UNIVERSITAT POLITÈCNICA DE VALÈNCIA

UNIVERSITAT POLITÈCNICA DE VALÈNCIA
CAMPUS D'ALCOI

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Politécnica Superior de Alcoy

Proyecto de Red y Sistemas para PYME

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Blasco Almerich, German

Tutor/a: Llinares Llopis, Raúl

CURSO ACADÉMICO: 2023/2024

El present TFG (Treball fi de grau) se centrarà en l'anàlisi i disseny d'un Projecte de Xarxa i Sistemes per a una PIME (Petita i mitjana empresa). En la primera fase, es durà a terme l'anàlisi de la situació actual i el disseny d'una solució. D'altra banda, en la segona fase, es realitzarà el desplegament de la solució proposada en la PIME en qüestió.

La solució a desenvolupar partirà d'una auditoria i anàlisi en una PIME real, localitzant els punts febles i de fallada únics que poden portar a situacions de parada del negoci. A partir de la informació obtinguda, es desenvoluparà la solució des dels següents punts:

1) Xarxa: s'actualitzarà l'electrònica de la xarxa que siga necessari, aconseguint una gestió tant física com remota dels equips electrònics. Serà necessari proveir de nous equips com puga ser un encaminador, varis switchos configurables, APs (punts d'accés) compatibles amb tecnologia de xarxes definides per software o SDN (Software Defined Networking) i nou cablejat Ethernet. També s'augmentarà l'amplada de banda de la xarxa implementant protocols per a això com puga ser LACP (Link Aggregation Control Protocol).

2) Sistemes: s'abordarà la possible millora de l'equip servidor, depenent de les necessitats del client i la criticitat de l'empresa. Les tecnologies que es tindran en compte seran: redundància hardware a tots els nivells (discos, fonts d'alimentació), virtualització, sistemes de còpies de seguretat (físics o en el núvol)

3) Accés Remot: s'implementarà accés remot al servidor, el qual permetrà als empleats accedir als programes i dades de l'empresa sense necessitat de acudir físicament a esta. Este punt s'aconseguirà mitjançant l'ús de protocols coneguts de VPN (SSTP, L2TP/IPSEC, PPTP...).

Paraules clau: Xarxa, Sistemes, VPN, Backups, PIME

El presente TFG (Trabajo Fin de Grado) se centrará en el análisis y diseño de un Proyecto de Red y Sistemas para una PYME (Pequeña Y Mediana Empresa). En la primera fase, se llevará a cabo el análisis de la situación actual y el diseño de una solución. Por otra parte, en la segunda fase, se realizará el despliegue de la solución propuesta en la PYME en cuestión.

La solución a desarrollar partirá de una auditoría y análisis en una PYME real, localizando los puntos débiles y de fallo únicos que pueden llevar a situaciones de parada del negocio. A partir de la información obtenida, se desarrollará la solución desde los siguientes puntos:

1) Red: se actualizará la electrónica de la red que sea necesario, consiguiendo una gestión tanto física como remota de los equipos electrónicos. Será necesario abastecer de nuevos equipos como pueda ser un enrutador, varios switches configurables, APs (puntos de acceso) compatibles con tecnología de redes definidas por software o SDN (Software Defined Networking) y nuevo cableado Ethernet. También se aumentará el ancho de banda de la red implementando protocolos para ello como pueda ser LACP (Link Aggregation Control Protocol).

2) Sistemas: se abordará la posible mejora del equipo servidor, dependiendo de las necesidades del cliente y la criticidad de la empresa. Las tecnologías que se tendrán en cuenta serán: redundancia hardware a todos los niveles (discos, fuentes de alimentación), virtualización, sistemas de copias de seguridad (físicos o en la nube)

3) Acceso Remoto: se implementará acceso remoto a el servidor, el cual permitirá a los empleados acceder a los programas y datos de la empresa sin necesidad de acudir físicamente a la misma. Este punto se conseguirá mediante el uso de protocolos conocidos de VPN (SSTP, L2TP/IPSEC, PPTP...).

Palabras clave: Red, Sistemas, VPN, Backups, PYME

The present TFG (Final Degree Project) will focus on the analysis and design of a Network and Systems Project for an SME (Small and Medium-sized Enterprise). In the first phase, the analysis of the current situation and the design of a solution will be carried out. In the second phase, the deployment of the proposed solution in the SME in question will be conducted.

The solution to be developed will start with an audit and analysis of a real SME, identifying unique weaknesses and points of failure that could lead to business downtime. Based on the information obtained, the solution will be developed from the following points:

1) Network: The necessary network electronics will be updated, achieving both physical and remote management of the electronic equipment. It will be necessary to provide new equipment such as a router, several configurable switches, APs (Access Points) compatible with SDN (Software Defined Networking) technology, and new Ethernet cabling. The network bandwidth will also be increased by implementing protocols such as LACP (Link Aggregation Control Protocol).

2) Systems: Possible improvements to the server equipment will be addressed, depending on the client's needs and the criticality of the business. The technologies to be considered will include hardware redundancy at all levels (disks, power supplies), virtualization, and backup systems (physical or cloud-based).

3) Remote Access: Remote access to the server will be implemented, allowing employees to access the company's programs and data without having to be physically present. This will be achieved through the use of well-known VPN protocols (SSTP, L2TP/IPSEC, PPTP, etc.).

Keywords: Networks, Systems, VPN, Backups, SOHO

Taula de Continguts

1. Introducció

1.1 Escenari

El projecte inicia el seu desenvolupament durant el període de practiques de l'alumne a una empresa de telecomunicacions, la qual porta anys al sector y es dedica al disseny i configuració de xarxes per a empreses de tot tipus i ISP (Internet Service Provider) o empresa proveïdora de internet i continua el seu desenvolupament per part del alumne amb l'assessorament del tutor del TFG (Treball de Final de Grau).

El present projecte es situa en un entorn empresarial, concretament a una empresa de subministres agrícoles, fontaneria, instal·lacions de regadiu i mes servicis del sector agrícola.

Es pretén aportar una solució real a una empresa física, la qual no compta amb un informàtic o departament de informàtica, ni sol destinar un pressupost anual al manteniment de la xarxa o equips informàtics, com puguen ser impressores, TPV (Terminals Punts de Venda), o els propis equips finals dels usuaris (Ordinadors, Tabletes, Portàtils, ...).

1.2 Objectiu principal

El objectiu del projecte es desplegar una implementació real de un muntatge de xarxa i sistemes a una empresa menuda. Mostrant la situació inicial a l'empresa, el disseny proposat, la configuració dels dispositius i la situació final.

1.3 Justificació del projecte

A les empreses, ja siguen grans o menudes, garantir una infraestructura tecnològica eficient, escalable i segura que garantisca a l'empresa treballar de manera optima es fonamental. Per aquest motiu cal garantir uns objectius específics com:

- **Optimitzar el Rendiment i la Productivitat**: Dissenyar una xarxa que oferisca un alt rendiment i baixa latència per a totes les aplicacions crítiques del negoci, la qual cosa contribuïx a una major eficiència i productivitat dels empleats.
- **Assegurar la continuïtat del negoci**: Implementar sistemes de redundància i de suport per a minimitzar el temps d'inactivitat en cas de fallades o desastres, assegurant que l'empresa puga continuar operant sense interrupcions significatives.
- **Garantir la Seguretat**: Implementar mesures de seguretat robustes per a protegir les dades i actius de l'empresa contra amenaces externes i internes, incloent Firewall, sistemes de detecció d'intrusos, càmeres de vigilància.

- **Facilitar l'Accés Remot**: Proveir solucions d'accés remot segur per a empleats, permetent-los treballar des de qualsevol lloc, la qual cosa és especialment important en entorns de treball flexibles o en situacions que requerisquen teletreball.
- **Escalabilitat i Flexibilitat**: Dissenyar una infraestructura que puga créixer i adaptar-se fàcilment a mesura que l'empresa s'expandix o canvia les seues necessitats, permetent la integració de noves tecnologies i servicis sense grans inversions addicionals.
- **Reducció de Costos Operatius**: Optimitzar els recursos i processos tecnològics per a reduir costos operatius, per exemple, mitjançant la virtualització de servidors, l'ús de servicis en el núvol i la consolidació de recursos.

La situació de la empresa en la qual es desenvolupa aquesta memòria, no complia amb cap d'aquests punts descrits amb anterioritat, es per aquest motiu, que es proposa la solució descrita a la present memòria.

1.4 Estructura de la memòria

La memòria consistirà de cinc punts:

El **primer punt** explicarà el perquè d'aquest projecte així com els seus objectius i la posada en escena d'aquest.

El **segon punt** recollirà els fonaments teòrics tècnics necessaris per a implementar del treball realitzat a la memòria, així com la descripció dels protocols i tecnologies utilitzades.

El **tercer punt** consistirà en la implementació real dels equips, disseny, instal·lació, muntatge i configuració de tot el necessari per al correcte funcionament d'aquests.

Al **quart punt** apareixen les conclusions i possibles línies de treball a futur.

El **cinquè punt** recull la bibliografia i fonts d'informació del projecte.

2. Fonaments teòrics

2.1 PIME

Una PIME (Petita I Mitjana Empresa) és una entitat empresarial que, per la seua grandària, se situa entre les microempreses i les grans empreses. Estes empreses solen ser més flexibles i adaptables que les grans corporacions, la qual cosa els permet respondre ràpidament als canvis del mercat.

Tipus de Pimes

Les Pimes es classifiquen generalment segons la seua grandària i el sector en el qual operen. A continuació s'enumeren els principals tipus:

1. **Microempresa**:
   - **Nombre d'empleats**: Fins a 10 empleats.
   - **Volum de negoci anual**: Fins a 2 milions d'euros.

2. **Petita empresa**:
   - **Nombre d'empleats**: Entre 11 i 50 empleats.
   - **Volum de negoci anual**: Fins a 10 milions d'euros.

3. **Mitjana Empresa**:
   - **Nombre d'empleats**: Entre 51 i 250 empleats.
   - **Volum de negoci anual**: Fins a 50 milions d'euros.

2.1.1 Entorn PIME

Als entorns PIME no tenim una estructura de disseny definida a la que cenyir-nos, es degut a que cada empresa te les seues necessitats, diferent nombre de usuaris o compta amb recursos diferents.

A microempreses o petites empreses busques dissenys on la simplicitat, l'eficiència i la reducció de costos son essencials, es ací on entra el concepte de disseny de xarxes de nucli col·lapsat o Collapsed core.

En el disseny de xarxa tradicional es sol emprar una arquitectura de tres capes: nucli o core, distribució i accés. No obstant això, en el disseny collapsed core, les capes de nucli i distribució es combinen en una sola. Això implica que els switchos o Routers que normalment estarien en la capa de distribució també assumixen les funcions de nucli.

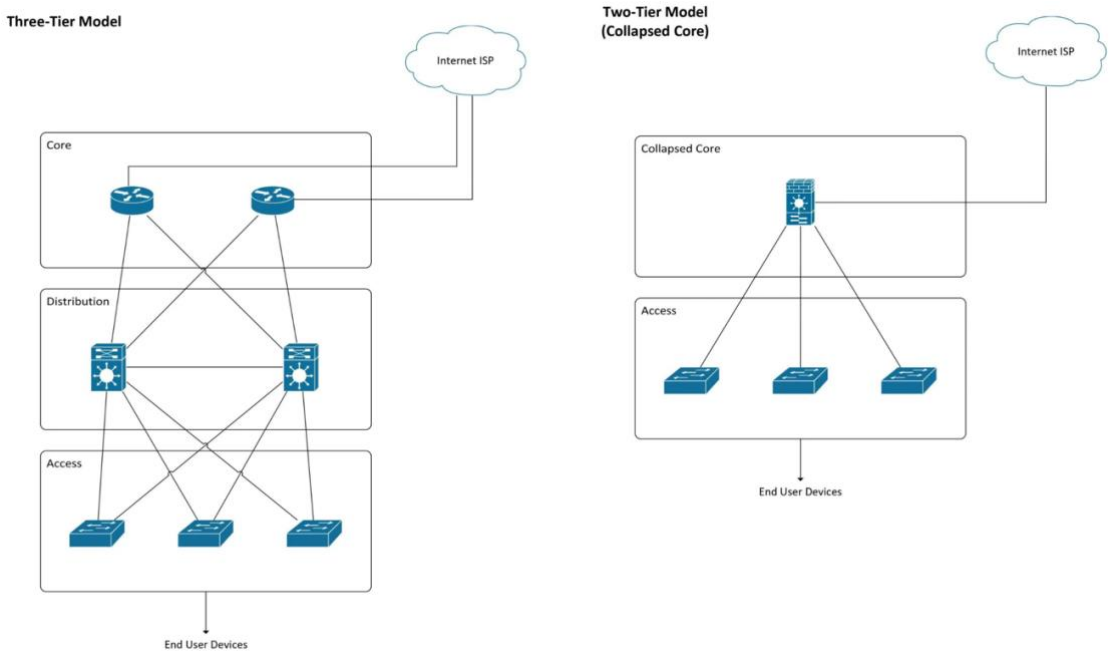
Avantatges del Disseny Collapsed Core

- **Reducció de Costos**: Menys hardware és necessari perquè s'eliminen els dispositius dedicats a la capa de nucli.

- **Simplicitat de Gestió**: Menys dispositius i una estructura més simple faciliten la gestió i el manteniment de la xarxa.
- **Menor Latència**: En combinar les capes, es reduïxen els salts de xarxa, la qual cosa pot resultar en una menor latència.
- **Menys Complexitat**: Menys capes i menys dispositius poden simplificar la implementació i la resolució de problemes.

Desavantatges del Disseny Collapsed Core

- **Escalabilitat Limitada**: Este disseny pot no ser adequat per a xarxes molt grans o complexes, ja que la capacitat dels dispositius de combinació nucli/distribució pot ser un factor limitant.
- **Redundància Reduïda**: En un disseny de tres capes, és més fàcil implementar redundància en cada capa. En un disseny collapsed core, la redundància pot ser més difícil d'aconseguir o pot requerir solucions més complexes.
- **Càrrega de Treball en els Dispositius**: Els dispositius en un disseny collapsed core poden tindre una major càrrega de treball, ja que han de manejar tant les funcions del nucli com de distribució.



Il·lustració 1 - Jerarquia de disseny

La **capa Core i Distribució**, es la encarregada de interconnectar l'empresa amb internet i, si cal, amb altres oficines o emplaçaments de la pròpia empresa, es fonamental que els dispositius i la configuració establida a aquesta capa, tinguen la capacitat de garantir la transmissió de paquets lo mes ràpid i estable possible.

1. **Alta disponibilitat**: Garantir que els recursos de la xarxa o externs, com servidors, siguen sempre accessibles, ja que son essencials per a les tasques diàries a una empresa.

2. **Connexions redundants**: proporcionar connexions redundants, es a dir, garantir l'operativitat de la xarxa si algun component falla, implantant per exemple, distints enllaços de comunicació.
3. **Seguretat**: Implementació de mides de seguretat que ajuden a protegir l'empresa davant amenaces externes però també internes. Amb Firewalls i sistemes de detecció que apliquen polítiques de seguretat per a protegir les dades de atacs i accessos no autoritzats.
4. **Enrutament i comunicació**: manejar el tràfic intern entre departaments, concepte VLAN (Virtual Local Area Network) o xarxes de àrea local virtuals, com ara ventes, comptabilitat, recursos humans, etc. assegurant que es les dades es moguen de una manera segura i eficient.

La **Capa d'accés** es la capa mes externa de la xarxa, es essencial perquè es el punt on dispositius finals, com computadores, telèfons IP, impressores, AP (Acces points) o punts d'accés es connecten a la xarxa, esta capa juga un gran paper en la connectivitat diària i l'experiència del usuari. Algunes de les seues raons son:

1. **Connectivitat de dispositius finals**: Cada empleat te la seua estació de treball connectada al switch d'accés, conjunt de Telèfon IP mes computadora i ames utilitza dispositius mòbils connectats a APs.
2. **Seguretat**: La capa d'accés es el primer límit de la xarxa i implementa mecanismes d'autenticació, per a assegurar que sols usuaris i dispositius autoritzats puguen connectar-se a la xarxa. Etiquetar els ports amb VLANs (Virtual Local Area Networks) o xarxes de àrea local virtuals per a separar el tràfic entre departaments.

2.1.1.1 Criticitat

La criticitat fa referencia a la importància de diferents sistemes, processos i recursos per al funcionament continu i amb èxit de la empresa. Saber identificar i gestionar adequadament la criticitat es fonamental per a garantir la productivitat y la continuïtat del negoci. Ací analitzarem alguns aspectes clau de la criticitat a un PIME.

1. Identificació dels recursos

Sistemes informàtics i de comunicació

- **Servidors i emmagatzemament**: Els servidors que allotgen les bases de dades, aplicacions critiques son fonamentals. Una fallada podria suposar paralitzar les operacions i causar pèrdues significatives.
- **Sistemes de comunicació**: Ferramentes de comunicació com VoIP (Voice over IP), correu electrònic i plataformes de videoconferència.

Infraestructura de xarxes

- **Electrònica de xarxa**: Switch, Routers y Firewalls son crítics per a la connectivitat y la seguretat de la xarxa.
- **Connexions de internet**: Una connexió a internet fiable i d'alta velocitat es fonamental per a casi totes les operacions, des de el correu electrònic fins a aplicacions en remot.

Aplicacions i software

- **Aplicacions empresarials**: ERP (Enterprice Resource Planning), CRM (Customer Relationship Manager) i altres aplicacions especifiques del negoci son essencials per a les operacions diàries
- **Software de seguretat**: Programes antivirus, antimalware i detecció d'intrusos son vitals per a mantenir la integritat i els sistemes de dades.

2. Avaluació de la criticitat

Impacte en el negoci

- **Pèrdua de ingressos**: Determinar quant podria costar a l'empresa en termes d'ingressos si un recurs crític falla.
- **Productivitat**: Avaluar com la interrupció d'un sistema afectaria la productivitat dels empleats.
- **Reputació**: Considerar com les fallades en sistemes crítics poden afectar la reputació de l'empresa davant clients i socis.

Disponibilitat i redundància

- **Tolerància al fallo**: Identificar la capacitat del sistema per a seguir funcionant en cas de fallada.
- **Temps de recuperació**: Establir el temps màxim acceptable per a la recuperació de sistemes crítics (RTO – Recovery Time Objective).

3. Gestió de la criticitat

Planificació d'estratègies

- **Plans de continuïtat del negoci**: Desenvolupar i mantenir un pla que incloga estratègies per a mantenir operacions critiques en cas de interrupcions.
- **Plans de recuperació de desastres**: Implementar un pla que detalle els procediments per a recuperar sistemes crítics després del desastre.

Implementació de mides de seguretat

- **Seguretat física i lògica**: Protegir físicament els equips crítics i assegurar la infraestructura lògica amb mides com Firewalls, encriptació i autenticació de dos factors.

- **Monitorització i alerta**: Utilitzar ferramentes de monitorització per a supervisar l'estat dels sistemes crítics i configurar alertes per a detectar i respondre ràpidament a problemes.

Redundància i Backup

- **Redundància de hardware:** Implementar redundància en hardware crític com servidors i dispositius de xarxa per assegurar l'alta disponibilitat.
- **Copies de seguretat:** Realitzar Backup regulars de dades i sistemes crítics i assegurar que les copies de seguretat s'emmagatzemen de manera segura i son recuperables ràpidament.

2.1.1.2 Criticitat de Sector

Considerem la PIME que opera al sector agrícola amb dos empleats sempre a tenda/oficina. L'empresa depèn de un ERP per a gestionar inventaris, ordres, logística i al mateix temps punt de venda final (TPV). Així mateix, també fa us de servicis de correu electrònic.

Recursos crítics identificats

- **Servidor ERP**: Crític per a operacions diàries
- **Connexió a internet**: Necessària per al correu electrònic, comandes online i comunicació
- **Sistema de comunicacions**: Ferramentes de videoconferència i VoIP per a interacció amb proveïdors i clients.

Avaluació de la criticitat

- **Impacte de fallades**: Una fallada del servidor ERP podria aturar les operacions de inventari i comandes, resultant en pèrdues significatives.
- **RTO i Redundància**: El objectiu es recuperar el servidor ERP el mes prompte possible. Implementant un servidor de suport i copies de seguretat diàries.

Mesures a implementar

- **Redundància**: Implementació de un servidor de suport per al ERP i connexions redundants a internet.
- **Seguretat**: Firewall robust i autenticació de doble factor per al accés a sistemes crítics.
- **Monitorització:** Sistema de monitorització que alerte sobre qualsevol problema tant amb el servidor ERP com amb la xarxa.

Com a resum, gestionar la criticitat d'una empresa implica identificar recursos i sistemes essencials, avaluar el seu impacte en el negoci, adoptar mesures per a assegurar la seua disponibilitat, i la segura i rapida recuperació en cas de fallades.

2.1.2 Recursos

L'empresa on es desenvolupa el present TFG es troba al sector primari posat que es un comerç de venda directa al públic, però també es dedica a les instal·lacions de regadiu, jardineria, fontaneria i manteniment de piscines.

L'empresa te una facturació anual de menys de 100.000 euros i no compta amb un pressupost destinat al manteniment i adquisició de material informàtic o electrònica de xarxa.

L'empresa em comunica que no pot destinar una gran quantitat dels seus recursos a la substitució del material informàtic ni de la electrònica de xarxa i em sol·licita que siga el mes ajustat possible.

2.1.3 Necessitats

El client ens contacta perquè ha patit una fallada al servidor de l'empresa, aquest ha deixat de funcionar després de un reinici a una actualització de Windows. Em comenta que l'equip no ha tornat a encendres, quedant així la producció de la persona encarregada de la comptabilitat parada i de la persona encarregada de les ventes i la atenció al públic, sense accés a la base de dates del clients i els productes.

En un primer moment el client sols necessita que el servidor comence a funcionar de nou i poder seguir amb la producció. En una segona xarrada amb ell, em comenta que fa temps que els equips no s'actualitzen i que pot ser, també, seria necessari fer una actualització de la xarxa per a millorar la producció a la empresa.

Em detalla una sèrie de necessitats que li han sorgit arrel de la fallada del servidor a mes, a aquestes necessitats, propose una sèrie de opcions des de el punt de vista tècnic i pràctic que el client accepta i aprova. Aquestes necessitats son les que es recullen als següents punts de la memòria, les quals estaran dividides entre disseny de xarxes i disseny de sistemes.

2.2 Disseny de xarxes

El disseny de xarxes en una petita i mitjana empresa (PIME) és una tasca essencial que busca establir una infraestructura de comunicació eficient, segura i escalable. En el context empresarial actual, on la connectivitat i l'intercanvi d'informació són fonamentals, una xarxa ben dissenyada pot marcar la diferència en termes de productivitat, seguretat i capacitat de resposta a les demandes del mercat.

