, ja que si el numero AP supera els recomanats pel fabricant el Ap podria començar a donar problemes, .
- **Usuaris connectats amb mala qualitat de senyal**: ens interessa saber la gent que està connectada a un AP amb una baixa qualitat del senyal, això pot indicar que un AP està mal ubicat o que hi ha gent treballant fora de la zona de bona cobertura.
- **Saturació d'un canal de Wi-FI:** una xarxa Wi-Fi funciona dintre d'una freqüència de ràdio sigui la de 2,4GHz o 5GHz si hi ha molts dispositius treballant a una mateixa freqüència al comunicar-se en un medi compartit com l'aire pot provocar moltes interferències i per tant una baixada del rendiment de la xarxa, per tant ens interessa saber si pel canal en el qual emeten cada AP està molt saturat de dispositius.
- **Ús de la CPU de cada AP a l'Emetre**: serà bo saber si CPU necessita treballar molt per poder gestionar tot el tràfic per emetre, ja que en el cas que estigui molt congestionada pot donar problemes.
- **Ús de la CPU de cada AP en rebre**: igual que en el cas anterior però aquesta vegada com està d'ocupada amb els paquets que rep.
- **número d'usuaris per cada AP connectats a cada SSID**: a part del número de dispositius connectats a cada AP també volem saber els usuaris de cada AP que estan connectats a un SSID concret (CXG,CXGMobil o visites), amb això podrem saber si per exemple es fa un mal ús d'una xarxa en concret o l'evolució de dispositius en el temps.

Bueno ara ja podem veure que funciona, ara hem de configurar els arxius de nagios perquè pugui començar a recopilar dades.

El primer que creem és un arxiu anomenat aps.cfg a /usr/local/nagios/etc/objects aquest arxiu serà el que tindrà la informació de tots els APs i farà crides als serveis que es han d'executar per cada AP.

El que farem serà copiar l'estructura de l'arxiu que ja està per defecte a nagios anomenat switch.cfg en el que primer part de l'arxiu es defineix els hosts i després els serveis.

7.3.1.-Creació de host APs

```
define host {

    use                     generic-switch,
    host_name               AP02                    ; T
    alias                   AP02-NAUB sobre mag Enines
    address                 192.168.101.232
    hostgroups              AP
}
```

Figura 15 Exemple configuració Host

Aquí tenim un exemple (figura 15) d'una definició d'un host es pot veure com indicarem la posició de el AP perquè si hi ha algun problema i té que enviar correus amb Warnings del sistema puguem veure on està ubicat.

D'altra banda també s'indica la IP del AP per poder fer PINGS i saber si el AP està funcionant o no, la resta com el USE és la utilització d'una plantilla predefinida i un hostgroup com el de AP que serveix per definir serveis per tots els APs.

El problema es que com ja hem vist amb anterioritat hi ha APs que són 5GHz i per aquest cas necessitem fer dos host (figura 16) un pel de 2,4 GHz i un pel de 5GHz

```
define host {

    use                     generic-switch                  ; Inherit default values from a template
    host_name               APT04                   ; The name we're giving to this switch
    alias                   APT04_MASJOALS OFICINA          ; A longer name associated with the switch
    address                 192.168.101.221                 ; IP address of the switch
    hostgroups              AP                      ; Host groups this switch is associated with
}

define host {

    use                     generic-switch                  ; Inherit default values from a template
    host_name               APT04_5GZ               ; The name we're giving to this switch
    alias                   APT04_5GZ_MASJOALS OFICINA          ; A longer name associated with the switch
    address                 192.168.101.221                 ; IP address of the switch
    hostgroups              AP                      ; Host groups this switch is associated with
}

################################################################################
```

Figura 16 Exemple configuració Host 5GHz

Una vegada hem afegit tots els APs també voldrem afegir la controladora WI-FI per controlar si cau o per fer-li alguna pregunta sobre la xarxa.

```
define host {

    use                     generic-switch                  ; Inherit default values from a template
    host_name               ControladoraWifi                ; The name we're giving to this switch
    alias                   Controladora            ; A longer name associated with the switch
    address                 192.168.101.230                 ; IP address of the switch
    hostgroups              AP                      ; Host groups this switch is associated with
}
```

1 Exemple configuracio host controladora

Una vegada fet tot això , hem de definir els serveis, això són les tasques i/o els scripts que nagios executa per poder mostrar informació, en el nostre cas serà preguntes amb el protocol SNMP i fer pings per saber si està connectat o no.

7.3.2.-Ping a un AP

Aquest servei fa un ping agafant del host la seva adress(IP) i mirant si està actiu o no, com no hi ha cap diferencia es poden afegir tots els hosts a host_name(veure figura 17).

```
define service {

    use                     generic-service                 ; Inherit values from a template
    host_name               AP01,AP12,AP09,AP27,AP32,AP28,AP29,AP15,AP13,AP22,AP23,AP21,AP02,AP26,AP35,AP10,AP24,AP11,AP04,AP34,AP25,AP31,AP30,AP17,AP16,AP19,AP33,APT02,APT03,APT04,AP16_5GZ,AP17_5GZ,AP
    service_description     PING                            ; The service description
    check_command           check_ping!200.0,20%!600.0,60%  ; The command used to monitor the service
    check_interval          5                               ; Check the service every 5 minutes under normal conditions
    retry_interval          1                               ; Re-check the service every minute until its final/hard state is determined
}
```

Figura 17 Configuració servei Ping

De tots els serveis que tenim implementats és el més fàcil, ja que està predefinit a nagios, utilitza el check_ping que és un petit script ubicat a /usr/local/nagios/libexec en què agafa de el host la adress i prova de fer pings si la resposta tarda molt o no arriba fa un avis al sistema.

7.3.3.-Saturació del canal per cada AP

Aquest servei serveix per mirar com de saturat està el canal de WI-FI en el qual cada AP emet.

A diferència del que hem vist en l'anterior en aquest cas és té que fer un a un per cada host que sigui un AP, ja que els APs no tenen el protocol SNMP obert es pregunta directament a la controladora amb el OID únic de cada AP.

Per saber com funciona això el primer que vam fer és preguntar el OID 1.3.6.1.4.1.14179.2.2.13.1.3 que ens indicarà la utilització del canal (veure figura 18).

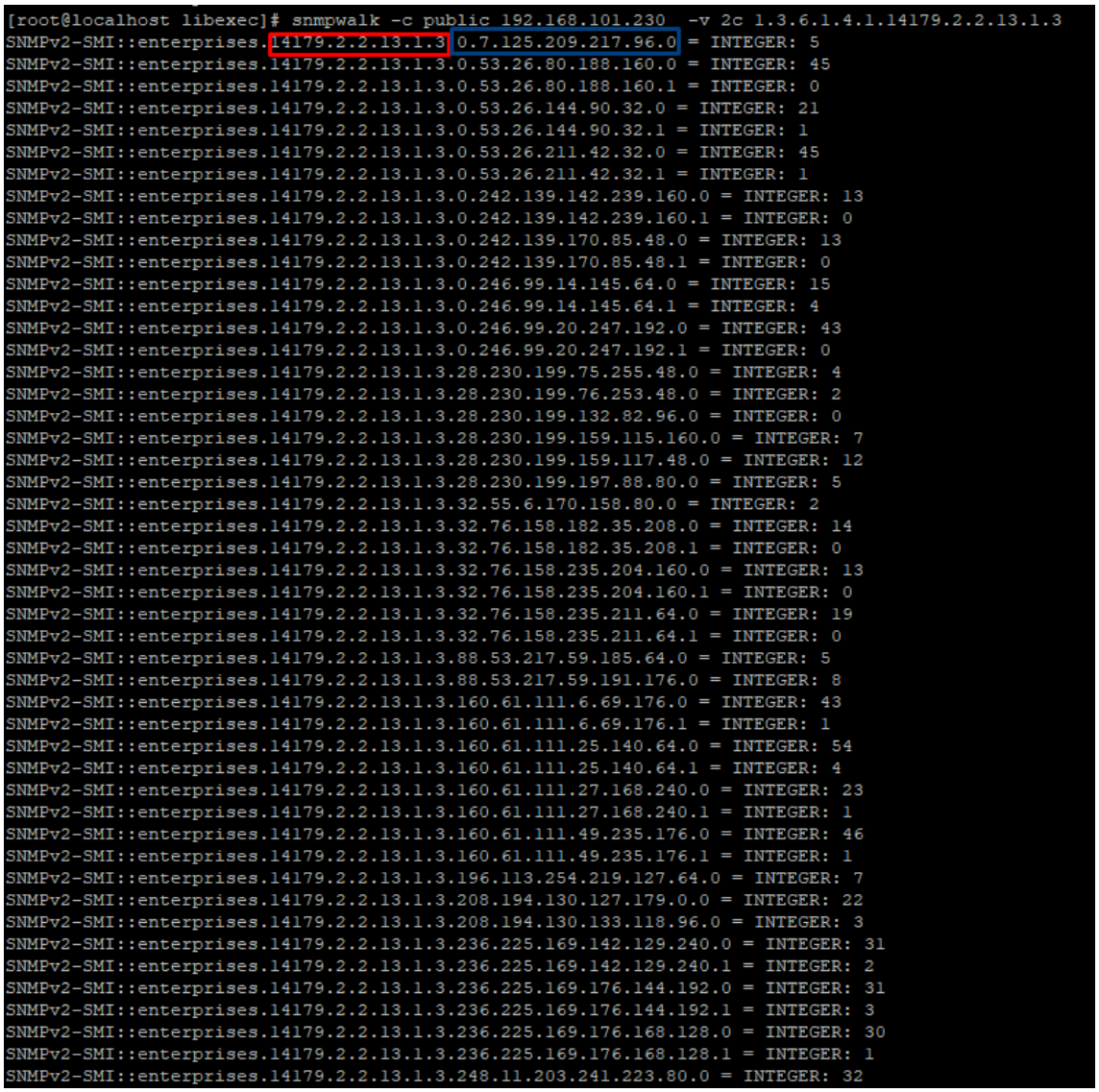


Figura 18 Exemple SNMP per saber la utilització del canal de cada AP

Com es pot veure al preguntar a la controladora respon no una cosa únicament sinó que dóna les dades per cada un dels APs que controla.

Però com podem fer per saber quin AP és cada un dels números que indica? Per fer això si ens fixem en la imatge podem veure en vermell que aquesta part a totes les línies és igual però la que està en blau no, això és un indicatiu per cada AP.

Ara el que hem de fer és buscar la relació de les MACS dels APs amb la que surt des de la pàgina web de la controladora de WI-FI.

Per fer això podem utilitzar EL OID 1.3.6.1.4.1.14179.2.2.1.1.1 (veure Figura 19)

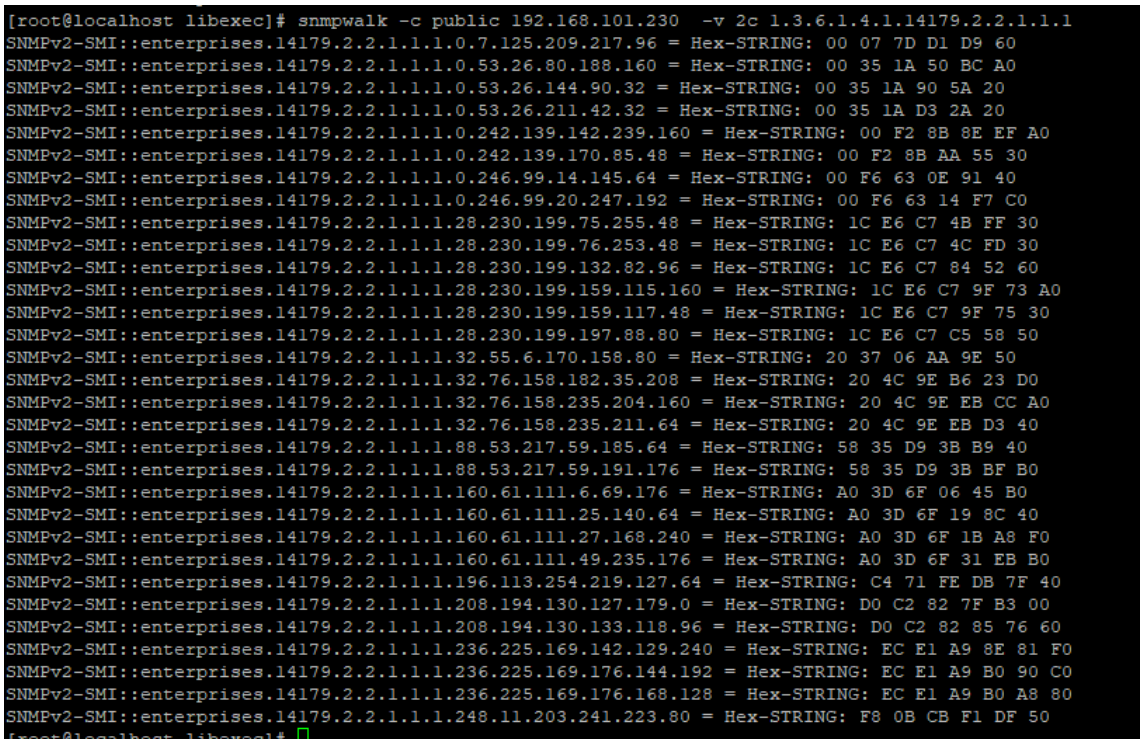


Figura 19 Crida SNMP per saber la mac de cada AP

Així podem veure les macs de tots els APs que gestiona la controladora , però falten abans havien sortit més línies, si ens tornem a fixar en la imatge podem veure una diferència(vegeu figura 20)

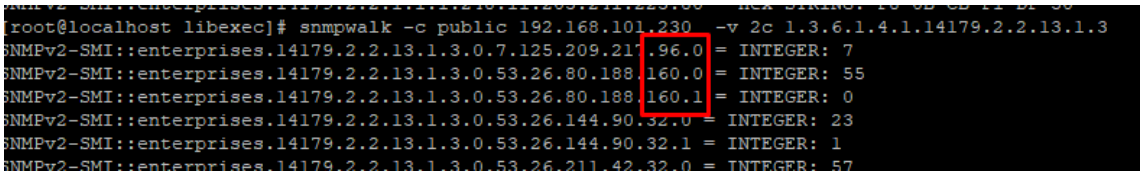


Figura 20 Diferencia entre AP 2,4GHz i 5GHz

Hi ha un número més marcat en vermell que acaba amb 0 o 1, el 0 indica que el AP 2,4 GHz i si hi ha un 1 al final és de 5GHz això vol dir que un mateix AP com serà per exemple el 17 que pot emetre en 2,4 i 5GHz el haurem de separar i preguntar per cada una de les seves freqüències.

Una vegada fet això i si ja sabem com funciona hem de modificar el comand CHECK_SNMP que té per defecte el nagios i crear el nostre propi que es dirà CHECK_SNMP_AP on fixarem que sempre pregunti a la controladora i només es passaran per paràmetre el OID i el llinda de Warning i de critical.

Per veure com funciona CHECK_SNMP hem d'anar a l'arxiu ubicar a /usr/local/nagios/etc/objects/comands.cfg i buscar la línia on està declarat (veure figura 21).

```
define command {

    command_name    check_snmp
    command_line    $USER1$/check_snmp -H $HOSTADDRESS$ $ARG1$
}
```

Figura 21 Configuració check_snmp

El que fa és executar el script que està a /usr/local/nagios/librexec amb el nom de check_snmp que el que fa és utilitzar l'argument HOSTADRESS per la IP a la que preguntar i ARG1 que ser el OID, el problema que HOSTADDRESS l'agafa del camp adress del HOST i no és el que volem, ja que necessitem utilitzar la IP de la controladora per això copiem la comanda i la modifiquem així (veure figura 22).

```
define command {

    command_name    check_snmp_AP
    command_line    $USER1$/check_snmp -H 192.168.101.230 -C public -P 2c  -o $ARG1$ -w $ARG2$ -c $ARG3$
}
```

Figura 22 Configuració Check_snmp_AP

Per obligació sempre preguntarà a la controladora i rebrà per paràmetres els valors del OID, els valors del llinda de warning i de critical

Si en fer la pregunta el valor que torna és superior a Warning farà un avis i es marcarà en groc i si és superior a critical igual però en vermell.

Després de fer tot això ja estem preparats per fer els serveis pels APs, definim com a argument el OID que volem mirar i l'hi afegim la part única de cada AP i en el cas de mirar la utilització el llinda dels avisos serà de 65% perquè digui que és un warning i un 85% perquè marqui un critical (veure figura 23).

```
define service {

    use                     generic-service                 ; Inherit values from a template
    host_name               AP01
    service_description     Utilitzacio
    check_command           check_snmp_AP!1.3.6.1.4.1.14179.2.2.13.1.3.32.55.6.170.158.80.0!65!85
}
```

Figura 23 Exemple de configuracio del servei Utilitzacio

7.3.4.-Dispositius connectats per cada AP

El que revisarem ara ser els dispositius connectats a cada AP, això serà molt útil per saber si algun AP té una càrrega superior a la recomanada, per defecte pels APs que tenim el recomanat pel fabricant està sobre els 30 dispositius, però el límit teòric és de 255, com que segurament 255 és molt posarem el warning a 25 i el critical a 40 indicant que el AP ja estarà molt saturat.

Ara ja no hem de modificar cap arxiu diferent només hem d'afegir el CHECK_SNMP_AP amb el OID que toca (1.3.6.1.4.1.14179.2.2.13.1.4) i el número únic de cada AP amb el avis de warning a partir de 25 i 40 pels criticals.

Com que ja tenim el que hem fet abans només hem de copiar tots els anterior i modificar la línia check_command(veure figura 24).

```
define service {

    use                     generic-service                    ; Inherit values from a template
    host_name               AP01
    service_description     usuaris
    check_command           check_snmp_AP!1.3.6.1.4.1.14179.2.2.13.1.4.32.55.6.170.158.80.0!25!40
}
```

Figura 24 Exemple configuració servei Usuaris

7.3.5.-Dispositius amb mala senyal per cada AP

Hi ha un OID (1.3.6.1.4.1.14179.2.2.13.1.24) que indica el número de usuaris connectats a cada AP que tenen una baix senyal o una mala senyal de WI-FI, això juntament amb els plànols que es van fer de la cobertura ens pot servir per veure si algun AP no està en una bona posició.

Igual que amb la part d'usuaris només és té que copiar i afegir a l'arxiu de APS.cfg les dades modificades amb el OID i els nous valors de warning i critical, que en aquest cas hem considerat 5 persones amb mala connexió ja és motiu de warning i 10 de critical tenint en compte que el recomanat de usuaris per el fabricant son uns 25 que la meitat tingui mala senyal és per tenir em compte (veure figura 25).

```
define service {

    use                     generic-service                    ; Inherit values from a template
    host_name               AP32
    service_description     MalaConexio
    check_command           check_snmp_AP!1.3.6.1.4.1.14179.2.2.13.1.24.0.246.99.20.247.192.0!5!10
}
```

Figura 25 Exemple configuració mala connexió

7.3.6.-Percentatge d'utilització de la CPU a l'hora de transmetre per cada AP

Aquest servei que l'anomenarem TX_utilitzacio, es crea per saber si algun dels APs consumeix molt de temps de CPU transmitent paquets, per saber això utilitzarem el següent OID: 1.3.6.1.4.1.14179.2.2.13.1.2 , que ens indicarà en un número de l'1 al 100 per indicar com de saturat està.

En seguir-la tècnica igual que els anteriors Nagios no acaba d'agafar bé el número que és un percentatge, per això modifiquem i crearem un altre CHECK_SNMP_X (veure figura 26) en aquest cas per obligar que el número de sortida sigui en % i així podem solucionar el problema de visualització.

```
define command {

    command_name    check_snmp_X
    command_line    $USER1$/check_snmp -H 192.168.101.230 -C public -P 2c -u % -o $ARG1$ -w $ARG2$ -c $ARG3$
}
```

Figura 26 configuració check_snmp_X

És semblant al que hem fet anteriorment però ara afegim l'opció de –u que indica quina és la unitat del valor de sortida.

Per el valors de warning escollim un valor una mica experimentals d'un 25 i 50 respectivament pels warning i critical (veure figura 27).

```
define service {

    use                     generic-service                 ; Inherit values from a template
    host_name               AP27
    service_description     Tx utilitzacio
    check_command           check_snmp_X!1.3.6.1.4.1.14179.2.2.13.1.2.0.246.99.14.145.64.0!25!50
}
```

Figura 27 Exemple Servei TX utilització

7.3.7.-Percentatge d'utilització de la CPU a l'hora de rebre per cada AP

és la contrapart de l'anterior servei que anomenarem TX_utilitzacio, en aquest cas el que fem és mirar el percentatge d'utilització de la CPU que està ocupada a l'hora gestionar els paquets que rep.

Utilitzarem la command que hem creat en el anterior anomenada CHECK_SNMP_X, amb els valors de warning i critical a 25 i 50 respectivament (veure figura 28).

Aquest igual que l'anterior es faran per tots els Dispositius AP.

```
define service {

    use                     generic-service                 ; Inherit values from a template
    host_name               AP22
    service_description     Rx utilitzacio
    check_command           check_snmp_X!1.3.6.1.4.1.14179.2.2.13.1.1.32.76.158.235.211.64.0!25!50
}
```

Figura 28 Exemple Servei TX utilització

7.3.8.-Usuaris a cada SSID per cada AP

Com ja hem indicat ens interessa saber com està la distribució d'usuaris a cada un dels SSID per saber si es fa una mala utilització de la xarxa de visites que tindria que ser només per clients i proveïdors.

Per vigilar això farem un script (veure figura 29) una mica diferent dels anteriors, ja que directament no existeix cap OID que ens doni la informació que volem

```
#!/bin/bash

mac=$1
ssid=$2

snmpwalk -c public 192.168.101.230 -Ovq -v 2c 1.3.6.1.4.1.14179.2.1.4.1.1>miau1.txt
snmpwalk -c public 192.168.101.230 -Ovq -v 2c 1.3.6.1.4.1.14179.2.1.4.1.7>miau3.txt
snmpwalk -c public 192.168.101.230 -Ovq -v 2c 1.3.6.1.4.1.14179.2.1.4.1.4>miau4.txt
paste miau1.txt miau3.txt > final1
paste final1 miau4.txt > final

grep $ssid final>FiltradoSSID
grep "$mac" FiltradoSSID>FiltradoAP
lineas=$(wc -l < FiltradoAP)

echo "usuaris="$lineas"|usuaris="$lineas";20;30;;"
```

Figura 29 Script Per adquirir els usuaris de cada SSID per AP

1.3.6.1.4.1.14179.2.1.4.1.1 =MAC del dispositiu connectat

1.3.6.1.4.1.14179.2.1.4.1.7= SSID al que està connectat el dispositiu

1.3.6.1.4.1.14179.2.1.4.1.4= MAC del AP al que està connectat el dispositiu

El que fa el nostre script és buscar les dades que dóna la controladora sobre els usuaris connectats ho ajuntarem tot en un fitxer en el farem un filtrat per la MAC del AP que volem buscar i després filtrem pel SSID de la xarxa que volem, una vegada fet això es mira la quantitat de línies que hi ha per saber els dispositius i és la informació que ens tornarà.