Objectius del Disseny de Xarxes per a una PIME

- Eficiència en la Comunicació: Proveir una infraestructura de xarxa que permeta una comunicació fluida i ràpida entre els empleats.
- Seguretat de la Xarxa: Implementar mesures de seguretat per a protegir la xarxa contra accessos no autoritzats, atacs i vulnerabilitats, garantint la integritat i confidencialitat de la informació.
- Escalabilitat i Flexibilitat: Dissenyar una xarxa que puga créixer i adaptar-se fàcilment conforme l'empresa expandisca les seues operacions o canvie les seues necessitats tecnològiques.
- Continuïtat del Negoci: Assegurar la disponibilitat constant de la xarxa mitjançant la implementació de mecanismes de redundància i recuperació davant desastres, minimitzant el temps d'inactivitat.
- Reducció de Costos: Optimitzar l'ús de recursos de xarxa per a reduir els costos operatius, mitjançant la implementació de tecnologies com la virtualització de xarxes i l'ús de solucions en el núvol.

Metodologia del Disseny

El desenvolupament del disseny de xarxes per a una PIME s'abordarà mitjançant una metodologia estructurada que inclou les següents fases:

- Anàlisi de Requeriments: Identificar les necessitats de comunicació i connectivitat de l'empresa, incloent-hi el nombre d'usuaris, dispositius, aplicacions i servicis crítics.
- Disseny de l'Arquitectura de Xarxa: Proposar una arquitectura de xarxa que complisca amb els requeriments identificats.
- Selecció d'Equipament: Triar el hardware i software adequat per a la xarxa, incloent-hi Routers, switch, Firewalls, punts d'accés i sistemes de gestió de xarxa.
- Implementació i Configuració: Desenvolupar i implementar la solució de xarxa, incloent-hi la configuració de dispositius, la segmentació de la xarxa mitjançant VLANs i la implementació de polítiques de seguretat.
- Proves i Validació: Realitzar proves exhaustives per a assegurar que la xarxa complix amb els requisits de rendiment, seguretat i disponibilitat, i validar el seu correcte funcionament en escenaris operatius reals.
- Documentació i Formació: Documentar detalladament la configuració i els procediments operatius.

2.2.1 Segmentació

Segmentar no es mes allò que separar o dividir alguna cosa. Una bona practica alhora de dissenyar i configurar una xarxa on hi ha diferents departaments com finances, logística, recursos humans, o diferents segments de la xarxa que no sols siguen el de producció, com puga ser, la xarxa per a convidats, la xarxa per a VoIP, CCTV (Closed Circuit Television), necessitem separar la xarxa per a millorar la organització, la seguretat i el rendiment entre els diferents segments.

Fins ara podríem pensar que per a dividir una xarxa d'una PIME en diferents dominis de broadcast en funció dels seus departaments, necessitaríem tants switch com departaments existiren interconnectats a un Router.

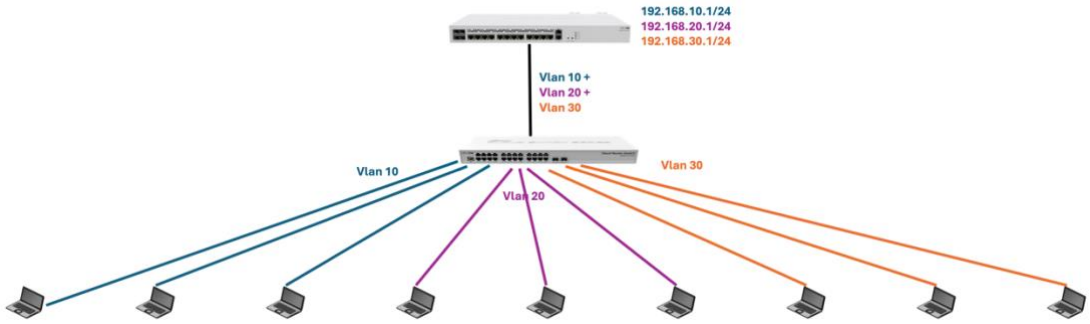
Il·lustració 2 - Xarxa no segmentada

Es ací on entra el concepte VLAN (Virtual Local Area Network).

Una VLAN es una subxarxa lògica configurada dins d'una xarxa física major per a segmentar el tràfic de la xarxa. Ens permet agrupar un conjunt de dispositius en una xarxa local de manera virtual, sense importar la seua ubicació física. Les VLANs milloren la gestió, la seguretat i la eficiència del tràfic de la xarxa, permetent-nos una major flexibilitat en l'organització i administració de la xarxa.

La VLAN permet segmentar a nivell lògic una xarxa, sense necessitat de re-configurar el hardware físic. Els dispositius dins d'una VLAN poden estar ubicats en diferents switch físics, però es comporten com si estigueren en la mateixa xarxa local.

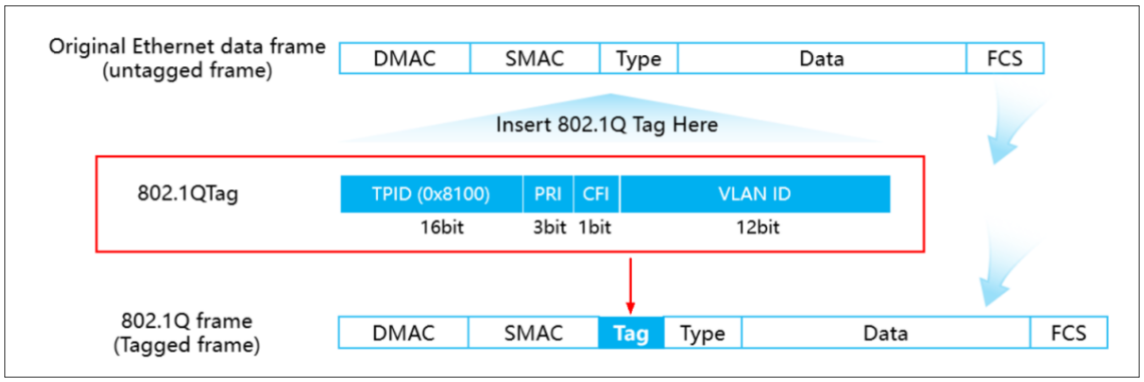
Al segmentar la xarxa, el tràfic VLAN es aïllat de altres VLANs.



Il·lustració 3 - Xarxa segmentada

Etiquetat VLAN (IEEE 802.1Q)

L'estàndard IEEE 802.1Q definix un mètode per a etiquetar trames Ethernet amb identificadors VLAN. Aquest estàndard introduix una capçalera 802.1Q dins la trama Ethernet.



Il·lustració 4 - Etiqueta VLAN

Una de les parts d'aquesta capçalera es la que identifica la vlan, el **VLAN ID**, reservat per 12 bits, es el que ens dona el nombre màxim de VLAN que es poden crear, 4096.

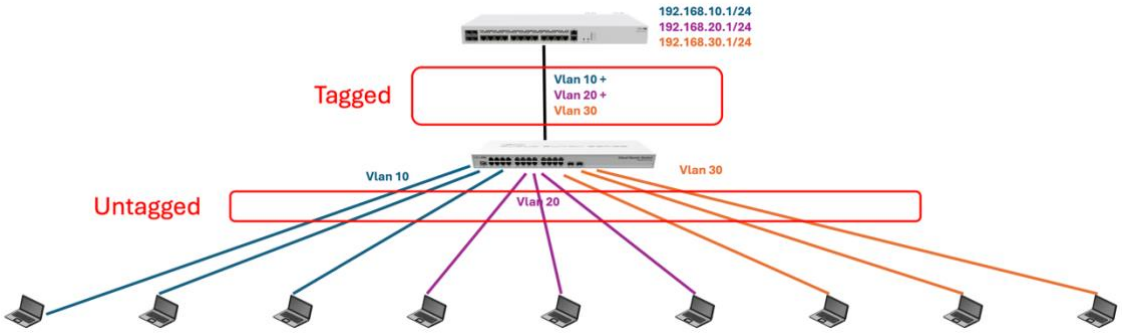
A una implementació de VLANs ens trobem amb dos tipus de ports principals:

- Port untagged/accés: la trama es transmet i rep sense etiqueta.
- Port tagged/trunk: la trama es transmet i rep amb etiqueta.

Les trames arriben al switch des de els dispositius finals sense etiquetar (untagged).

El switch lis afegeix etiquetes avanç d'enviar-les al port trunk segons el PVID (Port Vlan ID) del port d'entrada (tagged).

Totes les trames en un port tagged disposen de etiquetes VLAN. En cas de no disposar, s'afegix la "default vlan".



Il·lustració 5 - Tagged / Untagged

Els dispositius finals es solen connectar a ports untagged, ja que no "entenen" de VLANs.

La interconnexió amb altres switch sol configurar-se en modo tagged/trunk, ja que transporta mes de una VLAN.

Si comptem amb servidors es solen configurar també en mode tagged/trunk.

2.2.2 Connectivitat

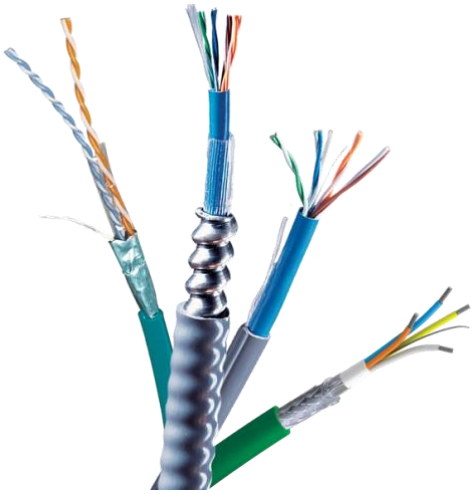
En l'entorn empresarial actual, la connectivitat de xarxa és un component essencial per a l'operació eficient de qualsevol empresa. Una xarxa ben dissenyada i gestionada garantix l'accés ràpid i segur a les dades i aplicacions. A la gran majoria d'empreses ens trobarem amb dos tipus de connectivitat, cablejada i sense fil (wireless).

2.2.2.1 Cablejat

A les empreses ens trobem majoritàriament diferents tipus de tecnologia de cablejat, el cablejat Ethernet o "par trenzado" del castellà, utilitzat en dispositius finals majoritàriament i cablejat de fibra òptica, utilitzat per a unir equips de xarxa a distancies superiors a 100 metres o els cables DAC (Directly Attach Cable)

Ethernet

El cable Ethernet es coneix com a parell creuat degut a la seua composició de huit cables de coure, creuats en conjunts de dos. Aquests cables poden ser blindats STP (Screen Shielding Pair) i FTP (Foil Shielding Twisted Pair) o no UTP (Unshielded Twisted Pair).



Il·lustració 6 - Cables Ethernet

Ames els diferenciem per les distintes categories, que ens permeten conèixer les capacitats i característiques dels cables que estan instal·lats o dels que anem a treballar amb ells.

Categoria	Velocitat màxima	Freqüència	Distancia
CAT5	100Mbps	100MHz	100 metres
CAT5E	1000Mbps	100MHz	100 metres
CAT6	10Gbps	250MHz	100 metres
CAT6A	10Gbps	500MHz	100 metres
CAT7	10Gbps	600MHz	100 metres
CAT7A	10Gbps	1000MHz	100 metres

Cables DAC

Els cables DAC són cables de connexió directa que s'utilitzen principalment per a interconnectar dispositius de xarxa com switchos, Routers i servidors. Són una alternativa econòmica i eficient als transceptors òptics i cables de fibra òptica o coure.

Consistixen en cables de coure amb transceptors integrats en cada extrem. No requerixen mòduls SFP (Small Form-factor Pluggable) separats, ja que els transceptors estan incorporats en el propi cable. Son cables generalment més econòmics que les combinacions de transceptors òptics i cables de fibra.

Connectors Comuns:

- SFP DAC: Per a connexions de fins a 1 Gbps.
- SFP+ DAC: Per a connexions de fins a 10 Gbps.
- QSFP+ DAC: Per a connexions de fins a 40 Gbps.
- QSFP28 DAC: Per a connexions de fins a 100 Gbps.

Il·lustració 7 - Cables DAC

2.2.2.2 Wireless

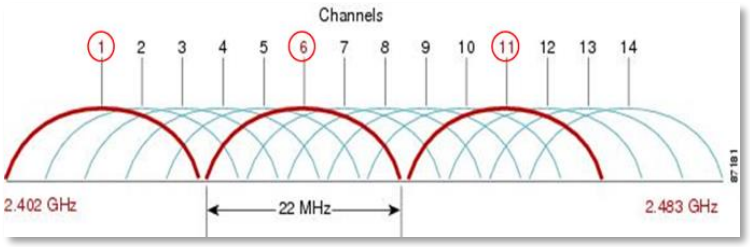
El terme wireless es referix a la transmissió de informació utilitzant ones electromagnètiques. Els exemples de de dispositius de comunicacions wireless inclouen, radios, forns de microones, auriculars Bluetooth, routers Wi-Fi, etc.

En l'estàndard 802.11, el IEEE va dividir la banda de freqüència de 2,4 GHz/5 GHz en canals més xicotets, per la qual cosa cada sistema de radio freqüència pot utilitzar alguns d'estos canals per a la comunicació wireless.

Canal i ampli de banda (bandwidth)

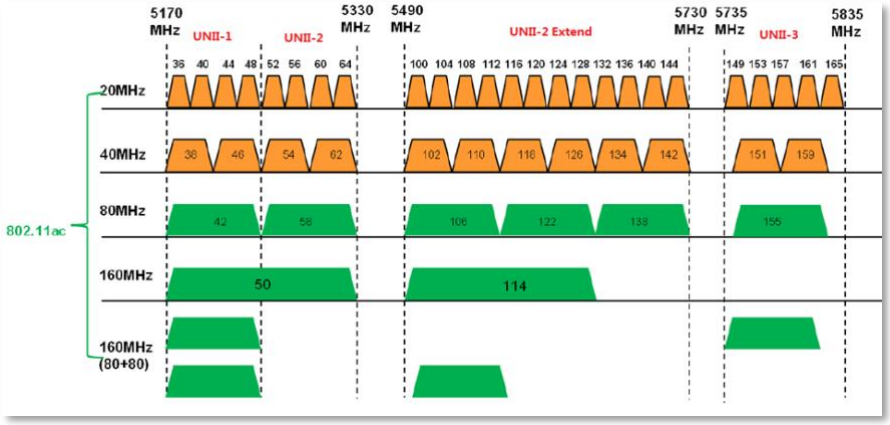
Els protocols 802.11 n/ac/ax permeten unir dos o més canals per a augmentar l'amplada de banda de la xarxa. Encara que la tecnologia d'unió de canals pot millorar l'amplada de banda, la major amplària del canal també significa que s'ocupen més recursos de freqüència i augmenta l'efecte d'interferència sense fil.

Per a la ràdio de 2,4 GHz, podem utilitzar 14 canals (la versió de la UE admet d'1 a 13 canals, la versió dels EUA admet d'1 a 11 canals), però només hi ha tres canals no solapats.



Il·lustració 8 - Distribució de canals en 2,4 Ghz

En el cas de la ràdio de 5 GHz, disposa de més recursos de canal, tots ells no solapats (amb una amplària de canal de 20 MHz). En el cas del protocol 802.11 ac/ax, es recomana utilitzar una amplària de canal menor per a reduir les interferències wireless, com l'amplària de canal de 40 MHz. Si la interferència és molt greu, es pot considerar l'ample de canal de 20 MHz, encara que disminuirà la velocitat wireless.



Il·lustració 9 - Distribució de canals en 5 Ghz

Atenuació

Quan un senyal de RF travessa obstacles com a parets de formigó , fusta o vidre, s'absorbirà part de l'energia del senyal. Este fenomen es traduïx en què la intensitat del senyal que ix de l'obstacle serà més feble que el senyal que entra. A menor longitud d'ona (majors freqüències), majors pèrdues en travessar objectes.

Il·lustració 10 - Atenuació de senyal

Tecnologia Wi-Fi

El Wi-Fi (Wireless Fidelity) es una tecnologia de xarxa wireless basada en els estàndards IEEE 802.11, utilitzada principalment per a crear xarxes sense fil d'àrea local (WLAN) en llars, oficines i espais públics.

Estàndards IEEE 802.11:

- 802.11a: Opera en la banda de 5 GHz i oferix velocitats de fins a 54 Mbps.
- 802.11b: Opera en la banda de 2.4 GHz i oferix velocitats de fins a 11 Mbps.
- 802.11g: També en la banda de 2.4 GHz, però amb velocitats de fins a 54 Mbps.
- 802.11n (Wi-Fi 4): Opera en les bandes de 2.4 GHz i 5 GHz, amb velocitats de fins a 600 Mbps.
- 802.11ac (Wi-Fi 5): Opera en la banda de 5 GHz i oferix velocitats de fins a diversos Gbps.
- 802.11ax (Wi-Fi 6 i Wi-Fi 6E): Millora l'eficiència i la capacitat, amb velocitats de fins a 10 Gbps i utilitza les bandes de 2.4 GHz, 5 GHz i 6 GHz.

Esta taula mostra la comparativa dels estàndards actuals mes utilitzats:

Chronicles.	Wi-Fi 4	Wi-Fi 5		Wi-Fi 6
Protocol	802.11n	802.11ac		802.11ax
		Wave 1	Wave 2	
Time	2009	2013	2016	2018+
Frequency	2.4 GHz 5 GHz	5 GHz		2.4 GHz 5 GHz
Max Band	40 MHz	80 MHz	160 MHz	160 MHz
MCS Range	0-7	0-9		0-11
Highest modulation	64QAM	256QAM		1024QAM
Single-stream bandwidth	150Mbps	433Mbps	867Mbps	1201Mbps
Maximum spatial streams	4X4	8X8		8X8
MU-MIMO			Downlink	Uplink Downlink
OFDMA				Uplink Downlink

Il·lustració 11 - Estàndards Wi-Fi

2.2.3 Teletreball

Hui en dia, i arrel de la pandèmia mes, les empreses han començat a valorar el teletreball i incorporar-lo a les seues oficines. Es una modalitat laboral en la que els empleats realitzen les seues tasques fora de les instal·lacions de l'empresa. Aquest model permet als empleats treballar des de els seus llars, espais de coworking o altres llocs.

Alguns dels avantatges son la flexibilitat i l'equilibri entre vida laboral i personal, degut al horari flexible per poder organitzar-se el temps de una forma mes eficient, adaptant la seua jornada laboral a les seues necessitats personals i familiars. Reduint estres degut al desplaçament diari fins les instal·lacions, degut a que els desplaçaments poden contribuir a empitjorar la salut mental.

També ens trobem amb la part de reducció de costos, posats a una PIME de pocs recursos, el estalviar en infraestructura com puga ser reduir preus d'alquilar d'oficines i el seu manteniment o el estalvi dels empleats alhora de desplaçar-se, ja siga amb vehicle propi o fent us del transport públic.

Encara que el teletreball ens ofereix nombrosos avantatges , també presenta reptes que deuen ser gestionats correctament, com la necessitat de mantenir la seguretat de la informació, garantir una comunicació efectiva i gestionar el benestar i la productivitat del empleat de forma remota.

Com a conclusió, el teletreball presenta una evolució significativa en la forma en la que les empreses i els treballadors aborden el treball. Son nombrosos els punts positius, des de la flexibilitat i estalvi de costos, fins a la sostenibilitat i la continuïtat del negoci, però per a aprofitar aquests beneficis, les empreses deuen implementar les tecnologies adequades que faciliten las gestió eficient del treball en remot.

2.2.3.1 VPN

Virtual Private Network o xarxa privada virtual, es la tecnologia que ens permet crear una connexió segura i xifrada a traves d'una xarxa publica, com Internet. Esta connexió simula una xarxa privada sobre una infraestructura publica, proporcionant privacitat i seguretat en les comunicacions i permetent que els usuaris puguen accedir als recursos d'una xarxa local, com la de la empresa, des de una ubicació remota.

Podríem dividir la VPN en quatre fases o quatre parts que la componen:

Client VPN: Software o dispositiu que inicia la connexió VPN des del usuari final. Pot ser una aplicació a l'ordinador, telèfon mòbil o al Router.

Servidor VPN: El punt final de la connexió VPN, que pot estar ubicat en qualsevol part del mon. Es l'encarregat de rebre i reenviar les dades del client VPN.

Túnel VPN: El camí a traves del qual viatgen les dades entre client VPN i servidor VPN. Aquest túnel pot ser encriptat o no, per tant es important decidir el següent punt.

Protocol VPN: Les regles i estàndards que determinen com s'ha d'establir la connexió i com s'ha de manejar la seguretat. Els protocols mes comuns son L2TP, PPTP, SSTP, OpenVPN.

Túnel o Tunneling

Encapsulació de un protocol de xarxa sobre altre creant un túnel virtual por on es transmetran i rebran dades.

Destaquen dos funcions:

- Aprovisionament del direccionalment IP amb AAA (Autenticació, Autorització i Auditoria)
- Interconnexió de xarxes privades a traves d'una xarxa publica (VPN) de forma segura (Autenticació i xifrat)

La tunelització la trobem en tres tipus de túnels:

- Túnels de domini de broadcast (entorns ISP)
- Túnels amb servidors VPN (entorns Corporatius, teletreball)
- Túnels Site to Site (entorns Corporatius, interconnexió)

PPP: Point to Point Protocol

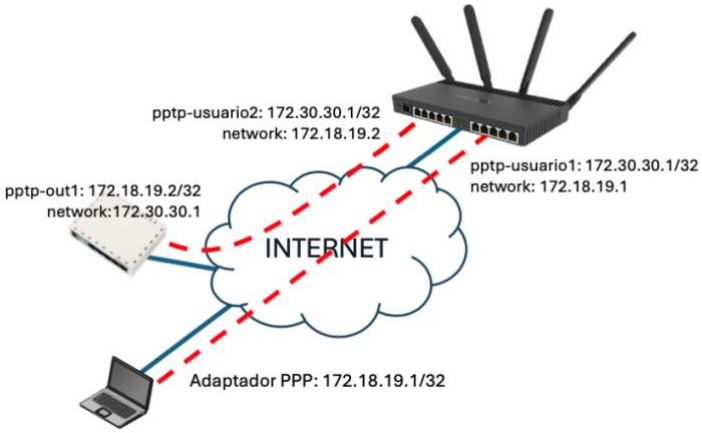
Es un protocol simètric peer to peer que transporta tràfic a nivell 2 i nivell 3 sobre enllaços punt a punt, on els datagrames (Paquets IP) van encapsulats en PPP.

La tunelització PPP s'utilitza als següents casos:

- Entorns ISP: servei PPPoE (Point to Point Protocol over Ethernet)
- Entorns corporatius: Connexions PPP esteses a traves de internet mitjançant L2TP, PPTP, SSTP

El direccionalment Punt a Punt als protocols PPP no utilitza una mascara /30 sinó un /32:

- Pot ser vist com un ID en ambdós extrems en forma de direcció IP
- Es possible utilitzar qualsevol direccionalment IP (en un /32 no existeixen direccions de xarxa ni de broadcast)



Il·lustració 12 - PPP

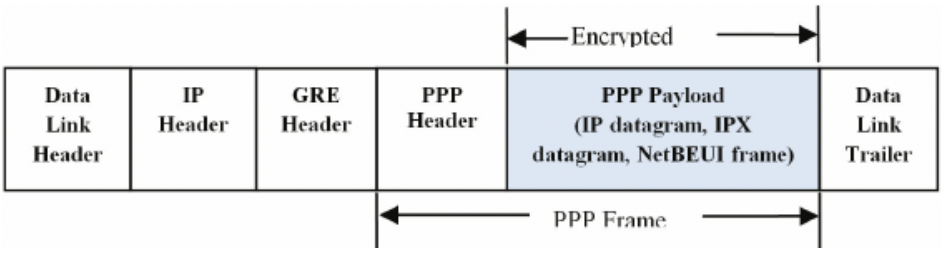
Protocols VPN

L'elecció del protocol de la nostra VPN es fonamental, ja que els diferents protocols que comptem en l'actualitat disposen de característiques que fan únic cada un d'ells, però a l'hora de una VPN de empresa, pensada per al teletreball son fonamentals la comoditat de configuració per part de l'usuari final i la seguretat.

PPTP (Point-to-Point Tunneling Protocol)

Un dels primers protocols VPN, fàcil de configurar però menys segur comparat amb opcions mes modernes.

- Encapsula trames PPP en datagrames IP per a la seua transmissió a traves de la xarxa
- MPPE (Microsoft Point to Point Encryption): encriptació màxima de 128 bits.
- Fàcil i ràpid de configurar.
- Port típic 1701



Il·lustració 13 - Frame PTPP

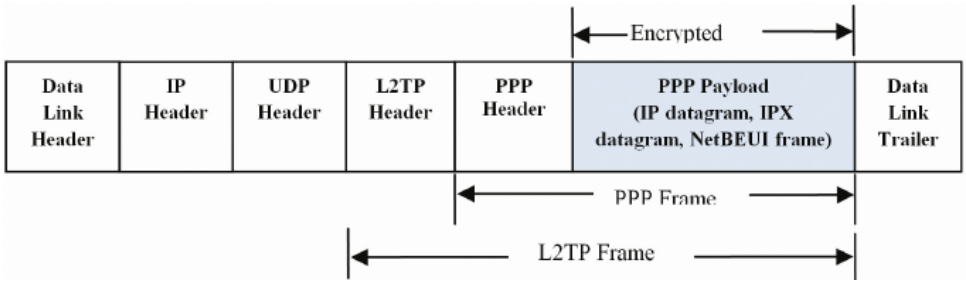
L2TP (Layer 2 Tunnel Protocol)

Es un protocol de tunelització on la comunicació se estableix sobre UDP (User Datagram Protocol). Aquest protocol per si sol, disposa de xifrat, per lo que el fa un protocol no segur. Es possible aplicar-li seguretat combinant-lo amb IPsec (Internet Protocol Security). Aquesta combinació el converteix en un protocol mes segur que PPTP.

Els ports utilitzats comunament a L2TP son:

- Port 1701 (L2TP)
- Port 500 (IPsec)

L2TP es compatible amb una amplia gama de dispositius de xarxa i sistemes operatius, el que facilita la seua implementació en diverses infraestructures.

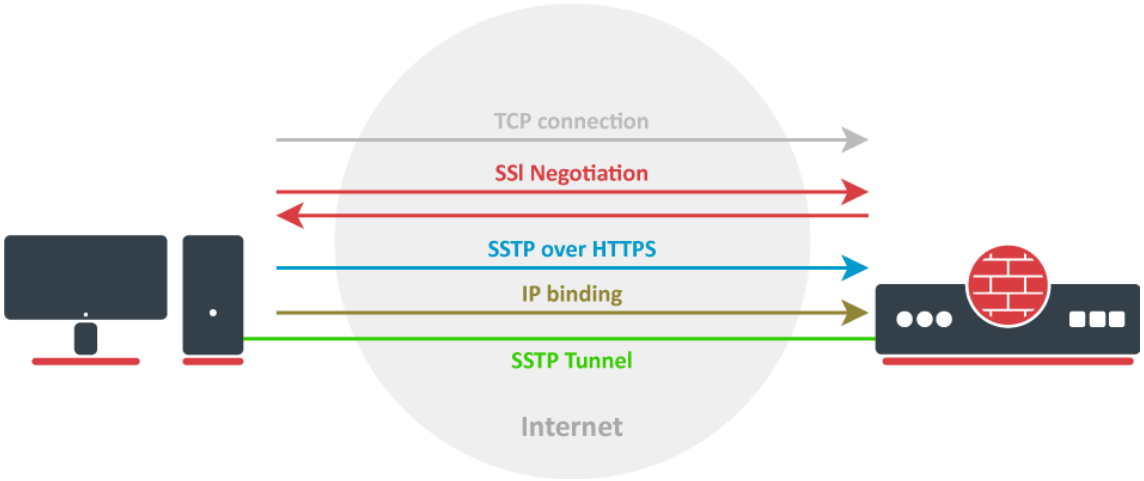


Il·lustració 14 - Frame L2TP

SSTP (Secure Socket Tunneling Protocol)

Protocol relativament nou de tunelització desenvolupat per Microsoft. Encapsula el tràfic PPP a traves d'un canal SSL (Secure Socket Layer) i utilitza el protocol HTTPS (Hipertext Transfer Protocol Secure) a traves del por 443 per a fer passar el tràfic a traves de Firewalls i proxis sense problemes.

Com funciona sobre SSL, es necessari un certificat digital per a l'autenticació del servidor, garantint que les dades se envien a un servidor legítim.



Il·lustració 15 - Frame SSTP

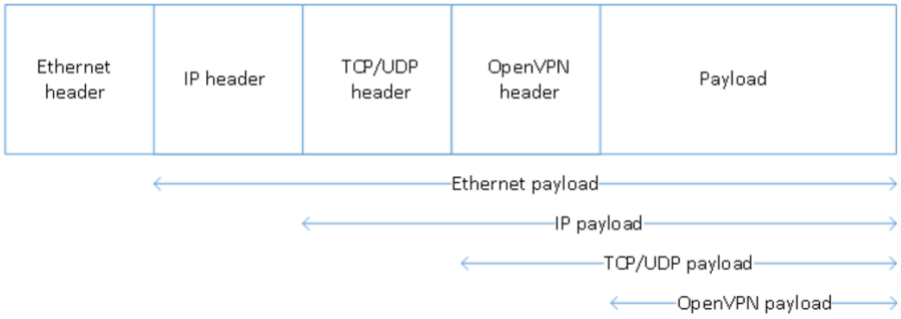
OpenVPN

El protocol OpenVPN es el mes actual del mencionats, es un protocol de codi obert que utilitza SSL/TLS (Secure Socket Layer/Transport Layer Security). S'ha convertit en una de les opcions mes utilitzades gracies a la seua flexibilitat, seguretat i compatibilitat multi plataforma.

Utilitza un robust xifrat ja que suporta una gran varietat de algoritmes de xifrat, com AES (Advanced Encryption Standard), proporcionant així un gran nivell de seguretat.

Compta amb diferents mètodes de autenticació, com puguen ser, certificats digitals, autenticació basada en usuari i contrasenya i autenticació de doble factor.

Pot configurar-se a qualsevol port i opera tant en UDP com en TCP (Transmission Control Protocol).



Il·lustració 16 - Frame OpenVPN

2.2.4 Tendències actuals

Per entrar en context, la demanda de les xarxes empresarials esta augmentant considerablement en l'actualitat. Algunes de les característiques típiques de les xarxes empresarials son aquestes:

Gran escala de dispositius administrats

- Gestió centralitzada
- Baix cost de operació i manteniment
- Fàcil implementació amb PoE (Power over Ethernet)

Alta densitat de clients

- Connexió de xarxa estable
- Fàcil d'utilitzar
- Malla, itinerància sense interrupcions

Altres característiques clau

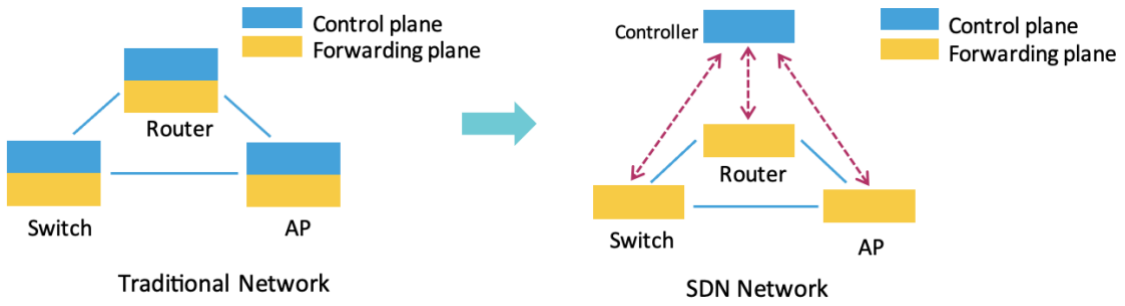
- Portal captiu
- WAN de Backup, balanceig de carrega, Alt rendiment

2.2.4.1 SDN

SDN significa Xarxa definida pel software (Software Defined Network)

Els dispositius de xarxa es poden dividir en dos plànols: Plànol de control i plànol de reenviament. A una xarxa tradicional, aquests plànols generalment estan al mateix dispositiu, per tant cada equip te el seu propi software exclusiu i ens vegem obligats a configurar cada dispositiu de forma independent.

SDN proposa el concepte de la separació del control i el reenviament. Açò significa que els dispositius de xarxa sols son responsables del reenviament de dades i hi haurà un controlador a càrrec del control i configuració dels dispositius.



Il·lustració 17 - Pla de control

Una vegada separat el control del reenviament, podem dissenyar la aplicació SDN basada directament en el plànol de control, lo que ens aporta nombrosos beneficis:

- **Gestió centralitzada**: Sols es necessita tractar amb un controlador centralitzat, per a distribuir polítiques a tots els dispositius connectats
- **Reducció de costos**: virtualització de hardware i servicis que anteriorment realitzava el hardware indicat, el que resulta en una impremta reduïda i costos mes baixos.
- **Control àgil**: pot canviar les regles de qualsevol switch de xarxa quan siga necessari, utilitzar switch basics menys costosos i tindre mes control sobre el flux de tràfic de la xarxa.

Mercat actual

Al mercat ens trobem amb diferents fabricants que aporten solucions SDN, ací s'esmenaran els mes utilitzats.

Cisco

Cisco es el proveïdor mes utilitzat a institucions públiques però els darrers anys també era el mes utilitzat al centres de dades. Compta amb tecnologia SND per a Data Center però també per a empreses i administradors de xarxa. El seu software s'anomena Nexus.

Gran varietat de tecnologies SDN en funció del escenari proposat:

- Cisco ACI solutions
- Cisco Secure Data Center
- SD-Access
- SD-Wan

Huawei

Fabricant de electrònica de xarxa mes utilitzat a l'actualitat. Oferix gran varietat de productes, des de el router de casa, passant per equipament a nivell de PIME i inclús sent la opció mes ferma en operadors ISP (Internet Service Provider) per a desplegar xarxes a nivell local, provincial i estatal. El seu software es conegut com a iMaster.

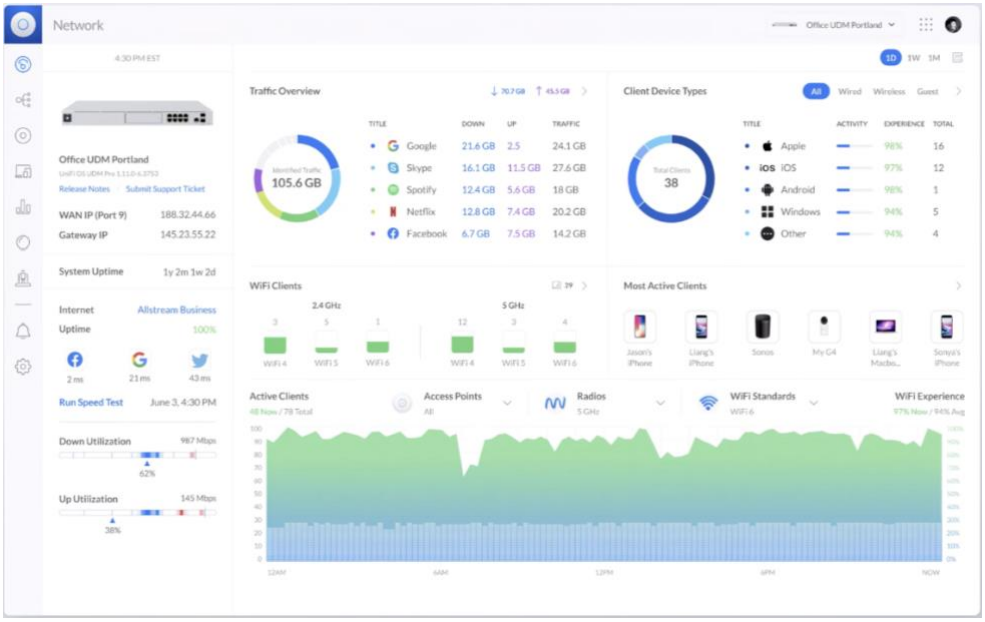
Gran varietat de tecnologies SDN en funció del escenari proposat:

- **Tecnologia SDN en Datacenters (CloudFabric)**
- **Tecnologia SDN a campus (CloudCampus)**
- **Tecnologia SDN en redes empresariales (SD-WAN)**

Ubiquiti Networks

Es una companyia nord-americana que es centra en tecnologia de xarxes sense fil (Wireless). Al ser aquesta la seua principal línia de producció, la convertix en una de les opcions mes estandarditzades en xarxes de ISP que interconnecten les xarxes de diferents localitats amb antenes de llarga distancia, a campus universitaris amb gran nombre de APs per a la connexió de estudiants i professorat, i a empreses, tan grans com menudes, per a les seues línies de producció.

La tecnologia utilitzada per Ubiquiti es coneix com a Uni-Fi i es la mes escollida del mercat com a SDN per el seu amigable i visual entorn Web de gestió.

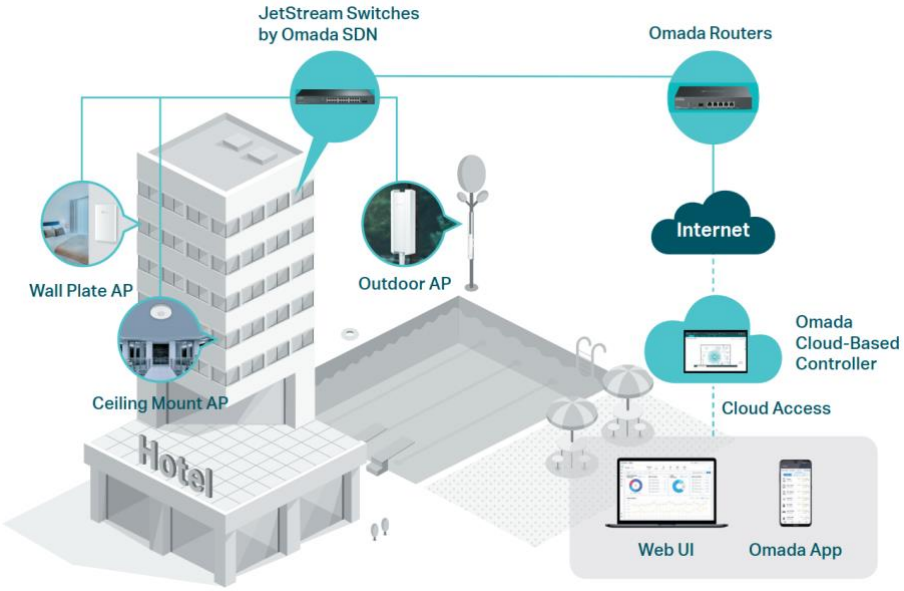


Il·lustració 18 - UniFi

TP-Link

TP-Link es una de les empreses de usuari final mes consolidades al mercat. Aporten solucions com Routers i repetidors domèstics per a les llars, però també compten amb una gama empresarial i mes tècnica amb un ampli catàleg.

Les solucions SDN de TP-Link ofereixen als clients solucions a xarxes comercials punt a punt de manera online. Estan dissenyades per hosteleria, educació, comerç minorista, oficina i altres industries. El SDN de TP-Link es conegut com OMADA i oferix productes basats en escenaris i un amplia gama de beneficis.



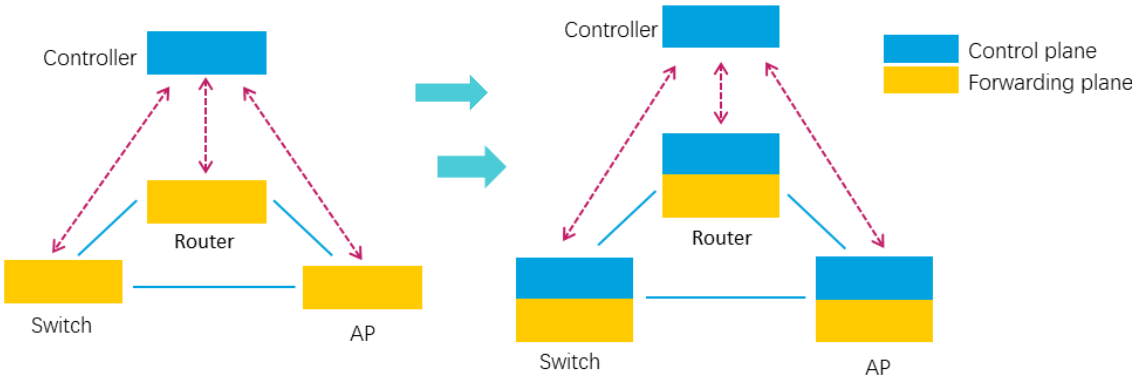
Il·lustració 19 - Omada TP-Link

OMADA

Es difícil exigir a tots els proveïdors de xarxa que reemplacen tots els dispositius de xarxa existents amb dispositius SDN, per lo que apareix una nova estructura:

Seguix mantenint el plànol de control i de reenviament en el mateixos dispositius de xarxa, pero proporciona un controlador centralitzat al mateix temps.

Basat en aquesta idea, TP-Link llança la solució OMADA



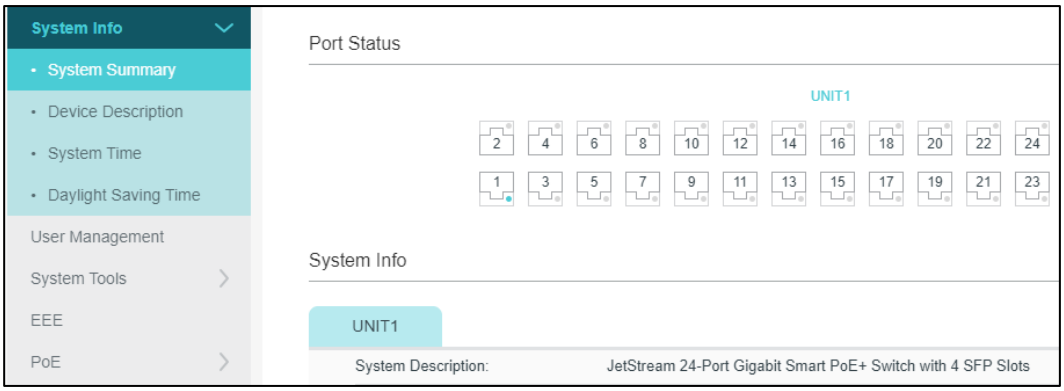
Il·lustració 20 - Pla control Omada

Mètodes de gestió

El mètode de gestió del dispositius **compatibles amb OMADA** es pot dividir en mode independent i en mode controlador.

Mode independent: gestió de dispositius de forma individual i directa, via interface web.

- Tots els productes per a pimes, excepte switch no gestionable.

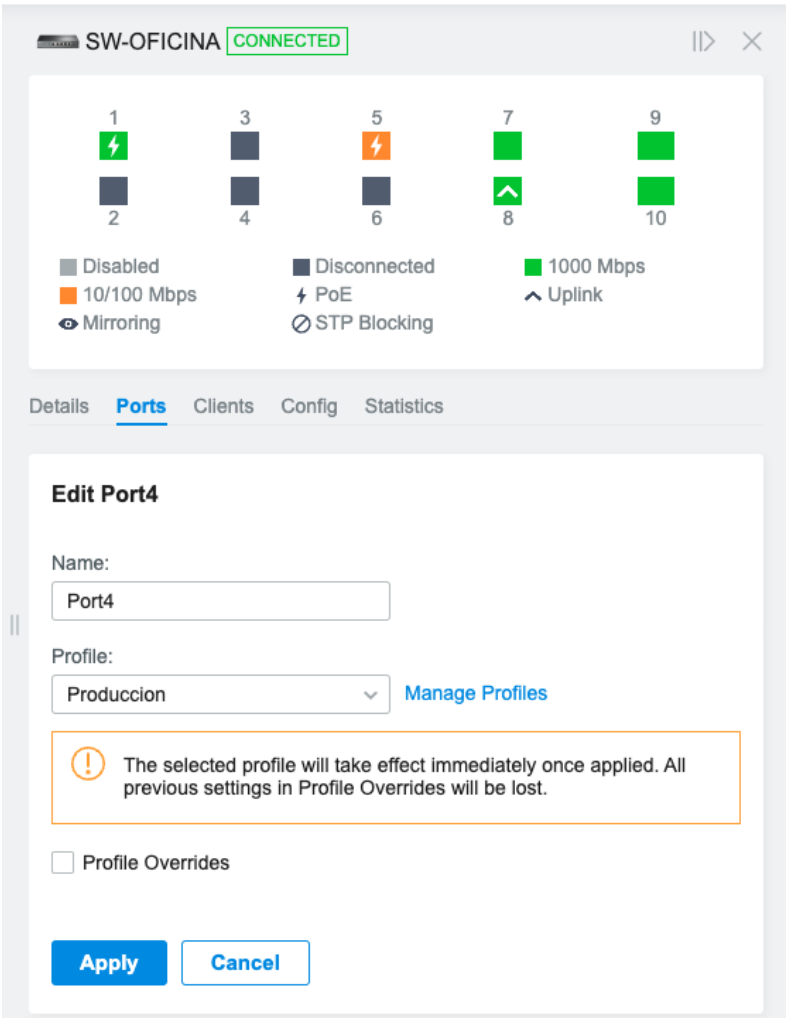


Il·lustració 21 - Entorn configuració TP-Link sense Omada

Comptem amb gestió via web, per la que deurem accedir als dispositius a traves de la adreça IP o via nom de domini (únicament els EAP) o amb gestió via APP, mes limitada ja que sols ens facilita la configuració de EAP i cal estar connectats a la xarxa per a obtindré una adreça IP valida.