Aquest script el posarem on estan els scripts que és a /usr/local/nagios/librexec i modificarem l'arxiu commands.cfg per afegir aquesta nova comanda (veure figura 30)

```
define command {

    command_name    UsuarisSSID
    command_line    $USER1$/ssid $ARG1$ $ARG2$
}
```

Figura 30 Comanda UsuarisSSID

ARG1 rebrà la MAC del AP i ARG2 el SSID que volem fer el filtratge (figura 31)

```
define service {

    use                     generic-service                 ; Inherit values from a template
    host_name               AP22
    service_description     usuaris Visites
    check_command           UsuarisSSID!"20 4C 9E EB D3 40"!"VISITES"
}

define service {

    use                     generic-service                 ; Inherit values from a template
    host_name               AP22
    service_description     usuaris CXG
    check_command           UsuarisSSID!"20 4C 9E EB D3 40"!"CXG"
}

define service {

    use                     generic-service                 ; Inherit values from a template
    host_name               AP22
    service_description     usuaris CXG MOVIL
    check_command           UsuarisSSID!'20 4C 9E EB D3 40'!'CXGMobil"
}
```

Figura 31 Exemple de configuració dels serveis usuaris Visites, usuaris CXG i usuaris CXG MOBIL

Això ens presenta un problema,no es pot diferenciar els usuaris connectats a un SSID d'un AP en la freqüència de 2,4GHz o de 5GHz , però per fer una idea de com evoluciona la distribució d'usuaris ja farà el que és necessari, a més instal·larem a posteriori el plugin PNP4Nagios que servirà per fer gràfiques i podrem veure l'evolució dels usuaris als diferents SSID en el temps.

7.3.9.-Configuració host de la controladora

Igual que amb els AP podem i volem controlar alguns paràmetres de la controladora ens interessarà revisar els usuaris totals a cada SSID i si està funcionant o no la controladora.

Primer igual que pels AP el que fem és crear el host(veure figura 32).

```
define host {

    use                     generic-switch                  ; Inherit default values from a template
    host_name               ControladoraWifi                ; The name we're giving to this switch
    alias                   Controladora                ; A longer name associated with the switch
    address                 192.168.101.230                 ; IP address of the switch
    hostgroups              AP                          ; Host groups this switch is associated with
}
```

Figura 32 Host controladora

7.3.10.-Connectivitat de la controladora

Igual que la resta de APs per saber si està funcionant o no el que ens servirem és de fer pings a la controladora i si no respon entendrem que està fora de funcionament.

Per fer això afegirem el host controladora que hem acabem de crear a servei de ping(figura 33)

```
define service {

    use                     generic-service                 ; Inherit values from a template
    host_name               AP01,AP12,AP09,AP27,AP32,AP28,AP29,AP15,AP13,AP22,AP23,AP21,AP02,AP26,AP35,AP10,AP24,AP11,AP04,AP34
,AP25,AP31,AP30,AP17,AP16,AP19,AP33,APT02,APT03,APT04,AP16_5GZ,AP17_5GZ,AP19_5GZ,AP21_5Gz,AP22_5GZ,AP23_5GZ,AP24_5GZ,
AP25_5GZ,AP26_5GZ,AP27_5GZ,AP28_5GZ ,AP29_5GZ,,AP30_5GZ,AP32_5GZ ,AP31_5GZ ,AP34_5GZ,AP35_5GZ,APT04_5GZ,ControladoraWifi                ; The name of the host the service is as
    service_description     PING                            ; The service description
    check_command           check_ping!200.0,20%!600.0,60%  ; The command used to monitor the service
    check_interval          5                               ; Check the service every 5 minutes under normal conditions
    retry_interval          1                               ; Re-check the service every minute until its final/hard state is determined
}
```

Figura 33 configuració Controladora al ping

7.3.11.-Numero d'usuaris totals a cada SSID

Per últim el que volem incloure per controlar amb nagios és els usuaris per cada SSID, per això utilitzarem el següent OID: 1.3.6.1.4.1.14179.2.1.1.1.38

Això ens dóna la informació de tots els usuaris per cada SSID, igual que amb els AP si hi ha més d'un SSID hem d'utilitzar el seu identificador únic en aquest cas és fàcil només és té que comprar amb el que dóna en preguntar els noms dels SSID (veure figura 34).

```
[root@localhost ~]# snmpwalk -c public 192.168.101.230   -v 2c 1.3.6.1.4.1.14179.2.1.1.1.2
SNMPv2-SMI::enterprises.14179.2.1.1.1.2.1 = STRING: "CXG"
SNMPv2-SMI::enterprises.14179.2.1.1.1.2.2 = STRING: "VISITES"
SNMPv2-SMI::enterprises.14179.2.1.1.1.2.3 = STRING: "CXGWMA"
SNMPv2-SMI::enterprises.14179.2.1.1.1.2.4 = STRING: "CXG2"
SNMPv2-SMI::enterprises.14179.2.1.1.1.2.5 = STRING: "CXGMobil"
[root@localhost ~]#
```

Figura 34 Codi SNMP dels SSID

Només volem revisar el SSID CXG amb l'identificador 1, el de la visita amb l'identificador 2 i el de CXGMobil amb el 5.

Crearem avisos si els dispositius superant els 175 i 250 usuaris connectats a una xarxa que seran els valors de warning i critical respectivament.

Aquí ens vam trobar un problema que en mostrar dades a nagios posava al final un C d'unitat, per eliminar això vam crear una nova comanda (figura 35)

```
define command {

    command_name    check_snmp_controladora
    command_line    $USER1$/check_snmp -H 192.168.101.230 -C public -P 2c  -o $ARG1$ -w $ARG2$ -c $ARG3$ sed 's/c//g'
}

define command {
```

Figura 35 Configuració CHECK_SNMP_CONTROLADORA

Després de buscar el valor amb el OID amb la comanda sed el que farem és eliminar la c que s'ha posat al final de valor.

Ara amb tot preparat ja podem crear els serveis utilitzant el valors dels SSID i la nova comanda que hem creat que l'hem deixat al fitxer de commands.cfg.

Els serveis són els mostrats en la següent figura (figura36) en el que tindrem un per cada SSID

```
define service {

    use                     generic-service                 ; Inherit values from a template
    host_name               ControladoraWifi
    service_description     usuaris CXG
    check_command           check_snmp_controladora!1.3.6.1.4.1.14179.2.1.1.1.38.1!175!250
}

define service {

    use                     generic-service                 ; Inherit values from a template
    host_name               ControladoraWifi
    service_description     usuaris visites
    check_command           check_snmp_controladora!1.3.6.1.4.1.14179.2.1.1.1.38.2!175!250
}

define service {

    use                     generic-service                 ; Inherit values from a template
    host_name               ControladoraWifi
    service_description     usuaris CXGMobil
    check_command           check_snmp_controladora!1.3.6.1.4.1.14179.2.1.1.1.38.5!175!250
}
```

Figura 36 Configuració Serveis controladora

7.4.-Configuració Plugin Nagios:PNP4NAGIOS

Com ja hem esmentat Nagios té la possibilitat de instalar Plugins que són petits programes per poder incrementar les funcionalitats del sistema, en el nostre cas volem instal·lar PNP4NAGIOS que amb les dades proporcionades per Nagios fa gràfiques de l'evolució en el temps, això ens servirà per veure si la xarxa millora o empitjora a llarg termini

Ara que ja ho tenim tot preparat instal·larem un plugin que guardarà les dades que preguntat el nagios cada 5 minuts i farà un gràfic amb la informació.

El que farem és seguir la documentació proporcionada per la mateixa gent de Nagios[19] que està adjuntada a la bibliografia, seguint tots els passos que indica ho tindrem instal·lat sense problemes.

A més del que hi ha a la documentació el que afegirem serà als templates de genèric host i del genèric servei la utilització de host-pnp i service-pnp que farà que el plugin pugui treballar amb les dades que genera el nagios.

```
define host {

    name                            generic-host            ; The name of this host template
    use                             host-pnp
    notifications_enabled           1                       ; Host notifications are enabled
    event_handler_enabled           1                       ; Host event handler is enabled
    flap_detection_enabled          1                       ; Flap detection is enabled
    process_perf_data               1                       ; Process performance data
    retain_status_information       1                       ; Retain status information across program restarts
    retain_nonstatus_information    1                       ; Retain non-status information across program restarts
    notification_period             workhours                   ; Send host notifications at any time
        register                        0                       ; DONT REGISTER THIS DEFINITION - ITS NOT A REAL CONTACT, JUST A T
}
```

Figura 37 Insercio del codi per PNP4NAGIOS

```
define service {

    name                            generic-service         ; The
    use                             service-pnp             ;
    active_checks_enabled           1                       ; Act
    passive_checks_enabled          1                       ; Pas
    parallelize_check               1                       ; Act
    obsess_over_service             1                       ; We
    check_freshness                 0                       ; Def
    notifications_enabled           1                       ; Ser
    event_handler_enabled           1                       ; Ser
    flap_detection_enabled          0                       ; Fla
    process_perf_data               1                       ; Pro
    retain_status_information       1                       ; Ret
    retain_nonstatus_information    1                       ; Ret
    is_volatile                     0                       ; The
    check_period                    24x7                    ; The
    max_check_attempts              3                       ; Re-
    check_interval                  10                      ; Che
    retry_interval                  2                       ; Re-
    contact_groups                  admins                  ; Not
    notification_options            w,u,c,r                 ; Sen
    notification_interval           60                      ; Re-
    notification_period             24x7                    ; Not
    register                        0                       ; DON
}
```

Figura 38 Insercio del codi per PNP4NAGIOS 2

Una vegada fet això ja podem revisar si tot funciona correctament al nagios.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
AP01	MalaConexio	OK	08-17-2019 13:09:05	7d 23h 27m 24s	1/3	SNMP OK - 0
	PING	OK	08-17-2019 13:12:27	9d 4h 12m 1s	1/3	PING OK - Packet loss = 0%, RTA = 0.56 ms
	Rx utilitzacio	OK	08-17-2019 13:06:10	9d 4h 8m 19s	1/3	SNMP OK - 0 %
	Tx utilitzacio	OK	08-17-2019 13:08:26	9d 4h 6m 3s	1/3	SNMP OK - 1 %
	Utilitzacio	OK	08-17-2019 13:05:51	5d 0h 30m 38s	1/3	SNMP OK - 9
	usuaris	OK	08-17-2019 13:12:56	2d 23h 41m 32s	1/3	SNMP OK - 1
	usuaris CXG	OK	08-17-2019 13:12:08	66d 0h 7m 40s	1/3	usuaris=0
	usuaris CXG MOVIL	OK	08-17-2019 13:13:35	66d 0h 7m 35s	1/3	usuaris=0
	usuaris Visites	OK	08-17-2019 13:05:07	65d 23h 45m 47s	1/3	usuaris=0
AP02	MalaConexio	OK	08-17-2019 13:06:15	73d 3h 35m 10s	1/3	SNMP OK - 0
	PING	OK	08-17-2019 13:12:30	86d 1h 9m 35s	1/3	PING OK - Packet loss = 0%, RTA = 0.56 ms
	Rx utilitzacio	OK	08-17-2019 13:06:29	51d 20h 58m 2s	1/3	SNMP OK - 0 %
	Tx utilitzacio	OK	08-17-2019 13:07:37	51d 20h 46m 52s	1/3	SNMP OK - 1 %
	Usuaris	OK	08-17-2019 13:14:17	86d 0h 10m 10s	1/3	SNMP OK - 0
	Utilitzacio	OK	08-17-2019 13:07:04	17d 3h 37m 28s	1/3	SNMP OK - 15
	usuaris CXG	OK	08-17-2019 13:12:09	66d 0h 6m 17s	1/3	usuaris=1
	usuaris CXG MOVIL	OK	08-17-2019 13:04:29	72d 0h 6m 48s	1/3	usuaris=0
	usuaris Visites	OK	08-17-2019 13:05:13	72d 0h 5m 18s	1/3	usuaris=0
AP04	MalaConexio	OK	08-17-2019 13:06:18	73d 3h 32m 29s	1/3	SNMP OK - 0
	PING	OK	08-17-2019 13:12:39	86d 1h 11m 40s	1/3	PING OK - Packet loss = 0%, RTA = 0.62 ms
	Rx utilitzacio	OK	08-17-2019 13:12:47	18d 1h 23m 41s	1/3	SNMP OK - 0 %
	Tx utilitzacio	OK	08-17-2019 13:09:23	51d 20h 45m 8s	1/3	SNMP OK - 1 %

Figura 39 Nagios + plugin PNP4NAGIOS

En Vermell podem veure la icona des d'on podrem consultar les gràfiques també està al costat de cada servei que controla nagios.

Quan entrem a veure les gràfiques amb el plugin el que veurem serà una cosa semblant a aquesta

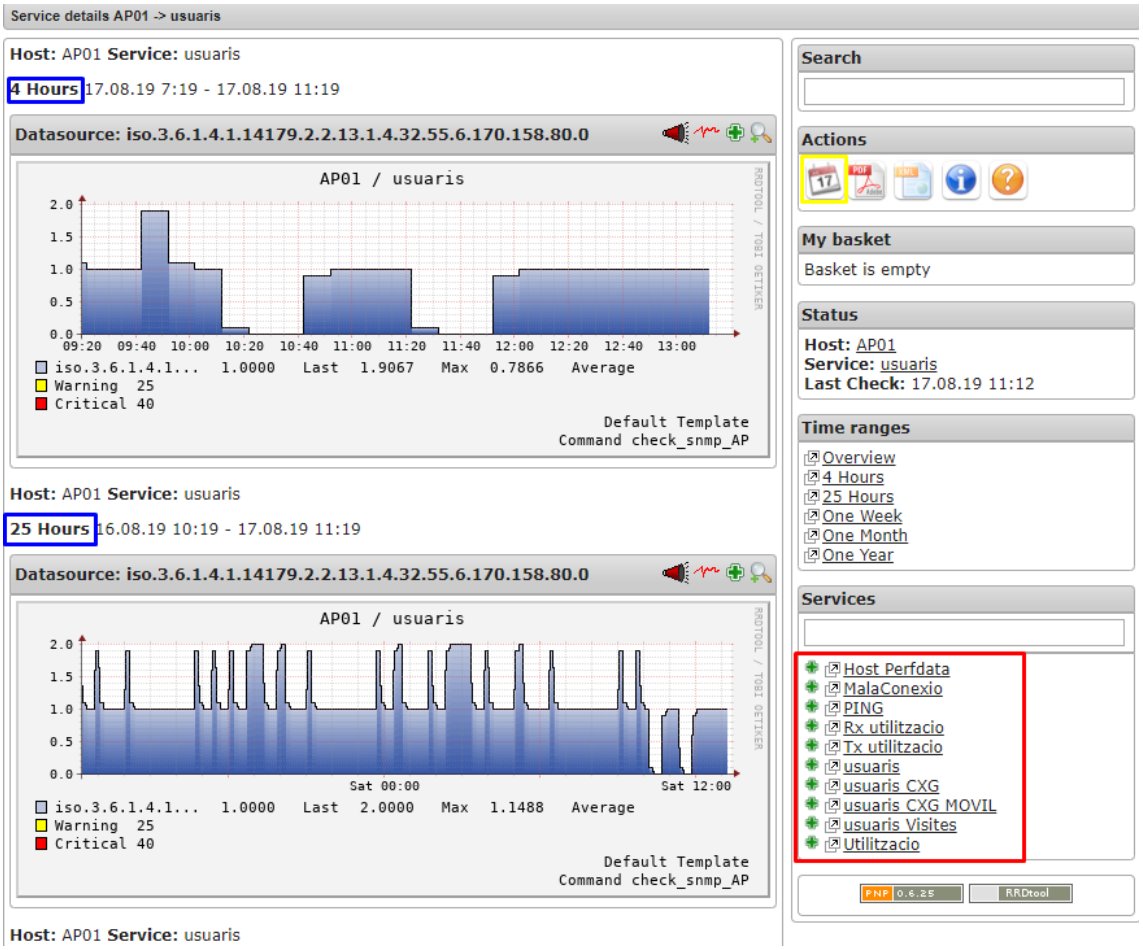


Figura 40 pantalla de visualitzacio de PNP4NAGIOS

En vermell podem veure de el host tot els controls que gestiona i en blau diferents temps horaris , també es pot buscar un dia determinat utilitzant la funció en groc.

8.-Anàlisi dels problemes la xarxa Wi-Fi i proposta de millora.

8.1.- Anàlisi dels problemes la xarxa Wi-Fi

Després de recollir dades durant 15(1 de juliol al 18 de juliol) dies laborals analitzem i revisarem els problemes més comuns i buscarem maneres de solucionar-ho.

El primer que hem de fer és recollir un a un les dades des del nagios, per fer això hem anat a veure els gràfics del PNP4nagios

Host	Service	Status	Last Check
AP01	MalaConexio	OK	08-17-2019 16:29:05
	PING	OK	08-17-2019 16:32:27
	Rx utilitzacio	OK	08-17-2019 16:36:10
	Tx utilitzacio	OK	08-17-2019 16:28:26
	Utilitzacio	OK	08-17-2019 16:35:51
	usuaris	OK	08-17-2019 16:32:56
	usuaris CXG	OK	08-17-2019 16:32:08
	usuaris CXG MOVIL	OK	08-17-2019 16:33:35
	usuaris Visites	OK	08-17-2019 16:35:07

Figura 41 Ubicacio del plugin PNP4NAGIOS

Després seleccionarem els serveis que volem recollir les dades

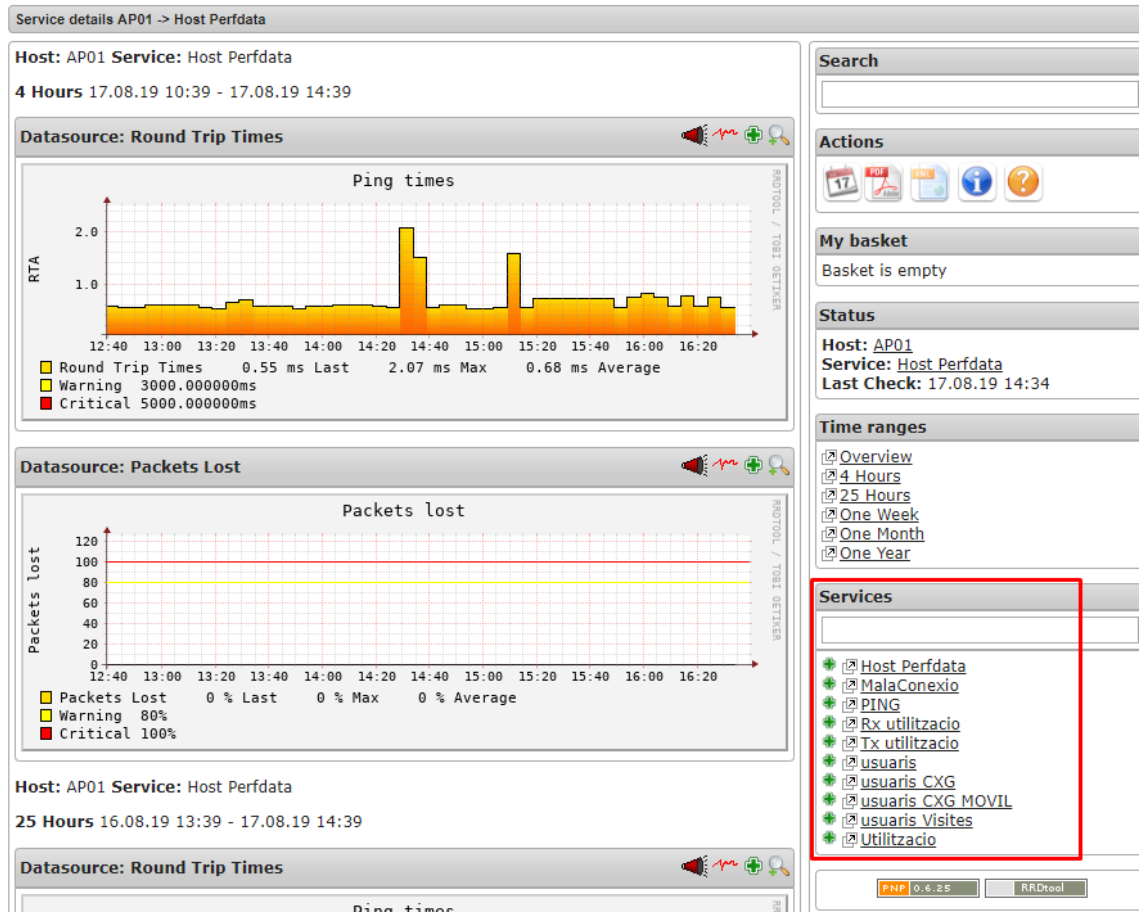


Figura 42 Pantalla de PNP4NAGIOS per un host

Una vegada hem escollit el servei, cliquem sobre la icona del calendari per posar l'interval de dates en les que volem recopilar tots els warnings i criticals que han aparegut per aquest AP

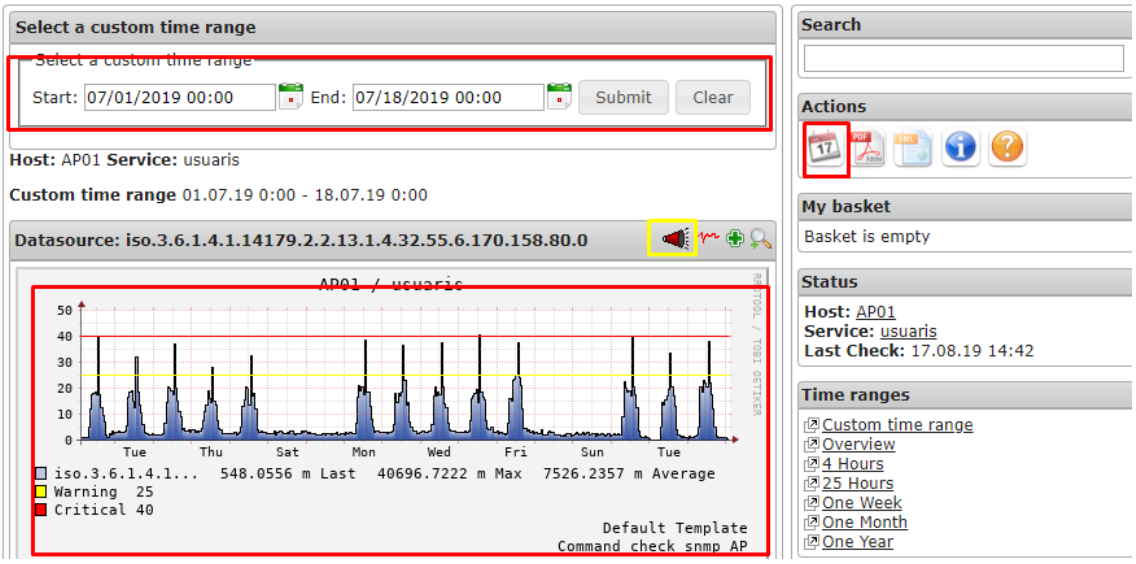


Figura 43 Filtratge d'un servei específic per un host en una data determinada

Quan ja estem en aquest punt anem sobre la icona marca en groc i ens genera un informe sobre tots els warnings i criticals per aquell servei en l'interval que hem seleccionat.