Mode controlador: gestió centralitzada de dispositius Omada amb el controlador Omada SDN.

- Router Omada
- Switch Jetstream
- EAP Omada



Il·lustració 22 - Entorn configuració TP-Link sense Omada

Amb el mode controlador comptem amb dos rames diferents:

- El controlador hardware (OC200/OC300): Controlador de software Omada incorporat, gestió local a traves del port 80 per a HTTP i 443 per a HTTPS.
- El controlador software:
    - Administrar controlador via web:
        - Gestió Local (L2/L3)
        - Gestió via núvol
    - Administrar controlador via APP Omada
        - Administració local
        - Gestió via núvol

2.2.5 Alta disponibilitat

L'alta disponibilitat o HA (High Ability) es una característica fonamental a les infraestructures TI, especialment per a Pimes. L'alta disponibilitat fa referencia a la capacitat de un sistema per a continuar funcionant i proporcionar servicis operatius a pesar de fallades o interrupcions.

A una PIME, la implementació de solucions de alta disponibilitat assegura que els sistemes i aplicacions critiques estiguen sempre accessibles, minimitzant el temps d'inactivitat i les pèrdues associades.

Importància de la Alta Disponibilitat a un PIME

Continuïtat del Negoci

- Operacions Ininterrompudes: L'alta disponibilitat permet que les operacions comercials continuen funcionant sense interrupcions, fins i tot en cas de fallades de hardware, software o xarxes.
- Reducció del Temps d'Inactivitat: Minimitza el temps d'inactivitat, la qual cosa és crucial per a mantenir la productivitat i evitar pèrdues econòmiques.

Confiança i Reputació

- Fiabilitat del Servici: Proporcionar un servici fiable i continu millora la confiança dels clients i socis, la qual cosa pot ser un factor diferenciador en mercats competitius.
- Imatge Corporativa: La capacitat de mantenir servicis sense interrupcions projecta una imatge de solidesa i professionalisme.

Protecció de Dades

- Seguretat i Recuperació: Implementar sistemes redundants i mecanismes de suport assegura que les dades estiguen protegides i puguen recuperar-se ràpidament en cas de fallades.

Competitivitat

- Millora Operacional: Permet a l'empresa mantenir un nivell operatiu òptim, la qual cosa pot traduir-se en un avantatge competitiu en termes de servici al client i eficiència operativa.

Entre les diverses estratègies que comptem per a implementar l'alta disponibilitat a les empreses en qüestió de xarxes, destaquem:

Redundància de hardware

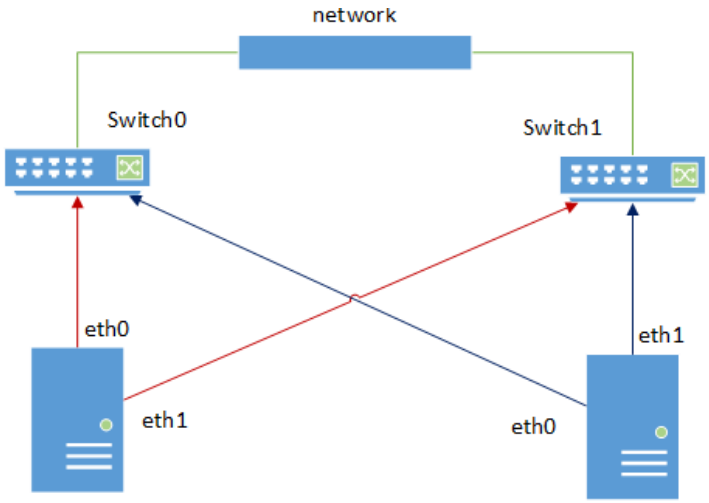
Gateway redundats: be siga un Firewall o un Router, duplicar la porta d'accés i eixida de la nostra xarxa ens donarà sempre la tranquil·litat que si falla un, seguirem tenint accés a internet i les operacions no es veuran afectades

Enllaços d'internet redundats: Implementar mes de un camí entre els dispositius que interconnecten la xarxa de l'empresa amb internet, contractant difunts ISP per a assegurar-nos que tenim servici si una companyia esta sofrint interrupcions al seu servici.

Agregació de enllaços: Combinació de múltiples interfases de xarxa en una sola connexió lògica. Esta tècnica a part de millorar la redundància i proporcionar una major tolerància a fallades, també ens pot servir per a augmentar el bandwidth (amplada de banda).

2.2.5.1 Bonding

El Bonding es la tècnica que s'utilitza a les xarxes per a millorar el rendiment i la fiabilitat de la connexió. El Bonding que consisteix en l'agregació d'enllaços (link aggregation) proporciona l'augment del bandwidth però mes important en alguns casos, la redundància i la tolerància a fallades.



Il·lustració 23 - Bonding

El Bonding compta amb diferents modes de configuració:

Round-Robin

- Distribució equitativa: El tràfic es distribuix de manera equitativa i seqüencial entre totes les interfases disponibles.
- Avantatges: Millora el rendiment general al utilitzar totes les interfases simultàniament.
- Desavantatges: Pot causar problemes de re-ordenament de paquets en certs entorns de xarxa.

Active-Backup (Actiu-Passiu)

- Commutació per error: Sols una Interface esta activa en qualsevol moment i les altres actuen com a Backup. Si la Interface activa falla, una de les passives agafa el seu lloc.
- Avantatges: Proporciona redundància i simplicitat

- Desavantatges: No augmenta tot el bandwidth disponible de la xarxa.

Mode Balanceig-XOR (Exclusive OR)

- Assignació de Trànsit: Assigna el trànsit a una Interface específica basada en una fórmula XOR entre les adreces MAC d'origen i destinació.
- Avantatge: Proporciona balanceig de càrrega eficient i manté l'orde dels paquets.
- Desavantatge: Requerix compatibilitat amb la configuració del switch de xarxa.

Mode Balanceig-TLB (Transmit Load Balancing)

- Balanceig de Càrrega de Transmissió: Equilibra la càrrega de transmissió de manera dinàmica entre les interfícies, sense requerir suport especial del switch.
- Avantatge: Millora el rendiment sense necessitat de configuració específica en el switch.
- Desavantatge: No balanceja la càrrega de recepció.

Mode Balanceig-ALB (Adaptive Load Balancing)

- Balanceig de Càrrega Adaptatiu: Proporciona balanceig de càrrega tant de transmissió com de recepció adaptant-se dinàmicament a les condicions de la xarxa.
- Avantatge: Oferix un balanceig de càrrega complet i millora el rendiment general.
- Desavantatge: Pot ser més complex de configurar i administrar.

2.2.5.2 LACP (Link Aggregation Control Protocol)

El LACP definit al estàndard IEEE 802.3ad es el protocol que ens permet combinar diverses interfases de xarxa física a un sol enllaç lògic. Es un protocol que treball en capa dos (L2) i que destinat en part a equips com switch.

Permet que els equips estableixen la agrupació automàtica de enllaços amb l'ús de paquets LACP al seu peer. Açò s'aconseguix gracies a que el protocol compta amb detecció i configuració dinàmica amb el continu reenviament de LACPDUs (Link Aggregation Control Protocol Data Units), paquets per a la detecció i configuració de enllaços agregats.

Aquet protocol compta amb failover, es a dir, quan LACP detecta alguna fallada en un dels enllaços, redirigix el tràfic als enllaços operatius restants, assegurant la continuïtat del servici.

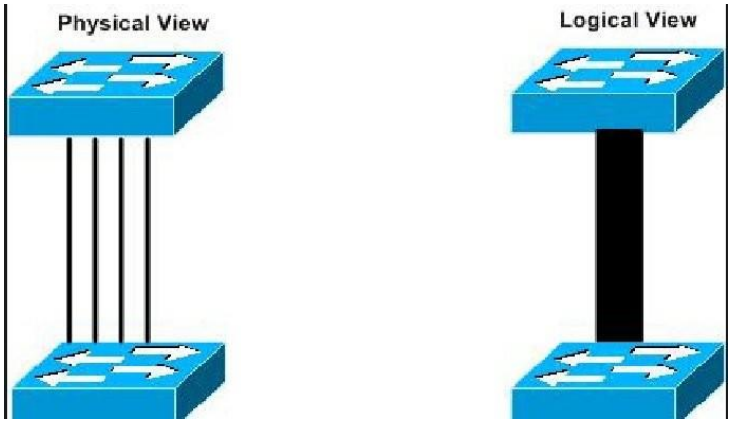
Modes de treball de LACP

- **Mode Actiu**
  - Envia i rep LACPDUs a traves dels ports actius per a sol·licitar la agregació de enllaços i responen a les sol·licituds d'altres ports.
  - Negociació Activa: Participa activament en la negociació de enllaços.

- **Mode Passiu**
    - Respon a LACPDUs: Els ports en mode passiu sol responen a les sol·licituds de LACPDU, sense iniciar-les.
    - Negociació Reactiva: Només s'agrega a l'agregació d'enllaços si un port en mode actiu el sol·licita.

Procés d'Agregació d'Enllaços amb LACP

1. **Intercanvi de LACPDUs**
    - Detecció d'Enllaços: Els dispositius intercanvien LACPDUs per a identificar quines interfícies poden agregar-se.
    - Negociació de Paràmetres: Paràmetres com a velocitat de l'enllaç, mode duplex i capacitats són negociats.
2. **Formació del LAG (Link Aggregation Group)**
    - Configuració del Grup: Una vegada que els enllaços són identificats i negociats, s'agrupen en un LAG.
    - Balanceig de Càrrega: El trànsit de xarxa es distribuïx a través dels enllaços en el LAG usant l'algorisme de hash configurat.
3. **Supervisió i Manteniment**
    - Monitoratge Continu: LACP supervisa l'estat dels enllaços en el LAG, enviant LACPDUs regularment per a verificar la seua operativitat.
    - Maneig de Fallades: En cas de fallada, LACP ajusta la configuració del LAG per a excloure l'enllaç fallit i redistribuir el trànsit.



Il·lustració 24 - LACP

2.3 Disseny de sistemes

El disseny de sistemes és un aspecte fonamental en la planificació i desenvolupament de la infraestructura tecnològica d'una organització. Este procés implica la creació d'una arquitectura que permeta integrar i optimitzar diversos components tecnològics per a complir amb els objectius empresarials. En el context modern, tres elements clau destaquen en el disseny de sistemes: els Sistemes de Planificació de Recursos Empresarials, la virtualització i la gestió de dades.

Objectius del Disseny de Sistemes per a una PIME

- Eficiència Operativa: Proveir una infraestructura que permeta als empleats fer les seues tasques de manera eficient, utilitzant ferramentes i aplicacions que milloren la productivitat i faciliten la col·laboració interna.
- Seguretat de la Informació: Implementar mesures de seguretat robustes per a protegir les dades crítiques de l'empresa contra amenaces internes i externes, garantint la confidencialitat, integritat i disponibilitat de la informació.
- Escalabilitat: Dissenyar sistemes que puguen créixer i adaptar-se conforme l'empresa s'expandix, evitant la necessitat de fer canvis disruptius o costosos en la infraestructura tecnològica.
- Continuïtat del Negoci: Assegurar la disponibilitat dels sistemes i la capacitat de recuperació davant desastres, minimitzant el temps d'inactivitat i assegurant la continuïtat operativa en cas de fallades.
- Reducció de Costos: Optimitzar els recursos tecnològics per a reduir els costos operatius, mitjançant la utilització de tecnologies com la virtualització, servicis en el núvol i consolidació de servidors.

Metodologia del Disseny

El desenvolupament del disseny de sistemes per a una PIME s'abordarà a través d'una metodologia estructurada que inclou les següents fases:

- Anàlisi de Requeriments: Identificar les necessitats tecnològiques específiques de l'empresa, incloent-hi les aplicacions crítiques, els fluxos de treball, els usuaris i les càrregues de treball.
- Disseny de l'Arquitectura: Proposar una arquitectura de sistemes que complisca amb els requeriments identificats, la selecció de hardware i software, i la implementació de mesures de seguretat.
- Implementació i Configuració: Desenvolupar i implementar la solució tecnològica, servidors, sistemes d'emmagatzematge i aplicacions.
- Proves i Validació: Realitzar proves exhaustives per a assegurar que la infraestructura complix amb els requisits funcionals i de rendiment, i validar el seu correcte funcionament en escenaris operatius reals.
- Documentació i Formació: Documentar detalladament la configuració i els procediments operatius.

2.3.1 ERP

Un ERP (Enterprise Resource Planning), o Planificació de Recursos Empresarials, és un sistema de software integral que permet a les organitzacions gestionar i automatitzar diversos processos de negoci en una plataforma unificada. Els ERP integren múltiples funcions empresarials, facilitant la coordinació i el flux d'informació entre diferents àrees de l'empresa, com ara finances, recursos humans, producció, vendes, inventari i més.

Característiques d'un ERP

- Integració de Mòduls
- Base de dades Centralitzada
- Automatització de Processos
- Estadístiques i Anàlisi

Tendències Actuals en ERP

- ERP en el Núvol: Cada vegada més empreses opten per solucions ERP basades en el núvol a causa de la seua flexibilitat, escalabilitat i menor cost inicial.
- Intel·ligència Artificial i Machine Learning: Els ERP estan incorporant tecnologies de IA i ML per a millorar l'automatització, anàlisi predictiva i presa de decisions.
- Mobilitat: La capacitat d'accedir al ERP des de dispositius mòbils permet als empleats treballar des de qualsevol lloc, millorant l'eficiència i la col·laboració.
- Internet de les Coses (IoT): La integració de IoT amb ERP ajuda a les empreses a gestionar millor els seus actius i optimitzar la cadena de subministrament.

2.3.1.1 WinOmega

Software català amb inicis al any 1989, comença a desenvolupar el software OMEGA MS-DOS. No es fins a 1999 quan es llança la versió que fins ara coneguem com a WinOmega.

Està dissenyat per a ajudar a petites i mitjanes empreses (Pimes) en l'administració de diverses àrees del seu negoci. WinOmega oferix mòduls per a la gestió d'inventaris, vendes, compres, facturació, comptabilitat i més. Algunes de les seues característiques principals:

- **Gestió d'Inventaris**: Permet portar un control detallat de l'estoc, gestionar magatzems, realitzar ajustos d'inventari i generar informes relacionats.
- **Vendes i Compres**: Facilita l'emissió de factures, albarans, pressupostos i comandes. A més, permet gestionar proveïdors i clients, portant un historial detallat de les transaccions.
- **Comptabilitat**: Inclou funcions per a portar la comptabilitat general de l'empresa, gestionar comptes per cobrar i per pagar, així com generar balanços i estats financers.

- **Facturació**: Automatitza el procés de facturació, permetent emetre factures electròniques i portar un registre detallat d'estes.
- **Informes i Anàlisis**: Oferix ferramentes per a generar una àmplia varietat d'informes i anàlisis que ajuden en la presa de decisions estratègiques.
- **Integració i Personalització**: El software és flexible i pot integrar-se amb altres ferramentes i sistemes utilitzats per l'empresa. També permet una certa personalització per a adaptar-se a les necessitats específiques de cada negoci.

WinOmega és conegut per la seua interfície amigable i la seua capacitat per a adaptar-se a diferents sectors industrials, la qual cosa el convertix en una opció popular entre les Pimes a Espanya i altres països de parla hispana.

2.3.1.2 SAGE Contaplus Elite

Contaplus Elite és un software de comptabilitat desenvolupat per Sage, una empresa coneguda per les seues solucions de gestió empresarial i comptabilitat. Contaplus és part d'una sèrie de productes dissenyats específicament per a ajudar petites i mitjanes empreses (Pimes) a gestionar les seues finances de manera eficient. Entre les seues característiques principals destaquen:

- **Comptabilitat General**: Facilita la comptabilitat general de l'empresa, incloent-hi la gestió d'assentaments comptables, balanços, i comptes anuals.
- **Gestió d'Impostos**: Inclou ferramentes per a la gestió d'impostos, com l'IVA i altres impostos locals, permetent una correcta presentació de les declaracions fiscals.
- **Pla General Comptable**: Adaptat al Pla General de Comptabilitat (PGC) espanyol, assegurant el compliment de les normatives comptables vigents.
- **Gestió de Comptes a Pagar i Cobrar**: Permet el seguiment dels comptes per cobrar i per pagar, facilitant la gestió de la tresoreria i el flux de caixa.
- **Informes Financers**: Oferix una àmplia varietat d'informes financers i comptables que ajuden en la presa de decisions, incloent-hi balanços, comptes de resultats, i altres informes personalitzats.
- **Conciliació Bancària**: Ferramentes per a la conciliació dels moviments bancaris amb els registres comptables de l'empresa.
- Integració amb Altres Sistemes: Pot integrar-se amb altres productes de Sage i software de tercers, facilitant la gestió integrada de l'empresa.

Contaplus Elite és una de les versions més avançades d'esta sèrie de productes, oferint funcionalitats addicionals i major capacitat de personalització per a adaptar-se a les necessitats específiques de cada empresa. És una ferramenta robusta i de confiança per a la gestió comptable, popular entre els comptables i administradors de Pimes a Espanya.

2.3.2 Virtualització

La virtualització és una tecnologia que permet la creació d'una versió virtual de recursos físics, com a servidors, emmagatzematge i xarxes, utilitzant software especialitzat. En lloc de dependre de múltiples màquines físiques, la virtualització permet que diverses màquines virtuals (VMs) operen en un sol servidor físic, compartint recursos de manera eficient. Esta tecnologia ha transformat la forma en què les empreses gestionen la seua infraestructura, proporcionant una major flexibilitat, escalabilitat i optimització de recursos.

Tipus de Virtualització

- **Virtualització de Servidors**: Consistix en particionar un servidor físic en diversos servidors virtuals, cadascun amb el seu propi sistema operatiu i aplicacions.
- **Virtualització d'Emmagatzematge**: Agrupa múltiples dispositius d'emmagatzematge físic en un únic dispositiu d'emmagatzematge virtual.
- **Virtualització de Xarxes**: Permet crear xarxes virtuals independents dins d'una mateixa infraestructura física, millorant la gestió i la seguretat de la xarxa.

Il·lustració 25 - Virtualització

Història i Evolució

La virtualització no és una tecnologia nova, els seus orígens es remunten a la dècada de 1960 amb la creació de màquines virtuals en mainframes. No obstant això, la seua adopció s'ha accelerat en les últimes dos dècades a causa dels avanços en la tecnologia de hardware i software, així com a la creixent demanda de solucions més eficients i flexibles en la gestió de TI (Tecnologies de la Informació).

Avantatges de la Virtualització

La virtualització oferix una sèrie d'avantatges significatius per a les empreses, especialment quan es tracta de sistemes de planificació de recursos empresarials (ERP). Algunes dels principals avantatges inclouen:

- **Reducció de Costos**: En consolidar múltiples servidors físics en un sol servidor virtual, les empreses poden reduir significativament els costos de hardware, energia i manteniment.
- **Flexibilitat i Escalabilitat**: La virtualització permet escalar recursos fàcilment segons les necessitats del ERP, millorant la capacitat de resposta als canvis en la demanda del negoci.
- **Recuperació davant Desastres i Continuïtat del Negoci**: La virtualització facilita la creació de còpies de seguretat i la recuperació davant desastres, assegurant la continuïtat del negoci en cas de fallades del sistema.
- **Optimització de Recursos**: Millora la utilització dels recursos de harware, permetent a les empreses maximitzar la seua inversió en infraestructura.
- **Facilitat de Gestió i Manteniment**: Simplifica la gestió de la infraestructura TI, permetent l'administració centralitzada i reduint el temps d'inactivitat durant el manteniment.

Requisits per a Virtualitzar un ERP

Per a virtualitzar un ERP de manera efectiva, és necessari complir amb uns certs requisits tècnics i d'infraestructura. Entre els més importants es troben:

- **Capacitat de hardware**: Un servidor robust amb suficient CPU, memòria RAM i emmagatzematge per a suportar les càrregues de treball del ERP.
- **Compatibilitat del software ERP**: Verificar que el software ERP siga compatible amb l'entorn de virtualització seleccionat.
- **Redundància i Alta Disponibilitat**: Implementar solucions de redundància i alta disponibilitat per a minimitzar el risc de fallades i assegurar el rendiment continu del ERP.
- **Xarxa d'Alta Velocitat**: Una xarxa ràpida i de confiança és essencial per a garantir la comunicació eficient entre els servidors virtuals i els usuaris finals.
- **Seguretat**: Implementar mesures de seguretat adequades per a protegir les dades i les aplicacions del ERP en l'entorn virtual.

Software de Virtualització

Existixen diversos software de virtualització en el mercat, cadascun amb les seues pròpies característiques i avantatges. A continuació, es presenta una comparativa d'alguns dels més populars:

VMware vSphere/ESXi

- Avantatges:
  - Alta fiabilitat i rendiment.
  - Àmplia gamma de funcionalitats avançades (vMotion, DRS, HA).
  - Gran suport i comunitat activa.
- Desavantatges:
  - Cost elevat.
  - Complexitat en la configuració inicial.

Microsoft Hyper-V

- Avantatges:
  - Integració amb l'ecosistema de Microsoft.
  - Menor cost en comparació amb VMware.
  - Bones funcionalitats de gestió i recuperació.
- Desavantatges:
  - Menor maduresa en algunes característiques avançades.
  - Requerix sistemes operatius Windows.

Oracle VM VirtualBox

- Avantatges:
  - Gratuït i de codi obert.
  - Fàcil d'usar i configurar.
  - Compatible amb múltiples sistemes operatius.
- Desavantatges:
  - Menor rendiment en comparació amb solucions comercials.
  - Menys adequat per a entorns de producció empresarial a gran escala.

KVM (Kernel-based Virtual Machine)

- Avantatges:
  - Integrat en el kernel de Linux.
  - Bona escalabilitat i rendiment.
  - Lliure i de codi obert.
- Desavantatges:
  - Corba d'aprenentatge pronunciada.
  - Menor suport comercial comparat amb VMware o Hyper-V.

Proxmox VE

- Avantatges:
  - Gratuït i de codi obert.
  - Suport per a contenidors i màquines virtuals.
  - Gestió centralitzada a través d'una interfície web intuïtiva.
  - Alta disponibilitat i replicació integrada.
- Desavantatges:
  - Menor suport comercial comparat amb VMware.
  - Corba d'aprenentatge inicial per a usuaris nous.