Most Recent Alerts For Host 'AP01'

07-01-2019 00:00:00 to 07-18-2019 00:00:00
Duration: 17d 0h 0m 0s

Displaying all 305 matching alerts

Time	Alert Type	Host	Service	State	State Type	Information
07-17-2019 16:05:47	Service Alert	AP01	Utilitzacio	OK	HARD	SNMP OK - 25
07-17-2019 16:03:47	Service Alert	AP01	Utilitzacio	WARNING	SOFT	SNMP WARNING - *68*
07-17-2019 16:01:47	Service Alert	AP01	Utilitzacio	WARNING	SOFT	SNMP WARNING - *76*
07-17-2019 14:20:53	Service Alert	AP01	usuaris	OK	SOFT	SNMP OK - 24
07-17-2019 14:18:53	Service Alert	AP01	usuaris	WARNING	SOFT	SNMP WARNING - *27*
07-17-2019 14:08:53	Service Alert	AP01	usuaris	OK	HARD	SNMP OK - 25
07-17-2019 13:48:53	Service Alert	AP01	usuaris	WARNING	HARD	SNMP WARNING - *40*
07-17-2019 13:28:53	Service Alert	AP01	usuaris	CRITICAL	HARD	SNMP CRITICAL - *47*
07-17-2019 13:08:53	Service Alert	AP01	usuaris	WARNING	HARD	SNMP WARNING - *27*
07-17-2019 13:06:53	Service Alert	AP01	usuaris	WARNING	SOFT	SNMP WARNING - *33*
07-17-2019 13:04:53	Service Alert	AP01	usuaris	WARNING	SOFT	SNMP WARNING - *31*
07-17-2019 12:29:47	Service Alert	AP01	Utilitzacio	OK	SOFT	SNMP OK - 7
07-17-2019 12:27:47	Service Alert	AP01	Utilitzacio	WARNING	SOFT	SNMP WARNING - *77*
07-17-2019 11:37:47	Service Alert	AP01	Utilitzacio	OK	HARD	SNMP OK - 44
07-17-2019 11:35:47	Service Alert	AP01	Utilitzacio	WARNING	SOFT	SNMP WARNING - *67*
07-17-2019 11:33:47	Service Alert	AP01	Utilitzacio	WARNING	SOFT	SNMP WARNING - *77*
07-17-2019 11:04:53	Service Alert	AP01	usuaris	OK	HARD	SNMP OK - 23
07-17-2019 11:02:53	Service Alert	AP01	usuaris	WARNING	SOFT	SNMP WARNING - *26*
07-17-2019 11:00:53	Service Alert	AP01	usuaris	WARNING	SOFT	SNMP WARNING - *26*
07-17-2019 10:48:53	Service Alert	AP01	usuaris	OK	SOFT	SNMP OK - 23
07-17-2019 10:46:53	Service Alert	AP01	usuaris	WARNING	SOFT	SNMP WARNING - *26*
07-17-2019 10:43:02	Service Alert	AP01	MalaConexio	OK	HARD	SNMP OK - 2
07-17-2019 10:36:53	Service Alert	AP01	usuaris	OK	HARD	SNMP OK - 24
07-17-2019 10:34:53	Service Alert	AP01	usuaris	WARNING	SOFT	SNMP WARNING - *26*
07-17-2019 10:33:02	Service Alert	AP01	MalaConexio	WARNING	HARD	SNMP WARNING - *6*
07-17-2019 10:32:53	Service Alert	AP01	usuaris	WARNING	SOFT	SNMP WARNING - *26*
07-17-2019 10:31:02	Service Alert	AP01	MalaConexio	WARNING	SOFT	SNMP WARNING - *6*
07-17-2019 10:29:02	Service Alert	AP01	MalaConexio	WARNING	SOFT	SNMP WARNING - *7*
07-16-2019 14:17:02	Service Alert	AP01	MalaConexio	OK	SOFT	SNMP OK - 5
07-16-2019 14:15:02	Service Alert	AP01	MalaConexio	WARNING	SOFT	SNMP WARNING - *6*
07-16-2019 14:13:47	Service Alert	AP01	Utilitzacio	OK	HARD	SNMP OK - 64
07-16-2019 14:12:53	Service Alert	AP01	usuaris	OK	HARD	SNMP OK - 23
07-16-2019 14:11:47	Service Alert	AP01	Utilitzacio	WARNING	SOFT	SNMP WARNING - *74*
07-16-2019 14:09:46	Service Alert	AP01	Utilitzacio	WARNING	SOFT	SNMP WARNING - *67*
07-16-2019 13:55:02	Service Alert	AP01	MalaConexio	OK	HARD	SNMP OK - 5
07-16-2019 13:53:02	Service Alert	AP01	MalaConexio	WARNING	SOFT	SNMP WARNING - *6*
07-16-2019 13:51:02	Service Alert	AP01	MalaConexio	WARNING	SOFT	SNMP WARNING - *8*
07-16-2019 13:42:53	Service Alert	AP01	usuaris	WARNING	HARD	SNMP WARNING - *36*

Figura 44 Filtratge d'un servei específic per un host en una data determinada

Fem això per tots els APs i per tots els serveis i tindrem les dades de totes els warnings i criticals que han aparegut en l'interval de 15 dies laborables que hem seleccionat.

Per fer més fàcil la visualització hem passat les dades a gràfiques en les que podrem veure quins AP presenten més problemes, hem utilitzat el nom dels serveis que ens mostra nagios.

- Utilització: Saturació del canal per cada AP
- Usuaris: numero usuaris connectats a cada AP
- Mala connexió: número d'usuaris amb baixa qualitat de senyal connectats a un AP
- RX: percentatge d'utilització de la CPU del AP que utilitza per processar els paquets que rep
- TX: percentatge d'utilització de la CPU del AP que utilitza per processar els paquets que envia

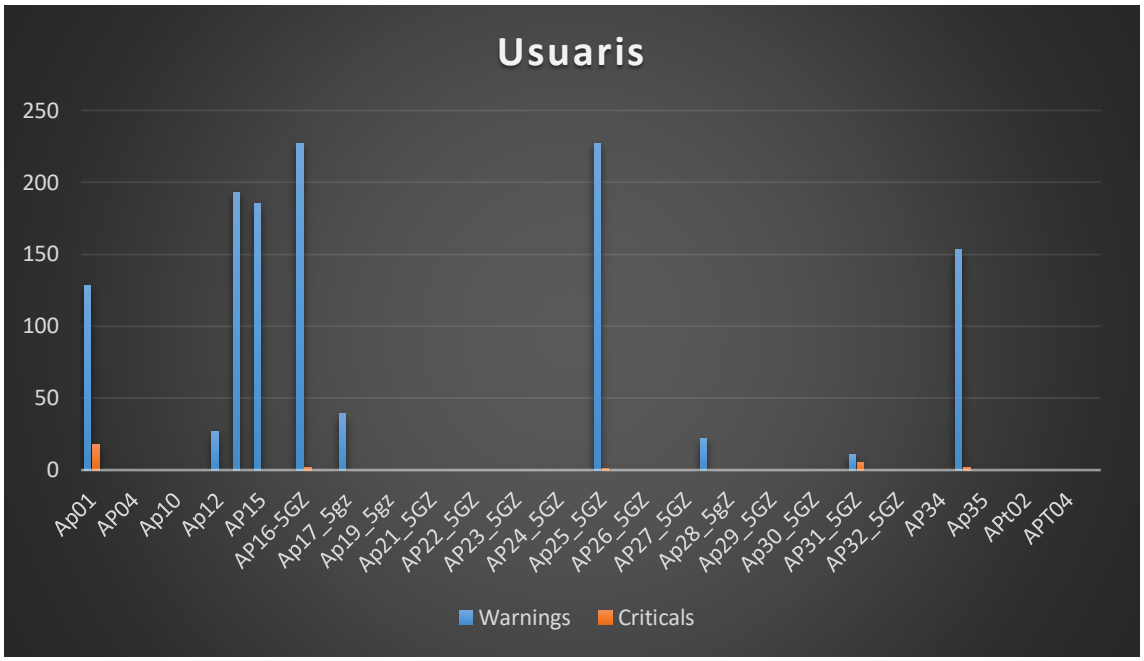


Figura 45 Gràfic amb el avisos per Numero d'usuaris per cada AP

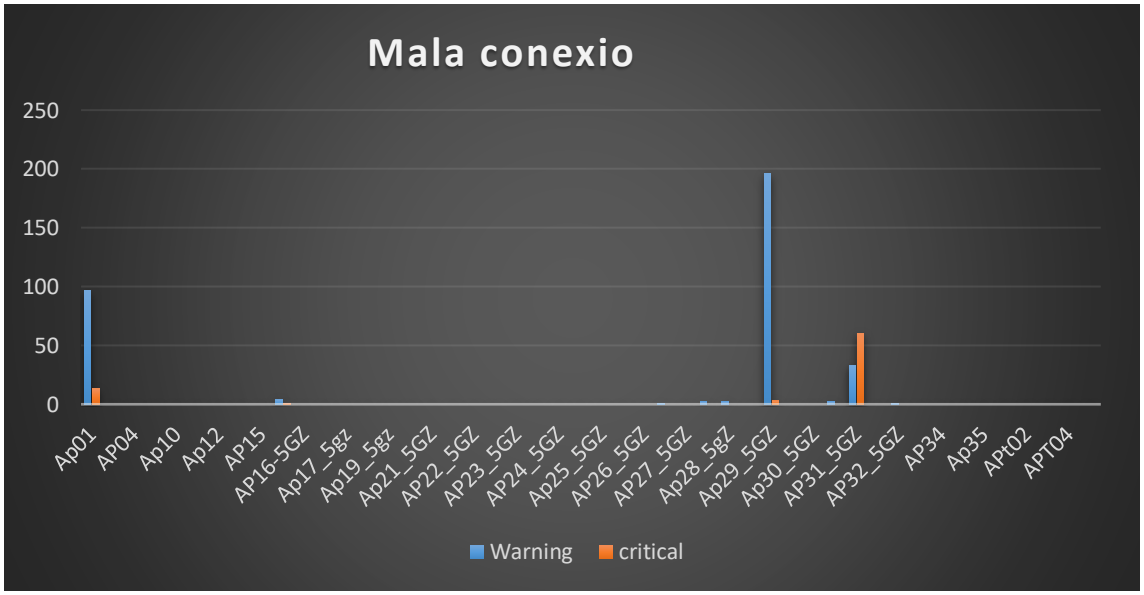


Figura 46 gràfic amb els avisos de dispositius connectats a un AP amb una baixa qualitat de la senyal

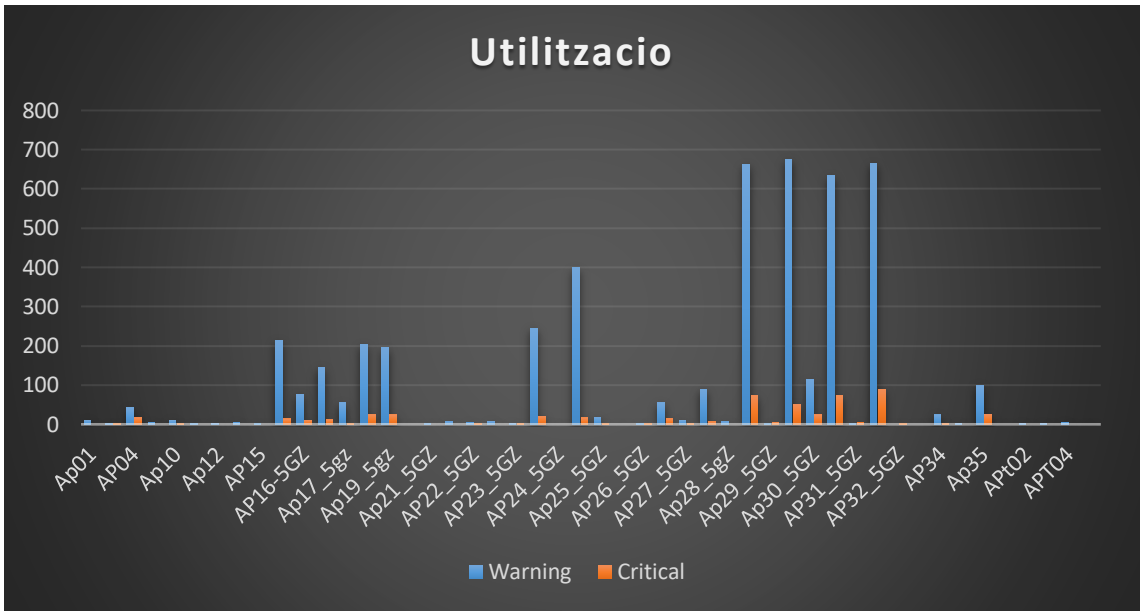


Figura 47 gràfic amb els avisos de saturació en la que treballa un AP

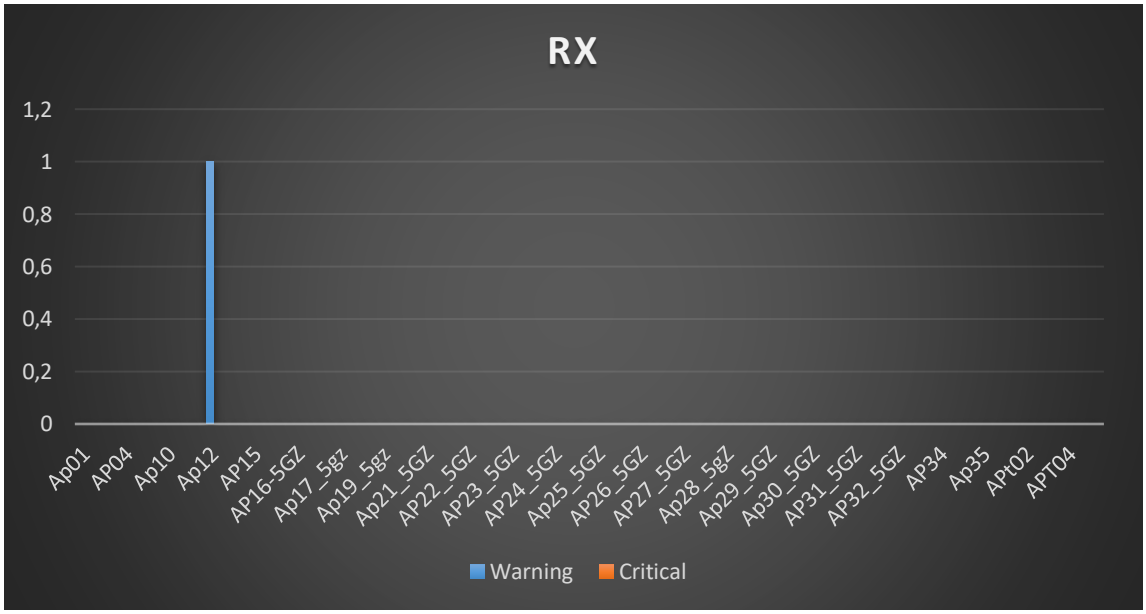


Figura 48 gràfic amb els avisos de percentatge de CPU a l'hora de processar els paquets que rep

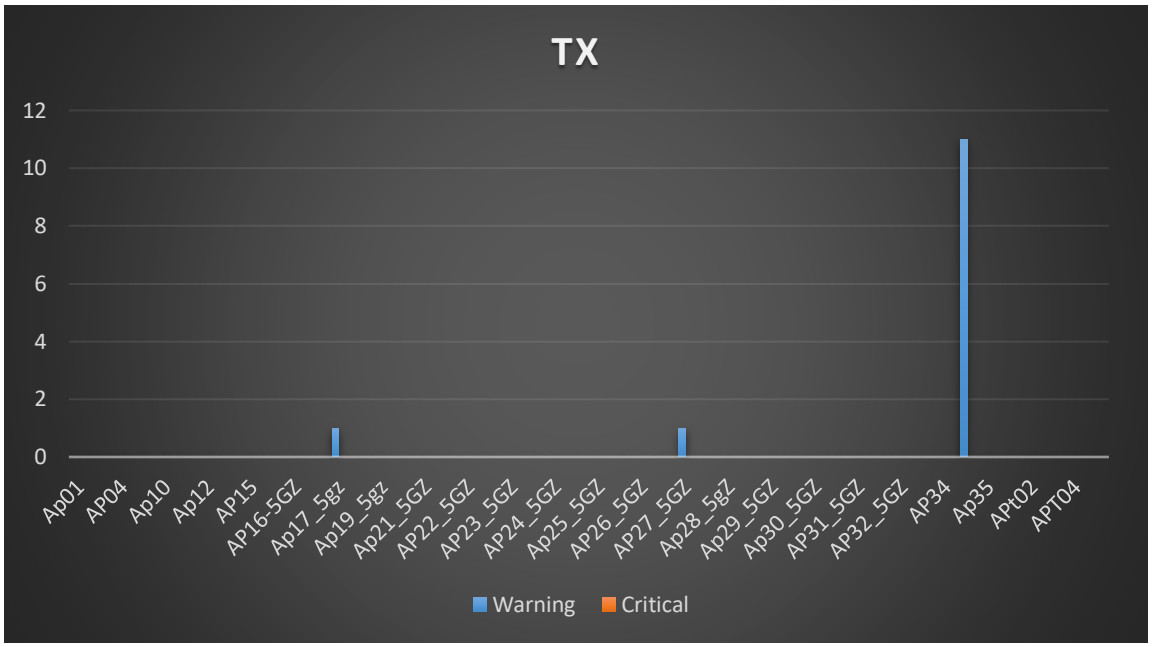


Figura 49 gràfic amb els avisos de percentatge de CPU a l'hora de processar els paquets que rep

Encara que semblin molts avisos de TX de mitjana no són ni un al dia i cal recordar que els warning vam programar perquè el warning avises amb un 25% de la utilització de la CPU, per tant no sembla que sigui un problema molt greu a tenir en compte, sembla que és més una càrrega puntual sobre una zona en la qual hi ha molta gent treballant

Després de buscar les dades i crear les següents gràfiques els APs que presenten més problemes són els següents (veure figura 50):

AP	Ubicació	Problemes
AP01	despatx tic	Usuaris, mala connexió
AP04	Sala Montserrat	Utilització
AP13	Recepció material/Mecanització	Usuaris
AP15	Procurement	Usuaris
AP16	Aplicacions	Utilització
A16_5GHz	Aplicacions	Usuaris, utilització
AP17	Gerència	Utilització
AP17_5Ghz	Gerència	Utilització
Ap19	Comercial	Utilització
AP19_5GHz	Comercial	Utilització
AP24	Planta 3 Xifra	Utilització
AP25	Planta 3	Utilització
AP25_5GHz	Planta 3	Usuaris
AP27	Nau A	Utilització
AP28	Nau A	Utilització
AP29	Nau A	Utilització
AP29_5Ghz	Nau A	Mala connexió

Ap30	Nau A	Utilització
ap30_5GHz	Nau A	Utilització
AP31	Nau A	Utilització
AP31_5Ghz	Nau A	Mala connexió
AP32	Nau A	Utilització
AP34_5Ghz	Servei	Usuaris
AP35	Nau A planta 2 paret	Utilització

Figura 50 Taula amb els problemes de cada AP

Després de fer la recollida de dades durant 15 dies laborals podem determinar que hi ha 3 tipus de dades són que fan saltar més els nivells de warning i critical que vam configurar:

- Alta quantitat d'usuaris connectats a un AP
- Usuaris amb senyal de baixa qualitat
- AP amb una alta saturació en el canal que estan treballant

Per determinar que els que hem vist abans són AP amb alguna d'aquestes problemàtiques hem determinat que el número de warnings i de criticals sigui molt gran per exemple el AP 30 té més de 600 avisos de warning per la saturació en el canal en el qual treballa el AP, igual pels usuaris amb una baixa qualitat i pel número d'usuaris connectats(als annexes es poden veure les gràfiques amb totes les dades) .

D'altra banda en els mapes de cobertura que es van generar es pot veure juntament amb la baixa qualitat del senyal que hi ha un parell de AP que potser no estan molt ben posicionats, també es veu zones sense cobertura (veure figura 51) la zona marcada en blau.

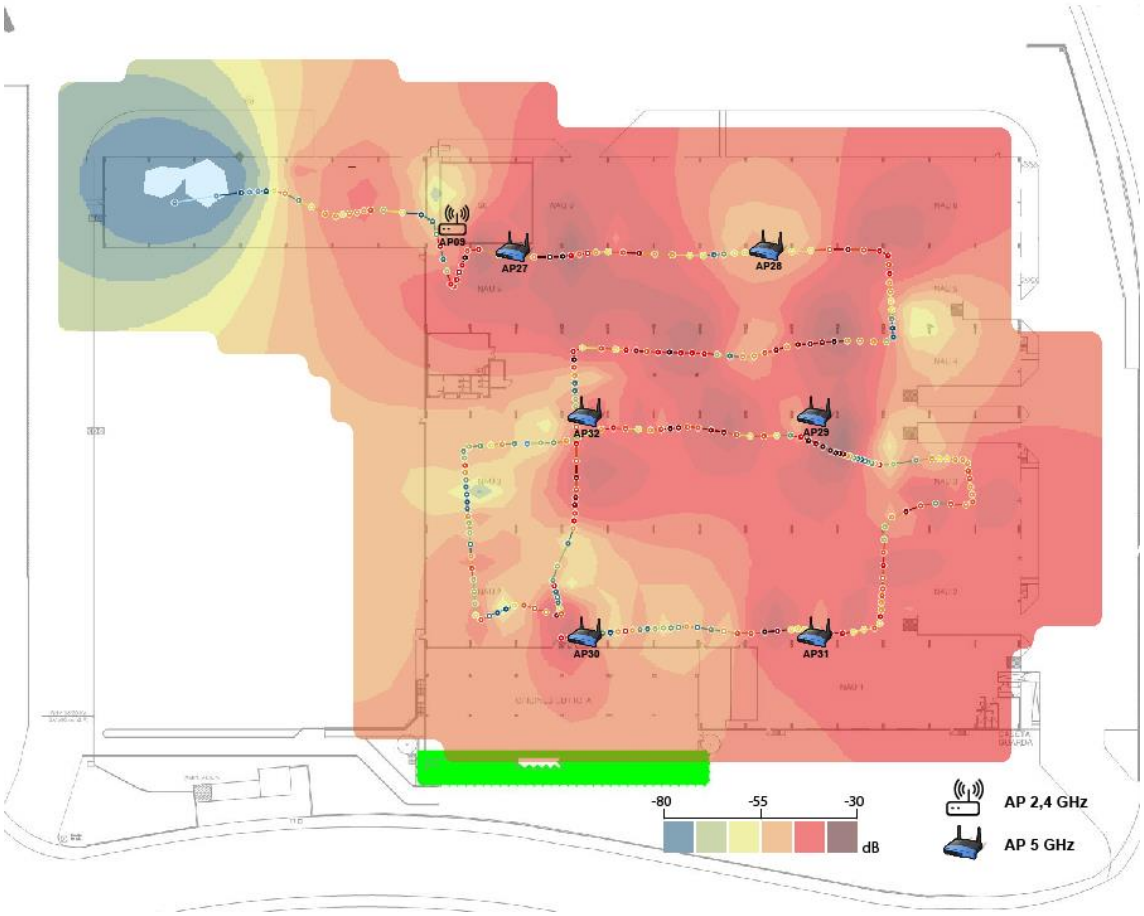


Figura 51 mapa cobertura planta nau A

També està el tema del número d'usuaris diaris de la xarxa de visites que és molt gran cada dia es connecten més de 150 persones a aquesta xarxa, que com ja hem comentat amb anterioritat només haguera de ser pels clients i els proveïdors (veure figura 52).