2.3.2.1 VMware ESXi

VMware ESXi és una de les solucions de virtualització més robustes i àmpliament adoptades en el mercat. A continuació, es detallen algunes de les seues característiques clau i beneficis específics:

Característiques Clau de ESXi

- **Hypervisor Bare-Metall**: ESXi és un hipervisor de tipus 1 que s'instal·la directament sobre el hardware, proporcionant un millor rendiment i seguretat.
- **Gestió Avançada**: Ferramentes com vCenter Server permeten la gestió centralitzada de múltiples hosts ESXi, facilitant l'administració de grans infraestructures virtuals.
- **Funcionalitats Avançades**: Suporta característiques avançades com vMotion (migració en viu de màquines virtuals), DRS (Distributed Resource Scheduler) i HA.
- **Seguretat i Compliment**: Inclou diverses característiques de seguretat, com el xifratge de màquines virtuals i el compliment de normatives.

Hipervisor

És un software que permet la creació i gestió de màquines virtuals (VMs) en un únic hardware físic. Actua com una capa intermèdia entre el hardware del servidor i els sistemes operatius de les VMs, permetent que múltiples sistemes operatius i aplicacions s'executen simultàniament en el mateix servidor físic. Els hipervisors poden ser de tipus 1 (bare-metall), que s'executen directament sobre el hardware, o de tipus 2 (hosted), que s'executen sobre un sistema operatiu amfitrió.

Beneficis Específics per a ERP

- **Rendiment i Fiabilitat**: ESXi oferix un rendiment excel·lent, essencial per a aplicacions ERP que requerixen alta disponibilitat i fiabilitat.
- **Escalabilitat**: Permet escalar recursos de manera eficient per a adaptar-se al creixement del ERP.
- **Reducció de Costos Operatius**: Encara que el cost inicial pot ser alt, l'optimització de recursos i la reducció de temps d'inactivitat compensen a llarg termini.

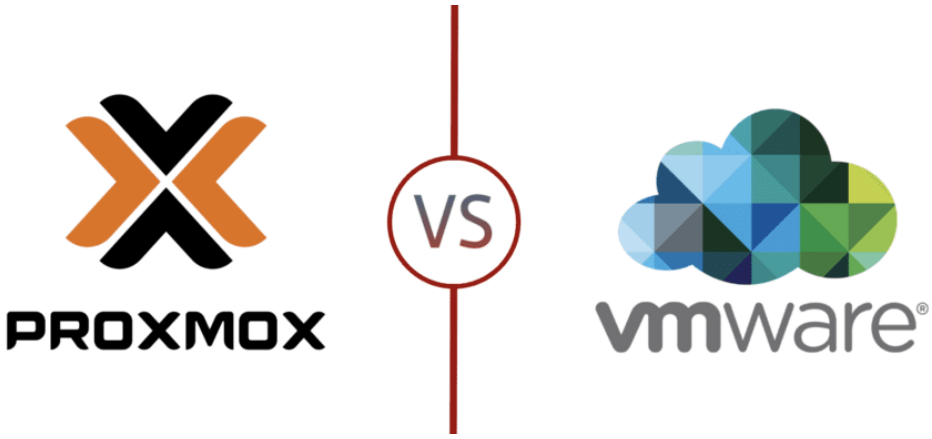
Comparativa: ESXi vs. Altre software de Virtualització

- **Cost**: ESXi sol ser més costós que solucions com Hyper-V o KVM, però oferix una gamma més àmplia de funcionalitats i millor suport.
- **Rendiment**: ESXi generalment proporciona un rendiment superior a causa de la seua arquitectura bare-metall.
- **Facilitat d'Ús**: Hyper-V pot ser més fàcil d'integrar en entorns Windows, mentres que ESXi oferix una interfície d'usuari robusta i rica en funcions.
- **Funcionalitats**: ESXi lidera en termes de característiques avançades, encara que requerix una inversió inicial major.

ESXi vs. Proxmox VE

- **Cost**:
    - ESXi: Generalment més costós a causa de les llicències i suport comercial.
    - Proxmox VE: Gratuït i de codi obert, encara que el suport empresarial té cost addicional.

- **Rendiment**:
  - ESXi: Oferix un rendiment superior a causa de la seua arquitectura bare-metall.
  - Proxmox VE: Bon rendiment, especialment amb la gestió de contenidors i KVM, però pot variar segons la configuració.
- **Facilitat d'Ús**:
  - ESXi: Oferix una interfície d'usuari robusta i rica en funcions, però pot ser complexa per als nous usuaris.
  - Proxmox VE: Gestió centralitzada a través d'una interfície web intuïtiva, fàcil d'usar per a la majoria dels usuaris.
- **Funcionalitats**:
  - ESXi: Lidera en termes de característiques avançades com vMotion, DRS i HA.
  - Proxmox VEU: Suporta tant contenidors com màquines virtuals, alta disponibilitat i replicació integrada, encara que pot mancar d'algunes característiques avançades de VMware.
- **Suport i Comunitat**:
  - ESXi: Ampli suport comercial i una comunitat activa.
  - Proxmox VE: Comunitat activa i suport comercial disponible, encara que menys extensa que VMware.



Il·lustració 26 - Proxmox vs ESXi VMware

En conclusió, l'elecció d'una solució de virtualització per a un ERP ha de basar-se en una anàlisi detallada de les necessitats específiques de l'empresa, el pressupost disponible i les capacitats del software de virtualització en qüestió. VMware ESXi, encara que més costós, proporciona una solució completa i altament eficient per a entorns empresarials crítics.

2.3.3 Gestió de dades

La gestió de dades és un conjunt de pràctiques i procediments utilitzats per a administrar, protegir i optimitzar l'ús de les dades dins d'una organització. Este procés inclou la recopilació, emmagatzematge, organització, manteniment i protecció de les dades per a garantir la seua disponibilitat, integritat i seguretat. En un entorn empresarial, la gestió de dades és indispensable per diverses raons:

- **Presa de decisions Informada**: Les dades precises i accessibles permeten a les empreses prendre decisions basades en informació real i actualitzada.
- **Compliment Normatiu**: Les empreses han de complir amb diverses normatives i regulacions sobre la protecció i privacitat de les dades.
- **Continuïtat del Negoci**: La protecció adequada de les dades assegura que les operacions puguen continuar fins i tot en cas de desastres o fallades del sistema.
- **Optimització de Recursos**: Una gestió eficient de les dades permet a les empreses utilitzar millor els seus recursos tecnològics i humans.

Mètodes de Gestió de Dades

Regla del 3-2-1

Un dels mètodes més recomanats per a la gestió de còpies de seguretat és la regla del 3-2-1. Esta estratègia assegura que les dades estiguen protegides contra una àmplia varietat de riscos. La regla consistix en:

- **3 Còpies de les Dades**: Mantindre almenys tres còpies de les dades: l'original i dos còpies de seguretat.
- **2 Tipus d'Emmagatzematge Diferents**: Emmagatzemar les còpies en almenys dos tipus de mitjans diferents (per exemple, discos durs i cintes).
- **1 Còpia Fora del Lloc**: Guardar almenys una de les còpies de seguretat en una ubicació física separada de la ubicació principal per a protegir les dades contra desastres locals.

Altres Mètodes de Gestió de Dades

- **Còpia de seguretat Incremental i Diferencial**: Les còpies de seguretat incrementals només copien les dades que han canviat des de l'última còpia de seguretat, mentres que els diferencials copien totes les dades que han canviat des de l'última còpia de seguretat completa. Tots dos mètodes ajuden a reduir el temps i l'espai d'emmagatzematge necessaris per a les còpies de seguretat.
- **Snapshots**: Els snapshots són còpies instantànies de l'estat d'un sistema en un moment específic. Són útils per a recuperacions ràpides i poden ser programades a sovint per a minimitzar la pèrdua de dades.
- **Replica de Dades**: La replicació de dades implica copiar dades d'un servidor a un altre en temps real o quasi en temps real. Això assegura una alta disponibilitat i ràpida recuperació en cas de fallada.

Software de Gestió de Dades

Existixen diverses ferramentes i software especialitzat en la gestió de dades i còpies de seguretat que poden integrar-se en entorns virtualitzats. Un dels més destacats és Veeam.

2.3.3.1 Veeam Backup & Replication

Veeam Backup & Replication és una solució de gestió de dades i còpies de seguretat dissenyada específicament per a entorns virtualitzats. Les seues característiques clau inclouen:

- **Compatibilitat amb Entorns Virtualitzats**: Suporta múltiples plataformes de virtualització com VMware vSphere, Microsoft Hyper-V i Nutanix AHV.
- **Còpia de seguretat i Restauració Eficients**: Oferix còpia de seguretat completa, incremental i diferencial, així com restauració granular i ràpida de dades.
- **Replica de Màquines Virtuals**: Permet la replicació de màquines virtuals per a garantir l'alta disponibilitat i recuperació davant desastres.
- **Gestió Centralitzada**: Proporciona una interfície centralitzada per a gestionar totes les activitats de còpia de seguretat i recuperació.
- **Seguretat i Compliment**: Inclou funcionalitats per al xifratge de dades i compliment de normatives de protecció de dades.

Veeam Backup & Replication CE (Community Edition)

Encara que Veeam compta amb una gran gama de productes en funció a les necessitats de cada usuari i empresa, compta amb una versió gratuïta suportada per la comunitat.

Aquesta ens permet protegir carregues de treball virtuals, físiques i cloud i pot protegir fins a 10 carregues de treball: VMWare, Hyper-V, servidors Windows i Linux, portàtils, NAS i molt mes.

Il·lustració 27 - Funcionalitat Veeam

D'altra banda, al ser la versió gratuïta no compta amb suport ni assistència tècnica, encara que disposem de gran varietat de vídeos i guies de instal·lació de la comunitat.

Implementació de Veeam en Entorns Virtualitzats

Configuració Inicial

- **Instal·lació**: Veeam pot instal·lar-se en un servidor físic o en una màquina virtual dins de l'entorn virtualitzat.
- **Integració**: Configurar la integració amb la infraestructura de virtualització, com vSphere o Hyper-V, per a detectar i gestionar automàticament les màquines virtuals.
- **Emmagatzematge de Còpies de seguretat**: Configurar els repositoris de còpia de seguretat utilitzant emmagatzematge local, emmagatzematge en xarxa (NAS) o servicis d'emmagatzematge en el núvol.

Estratègies de Còpia de seguretat i Recuperació

- **Planificació de Còpies de seguretat**: Establir polítiques de còpia de seguretat que definisquen la freqüència i el tipus de còpies de seguretat (complet, incremental, diferencial).
- **Monitoratge i Reports**: Utilitzar les ferramentes de monitoratge i reports de Veeam per a assegurar que les còpies de seguretat es realitzen correctament i per a identificar qualsevol problema potencial.
- **Proves de Recuperació**: Realitzar proves regulars de recuperació per a assegurar-se que les còpies de seguretat siguen vàlides i que les dades puguen restaurar-se correctament.

Veeam Backup & Replication CE vs. Proxmox VE

Per a comprendre millor com Veeam Backup & Replication CE i Proxmox VE es comparen en termes de característiques, funcionalitats i casos d'ús, és important analitzar les seues fortaleses i debilitats específiques. A continuació es presenta una comparativa detallada entre totes dues solucions.

Veeam Backup & Replication CE

Característiques Clau:

- **Còpia de seguretat i Recuperació**: Oferix còpia de seguretat completa, incremental i diferencial. Suporta restauració granular i ràpida de dades, aplicacions i sistemes complets.
- **Replica de Màquines Virtuals**: Permet la replicació de VMs per a alta disponibilitat i recuperació davant desastres.
- Compatibilitat: Suporta múltiples plataformes de virtualització, incloent VMware vSphere i Microsoft Hyper-V.
- **Gestió Centralitzada**: Proporciona una interfície de gestió centralitzada per a totes les activitats de còpia de seguretat i recuperació.

- **Seguretat i Compliment**: Inclou funcionalitats de xifratge de dades i verificació automàtica de còpies de seguretat.
- **Limitacions de l'Edició Comunitària**: L'edició comunitària és gratuïta però limitada a la protecció de fins a 10 instàncies (màquines virtuals, servidors físics, etc.).

Avantatges:

- **Alta Fiabilitat i Rendiment**: Confiabilitat en operacions de còpia de seguretat i recuperació.
- **Funcionalitats Avançades**: Característiques robustes fins i tot en l'edició comunitària.
- **Compatibilitat**: Suporta múltiples plataformes de virtualització.
- **Cost**: Gratuït per a fins a 10 instàncies.

Desavantatges:

- **Limitacions en Capacitat**: Limitat a 10 instàncies, la qual cosa pot no ser suficient per a empreses mitjanes o grans.
- **Configuració i Gestió**: Pot ser complex per a usuaris sense experiència prèvia.
- **Suport**: Suport limitat en l'edició comunitària.

Proxmox VE

Característiques Clau:

- **Virtualització Combinada**: Suporta tant KVM (per a virtualització completa) com LXC (per a contenidors lleugers).
- **Gestió de Còpies de seguretat**: Funcionalitats integrades de còpia de seguretat i restauració.
- **Interfície Web Centralitzada**: Proporciona una interfície web intuïtiva per a la gestió de màquines virtuals i contenidors.
- **Alta Disponibilitat**: Suporta configuracions d'alta disponibilitat.
- **Codi Obert**: Gratuït i de codi obert, amb una versió empresarial disponible amb suport addicional.
- **Suport de Clústers**: Permet la creació i gestió de clústers de servidors per a millorar la disponibilitat i l'escalabilitat.

Avantatges:

- **Cost**: Gratuït i de codi obert, amb opció de subscripció per a suport comercial.
- **Flexibilitat**: Suport per a KVM i LXC, permetent una gestió flexible de recursos.
- **Interfície Intuïtiva**: Fàcil d'usar amb una interfície web robusta.
- **Alta Disponibilitat i Escalabilitat**: Suport natiu per a clústers i alta disponibilitat.
- **Comunitat Activa**: Gran comunitat d'usuaris i desenvolupadors.

Desavantatges:

- **Funcionalitats de Còpia de seguretat Menys Avançades**: Les funcionalitats de còpia de seguretat i recuperació no són tan avançades com les de Veeam.
- **Requerix Coneixements de Linux**: Pot requerir coneixements més profunds de Linux per a configuracions avançades.
- **Menys Integració amb Altres Sistemes**: Menys integració i suport per a plataformes no basades en Linux comparat amb Veeam.

Aspecte	Veeam Backup & Replication CE	Proxmox VE
Cost	Gratuït fins a 10 instancies	Gratuït
Tipus de Virtualització	No aplica (Software Backup)	KVM y LXC
Backup i restauració	Avançat amb backup complet, incremental i diferencial	Basic, integrat en la plataforma
Compatibilitat	VMWare vSphere, Microsoft Hyper-V	KVM, LXC, sistemes basats en Linux
Gestio centralitzada	Si	Si, via interfaz web
Seguretat	Xifrat de dades, verificació automàtica	Basic
Alta Disponibilitat (HA)	Si (Replica de VMs)	Si
Escalabilitat	Limitat a 10 instancies	Suport de clústers, altament escalable
Suport i Actualitzacions	Limitat en la edició de la comunitat	Comunitat activa, Opció de suport comercial

Conclusió

Veeam Backup & Replication CE és ideal per a petites empreses i entorns que no superen les 10 instàncies, oferint funcionalitats avançades de còpia de seguretat i recuperació amb alta fiabilitat. No obstant això, el seu ús gratuït està limitat en capacitat i suport.

Proxmox VE, d'altra banda, és una solució de virtualització completa i flexible, adequada per a una àmplia gamma d'aplicacions, des de petites empreses fins a grans centres de dades. La seua capacitat per a manejar tant KVM com LXC, juntament amb el suport per a clústers i alta disponibilitat, el fa extremadament escalable i adaptable. Encara que les seues capacitats de còpia de seguretat no són tan avançades com les de Veeam, oferix una bona solució integrada per a la gestió de màquines virtuals i contenidors en entorns Linux.

2.3.4 Alta disponibilitat

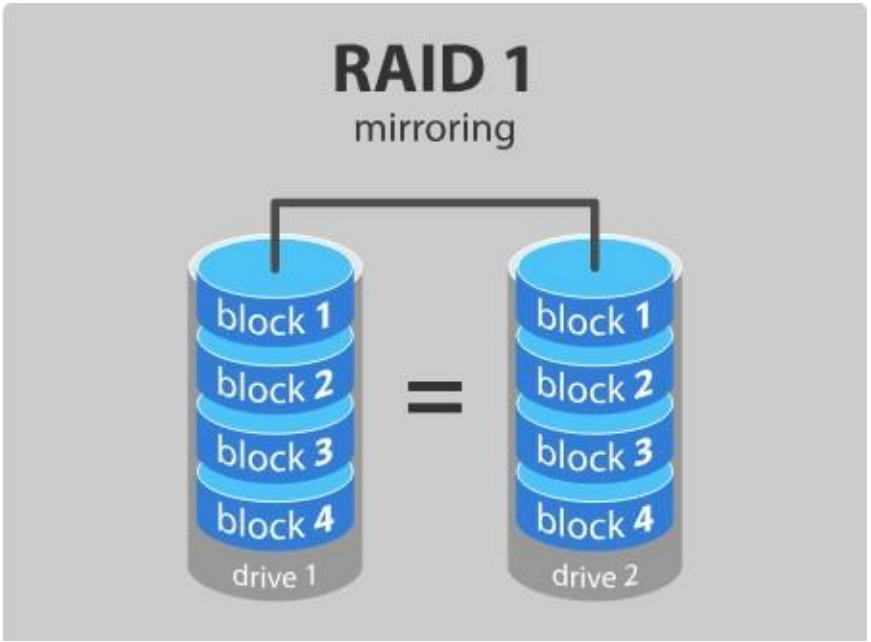
Parlant de l'alta disponibilitat al disseny de sistemes un dels punts mes importants es la redundància, es a dir, duplicar hardware ja siga físic com virtual. La practica mes freqüent per a aconseguir un sistema de alta disponibilitat es la redundància de discs.

2.3.4.1 RAID

Conjunt Redundant de Discs Independents o RAID (Redundant Array of Independent Disks), és una tecnologia d'emmagatzematge que combina múltiples discs durs per a millorar el rendiment, la redundància i la capacitat d'emmagatzematge d'un sistema. En distribuir les dades i/o la paritat entre diversos discos, els sistemes RAID poden oferir majors velocitats de lectura i escriptura, així com protecció contra fallades de disc.

Existixen diversos tipus de RAID, encara que els més comuns són:

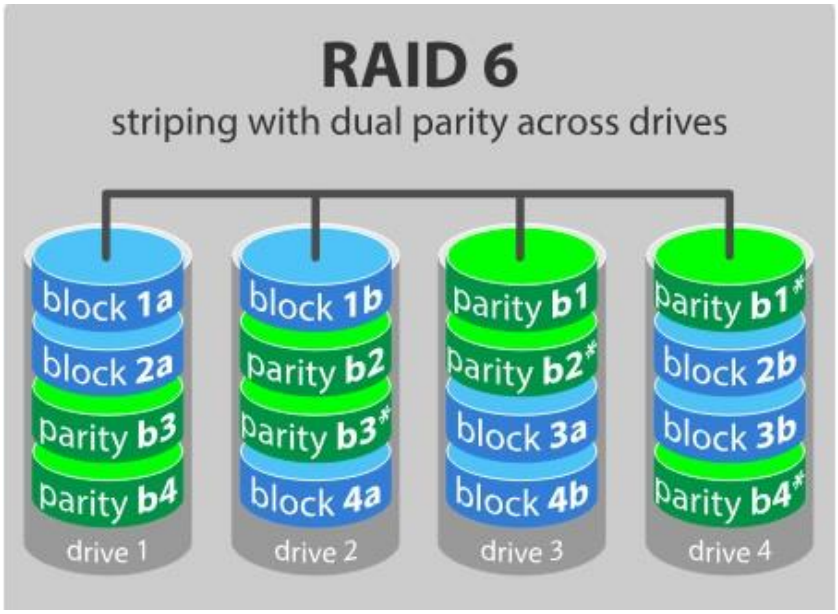
- **RAID 0**: Requerix almenys 2 discs. Dividix la informació entre els discs que formen part del RAID 0 per a tindre un accés més ràpid a les dades. Això fa que no siga redundant.
- **RAID 1**: Requerix almenys 2 discs. Configuració tipus espill. La informació s'escriu de manera simultània en els discs que formen el RAID. Per tant, tenim redundància, però el sistema reconeixerà un únic volum.



Il·lustració 28 - Raid 1

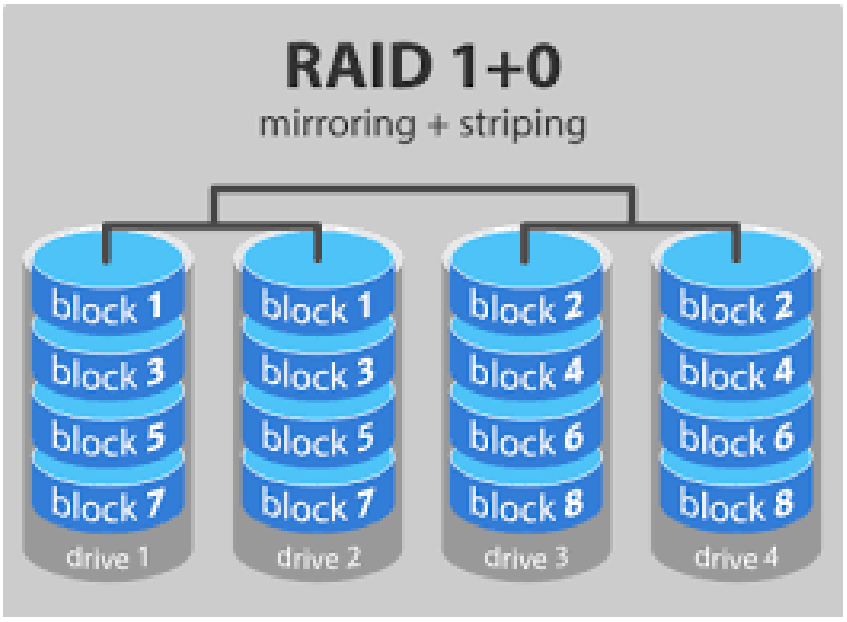
- **RAID 2**: Requerix almenys 3 discs. Els dos primers actuen com RAID 0 i el tercer com a verificador de dades. Com a característica, fa girar els discos en la mateixa orientació. Les dades es dividixen a nivell de bit i no de bloc.
- **RAID 5**: Requerix almenys 3 discs. Les unitats d'emmagatzematge es dividixen en blocs. Els blocs de cada disc són per a dades menys un que és per a paritat. Això permet la fallada d'un disc dur sense perdre les dades de tot el sistema RAID.