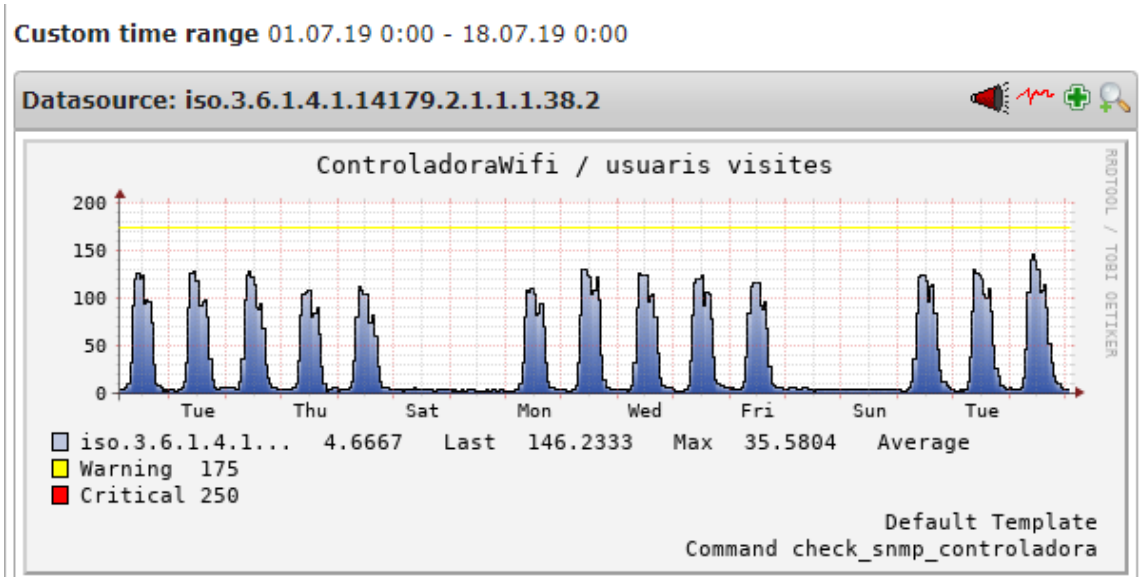


Figura 52 Usuaris conectats a visites del 01/07 al 18/07

8.2.-Propostes de millora

8.2.1.-Moure AP01

Com ja hem vist el AP01 el tenim marcat amb dos problemes: usuaris connectats amb baixa qualitat de senyal i el número d'usuaris que és connecten.

El AP01 està al costat del menjador i es pot veure que a les hores on dóna problemes és sobretot al migdia quan més usuaris es connecten a aquest AP, el que podem provar és si millora la cobertura i la qualitat del senyal si es mou el AP (veure figura 53).

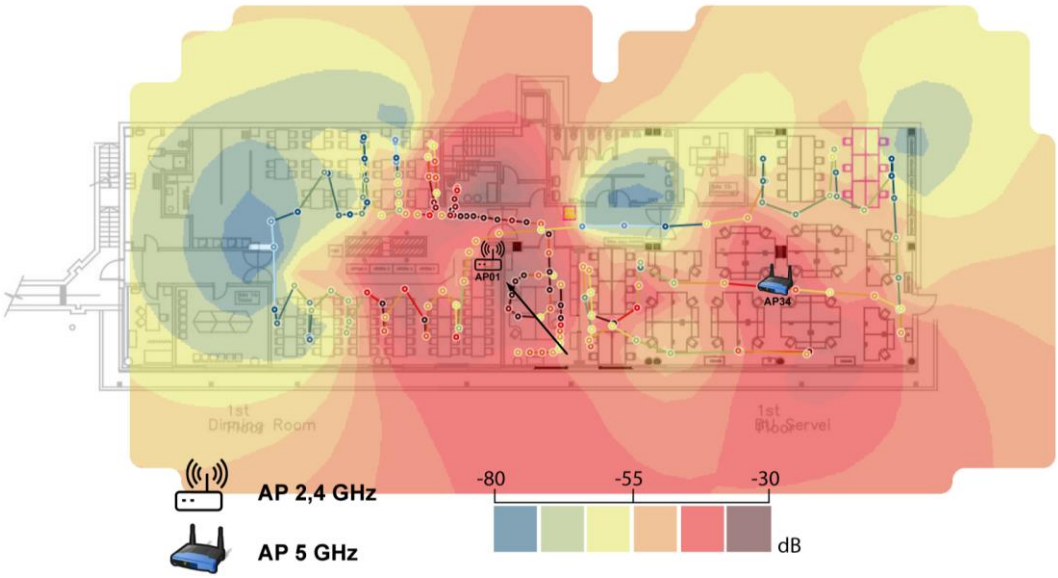


Figura 53 cobertura després de canviar AP01

Es pot veure una millora de la cobertura a la zona propera al AP però la més distant per la disposició de les columnes no es nota millora, però encara que al mapa de calor de cobertura no es nota una millora la posició és temporal i es podria buscar una posició millor el problema que hem tingut a l'hora de col·locar el AP és que només teníem endoll al costat de la paret, per millorar més es haguera de passar un cable pel sostre i ubicar el AP a la següent posició marcada en vermell (veure figura 54).

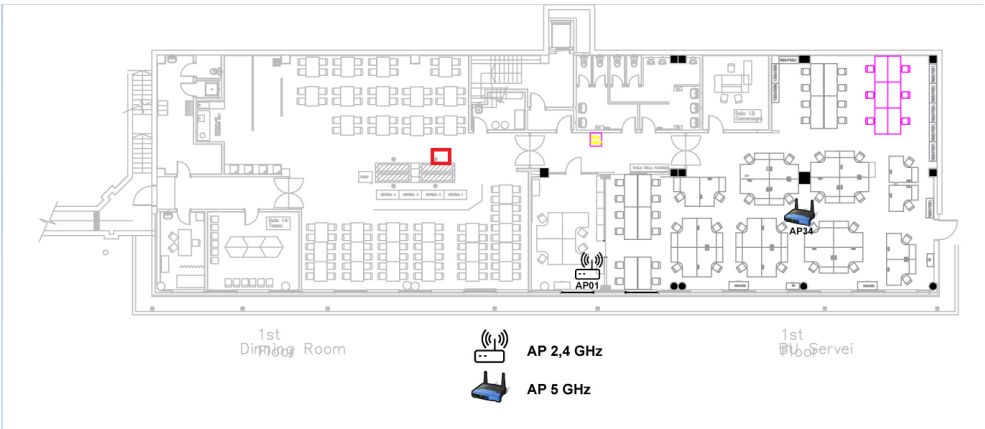


Figura 54 posició per moure el AP01

Però les dades del dia que es va realitzar la prova van ser molt bones millorant notablement, ja que no es va notar cap avis per usuaris connectats amb baixa qualitat del senyal.

Per fer això haurem de demanar un pressupost perquè no ho podem fer sense gastar diners i necessitarem l'aprovació del cap de informatica per portar a terme aquest canvi.

Aquesta millora proporcionaria a una zona una millor cobertura i qualitat de senyal pels treballadors, encara que no és una zona normalment destinada pel treball a vegades si les sales de reunió estan ocupades es fan reunions al menjador, per tant seria una bona idea fer aquesta inversió.

8.2.2.-afegir un AP a les zones amb baixa cobertura

Com hem pogut veure als mapes hi ha dues zones en la que la cobertura no és molt bona la part de bombos a la NAU A i una sala de reunions a BU Procurement.

Seria bon afegir una AP en aquest dos llocs per poder millorar la cobertura, però els dos llocs no són iguals en el primer la zona de bombos de la nau A és una zona en la qual només es fa treball manual i no es necessita dispositius Wi-Fi aquesta inversió seria una inversió per a futur si la disposició de la planta canvies.

A continuació(vegeu figura 55) es pot veure la ubicació proposada per posat el AP

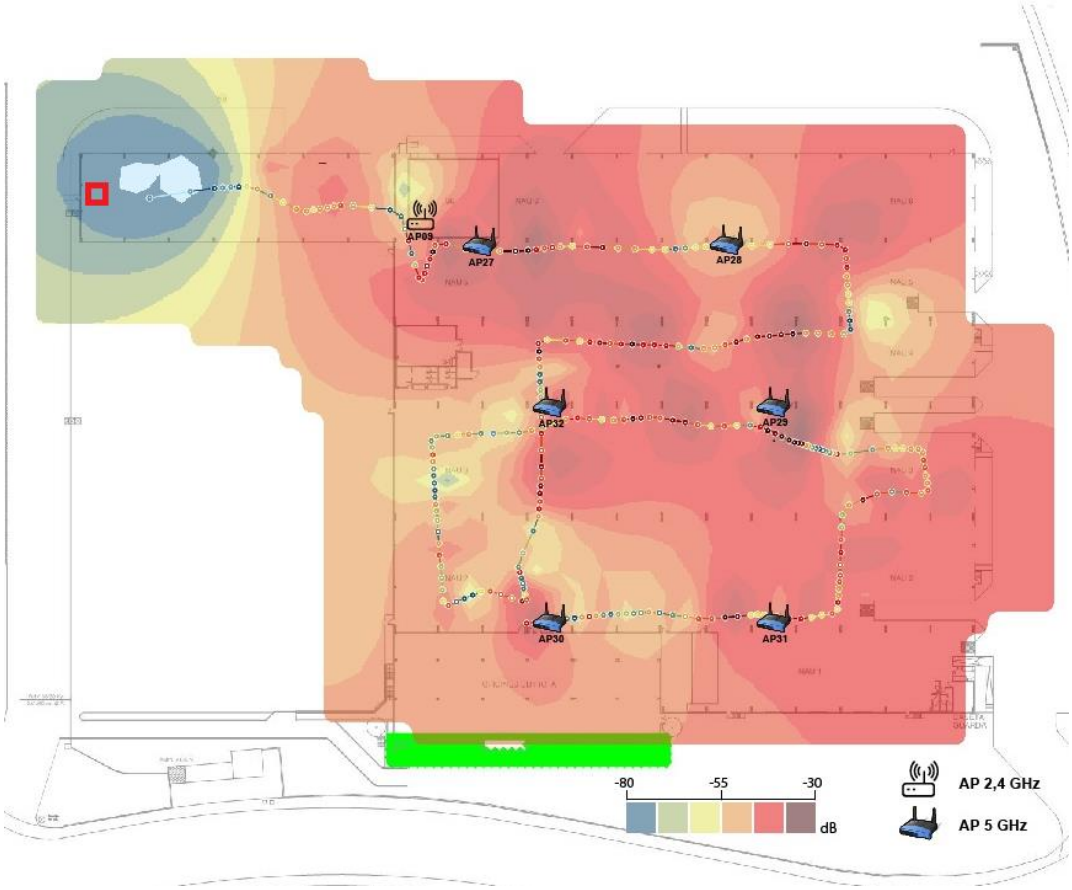


Figura 55 Ap proposat nauA bombos

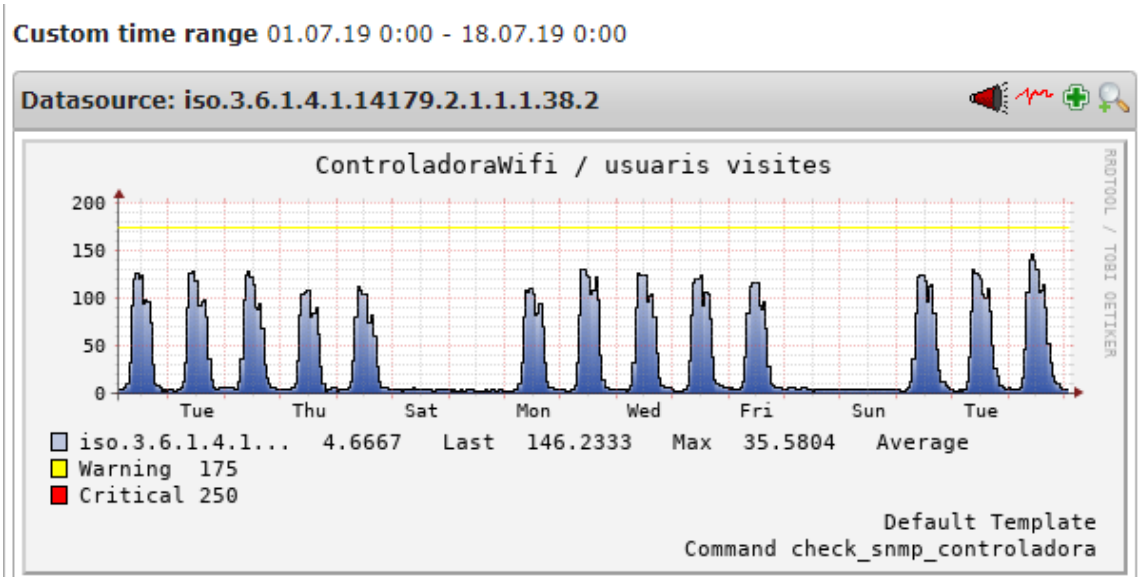
En la segona zona es pot afegir també un AP però tindrà que tenir la seva potencia disminuïda perquè generi poca interferència amb el AP que està a les oficines. Per aquest AP sí que seria bo fer una

inversió com més aviat millor ja que és una zona on es fan reunions diàriament i els usuaris es queixen de què moltes vegades perden el senyal de Wi-Fi.

Es haguera de posar la connexió de ethernet i passar un cable des del switch, ja que actualment la infraestructura no aquesta pensada per posar un AP.

8.2.3.-Revisar els usuaris que és connecten a Visites

Com ja hem senyalat la xarxa de visites és una que només es haguera de connectar clients i proveïdors però al dia a dia això no és real, molts treballadors es connecten a la xarxa.



Aquest és el gràfic dels usuaris connectats a visites durant la data que es va fer la recollida de dades, pràcticament cada dia hi ha de mitja 100 usuaris connectats, això podria està fent que la xarxa funcioni pitjor del que tocaria.

Per corroborar que això pot empitjorar la xarxa durant un dia posarem contrasenya a la xarxa , ja que a Comexi tenim un gran número de clients i proveïdors cada dia i per molestar el mínim possible només es pot fer això sense avisar durant un dia.

Amb les dades recollides durant un dia es pot veure una notable millora de tots els aspectes que hem estat monitorant, per poder dir això el que hem fet és buscar la mitja diària sobre les dades que es van recollir els 15 dies per comparar amb les dades del dia amb la xarxa de visites amb contrasenya, per poder veure això hem creat unes gràfiques que es poden veure a l'annex.

Una vegada podem veure que limitar la gent connectada a visites millora l'estat de la xarxa Wi-Fi i genera menys avisos a nagios hem de veure quines opcions tenim per fer-ho.

- **Posar una contrasenya a la xarxa**: és una idea senzilla i fàcil d'aplicar posar una contrasenya perquè no tothom pugui entrar però es haurà de donar als clients i proveïdors que vinguin a l'empresa . Aquesta manera de fer-ho té un problema i és que la contrasenya es digui pel boca a boca i acabem amb tots els treballadors una altra vegada amb el seu dispositiu personal connectats a la xarxa.

- **Filtrar i eliminar les macs dels dispositius personals dels treballadors**: es pot fer un filtratge de les macs perquè no es puguin connectar a la xarxa de visites, això es pot fer buscant durant un parell de setmanes totes els dispositius que estan connectats a la xarxa per exemple a les 12 del migdia i a les 4 de la tarda i les adreces mac que estiguin moltes vegades repetides en aquest espai de temps seran dispositius personals. Aquesta manera no és 100% infal·lible possiblement tenim algun dispositiu personal però serant inferiors al que hi ha actualment però a diferència no es molestarà de cap manera a la gent externa a Comexi.
- **Crear un sistema d'usuaris i contrasenyes per facilitar als visitants: es** pot utilitzar una plataforma d'autentificació d'usuaris que les dades es podrien donar als visitants per exemple tenir 30 usuaris o 50 autoritzats i seria els unics que podrien accedir a la xarxa. Això crea molta més seguretat que els altres sistemes encara que està el problema que els visitants han d'introduir alguna mena de dades per poder accedir a la xarxa.

De les opcions abans plantejades anteriorment teníem un sistema entre l'1 i el 3 a l'entrar un visitant des de recepció es facilitava un usuari i contrasenya de la xarxa, però l'usuari i contrasenya a diferència de la tercera opció era el mateix per a tot el món i es canviava cada setmana, aquest sistema perquè als directius no els hi era còmode es va treure i es va deixar tal com és avui en dia sense cap mena de seguretat.

La millor de les opcions és la 3 en la que es millora la seguretat i es pot controlar una mica el tràfic de cada usuari, però si anteriorment des de direcció no volien que els clients haguessin d'introduir cap mena de dades per poder connectar-se a la xarxa no crec que sigui la ideal encara que és al millor, per això jo crec que la que és més fàcil i invisible és l'opció 2 la de bloquejar les macs dels dispositius particulars dels treballadors perquè no accedeixin a la xarxa.

Com hem vist amb el resultat d'estar un dia sense la xarxa de visites accessible a tot el món és una millora que proporcionarà menys dispositius connectats i també un menor ús del canal per el qual treballen els AP el que genera menys interferències.

8.2.4.-Canviar AP antics i actualitzar els dispositius Wi-FI

Una manera de fer que la xarxa millori és fer una inversió i canviar tots els APs que són més antics i encara no tenen la capacitat per treballar sobre la banda de 5GHz, ja que al fer aquest canvi tots els dispositius que estan al d'aquest AP i tenen una antena que pugui emetre en el canal de 5GHz ho podrà fer, deixant més lliure la banda de 2,4GHz que és més petita i tarda menys en saturar-se de dispositius i generar interferències.

Juntament amb això també es podria mirar de canviar tots els dispositius de l'empresa (Portatil, smartphone,PDA o tablet) que encara no tenen una antena que pugui treballar en la banda de 5GHz.

Amb això es millora la infraestructura de la xarxa al modernitzant tots els AP i es permet que tots els dispositius que poden treballar sobre la banda de 5GHz ho puguin fer i es quedi amb menys dispositius connectats la banda de 2,4GHz, el farà que baixi el número d'avisos de nagios per la saturació del canal en el qual treballa cada AP.

8.2.5.-Limitar el número d'usuaris per cada AP

Hi ha una opció per des de la controladora (vegeu figura 56) per limitar el número de clients que estan connectats a cada AP per un SSID en concret, podem llavors limitar el numero i si algun SSID està ja molt ocupat de persones el client es connectarà a un altre AP que tingui a rang i amb la millor senyal.

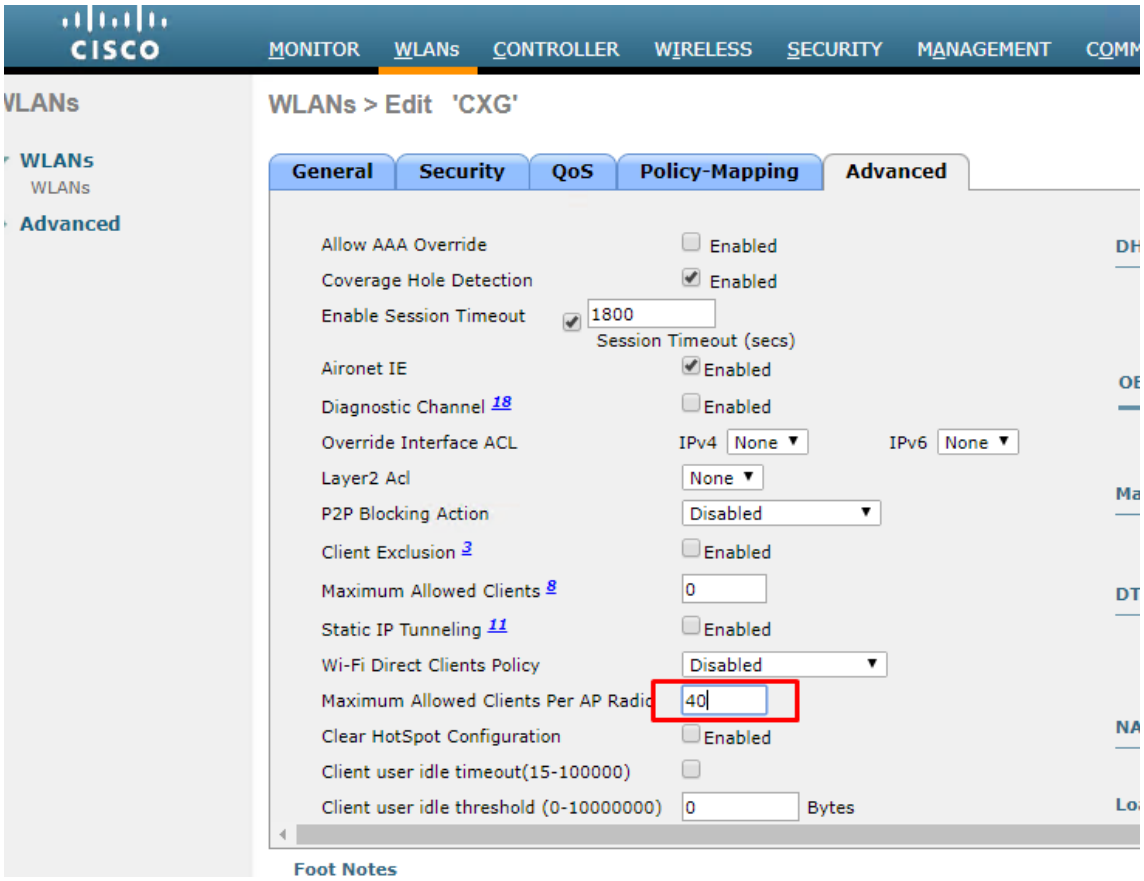


Figura 56 limitar el numero de clients de un SSID a un AP

Si implementem aquesta millora, rebaixant el número de clients a 40 (abans estava en 200)limitarem que un sol AP estigui molt ocupat amb un sol tipus de client per exemple quan es fan reunions multitudinàries en alguna sala de reunions és fàcil que es puguin reunir 30-40 persones.

Llavors aquesta implementar això farà que el número d'usuaris a un sol AP no pugui incrementar molt fent que no arribi a donar un mal servei.

9.-Conclusions

Després de fer tot el treball podem afirmar que la xarxa de Comexi ja va ser pensada i es van posicionar bé tots els APs ,ja que en fer el mapa de la cobertura tot estava correcte menys la cobertura al menjador, a una zona on no hi ha pràcticament treballadors i el pitjor cas era una sala de reunions

Hem pogut crear un sistema gràcies al nagios que ens ajudarà a controlar i mantenir el sistema vigilar per si hi ha problemes a la xarxa i al ser tan configurable sempre serà fàcil d'afegir o modificar, també el podrem exportar i controlar els AP i la xarxa WI-FI de les divisions de Brasil i Miami gràcies a la xarxa VPN de la que disposem.

Dels objectius que ens havíem marcat hem aconseguit tots, la cobertura a l'empresa és bona, i podrem millorar encara més la cobertura comprant un parell de AP i movent un, he aconseguit configurar i posar en funcionament una eina que útil que dóna informació en temps real i que podrà ser amplada i millorada en un futur si fos necessari.

Hem proposat millores algunes ja les hem pogut demostrar i implementar com seria la vigilància de la xarxa de visites i d'altres estan pendents del pressupost i saber si compensa per part del cap d'informàtica implementar-les.

En l'àmbit personal puc afirmar que he adquirit uns coneixements sobre el protocol SNMP que no tenia , també a instal·lar configurar tant Nagios com el plugin PNP4Nagios, i coneixements sobre com funcionen les xarxes Wi-Fi i els problemes que poden generar.

Després de fer aquesta valoració podrem dir que ha sigut un bon projecte i s'ha complert tots els objectius que ens vam marcar i hem pogut donar valor extra a l'empresa com seria fer plànols actualitzats amb la ubicació dels APs i un sistema útil i que servirà durant molt de temps.

10.-Annexos

10.1.-Plànols de l'empresa amb la Ubicació dels APs

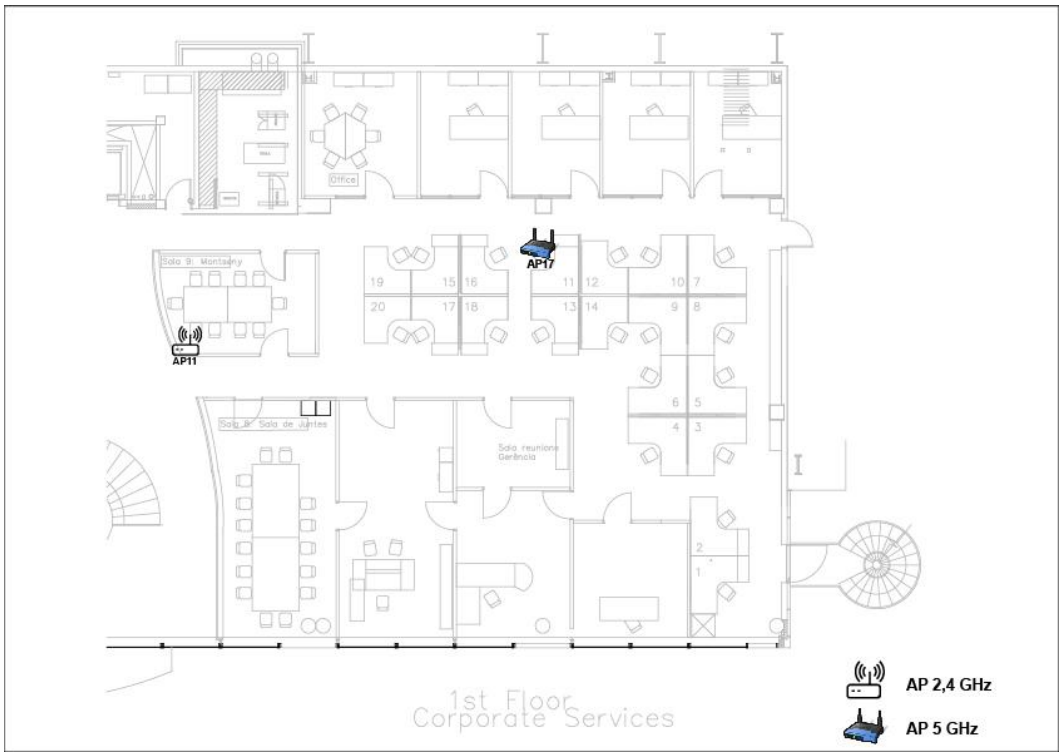


Figura 57 plànol de BU corporate services

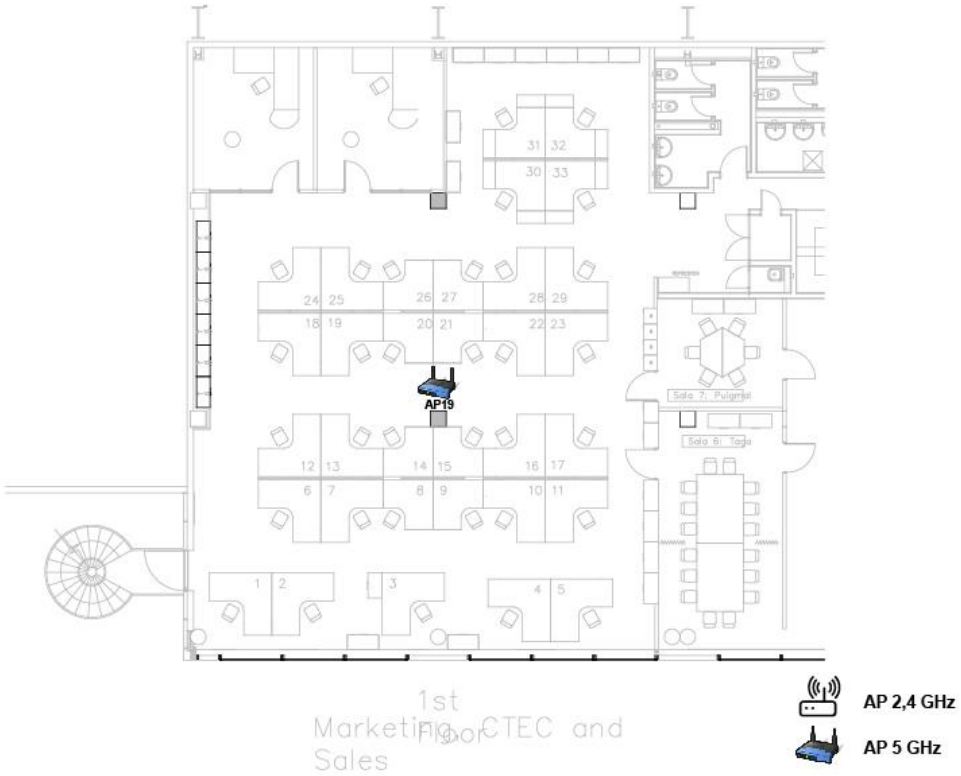


Figura 58 plànol de la BU Sales

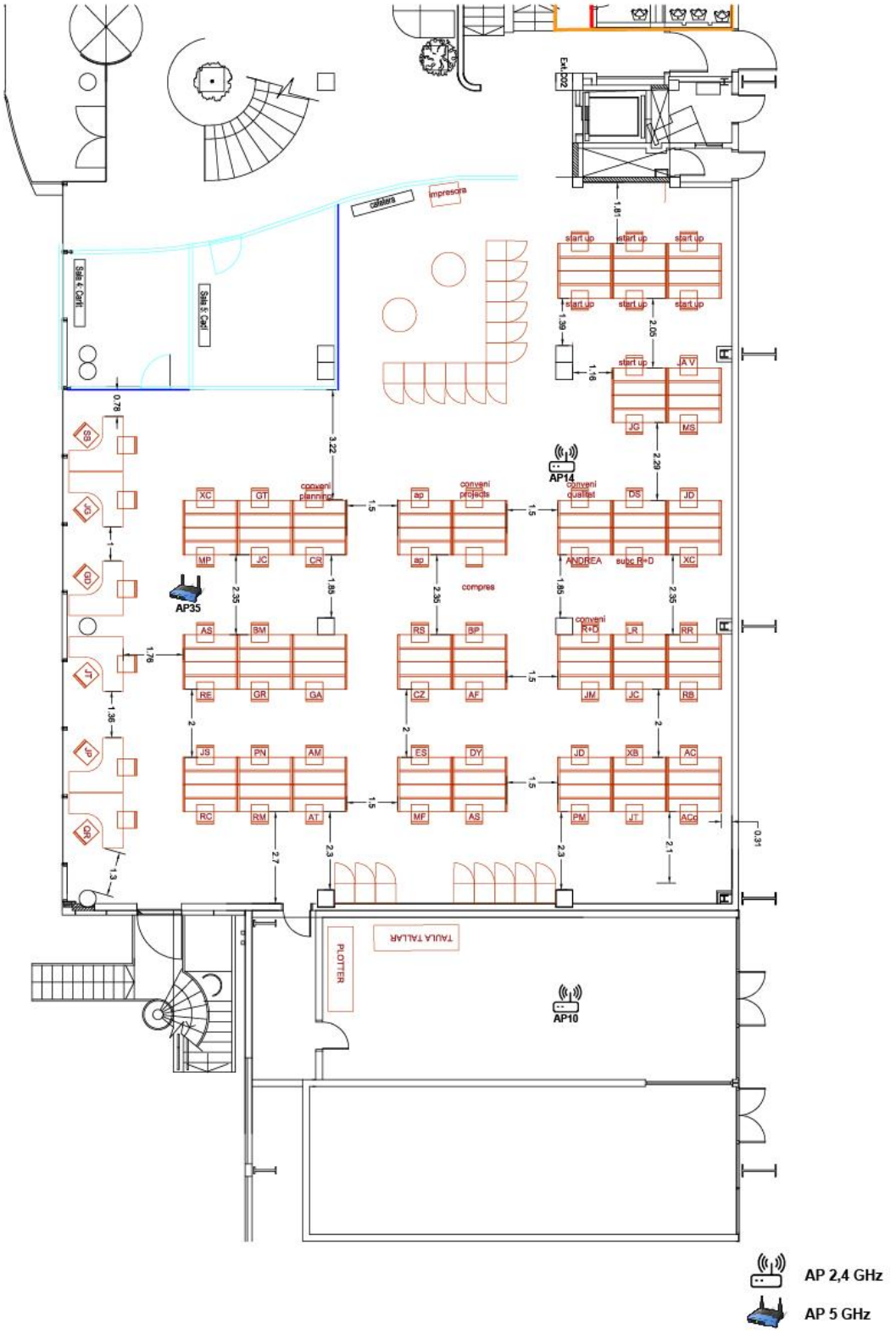


Figura 59 plànol BU flexo

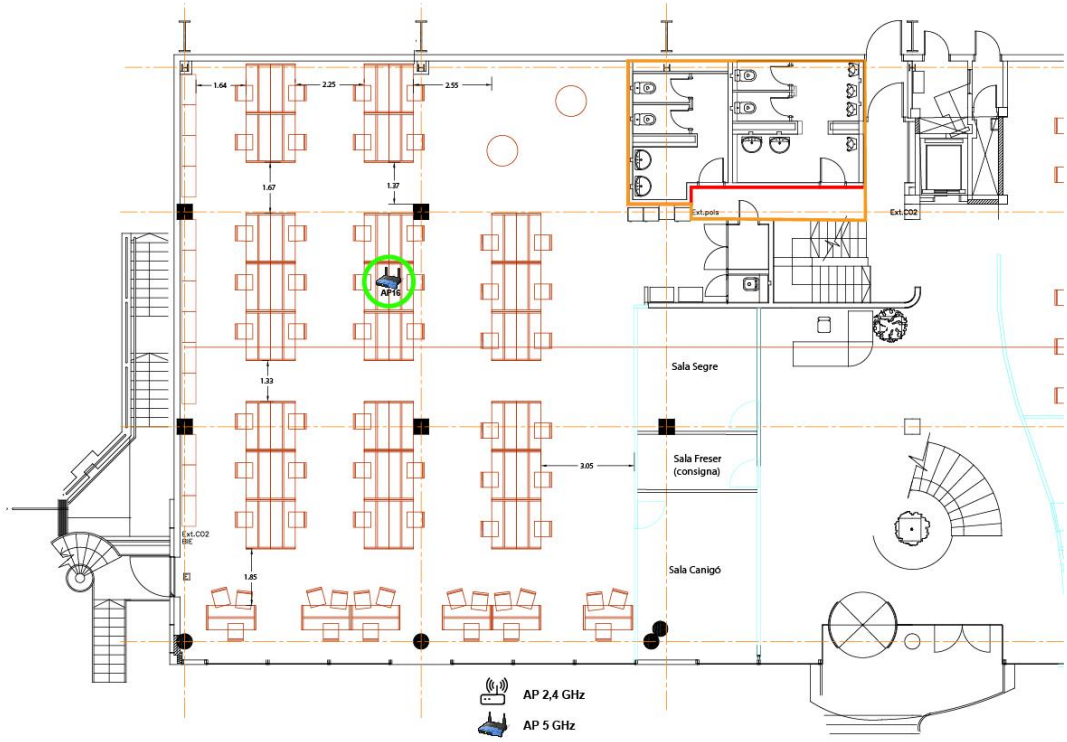


Figura 60 plànol BU offset

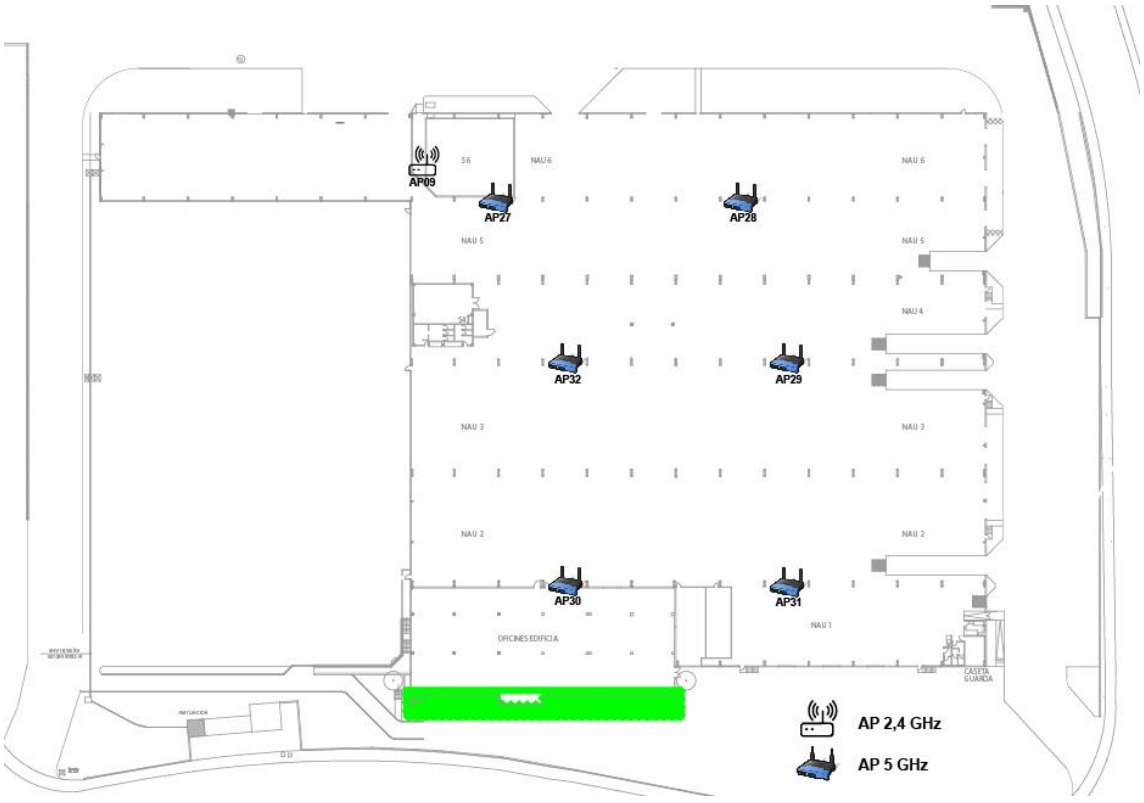


Figura 61 plànol planta nau A

Figura 62plànol planta nau B

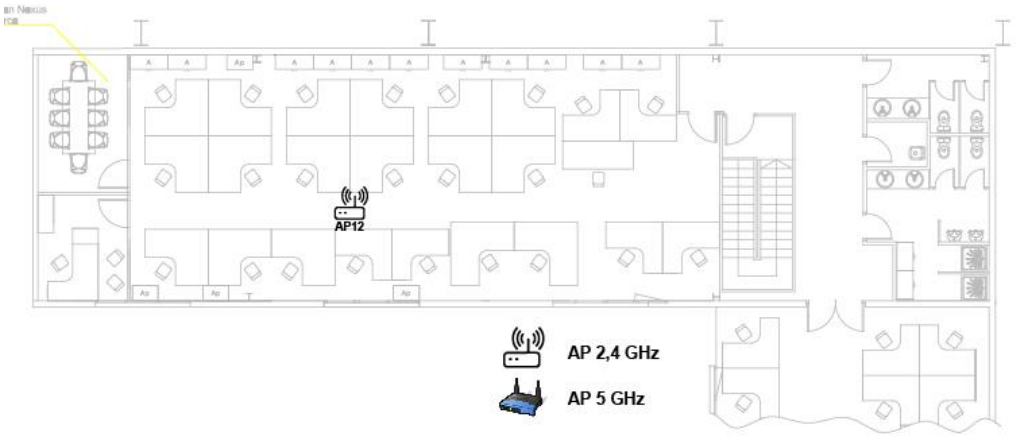


Figura 63 plànol BU Lamination

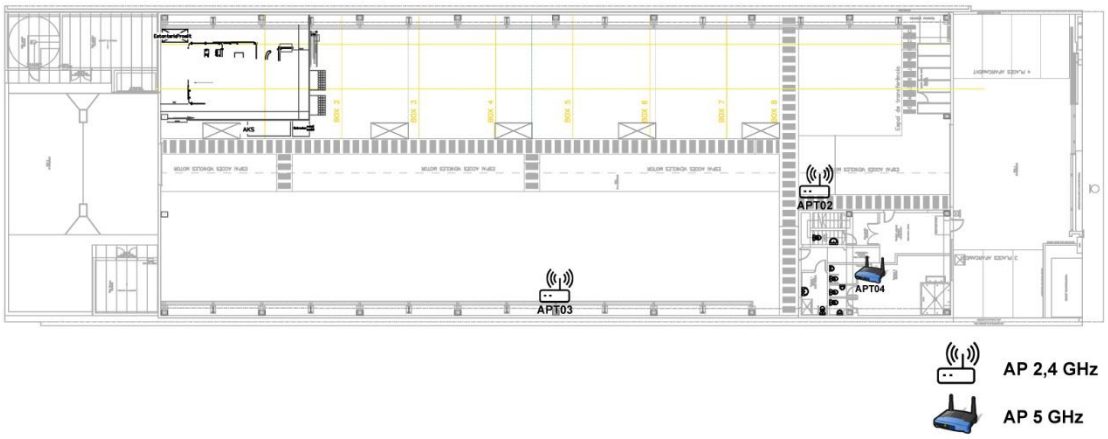


Figura 64 planol Mas Joals

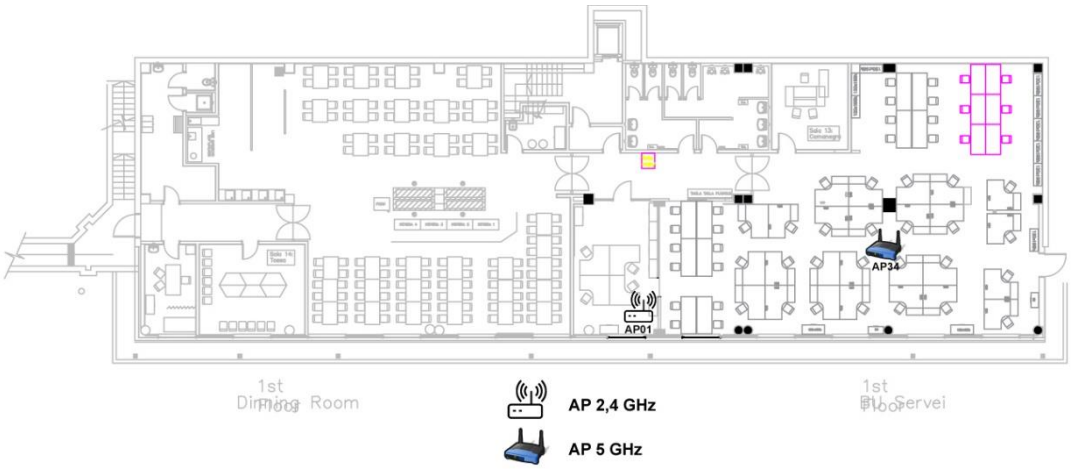


Figura 65 BU service i menjador

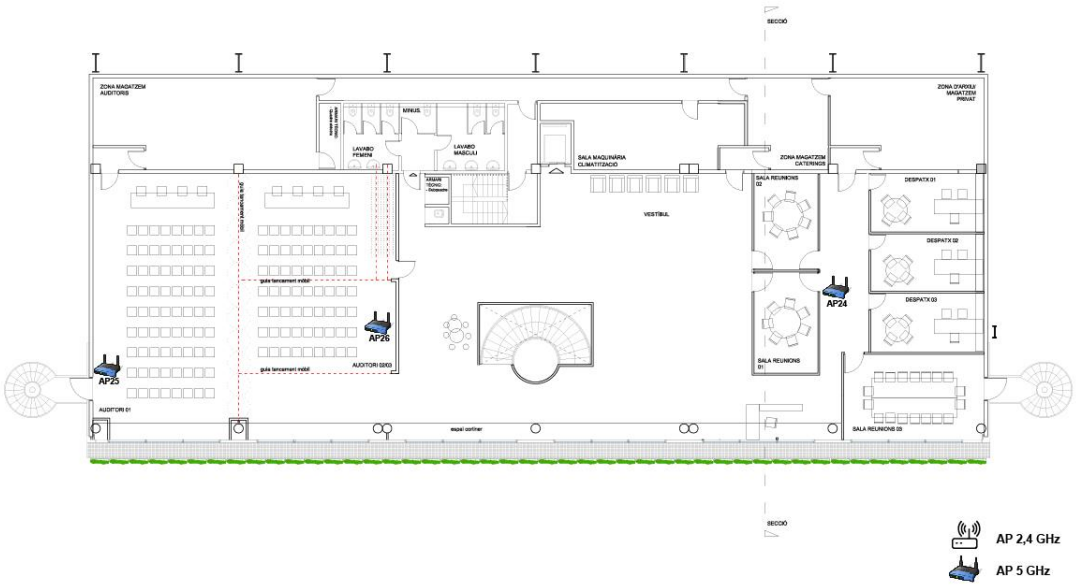


Figura 66 plànol planta 3 direcció i auditori