- **RAID 6**: Requerix almenys 4 discs. És la versió avançada de RAID 5. Té dos blocs de paritat. Augmenta la tolerància a fallades, per la qual cosa, poden fallar dos discs simultàniament.



Il·lustració 29 - RAID 6

- **RAID 01**: Requerix almenys 4 discos. És el resultat de combinar dos RAID 0 i unir-los amb un RAID 1 (RAID 0 + 1). Està pensat perquè tots els discos d'una configuració RAID 0 fallen. Té tolerància a fallades molt limitada.
- **RAID 10**: Requerix almenys 4 discs. És el resultat de combinar dos RAID 1 i unir-los amb un RAID 0 (RAID 1 + 0). Este sistema oferix redundància a dades i una elevada velocitat de lectura i escriptura.



Il·lustració 30 - Raid 10

3. Implementació pràctica

Una vegada posats en coneixement tots els fonaments teòrics necessaris per a abordar el projecte, començarem amb la part pràctica, que recollirà la guia de instal·lació i configuració i els protocols, tecnologies i procediments escollits i els perquè d'aquets.

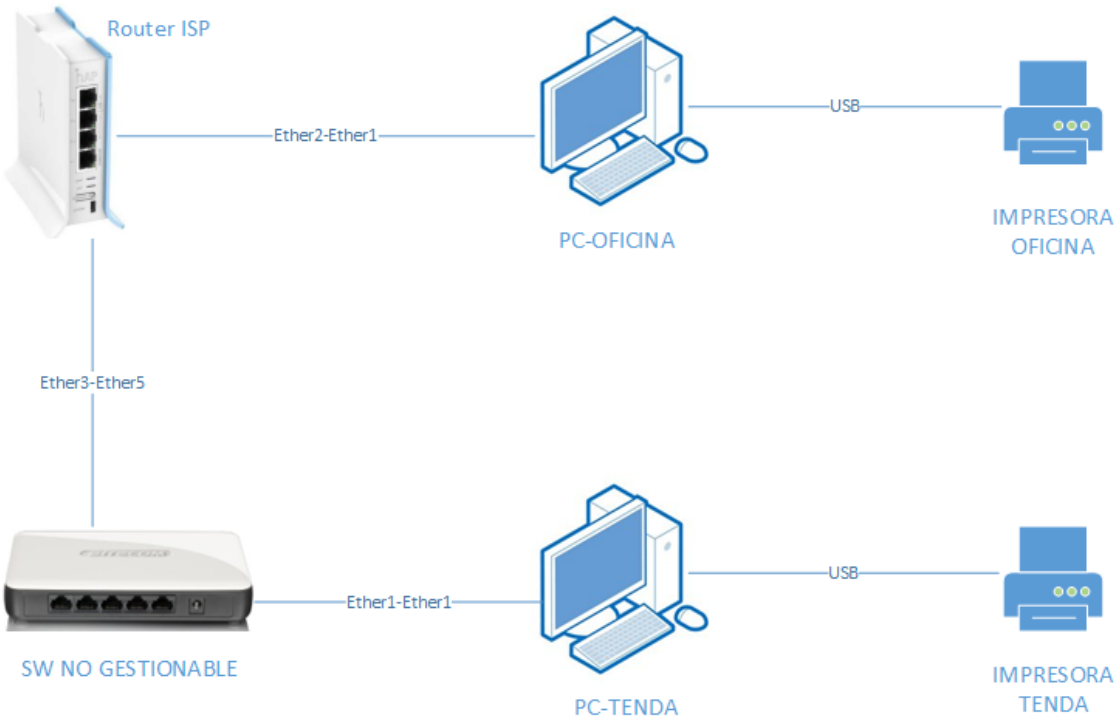
3.1 Disseny de xarxa

El disseny de xarxa s'estructurarà en dues parts, la primera, **situació inicial**, recollirà un anàlisis de com estava estructurada la xarxa, quina era la electrònica de la xarxa i com estaven connectats a aquesta, els equips informàtics que s'utilitzaven a la empresa.

La segona, **situació final**, mostrarà el procés de configuració i l'elecció dels equips per a millorar la infraestructura inicial de la xarxa.

3.1.1 Situació inicial

L'empresa compta amb una instal·lació inicial bàsica, com mostra el esquema següent:



Il·lustració 31 - Esquema de xarxa actual

Com s'aprecia al esquema, els dos equips de treball, estan connectats directament al Router de la companyia, aquest mateix Router es també l'encarregat de crear la xarxa Wireless. El equip de la tenda està connectat al Router a traves d'un switch no gestionable, es a dir en pla, que fa de enllaç via cable Ethernet amb la planta superior. El equip de l'oficina, penja directament del equip de la companyia ISP. Les impressores no estan connectades a la xarxa i esta tot en el mateix segment de xarxa o mateixa VLAN.

3.1.1.1 Router

El Router de la companyia ISP es un Mikrotik hAP Lite rb941, model que per a una oficina amb dos equips a priori podria ser suficient però no compta amb tecnologies Wireless actuals com Wi-Fi 6 (Actualment equips implementant Wi-Fi 7). El nombre de ports del Mikrotik es de quatre, contant que un dels ports es el que va connectat a la ONT (Optical Network Terminal), equip que convertix la senyal òptica de la fibra a una senyal Ethernet, ens deixa un total de tres ports lliures, però dos d'ells ja ocupats pels dos equips de treball, per lo tant sols disposem d'un port. D'altra banda, no disposem de les claus d'accés al equip degut a les polítiques de la companyia proveïdora d'internet. Per lo tant no podem crear túnels ni modificar paràmetres segons les nostres necessitats.

Ací algunes especificacions de la web del fabricant:

Wireless capabilities

Details	
Wireless 2.4 GHz Max data rate	300 Mbits/s
Wireless 2.4 GHz number of chains	2
Wireless 2.4 GHz standards	802.11b/g/n
Antenna gain dBi for 2.4 GHz	1.5
Wireless 2.4 GHz chip model	QCA9533
Wireless 2.4 GHz generation	Wi-Fi 4

Ethernet

Details	
10/100 Ethernet ports	4

El cablejat es de tipus Ethernet CAT 5, aquest cable es el mes antic de les categories actuals de cable de tipus Ethernet que comptem al mercat, esta pràcticament en desús ja que la seua velocitat de transmissió màxima es de 100 Mbps i esta dissenyat per a una freqüència de transmissió de 100 MHz.

Il·lustració 32 - Router Actual

Com es pot apreciar a la imatge, el Router esta deixat al terra, interferint en el pas del empleat que esta treballant a la oficina i amb part del cablejat a l'exterior sense estar passat per cap tipus de canaleta, fent-lo així vulnerable a ruptures i deteriorament per part dels usuaris.

3.1.1.2 Switch

L'instal·la cio compta amb un únic switch a la planta inferior, que servix per a connectar l'equip de la tenda a la xarxa, es un switch no gestionable de 8 ports, el que significa que no admet l'ús de VLANs, per lo que no es podria utilitzar per a la segmentació de la xarxa. Tampoc compta amb tecnologia PoE, el que impossibilita la instal·lació de equips de xarxa com APs en punts de la tenda que no disposen de endoll prop d'ells, com per exemple al sostre de la tenda.

Il·lustració 33 - Switch actual

Com s'aprecia a la imatge, el switch esta "protegit" per un poal amb bosses de plàstic al voltant, esta connectat al Mikrotik de la oficina via Ethernet i al equip de la tenda en altre port. S'observa que te un segon dispositiu sense cap tipus de funció connectat a ell. Configuració residual antiga.

Il·lustració 34 - Electrònica de xarxa residual

3.1.1.3 Xarxa Wireless

El dispositiu encarregar de la connexió wireless es el propi Router del ISP, com he comentat a les seues característiques, es un equip amb tecnologia Wi-Fi 4, tecnologia ja antiquada per a als dispositius mòbils del dia a dia.

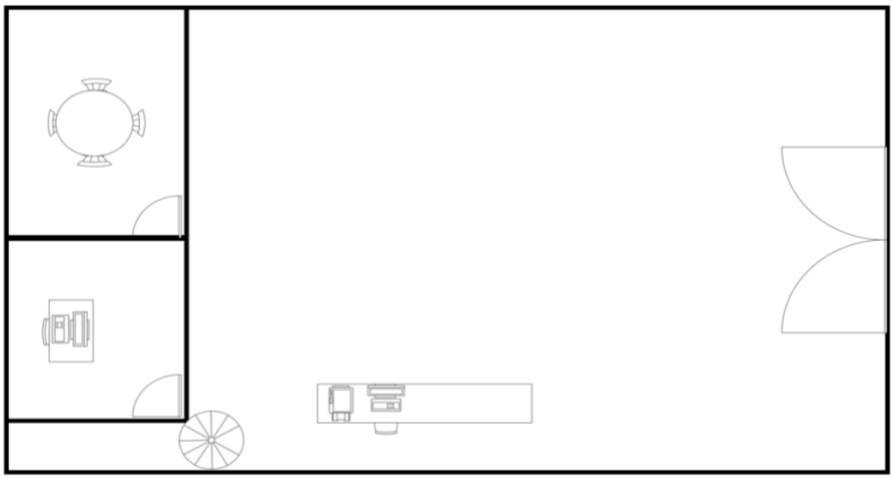
A l'empresa la xarxa Wireless es important per diversos motius:

- Connexió del empleats amb els dispositius mòbils
- Connexió del Datàfon (Terminal de cobro)
- Connexió a internet dels comercials i convidats.

Ekahau Heatmapper

Per a realitzar un estudi de la xarxa wireless, faig us d'un software que genera mapes de calor. Amb aquest software podrem analitzar quines son les zones mes critiques de l'oficina i quin es l'abast de la ona wireless.

Primer necessitarem comptar amb un plànol de la oficina o lloc a analitzar o pel contrari, dissenyar-lo amb les mesures reals del emplaçament.



Il·lustració 35 - Plànol oficina

L'empresa compta amb unes instal·lacions que es distribuixen en 8 metres de amplada per 15 de llargària. El Router esta situat a la oficina, que esta separada de la resta de la tenda per una paret de pladur, material que te una certa degradació de la ona wireless emesa pel Router.

La intensitat de senyal es mesura en dBm i s'expressa en valors negatius. Una major intensitat aporta una millor experiència de xarxa wireless.

Per a zones principals, la intensitat de la senyal deu de controlar-se en el rang de -40dBm a -65dBm. Per a zones secundaries, la senyal deu ser superior a -75dBm per a garantir la connexió wireless bàsica.

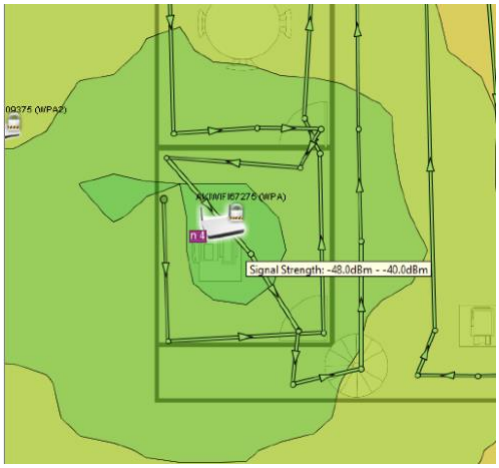
Sabent açò procedia a realitzar el mapa de calor, per a allò es necessari un equip Windows ja que el software es compatible únicament amb aquest sistema operatiu i connectar-se a la xarxa wireless de la empresa.

El procediment es el següent, partint des de el punt mes proper al Router, clicarem sobre el plànol, intentant ser el mes precisos possible respecte a la nostra ubicació en la empresa, aço ens crearà un punt al mapa. Després anirem recorrent cada instancia i racó de l'empresa clicant sobre el plànol en cada punt escollit, cal dir que quan mes punts realitzem sobre el plànol, mes precís serà el mapa de calor realitzat.

Il·lustració 36 - Mapa calor

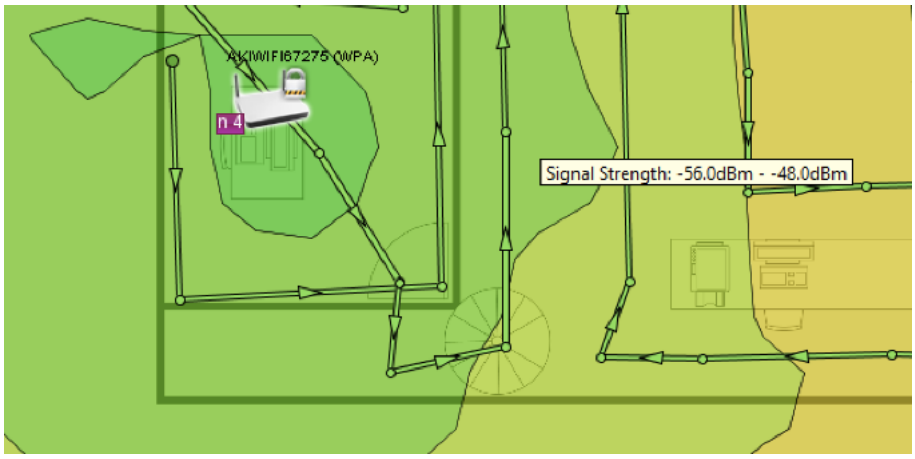
Una vegada realitzat el recorregut per l'empresa, el software ens representa un mapa de calor de l'abast de l'ona wireless a l'empresa.

Zona verd obscur: situada en una senyal de entre -48 a -40 dBm, excel·lent intensitat de senyal, tot el que estiga a aquest nivell obtindrà una experiència perfecta.



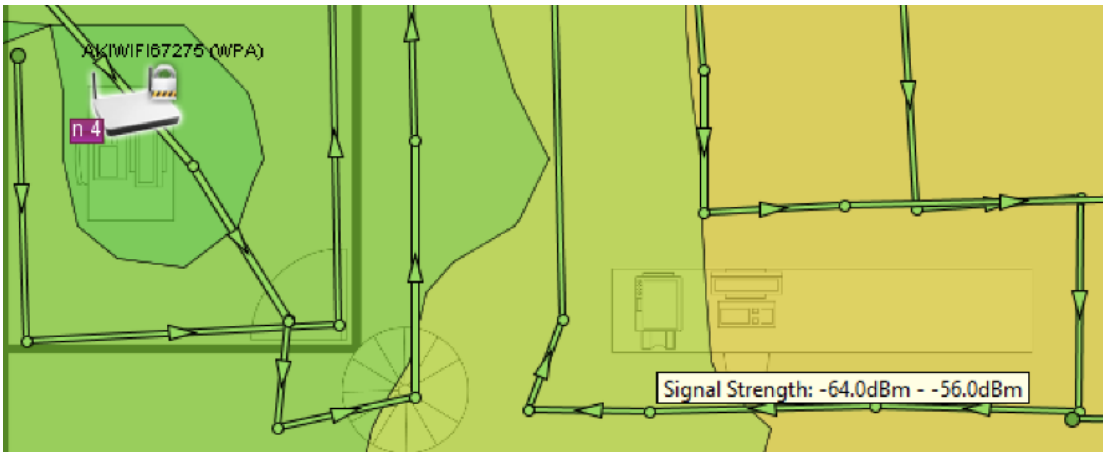
Il·lustració 37 - Zona wireless 1

Zona verd clar: situada en una senyal de entre -48 a -56dBm. La intensitat seguix sent bona i fiable.



Il·lustració 38 - Zona wireless 2

Zona groga: situada en una senyal de entre -56 a -64dBm, la intensitat no es molt forta, però per a algun tipus de navegació pot ser suficient



Il·lustració 39 - Zona wireless 3

Zona taronja: situada entre -64 a -72dBm, zona mes critica ja que el nivell de senyal mínim necessari per a establir una connexió es de -75dBm.

Il·lustració 40 - Zona wireless 4

3.1.2 Situació final

Una vegada analitzada la xarxa de la empresa i anotades les carències i punts vulnerables com son la xarxa wireless, la mala ubicació i protecció dels elements i la velocitat màxima de transmissió de dades degut al cablejat i també vegada recollides les necessitats del client, comence amb el disseny de la xarxa.

3.1.2.1 Segmentació

Se planteja un disseny amb quatre VLANs, es a dir, quatre segments de xarxa.

- VLAN 10 – Producció
- VLAN 20 – Convidats
- VLAN 50 – CCTV
- VLAN 99 – Gestió

VLAN 10 - PRODUCCIÓ:

Segment de xarxa on estaran els equips i recursos de la empresa, servidor, llocs de treball personals, dispositius mòbils, impressores, etc...

- Assignació dinàmica de IP per a PC i dispositius mòbils.
- Assignació estàtica de IP per a servidors de la xarxa.

VLAN 20 - CONVIDATS

Xarxa wireless que es crea a cada empresa o emplaçament on no volem que la gent externa a l'empresa tinga accés al recursos locals i ames queden aïllats per complet del tràfic de les xarxes d'aquesta. Només podran connectar-se mitjançant Wi-Fi a través dels AP instal·lats en l'empresa

- Assignació dinàmica de IP per als dispositius que es connecten a la xarxa.

VLAN 50 CCTV:

S'inclou un xicotet circuit de càmeres per petició expressa del client, ja que necessita seguretat a l'empresa, la qual fa anys no disposa de cap tipus de sistema. Tindran direccionalment IP estàtic

- Assignació estàtica de IP per a càmeres i sistemes de gravació.

VLAN 99 – GESTIÓ

VLAN per a manteniment i gestió dels equips per a l'administrador de la xarxa. Aquesta xarxa es fonamental en tots els dissenys de xarxa empresarial. Proporciona al administrador de la xarxa la flexibilitat per a accedir a qualsevol equip i recurs.

- Assignació estàtica de IP per als equips de la xarxa: Router, Switch, AP.
- Assignació estàtica de IP per als servidors.

3.1.2.2 Disseny de xarxa

Direccionament IP

Una vegada sabem les VLANs que anem a introduir a la nostra xarxa, hem de plantejar el direccionament IP que s'implementarà i quin seria el ordre d'assignació de IPs ja que es deurà de seguir a mesura que s'amplien la xarxa o el material informàtic de l'empresa. Cada VLAN es trobarà en un segment de xarxa diferent i com a tal deuran de tindre un direccionament diferent:

- VLAN 10 – Producció: 192.168.10.0/24
- VLAN 20 – Convidats: 192.168.20.0/24
- VLAN 50 – CCTV: 192.168.50.0/24
- VLAN 99 – Gestió: 192.168.99.0/24

VLAN 10 – Producció

- Assignació dinàmica de IP per a PC i dispositius mòbils.
    - Servidor DHCP (Dynamic Host Configuration Protocol)
        - 192.168.10.10 - 192.168.10.30
- Assignació estàtica de IP per a servidors de la xarxa.
    - A partir de la direcció: 192.168.10.100

VLAN 20 – Convidats

- Assignació dinàmica de IP per als dispositius que es connecten a la xarxa.
    - Servidor DHCP
        - 192.168.20.2 – 192.168.20.254

VLAN 50 - CCTV

- Assignació estàtica de IP per a càmeres i sistemes de gravació.
    - Gravador 192.168.50.100
    - Càmera 1: 192.168.50.101
    - Càmera 2: 192.168.50.102
    - ...
    - Càmera X: 192.168.50.1X

VLAN 99 – Gestió

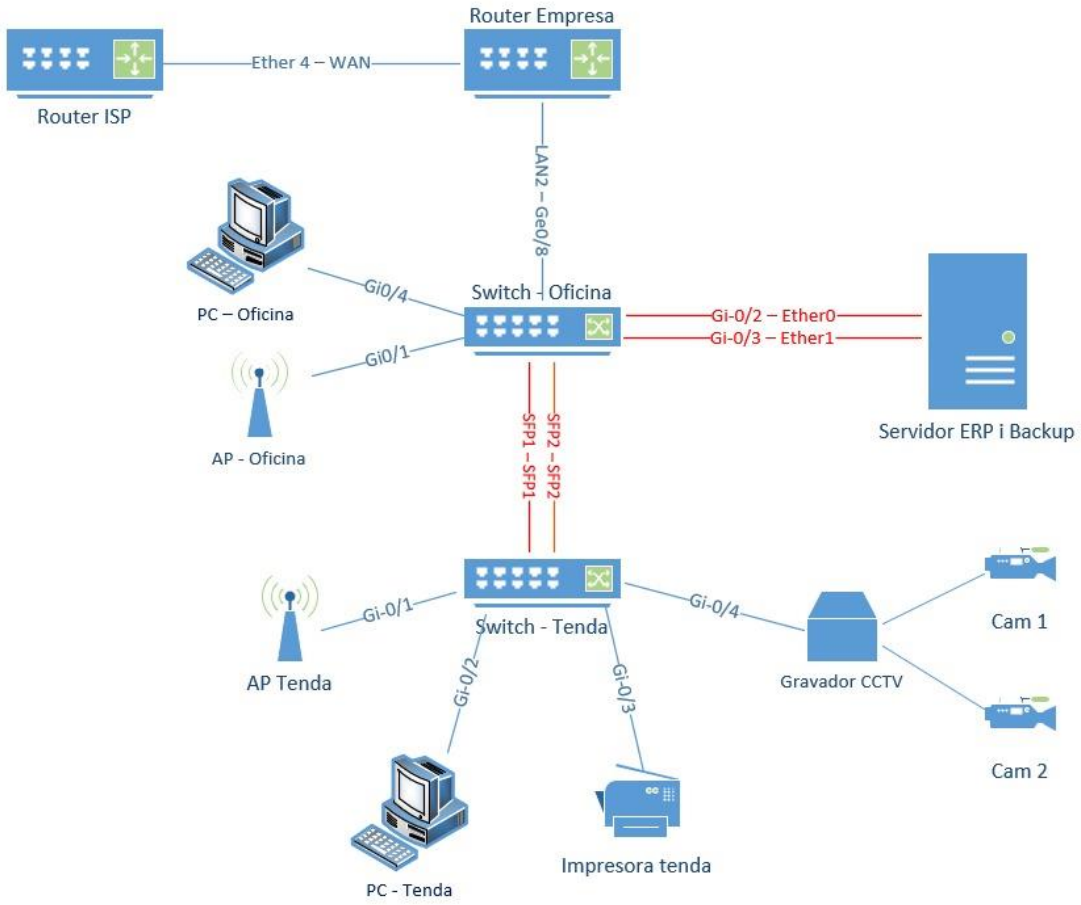
- Assignació estàtica de IP per als equips de la xarxa: Router, Switch, AP.
    - Router: 192.168.99.1
    - Switch-01: 192.168.99.2
    - Switch-02: 192.168.99.3
    - AP: 192.168.99.4
- Assignació estàtica de IP per als servidors.
    - Servidor Virtualització: 192.168.99.100
    - Servidor ERP: 192.168.99.101
    - Servidor de copies de seguretat: 192.168.99.102

Esquema de xarxa

Degut als recursos econòmics de l'empresa i les necessitats reals d'aquesta, l'esquema de la xarxa mes adequat es el anomenat collapsed core:

- La capa accés: Encarregada de connectar els equips finals però també de transportar les dades entre els equips finals i la capa core.
- La capa Collapsed Core: encarregada de comunicar la xarxa amb l'exterior i també l'encarregada de encaminar el tràfic entre els diferents segments de la xarxa.