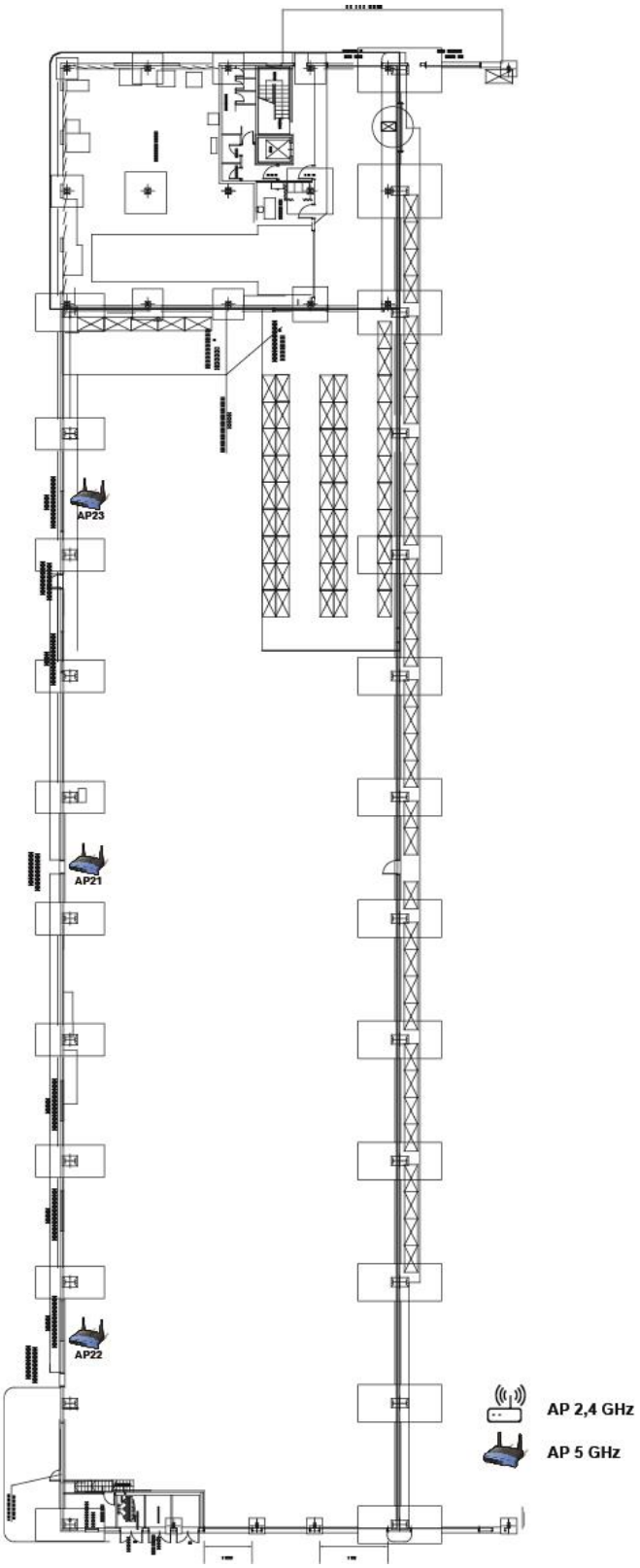


Figura 67 plànol planta nau Offset

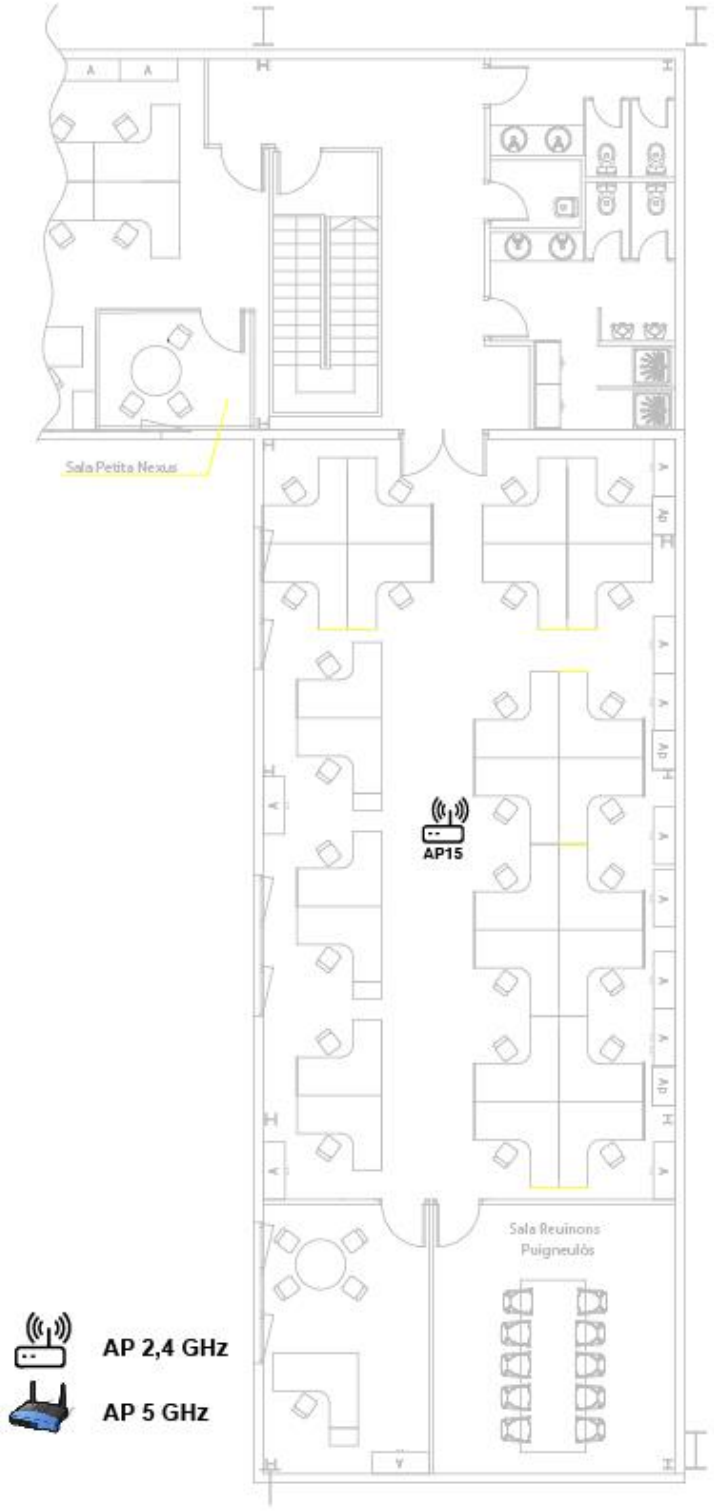


Figura 68 plànol BU procurement

10.2.-plànols de l'empresa amb mapa de cobertura i ubicació dels AP

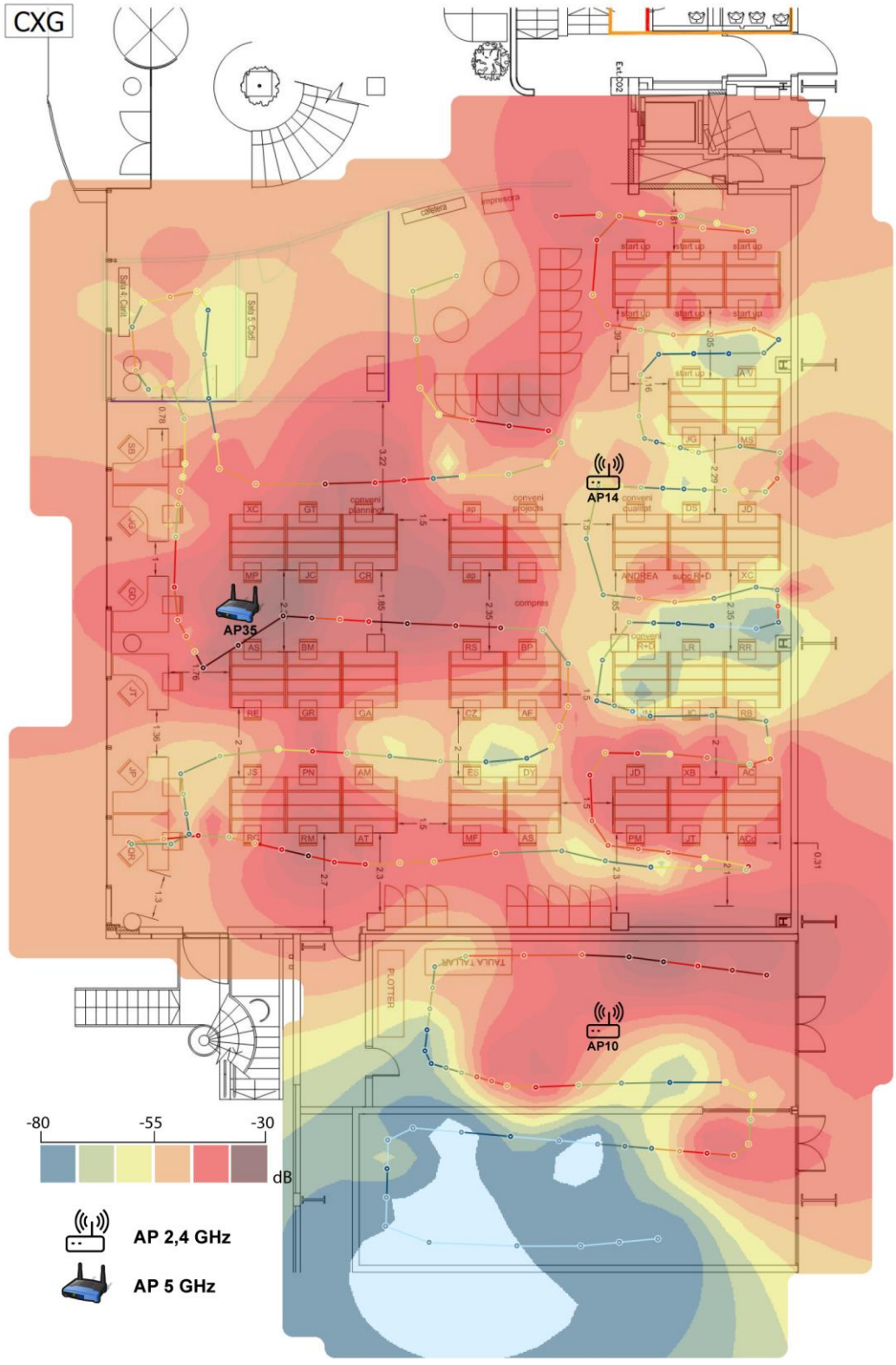


Figura 69 Mapa de cobertura BU offset

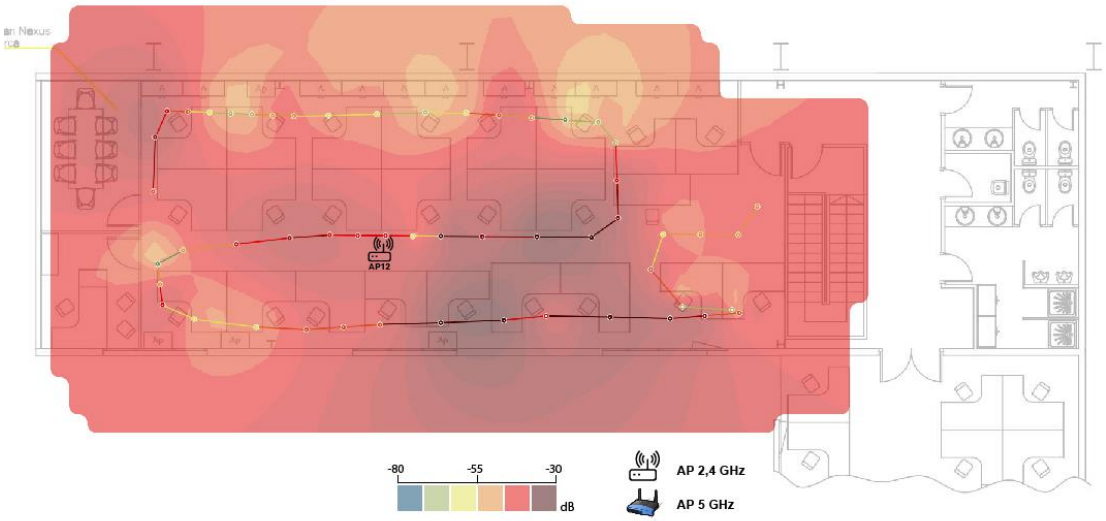


Figura 70 Mapa cobertura BU Lamination

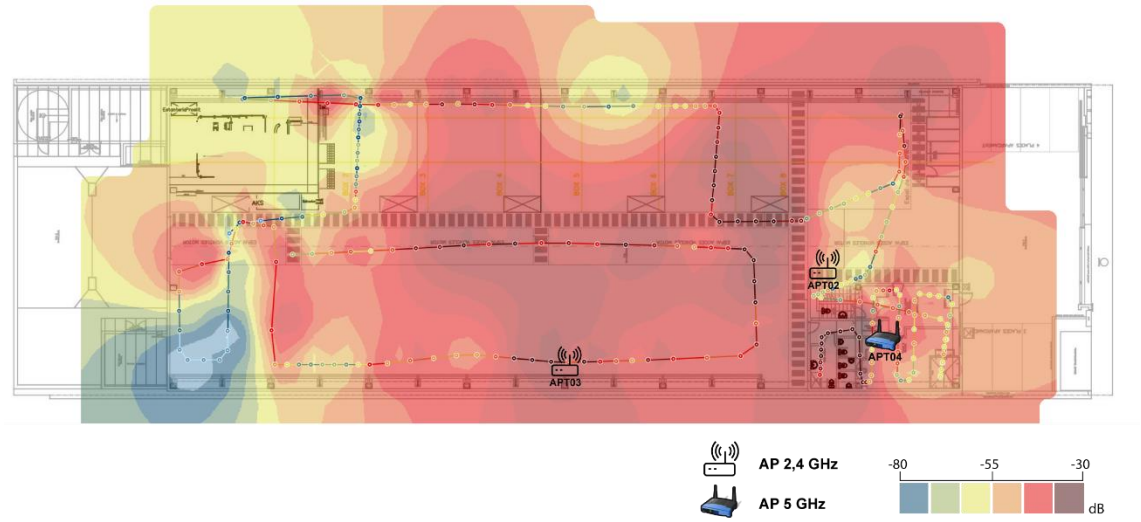


Figura 71 Mapa cobertura Mas Joals

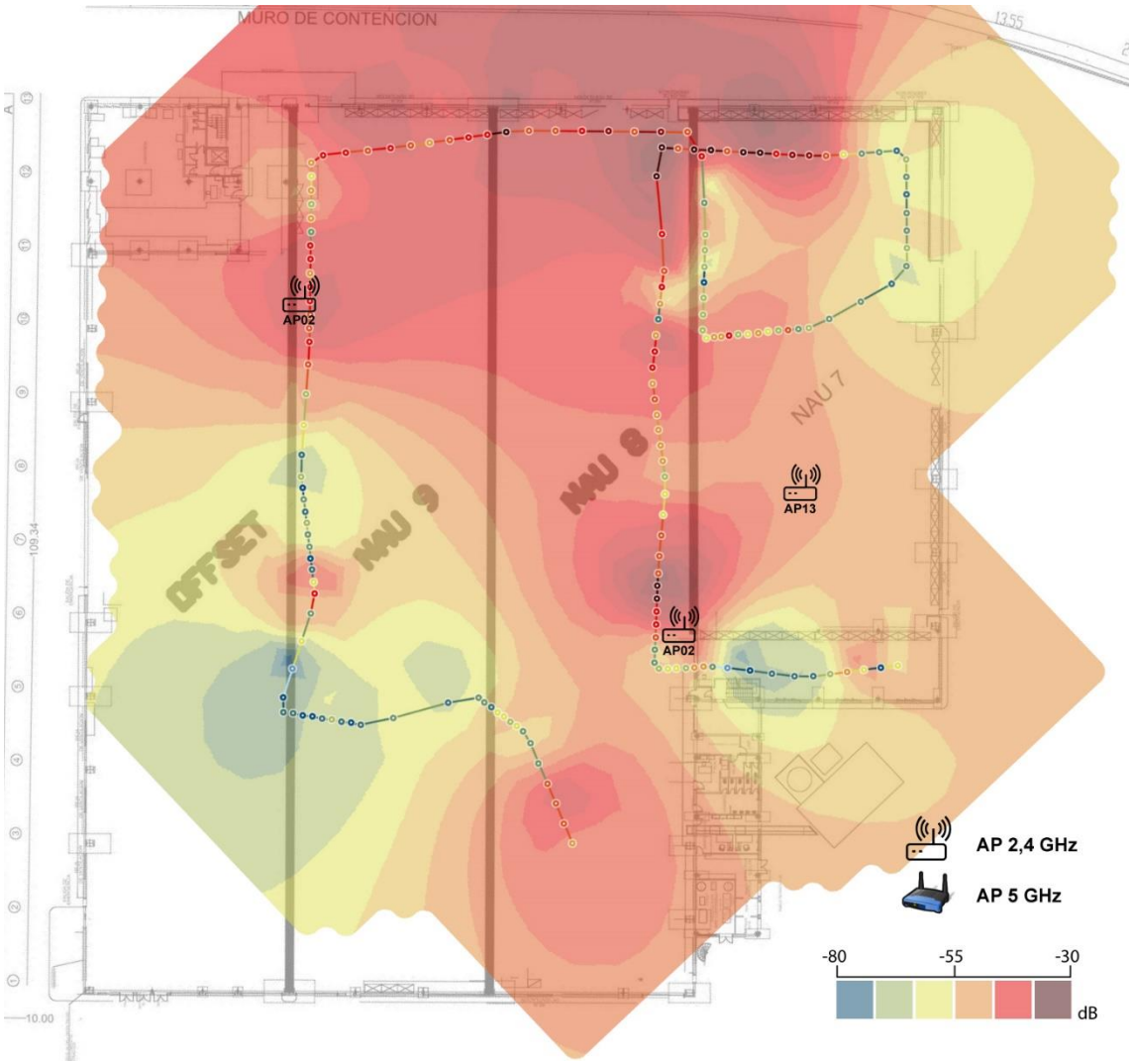


Figura 72 Mapa cobertura planta nau B

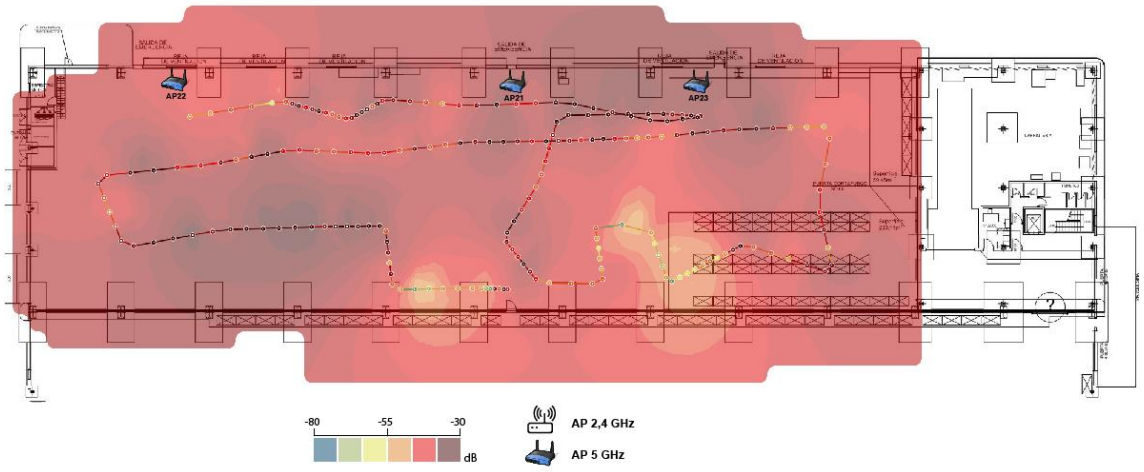


Figura 73 Mapa cobertura planta nau Offset

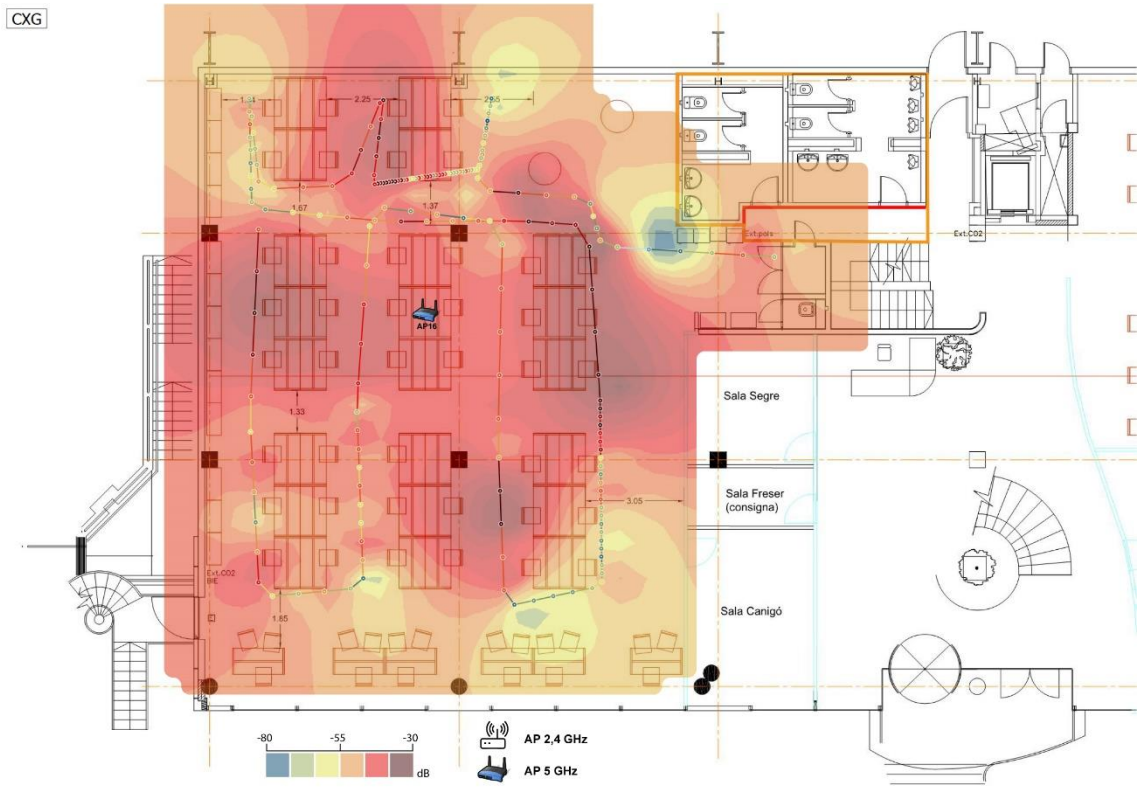


Figura 74 Mapa cobertura Bu Flexo

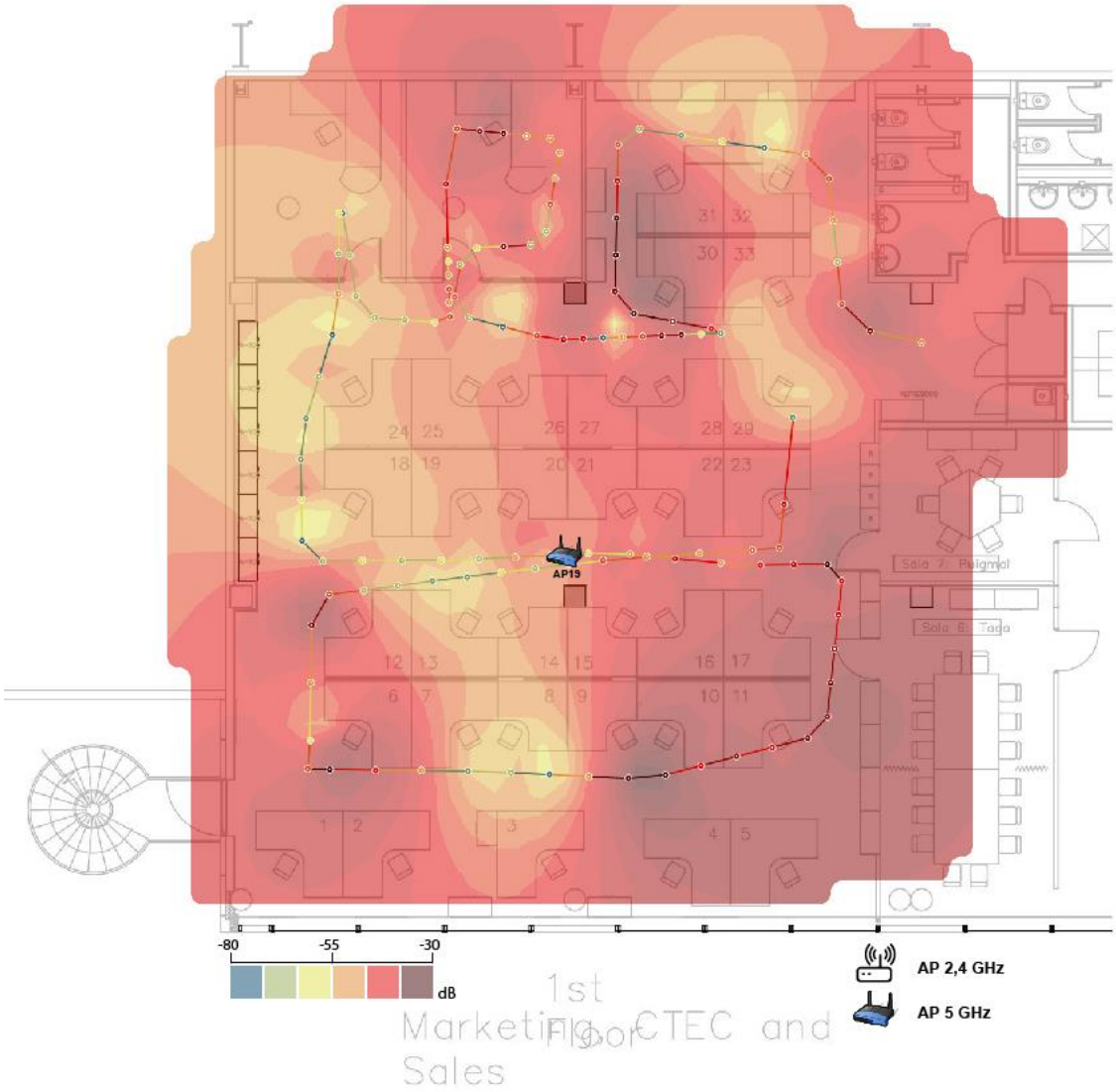