Per aconseguir-ho, l'esquema de xarxa proposat queda de la següent forma:



Il·lustració 41 - Esquema final de xarxa

Els equips de la oficina estaran connectats al anomenat Switch-oficina mentre que la resta de equips i càmeres aniran connectats al switch tenda i els dos switchos connectats entre formant el anomenat UPLINK, cable troncal pel que es transmeten totes les VLANs.

La connexió física de la xarxa quedarà de la següent manera

Router Core

- WAN a Mikrotik de ISP
- LAN 1 cable backup
- LAN 2 a SW-Oficina (DOWNLINK – VLAN 10,20,50,99)

Switch SW-OFICINA

- Gi-0/1 a AP-OFICINA (VLANs 10,20,99)
- Gi-0/2 a Servidor (VLANs 10,99)
- Gi-0/3 a Servidor (VLANs 10,99)
- Gi-0/4 a PC-Oficina en VLAN 10
- Gi-0/5 a Controlador de la xarxa en VLAN99
- Gi-0/8 a Router TP-Link (UPLINK – VLAN 10,20,50,99)
- SFP1 a SFP1 SW-TENDA (DOWNLINK – VLAN 10,20,50,99)
- SFP2 a SFP2 SW-TENDA (DOWNLINK – VLAN 10,20,50,99)

Switch SW-TENDA

- Gi-0/1 a AP-TENDA (VLANs 10,20,99)
- Gi-0/2 a PC-Tenda en VLAN 10
- Gi-0/3 a Impressora Tenda en VLAN 10
- Gi-0/4 a Gravador en VLAN 50
- Gi-0/5 a Camara 1 en VLAN 50
- Gi-0/6 a Càmera 2 en VLAN 50
- SFP1 a SFP1 SW-TENDA (UPLINK – VLAN 10,20,50,99)
- SFP2 a SFP2 SW-TENDA (UPLINK – VLAN 10,20,50,99)

3.1.2.3 Electrònica de xarxa

L'elecció del equipament de la xarxa es fonamental, ha de ser fiable, a la par que escalable però també ha de proporcionar tecnologies modernes i facilitar el treball del administrador de la xarxa. Per aquest motius, però sobretot per la gestió unificada de la xarxa i pel pressupost de l'empresa, em decante per la gama de dispositius OMADA del fabricant TP-Link.

Il·lustració 42 - Omada

Router

L'equip encarregat del direccionament IP de les diferents VLANs, també encarregat de la connexió a internet i servidor de les VPN per a la implementació del teletreball de l'empresa es el Router TP-Link ER605_V2.

Aquest Router compta amb integració OMADA SDN, que es necessària per a poder configurar-lo a traves controlador.

Compta amb 5 ports Gigabit, es a dir, a velocitat de 1000Mbps, 1 port WAN i 4 ports LAN, dos dels quals es poden convertir a WAN per a redundar la connexió amb internet.

En quan a la connexió de VPN ens oferix fins a 100 connexions repartides en distints protocols com puguen ser L2TP, OpenVPN, PPTP o Site-to-Site IPSEC.

Altres característiques hardware com son:

- IEEE 802.3, 802.3u, 802.3ab, IEEE 802.3x, IEEE 802.1q
- TCP/IP, DHCP, ICMP, NAT, PPPoE, NTP, HTTP, HTTPS, DNS, SNMP

Il·lustració 43 - Router ER605 Omada

Switch

A l'empresa s'instal·laran dos switch TL-SG2210MP, aquest també compatibles amb la tecnologia OMADA SDN, que ens permetran configurar-los i gestionar-los de una forma unificada i senzilla.

Per als switch era fonamental que comptarem amb tecnologia PoE, per això poder alimentar equips com AP i càmeres de vigilància sense necessitat d'una font d'alimentació externa, aquest complixen amb les necessitats ja que compten amb 8 ports Ethernet 1Gbps amb PoE+, que seran utilitzats tant per a PC o impressores com per a AP i càmeres de vigilància, ames aquest switch compta amb dos ports SFP (small form-factor) de 100/1000 Mbps, que s'utilitzaran per a la connexió UPLINK, connexió entre switch tenda i switch oficina, deixant així els ports Ethernet lliures per a equips finals.

Il·lustració 44 - Switch TL-SG2210MP JetStream Omada

AP (Access Point)

Per a millorar la xarxa wireless actual de l'empresa, seran necessaris dos AP, un estarà ubicat a l'oficina i altre a la tenda. Els AP seran també compatibles amb OMADA SDN i PoE.

AP-Oficina: es el EAP615-Wall, pensat per a ser instal·lat a parets, ja que el que busquem es millorar el mapa de calor aconseguit amb el Router del ISP, el dispositiu EAP615-Wall tindrà el seu lloc de muntatge a la paret de l'oficina i estarà orientat cap a la resta de la empresa. Compta amb tasses de senyal de fins a 1200 Mbps, tecnologia Wi-Fi 6 i Roaming, tecnologia encarregada de distribuir els clients connectats entre els diferents AP per a garantir la bona connexió i experiència en tot moment.

Il·lustració 45 - EAP615-Wall Omada

AP-Tenda: EAP653, muntatge de sostre, compta amb tecnologia Wi-Fi 6 i Roaming, amb una tassa de senyal de fins a 3000 Mbps, juntament amb el EAP de l'oficina formaran la xarxa mesh o malla que millorarà la connectivitat wireless de l'empresa.

Il·lustració 46 - EAP653 Omada

Omada Controller

Per a la configuració i gestió unificada de la xarxa es necessària la tecnologia TP-Link Omada SDN. Aquesta tecnologia com s'explica al punt SDN dels fonaments teòrics pot ser gestionada amb un controlador software o hardware. A l'empresa s'adquirix la tecnologia hardware OC200, esta encara que esta destinat a empreses menudes, te capacitat per 100 AP Omada, 20 Switch, 10 Routers. Capacitats mes que suficients per a les necessitats de la xarxa.

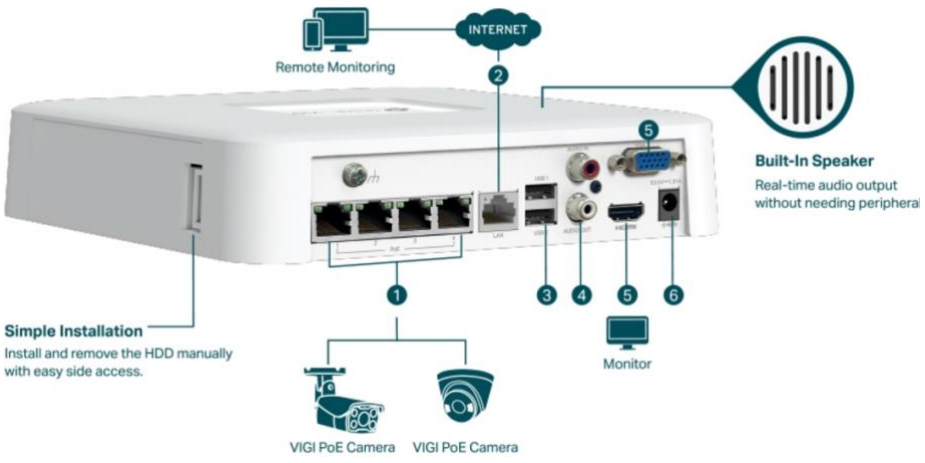
Il·lustració 47 - Omada Controller 200

Gravador VIGI

El gravador es un dispositiu electrònic semblant a un Router, que ens permet guardar fragments de vídeo o fotografies de les càmeres instal·lades al nostre CCTV i al mateix temps, actua de concentrador i ens permet unificar les imatges en directe de cada una de les càmeres al mateix lloc.

La gama VIGI compta amb un software per a dispositius mòbils que facilita l'accés a les càmeres en remot, tot i que es configure després per a vores en local i via VPN.

Per a l'empresa s'ha escollit el gravador VIGI NVR1104H-4P, gravador de 4 canals, el que significa que podem visualitzar 4 càmeres simultàniament amb la divisió de la pantalla. Compta amb ports PoE+ pel que ens alliberaria de carrega PoE al switch i ens alliberaria 4 ports en cas de necessitar-los al switch.



Il·lustració 48 - Gravador VIGI

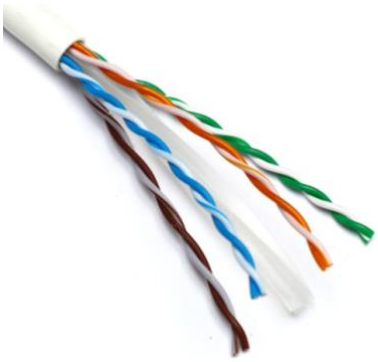
Cablejat

Per a la connexió dels equips finals a la capa d'accés s'ha escollit el cable Ethernet RJ54 UTP CAT 6. Com busquem una millora en quant a velocitat, els equips escollits compten amb ports de 1 Gbps (1000 Mbps), per tant necessitem un nou cablejat concorde amb aquestes velocitats.

L'anterior cablejat, CAT5, ens permetia velocitats de 100 Mbps i degut a que no comptava amb un blindatge suficient, era susceptible a interferències.

El cable CAT6 compta amb una creueta de plàstic, que aïlla els 4 parells del cable minimitzant les interferències i mantenint la integritat de la senyal.

Després de realitzar el disseny, s'estima que amb una bobina de cable de 100 metres, serà suficient, ja que la connexió de cable mes llarga serà amb una càmera situada a 15 metres del switch.



Il·lustració 49 - Cable RJ45 CAT.6

Per a la connexió entre el SW-TENDA i el SW-OFICINA, utilitzarem els dos ports SFP amb els que compten els switch. Aquests ports estan pensats per a una connexió de fibra, que pot ser connectada amb AOC (Active Optical Cable) o amb cables de coure d'alta velocitat coneguts com DAC (Direct Attach Cable).

El cable AOC te majors velocitats, ens oferix majors distancies i utilitza tecnologia de fibra òptica mentre que el cable DAC, te un preu mes econòmic i es el motiu de la seua elecció

Per comoditat i simplicitat es compren dos cables de 7 metres a la tenda FS, encarregada de fer aquest cables a mesura.

Il·lustració 50 - Cable DAC

Connectors RJ-45

Els connectors seran de categoria 6 com el cable Ethernet ja que el cables de coure del interior tenen mesures diferents segons la categoria del cable. La manera de unir el connector amb el cable Ethernet es coneix com a “crimpar”.

Il·lustració 51 - Connector RJ45

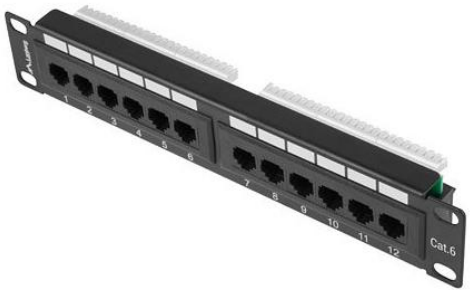
Armari o Rack

Per a mantenir un ordre dels equips i tindre'ls protegits dels usuaris s’adquirixen dos armaris de 10 polzades. Un dels armaris estarà protegint els switch de la oficina junt amb el Router TP-Link i el Router IS, mentre que el altre estarà ubicat a la tenda protegint el switch de la tenda i el gravador

Il·lustració 52 - Armari

Patch panel

El Patch panel o panel de connexions s’utilitza per a mantenir una organització dels cables Ethernet, ens permet tindre una visió clara en un primer reconeixement de on esta connectat cada cable del armari. Per a l’instal·la cio he escollit un patch panel de la marca lamberg de CAT6 i 10 polzades per a ser compatible amb el armari.



Il·lustració 53 - patch panel

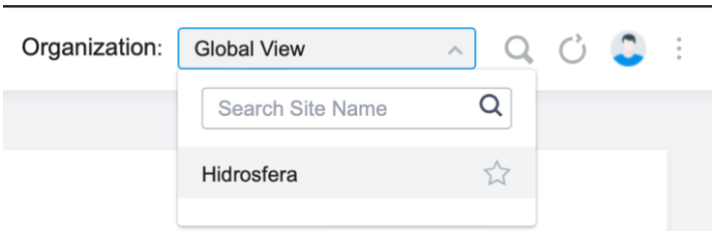
3.1.2.4 Configuració

La configuració dels equips es realitza al banc de proves, a casa, abans d'anar a la empresa a muntar cap cosa, primer ha de ser configurada i provada. Esta feina ens estalvia temps al lloc de la instal·lació i ens dona flexibilitat ja que sempre poden sorgir errors per moltes configuracions semblants realitzades en anteriors empreses o clients.

Il·lustració 54 - Banc de proves

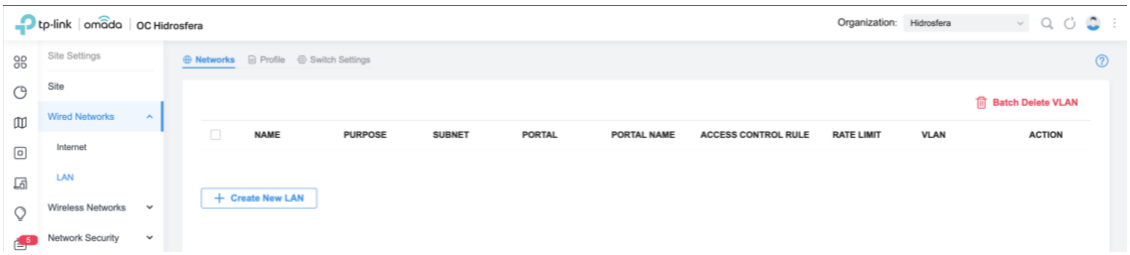
Configuració dels segments (VLAN)

Per a configurar les xarxes mencionades al punt de segmentació ens dirigim a la part superior dreta del navegador i en la pestanya **Organization** escollim el nostre Site



Il·lustració 55 - Accedir al Site

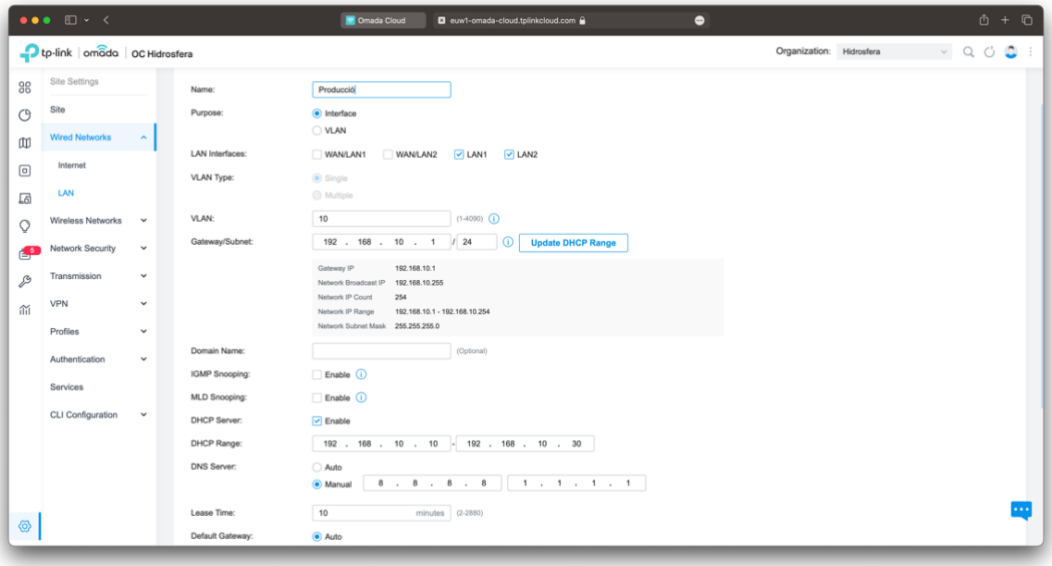
Al apartat de **Settings** en la secció de **Wired Networks - LAN** podrem definir les xarxes de la nostra empresa



Il·lustració 56 - Secció de LAN

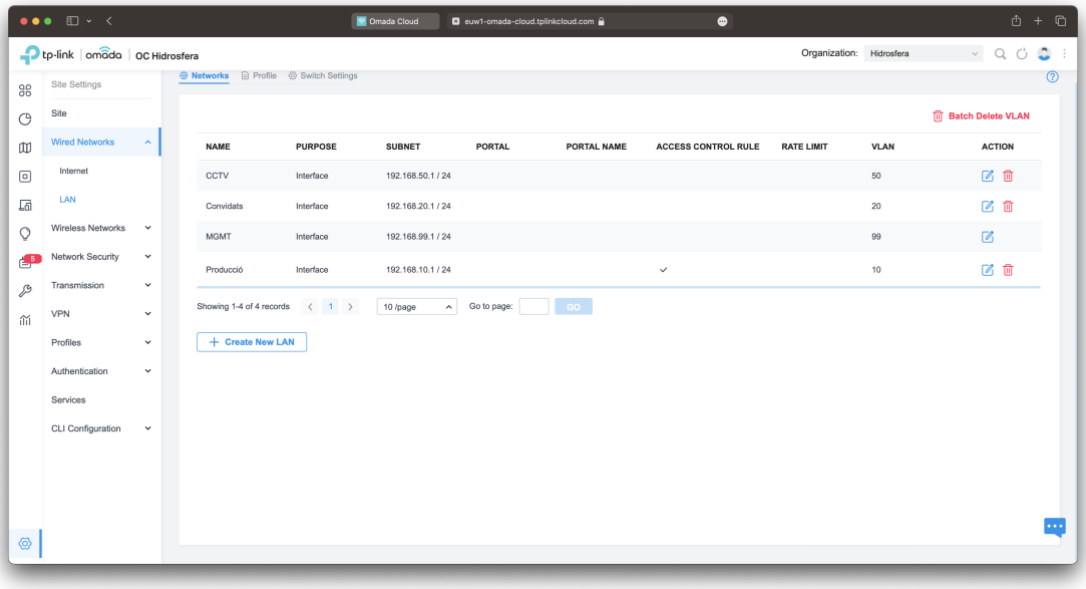
Exemple de configuració VLAN 10 – Producció

- Nom: Producció
- Tipus: Interface
- Ports del Router per la qual passarà (TAGGED): LAN1 i 2
- VLAN ID: 10
- Porta d'accés o Gateway: 192.168.10.1/24
- Servidor DHCP: 192.168.10.10-192.168.10.30
- DNS manual: 8.8.8.8 1.1.1.1



Il·lustració 57 - Configuració de VLAN 10

Per a l'empresa finalment he creat les quatre VLAN detallades a la memòria:



Il·lustració 58 - VLANs Empresa

Al estar treballant en mode controlador les VLAN es distribuixen per tots els equips que tenim adoptats, estalviant-nos així molta configuració repetitiva sobretot si la xarxa integrés un gran nombre de equips.

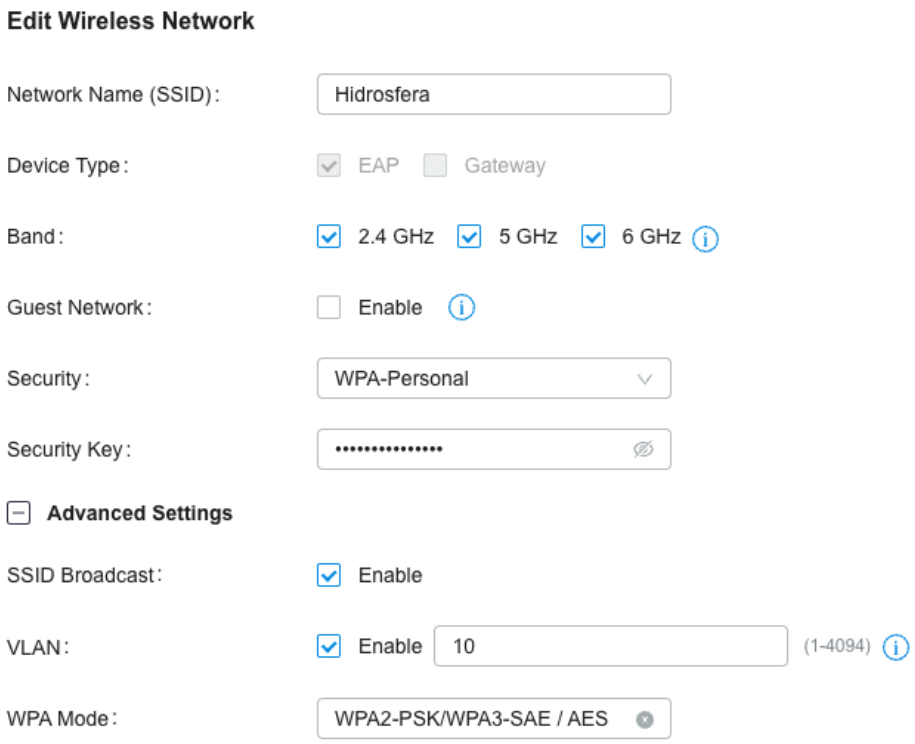
Configuració de xarxa wireless (Wi-Fi)

Per a la xarxa Wi-Fi de la empresa seguirem amb el disseny segmentat de VLANs, una xarxa serà per a la connexió dels empleats i dispositius de la empresa, amb accés a recursos com puguen ser servidors, impressores i demes equips en la VLAN de producció. Altra xarxa serà per a convidats (Hidrosfera_Invitados) a la VLAN 20 i comptarà amb certes restriccions.

Wi-Fi Producció

Es crea una xarxa anomenada Hidrosfera amb clau compartida, PSK (Pre Shared Key) a la qual es connectaran els empleats amb els dispositius mòbils i el datàfon per a les transaccions amb targeta.

Per a configurar-la ens dirigirem a la secció de de **Wireless Networks – WLAN**



Il·lustració 59 - Creació xarxa Wireless

Els requeriments mínims per a ferla funcionar seran:

- SSID
- Tipus de dispositiu (EAP): Indica que es crea als AP adoptats.
- Banda de emissió
- Seguretat: WPA-Personal (tipus de autenticació del usuari)
- Contrasenya
- VLAN 10 - Producció

El següent pas serà indicar a cada equip quines VLAN podran travessar cada port. Açò anirà en funció del esquema de xarxa i del disseny de la xarxa.