Figura 75 Mapa cobertura BU Sales

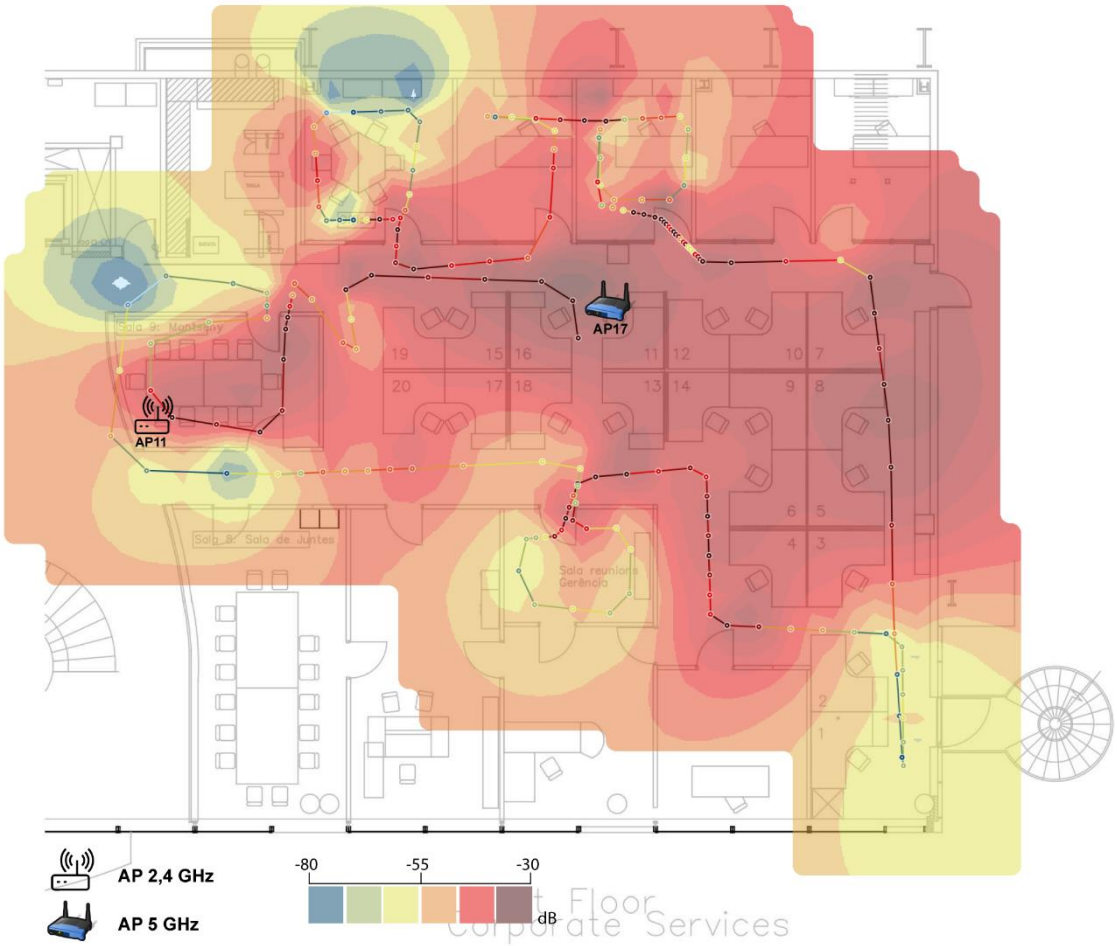


Figura 76 Mapa cobertura BU Corporate services

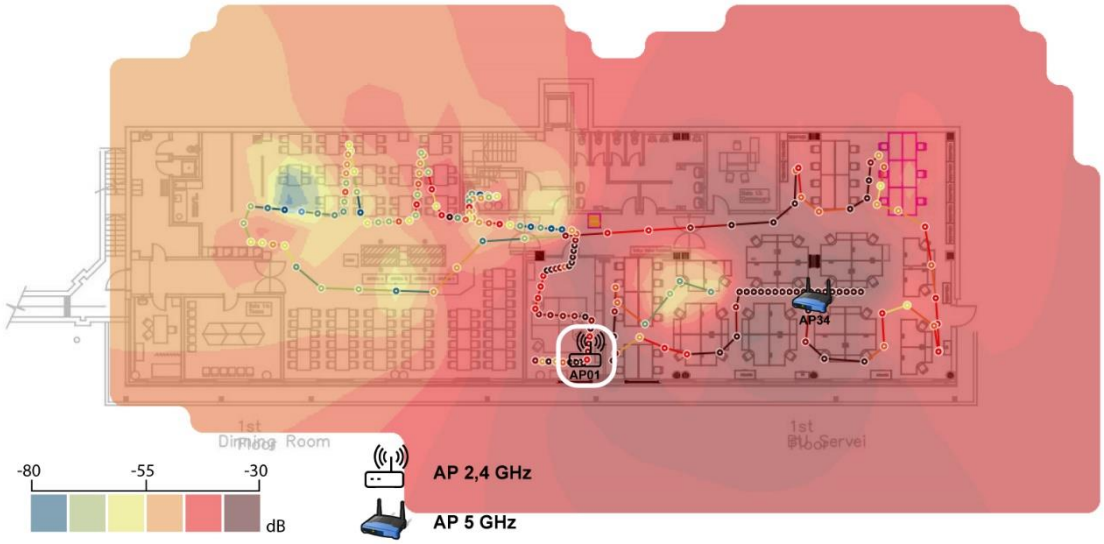


Figura 77 Mapa cobertura BU Service i menjador

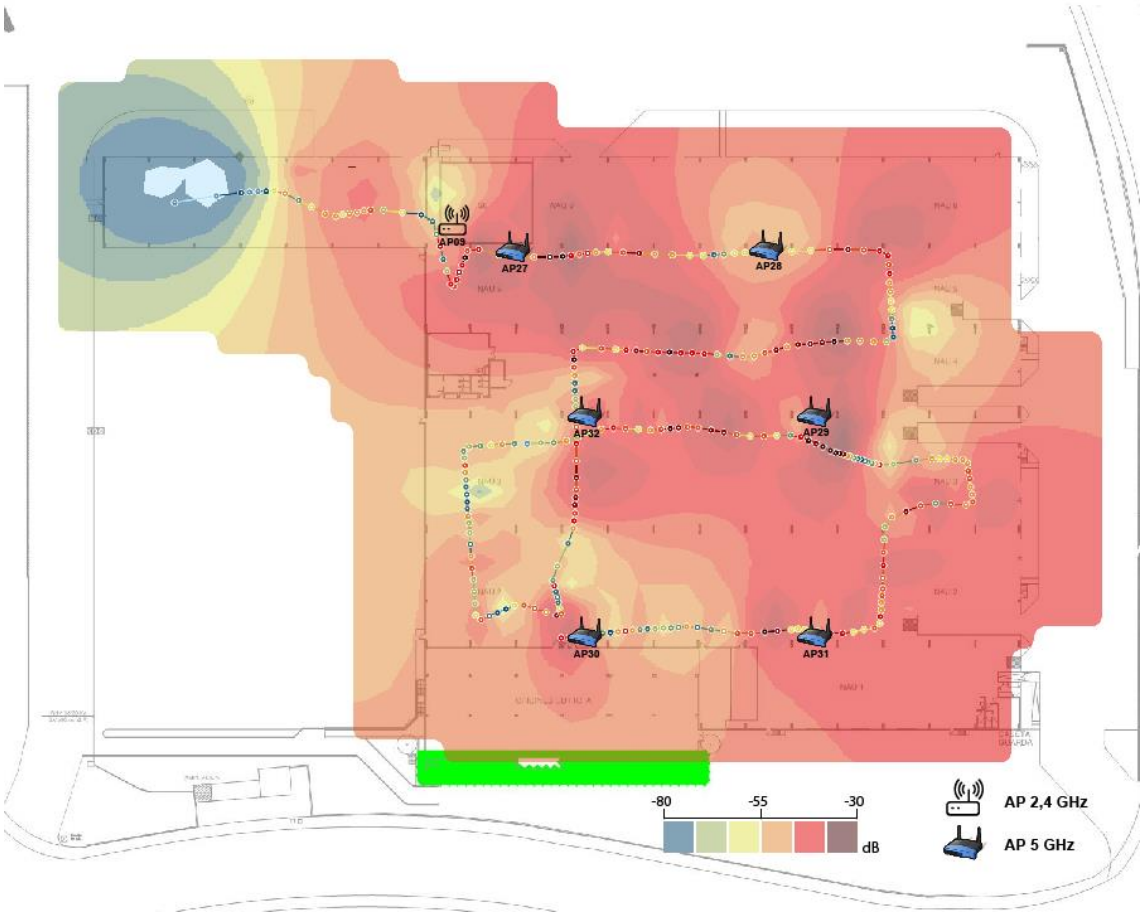


Figura 78 Mapa cobertura planta Nau A

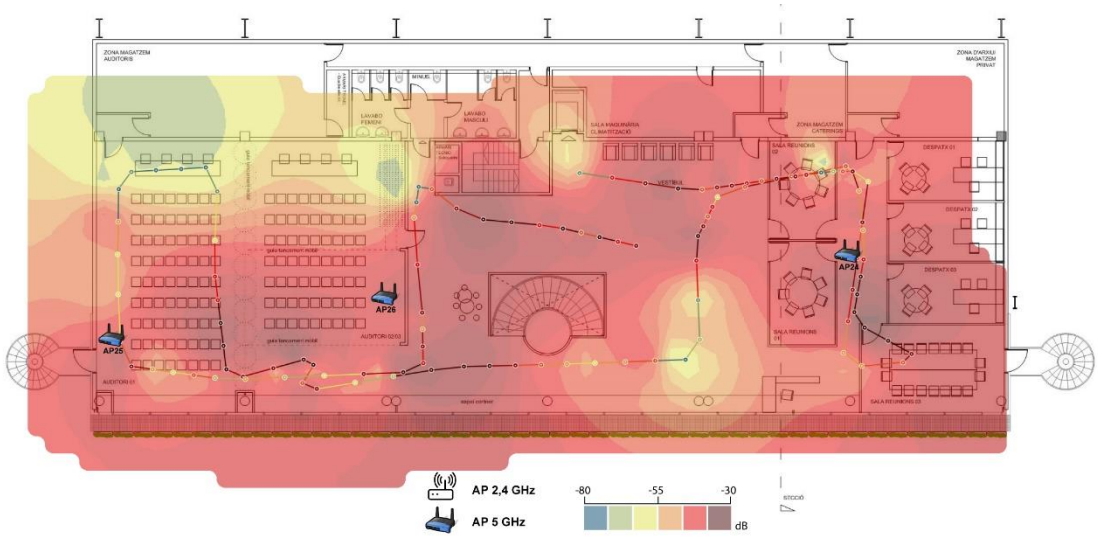


Figura 79 Mapa cobertura direció i auditori

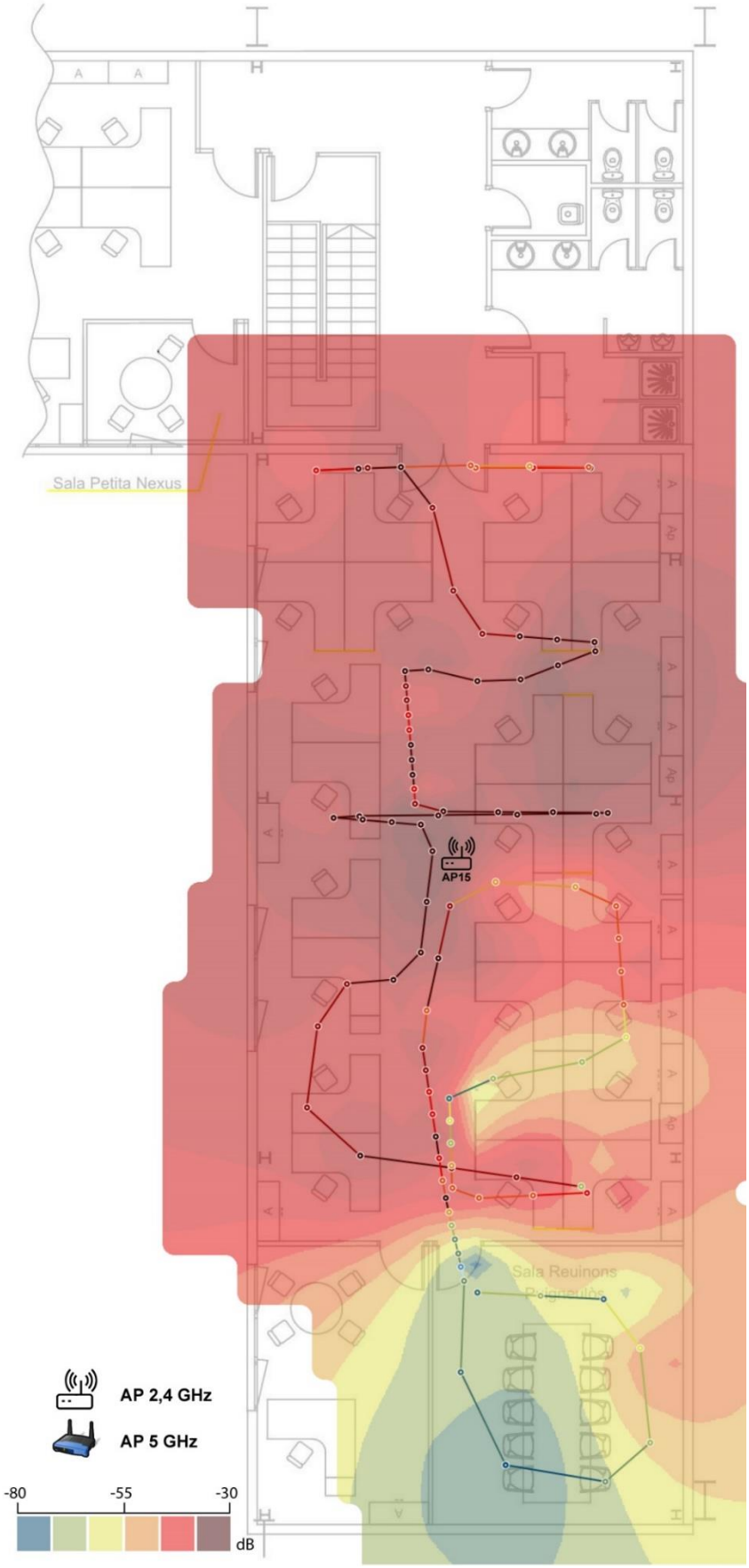


Figura 80 Mapa cobertura BU Procurement

10.3.-gràfiques de la recol·lecció de dades

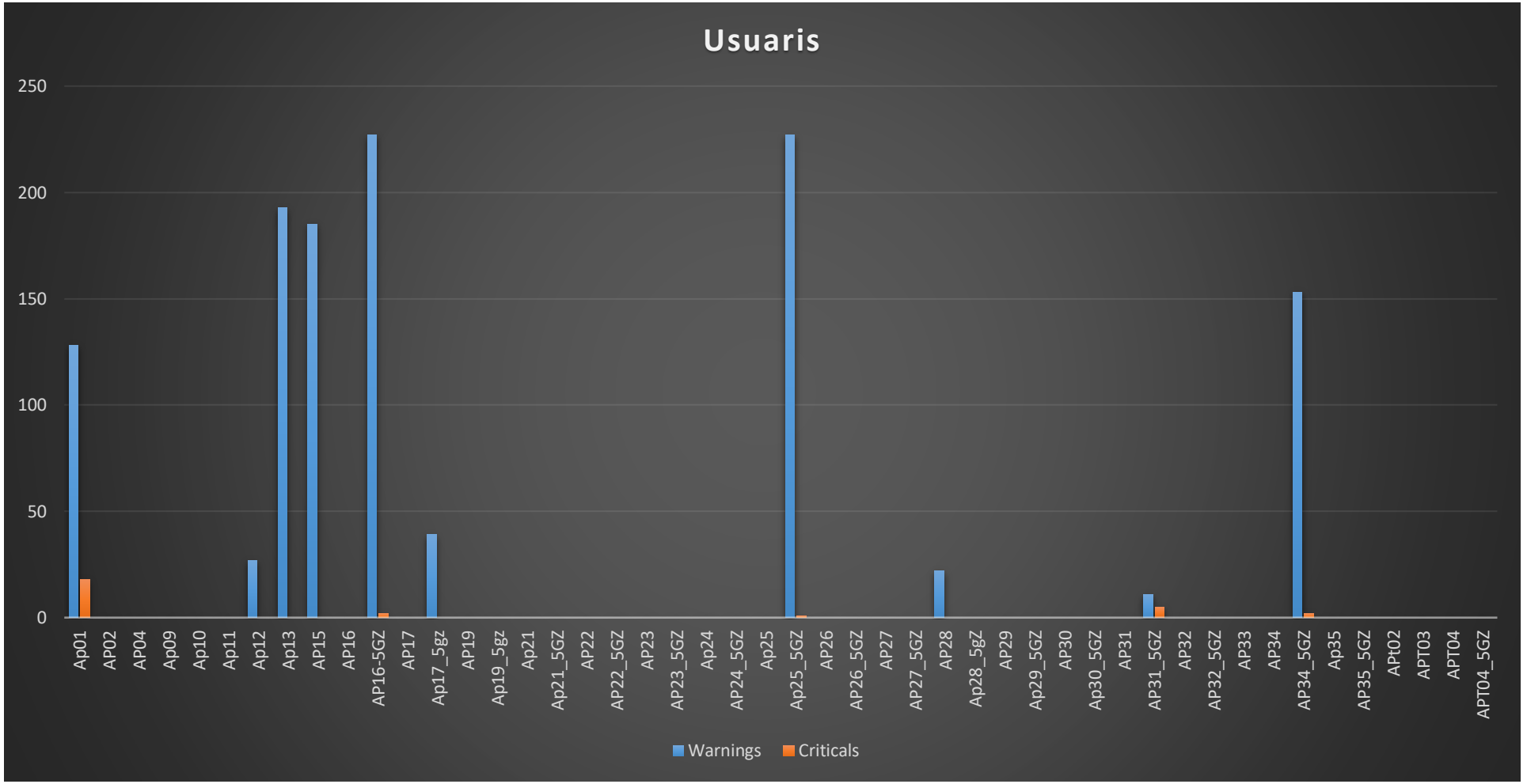


Figura 81 Gràfica amb el numero d'avisos de usuaris connectats a cada AP

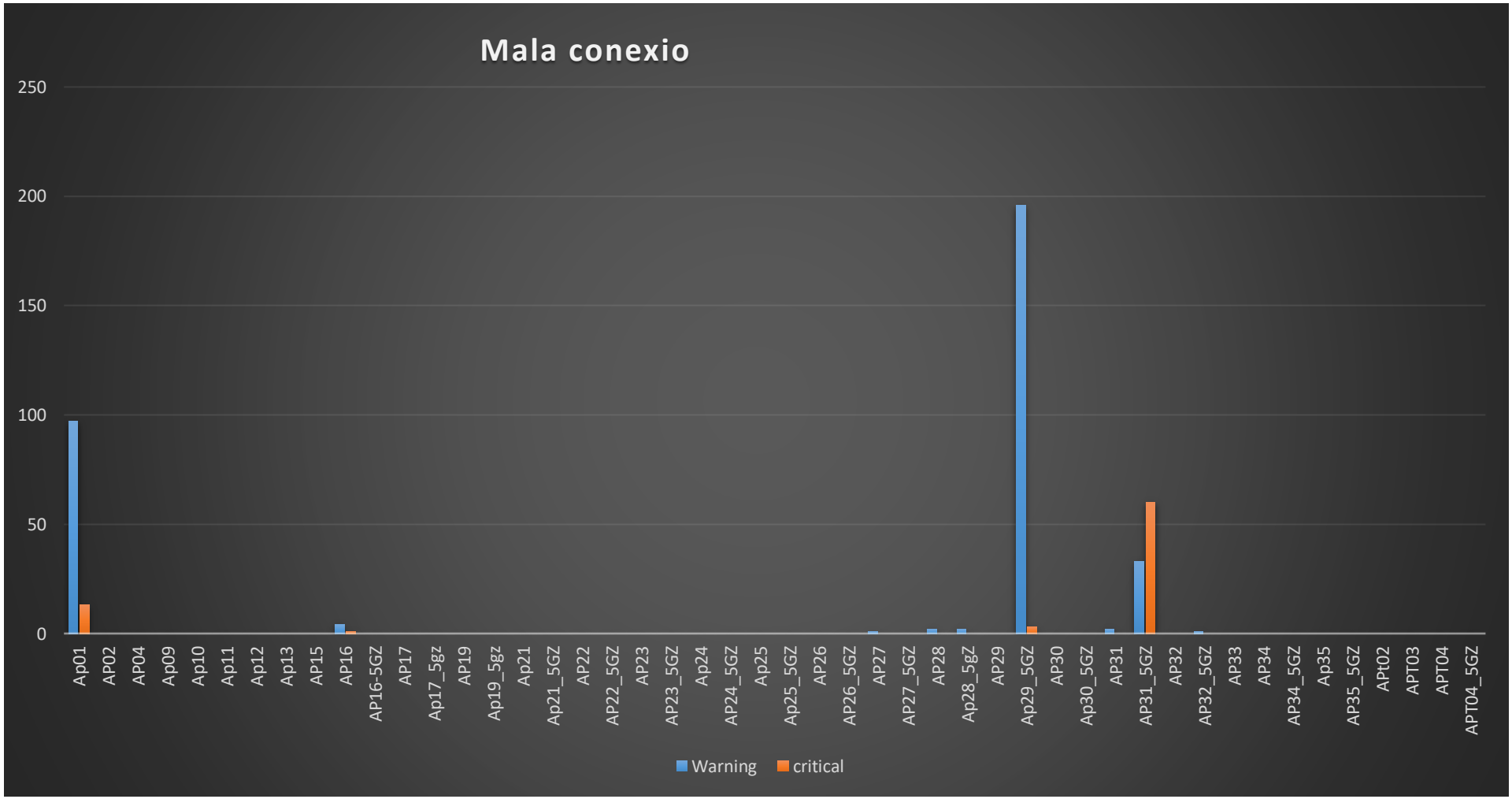


Figura 82 Gràfica amb el numero de dispositius amb mala senyal connectats a un AP

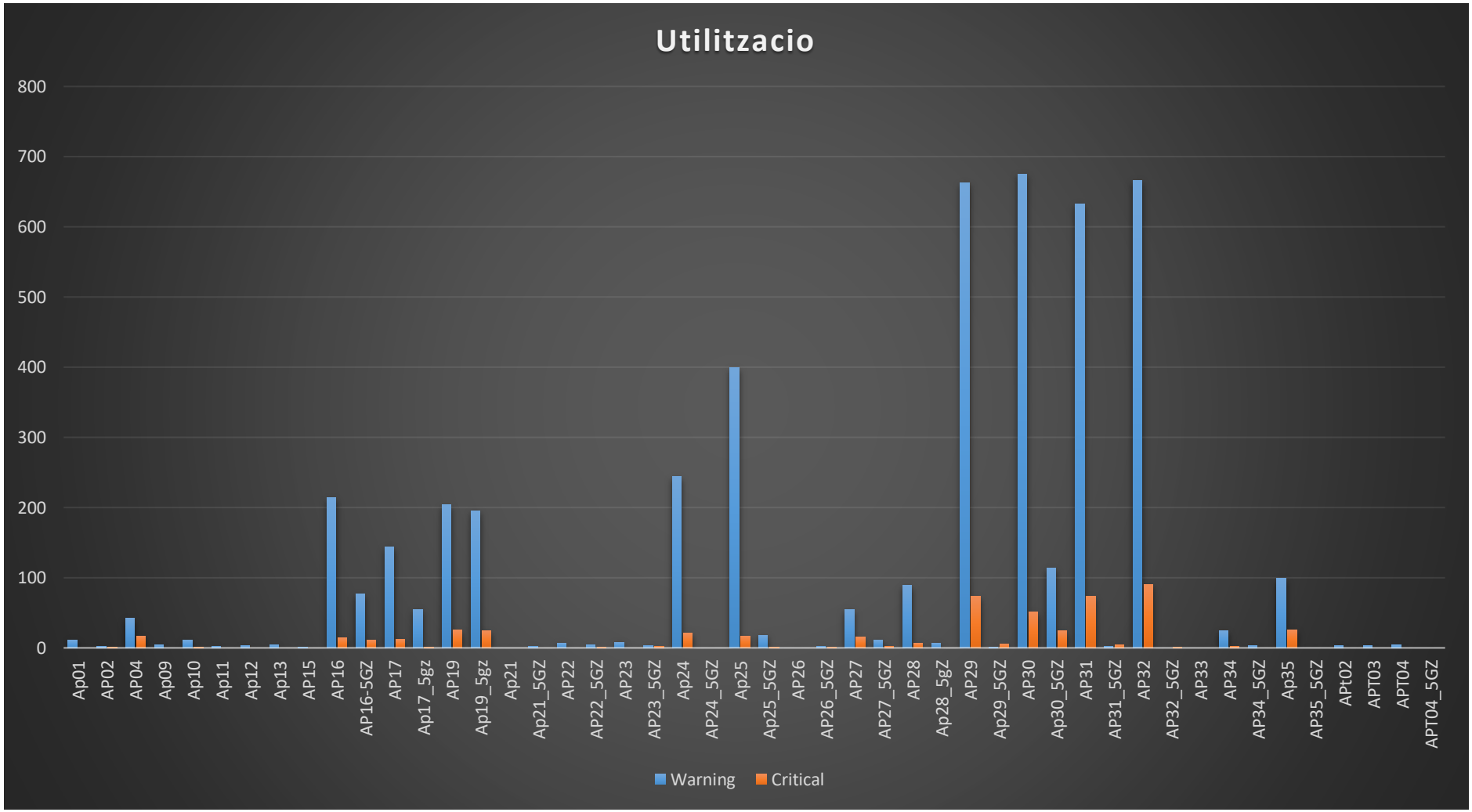


Figura 83 Gràfica amb el numero d'avisos del percentatge d'utilització de el canal per el que emet un AP

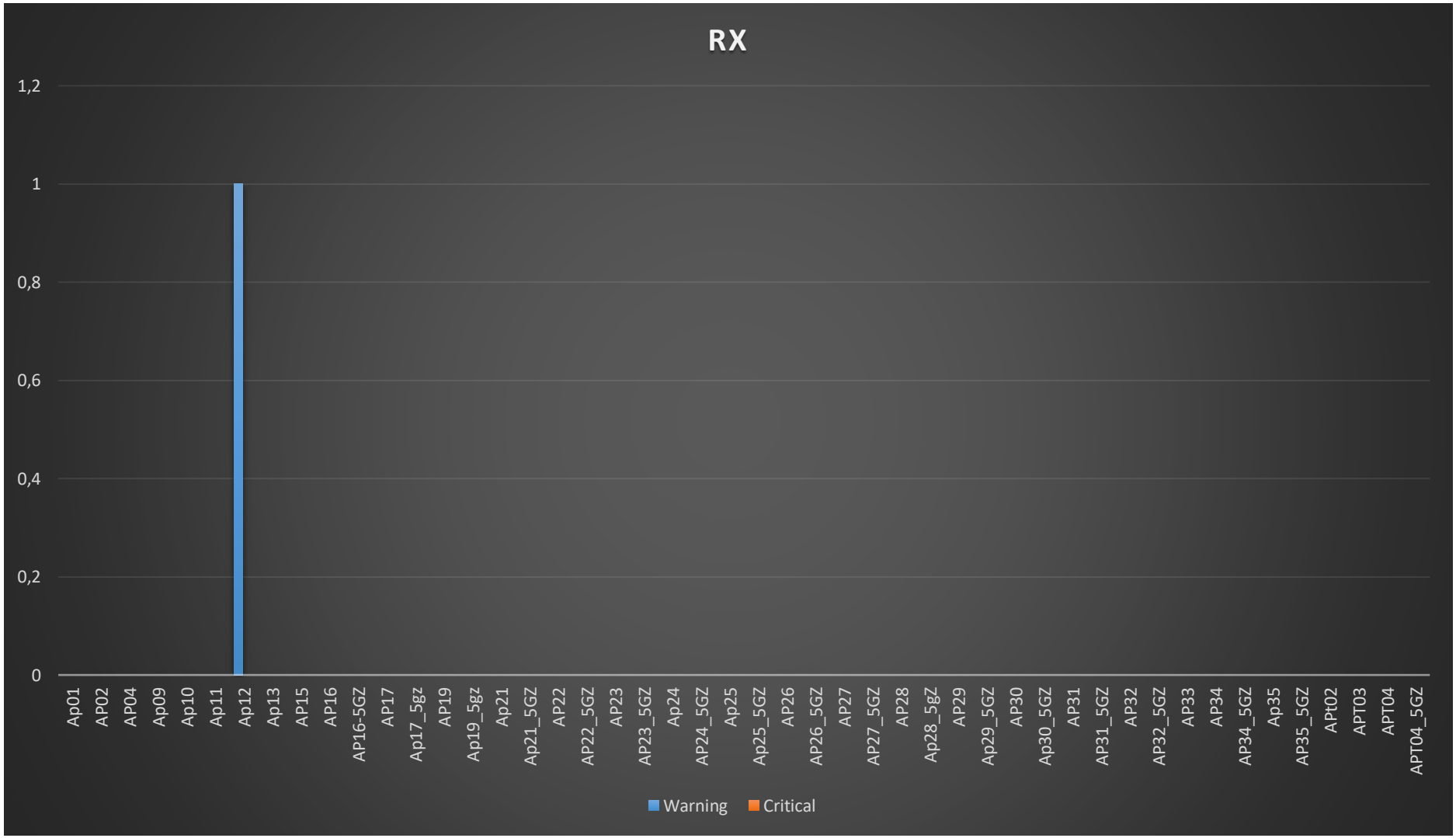


Figura 84 Gràfica amb el numero d'avisos del percentatge d'utilització de la CPU a l'hora de processar els paquets que rep

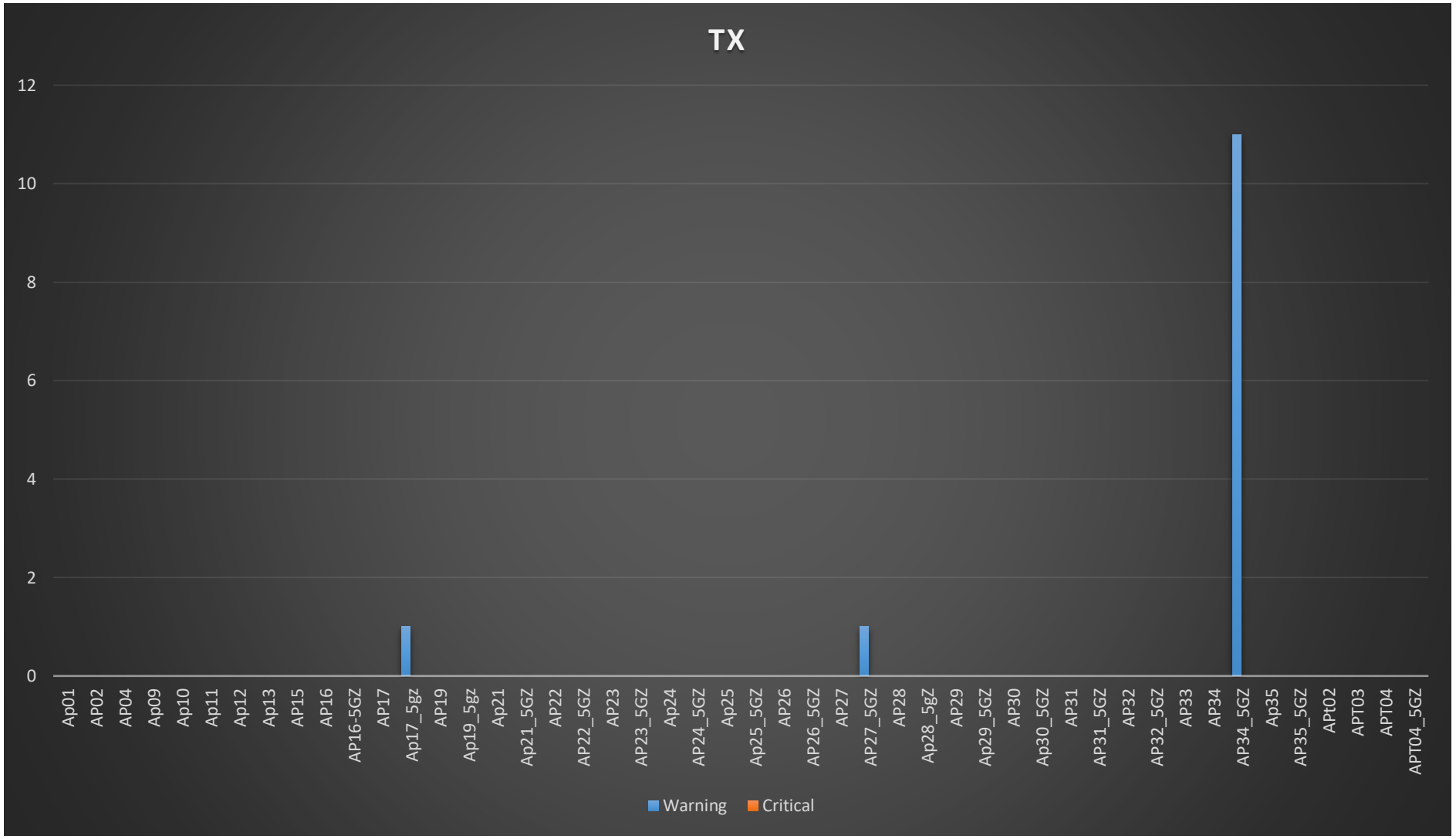


Figura 85 Gràfica amb el numero d'avisos del percentatge d'utilització de la CPU a l'hora de processar els paquets que envia

10.4.-Gràfiques de la recol·lecció de dades del dia sense la xarxa de visites

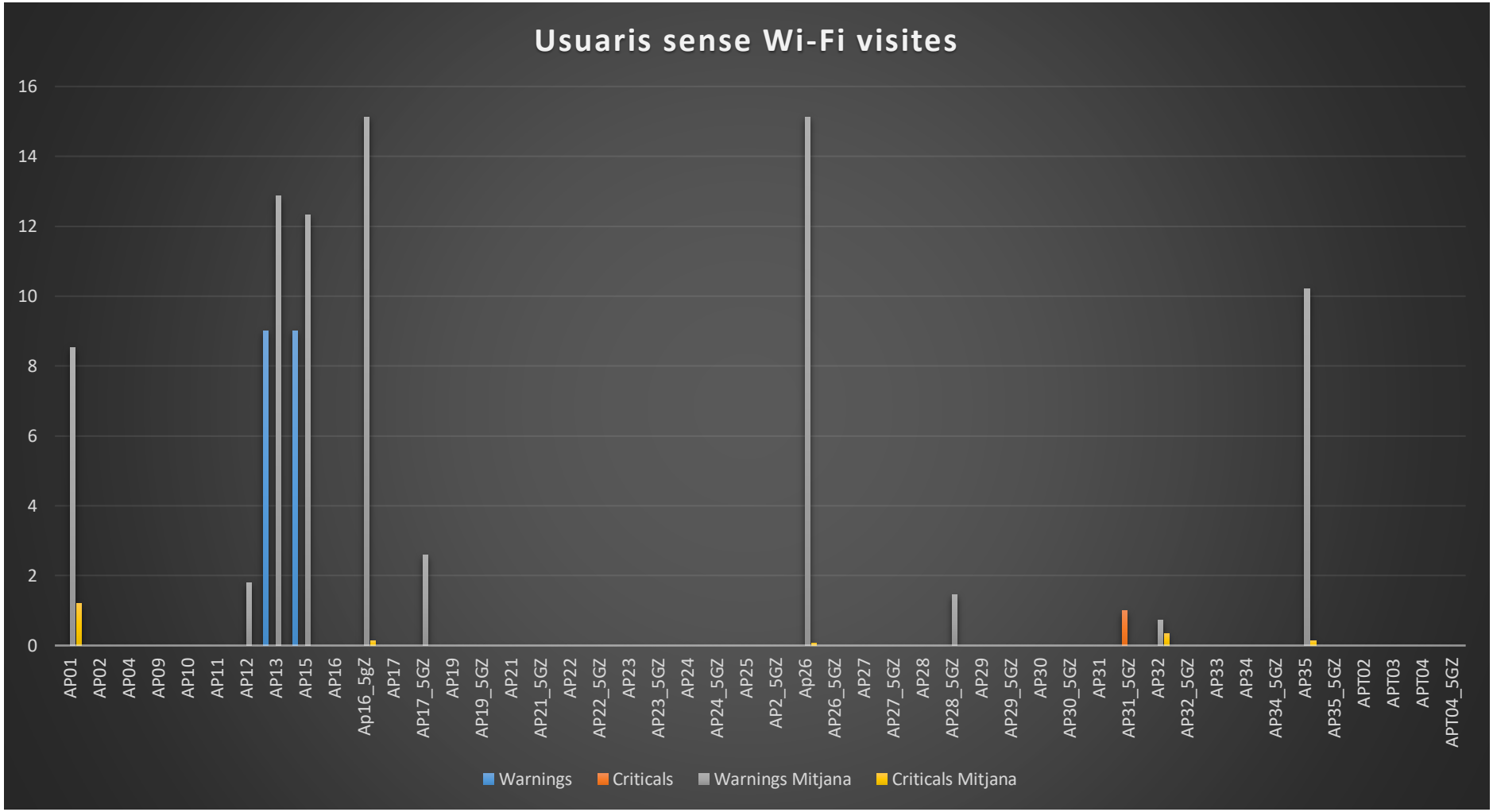


Figura 86 Gràfica amb el numero d'avisos de usuaris connectats a cada AP

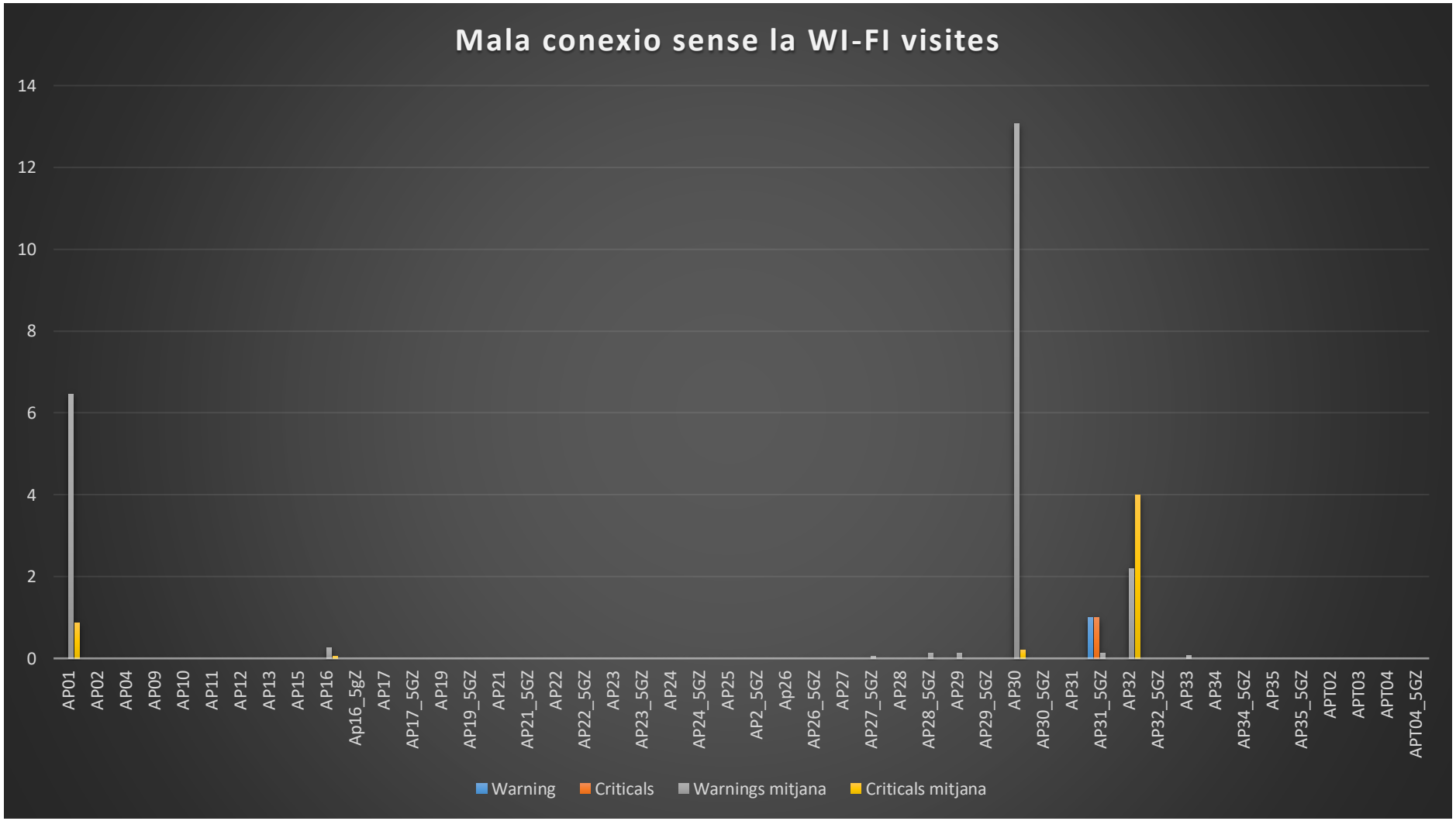


Figura 87 Gràfica amb el numero de dispositius amb mala senyal connectats a un AP

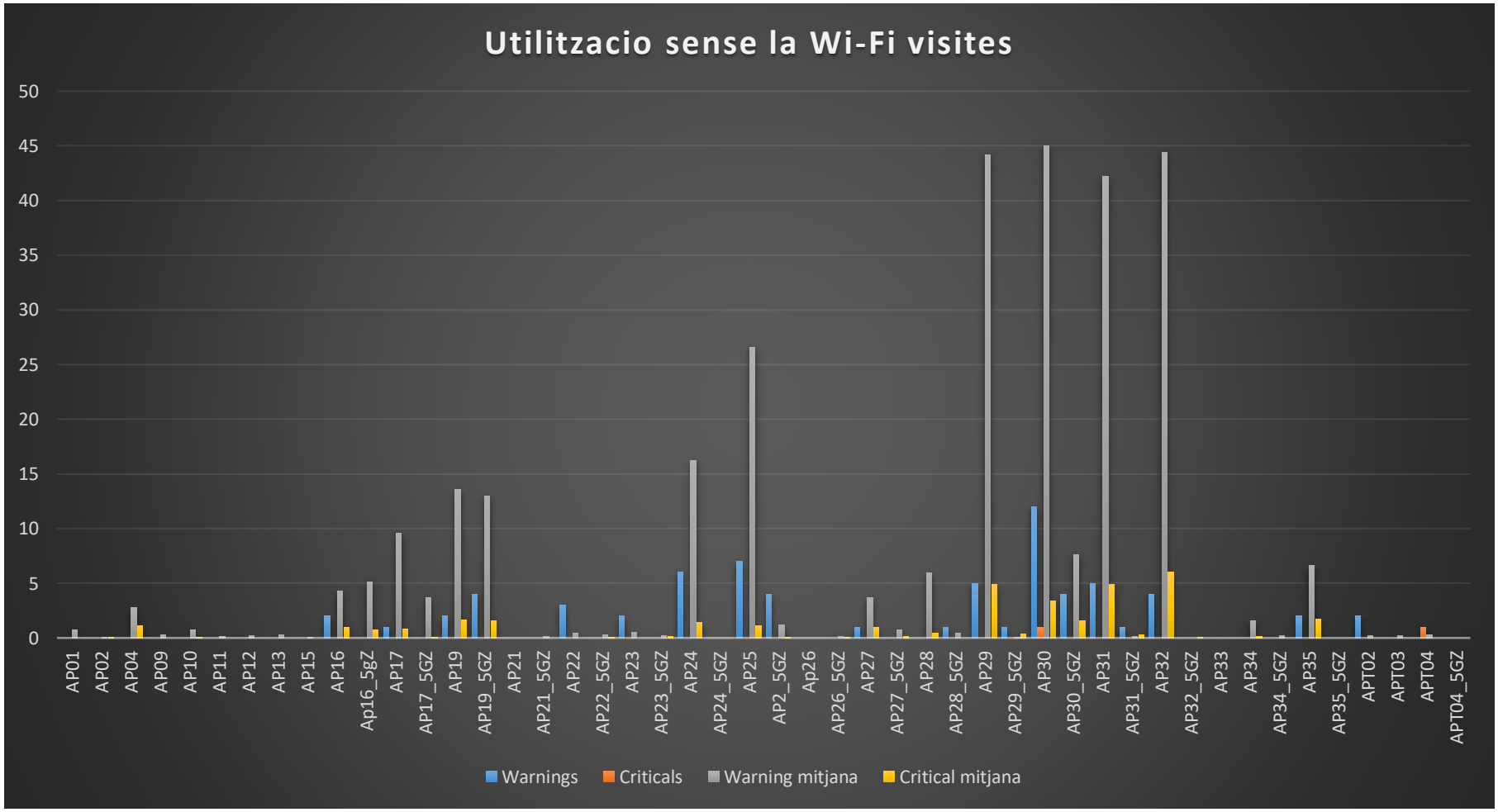


Figura 88 Figura 83 Gràfica amb el numero d'avisos del percentatge d'utilització de el canal per el que emet un AP

11.-Bibliografia

1] **Standard 802.11** https://ieeexplore.ieee.org/browse/standards/get-program/page/series?id=68

2]**Wi-Fi** https://en.wikipedia.org/wiki/Wi-Fi

3] **Banda Wi-Fi** https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/channels-frequencies-bands-bandwidth.php

4] **Diferencia entre 2,4GHz i 5GHz** https://techviral.net/difference-between-2-4-ghz-and-5-ghz-wi-fi/

5] **Controladora Wireless** http://www.excitingip.com/673/features-of-todays-centralized-wireless-wi-fi-networks/

6] **CAPWAP** https://tools.ietf.org/html/rfc5415 7]

7] **visiwave** https://www.visiwave.com/wifi/demo.php

8] **Nagios** https://www.nagios.org/

9 **graphite** http://graphiteapp.org/#integrations

10 **prometheus** https://prometheus.io

11] **Cacti** https://www.cacti.net**/**

12] RRDTool https://oss.oetiker.ch/rrdtool/

13] **Que és SNMP** https://pandorafms.com/blog/es/que-es-snmp/

14] **SNMP es simple** https://www.incibe-cert.es/blog/snmp-tan-simple-el-nombre-indica

15] **Com funciona SNMP , mibs i els oid** https://kb.paessler.com/en/topic/653-how-do-snmp-mibs-and-oids-work

16] **Funcionament dels SNMP** https://www.paessler.com/it-explained/snmp

17] **Tipus de verions SNMP** https://www.logicmonitor.com/blog/whats-with-the-different-snmp-versions-s1-v2c-v3/

18] **Instal·lar nagios** https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/quickstart.html

19] **Instal·lar PNP4NAGIOS** https://support.nagios.com/kb/article/nagios-core-performance-graphs-using-pnp4nagios-801.html#RHEL