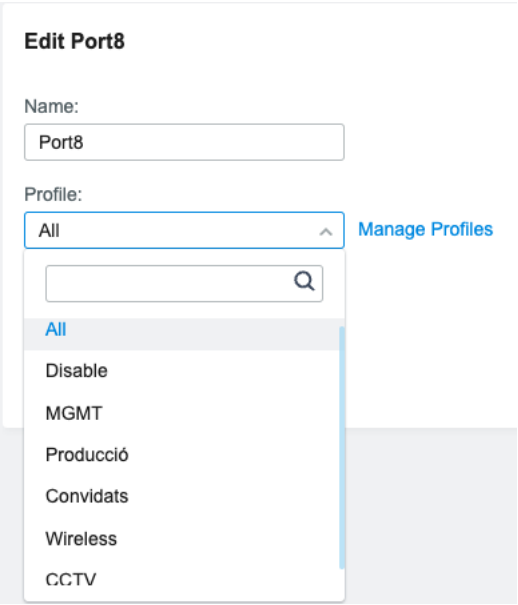
Router

El Router es la porta d'enllaç i el servidor DHCP de totes les VLAN, per tant deu de enviar totes les VLAN cap al switch SW-Oficina. Deurem de marcar per quines interfícies del Router anem a emetre aquestes VLAN. Aquest procés configura la Interface LAN1 i LAN 2 en interfícies TRUNK. Encara que açò es fa a totes les xarxes creades, ací es mostra com es crearia amb la xarxa de producció.

Il·lustració 60 - Trunk port Router

Switch Oficina

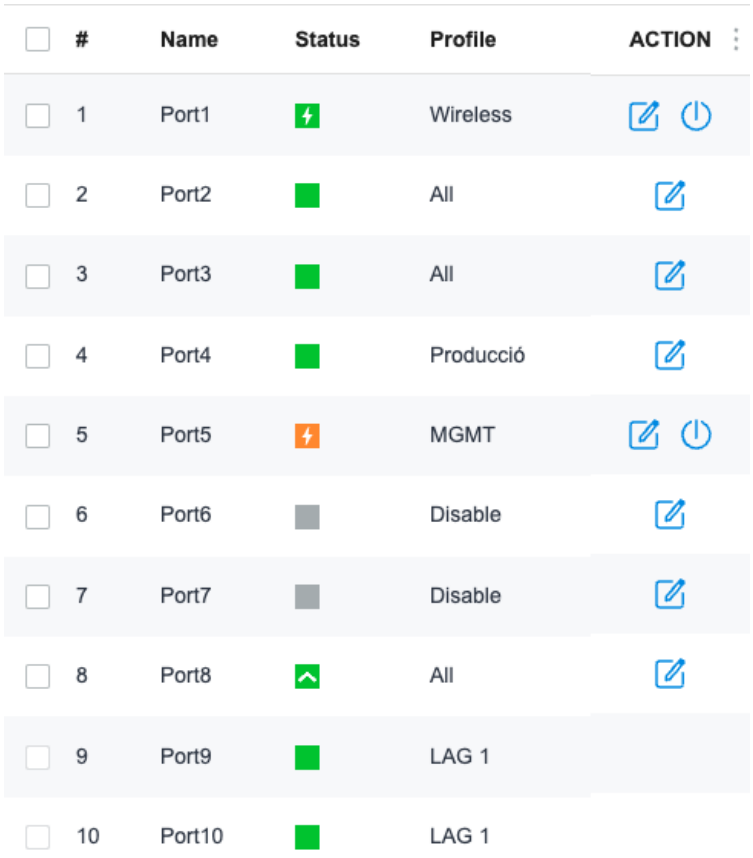
El switch oficina rep les 4 VLANs pel port Gi-0/8, per lo que hi haurà que configurar-lo en mode TRUNK per a que tinga comunicació amb el Router TP-Link.



Il·lustració 61 - Trunk port Switch Oficina

El port ens permet indicar quin perfil (xarxa) el travessarà. Si indiquem "ALL", es convertix en mode trunk amb totes les nostres VLAN declarades.

Seguirem esta configuració amb cada port del switch en funció el equip connectat a ell.



#	Name	Status	Profile	ACTION
1	Port1		Wireless	
2	Port2		All	
3	Port3		All	
4	Port4		Producció	
5	Port5		MGMT	
6	Port6		Disable	
7	Port7		Disable	
8	Port8		All	
9	Port9		LAG 1	
10	Port10		LAG 1	

Il·lustració 62 - Resum etiquetat ports SW-Oficina

- Port 1 compta amb el perfil Wireless, perfil creat amb les VLAN 10,20 i 99, ja que la VLAN 50 CCTV no es necessari que se emeta pels AP.
- Ports 2 i 3 corresponen a un servidor, el qual esta pensat per a la VLAN 10 i 99, per es podria utilitzar per virtualitzar un gravador i necessitar també la VLAN 50, per lo que es decidix deixar-lo amb totes les VLAN en mode trunk.
- Port 4 correspon al PC-Oficina que estarà únicament en la VLAN 10 de producció
- Port 5 per a la connexió del Omada Controller, VLAN 99 ja que volem que siga per a gestió.
- Ports 6 i 7 queden sense cap configuració i des-habilitats ja que no tenim dispositius.
- Ports 8 es el UPLINK, per tant en mode trunk amb totes les VLAN.
- Ports 9 i 10* son el DOWNLINK cap al SW-Tenda, per tant es configuren mode trunk amb totes les VLAN

*Ports redundats on se expliquen mes avant.

Switch Tenda

El switch tenda es el mateix model i mateixa versió que el SW-Oficina pel que la forma en que es configuren els ports serà idèntica, el que canvia es les VLAN de cada port ja que tenim dispositius diferents a cada un d'ells.

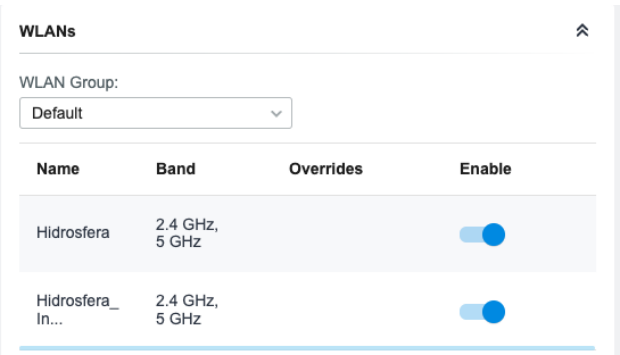
#	Name	Status	Profile	ACTION
1	Port1		Wireless	
2	Port2		Producció	
3	Port3		Producció	
4	Port4		CCTV	
5	Port5		Disable	
6	Port6		Disable	
7	Port7		Disable	
8	Port8		Disable	
9	Port9		LAG 1	
10	Port10		LAG 1	

Il·lustració 63 - Resum etiquetat ports SW-Tenda

- Port 1 compta amb el perfil Wireless, perfil creat amb les VLAN 10,20 i 99, ja que la VLAN 50 CCTV no es necessari que se emeta pels AP.
- Ports 2 correspon al PC-Tenda que esta a la VLAN 10 de producció.
- Ports 3 correspon al PC-Tenda que esta a la VLAN 10 de producció.
- Port 4 correspon al gravador que estarà únicament en la VLAN 50 de CCTV
- Ports 5, 6 , 7 i 8 queden sense cap configuració i des-habilitats ja que no tenim dispositius.
- Ports 9 i 10* son el DOWNLINK cap al SW-Tenda, per tant es configuren mode trunk amb totes les VLAN

APs

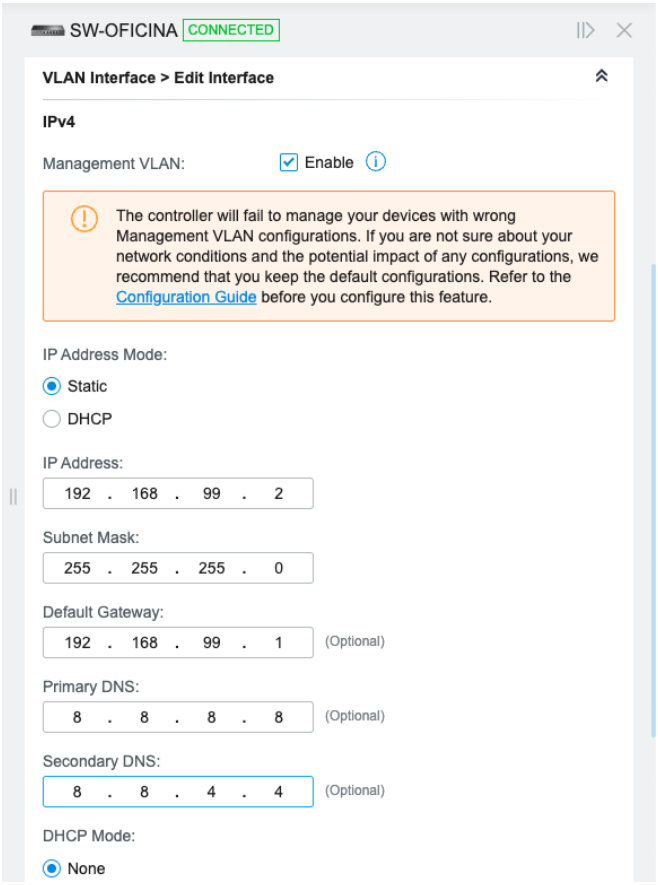
Una vegada creades les xarxes wireless als AP nomes caldrà declarar quines d'aquestes poden funcionar a ells, es podria donar el cas que un AP estigues en una habitació separada exclusivament per a visites i nomes caldria la VLAN 20 – Convidats.



Il·lustració 64 - Xarxes AP

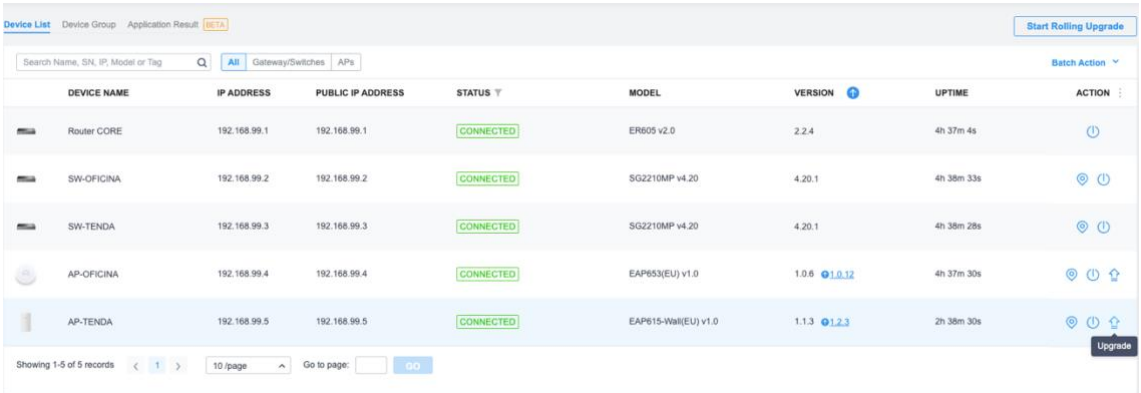
Una vegada creades les VLAN i assignats els ports pels quals van a passar, deurem de assignar la IP de gestió a els equips de la xarxa. La VLAN de gestió deu ser sols accessible per l'administrador de la xarxa i els usuaris de la empresa no han de ser capaços de connectar a ella, ja que suposaria una vulnerabilitat i un risc per a la integritat de la xarxa.

Com s'indica al apartat de direccionament IP de la memòria, els equips de la xarxa comptaran amb una IP estàtica en la VLAN de gestió. Per a assignar-la, deurem de seleccionar els equips adoptats al nostre OC i a la seua configuració **IP Settings**



Il·lustració 65 - Configuració IP estàtica

Una vegada fixada la IP, els dispositius que formaran la xarxa de la oficina son els següents:



Il·lustració 66 - Visio global electrònica de xarxa Omada

Redundància

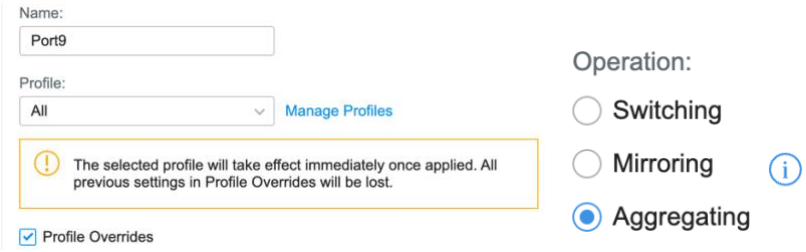
El disseny de xarxa de tipus collapsed core ens limita en quant a la implementació de redundància, per tant el que s'implementa a l'empresa es la agregació de enllaços entres switchos.

LACP

Amb el LACP a l'empresa aconseguirem duplicar el Bandwidth entre switchos i guanyar redundància en cas de que un dels enllaços falle.

En el cas dels switch de la empresa, els ports que formaran part del LACP seran els dos SFP, anomenats port 9 i port 10.

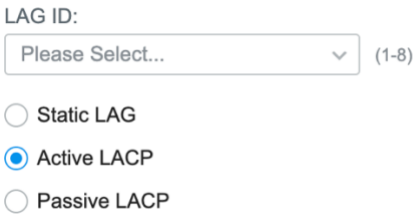
Primer hi haurà que configurar-ho al SW-Oficina a un dels dos ports. Indicarem com a perfil "All" indicant així que el port actuarà com a trunk.



Il·lustració 67 - Configuració Port 9

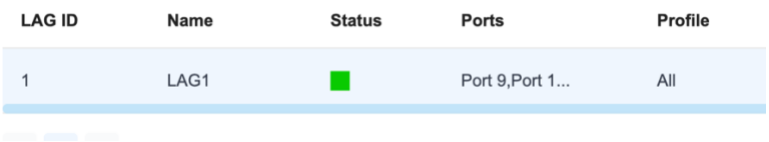
Com a operació activarem "Aggregating", es a dir, agregació de ports. "Switching" seria per a configurar el port per a treballar de forma individual mentre que "Mirroring" seria per a copiar tràfic de altres ports en estat "Mirroring".

Al crear una agregació de enllaços s'identifiquen amb el nom de LAG, es necessari que compten amb un identificador LAG ID i que indiquem en quin mode de treball van a funcionar. El cas de la empresa funcionarà en ACTIVE/PASIVE per tant el SW-Oficina estarà en mode actiu per tant el SW-Tenda el configurarem en mode passiu.



Il·lustració 68 - Mode LACP

Resultat final de la agregació.



Il·lustració 69 - LAG 1

VPN

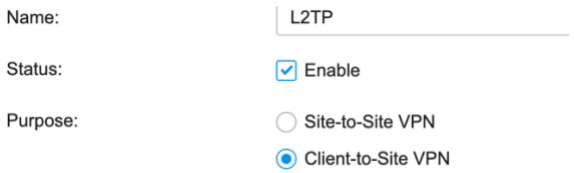
Els protocols escollits per a la connexió a l'empresa seran:

- L2TP/IPsec per a la connexió del administrador de la xarxa degut a que es un protocol segur, estable i compatible tant amb Windows com amb MacOS, sistemes operatius dels quals soc usuari diari.
- OpenVPN per als empleats ja que ens permet exportat e importar la configuració del client OpenVPN i instal·lar-la en gran varietat de dispositius i plataformes de forma rapida i inclús un usuari sense experiència podria configurar-la.

L2TP / IPsec

Primer haurem de crear un servidor VPN L2TP, aquest serà al que connectaré cada vegada que necessite accedir a la xarxa per qualsevol tipus de configuració.

Per a configurar-lo es crea una política VPN que ha de ser de tipus Client-to-Site, es a dir usuari a servidor.

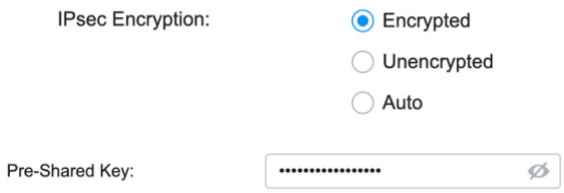


Il·lustració 70 - L2TP Server (1)

Com l'equip al que estem configurant la VPN actuarà de servidor, la VPN serà de tipus Server L2TP.

Il·lustració 71 - L2TP Server (2)

Per a securitzar-la haurem de combinar-la amb IPsec amb clau compartida.

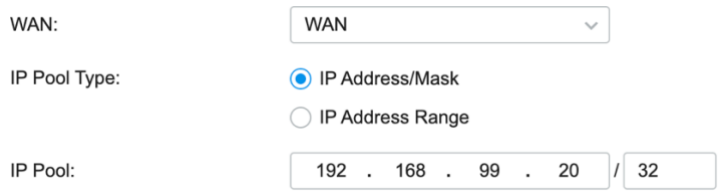


Il·lustració 72 - L2TP Server (3)

La forma en la que ens autentiquem serà amb usuari local i les xarxes a les que tindrem accés seran totes ja que es una VPN per a administrador de xarxa.

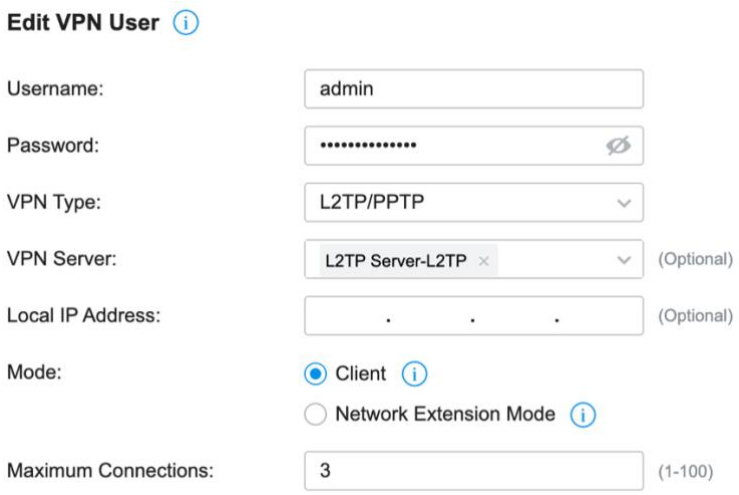
Il·lustració 73 - L2TP Server (4)

Per últim haurem de indicar-li per quina Interface estarà accessible la VPN i quin serà el Pool (IP o nombre de IPs que entregarà al usuari quan es connecte).



Il·lustració 74 - L2TP Server (5)

Una vegada configurada hem de crear un usuari indicant de quin tipus es, en el nostre cas L2TP/PPP i com a opcional el servidor al que poden connectar en lloc de tindre mes d'un.



Il·lustració 75 - L2TP User

Com a resultat de la creació de les dos VPN podem veure que comptem amb el servidor OpenVPN amb accés a les VLAN 10 i 50 i el Servidor L2TP amb accés a tota la xarxa de la empresa.

NAME	ENABLED	PURPOSE	VPN TYPE	INTERFACE/IP	WAN
OpenVPN		Client-to-Site VPN	OpenVPN(Server)	Producció CCTV	WAN
L2TP		Client-to-Site VPN	L2TP(Server)	MGMT Producció Convidats CCTV	WAN

Il·lustració 76 - Resum VPN

Seguretat

Per a la seguretat de la empresa crearem ACL, llistes de control de accés, que garantiran la seguretat dels recursos i equips de l'empresa i els protegiran davant intents de accessos no autoritzats.

Al Router es crearan dos regles de xarxa:

- la primera denegarà el accés del empleats a qualsevol xarxa que no siga la de producció i la de CCTV.
- La segona regla permetrà el accés de la xarxa de gestió a qualsevol de les altres xarxes.

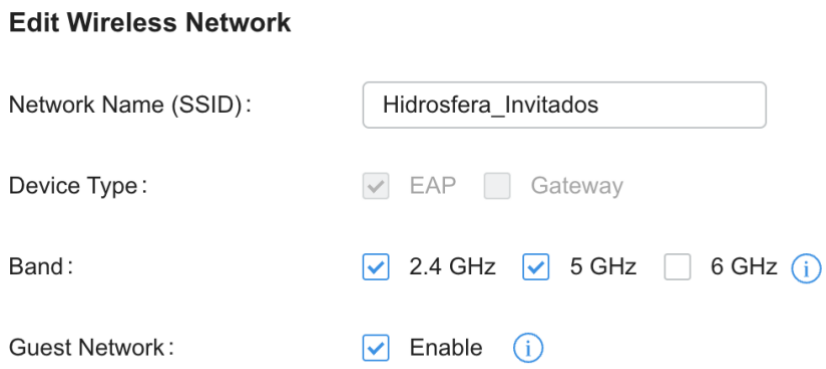
ACL Rules Tip: Drag ⋮⋮ to re-order rows.

	INDEX	ENABLED	DESCRIPTION	DIRECTION	POLICY	PROTOCOLS	SOURCE	DESTINATION
⋮⋮	1		Produccion to LAN	LAN->LAN	Deny	All	Network:Producció	Network:Convidats, MGMT
⋮⋮	2		MGMT	LAN->LAN	Permit	All	Network:MGMT	Network:Producció, Convidats, CCTV

Il·lustració 77 - Resum ACL

Al switch es crearà una regla que denegarà la resposta ping, protocol ICMP, als empleats de la xarxa cap a les xarxes de gestió i convidats, quedant així aïllats per complet a la xarxa de producció i CCTV.

Als AP no caldrà crear cap regla, sols es podran connectar a traves de la xarxa wireless, compten amb una funció a al menú de configuració de la xarxa wireless anomenat “guest network” que s’encarrega d’aïllar la xarxa sense necessitat de configurar cap tipus de regla.



Il·lustració 78 - Aïllar VLAN 20

3.1.2.5 Instal·lació

Una vegada configurats els equips i comprovat el seu correcte funcionament, es el moment de instal·lar-los a l’empresa.

La primera feina es substituir el cablejat antic pel nou i passar cable per zones noves. Per a dur a terme aquest punt es necessari saber on s’ubicaran els equips a l’empresa, en concret els dos armaris amb els equips, les càmeres i els AP. Els ordinadors estaran al mateix lloc on havien estat.

Un dels armaris s’ubica a la sala de reunions de la empresa, que compta a un sol de aglomerat, al estar en una estructura feta a posterior a l’empresa. L’altre armari s’ubica a la paret del fons de la tenda, ubicada justament baix de les oficines i la sala de reunions.

CABLE DAC

Es decidix passar el cable DAC a traves de un forat fet amb martell elèctric i broca per a fusta al sol de la sala de reunions i posteriorment assegurar el cable amb brides a una tuberia rugosa que naix de la mateixa sala de reunions.

Il·lustració 79 - Instal·lació cable DAC

Cablejat Oficina

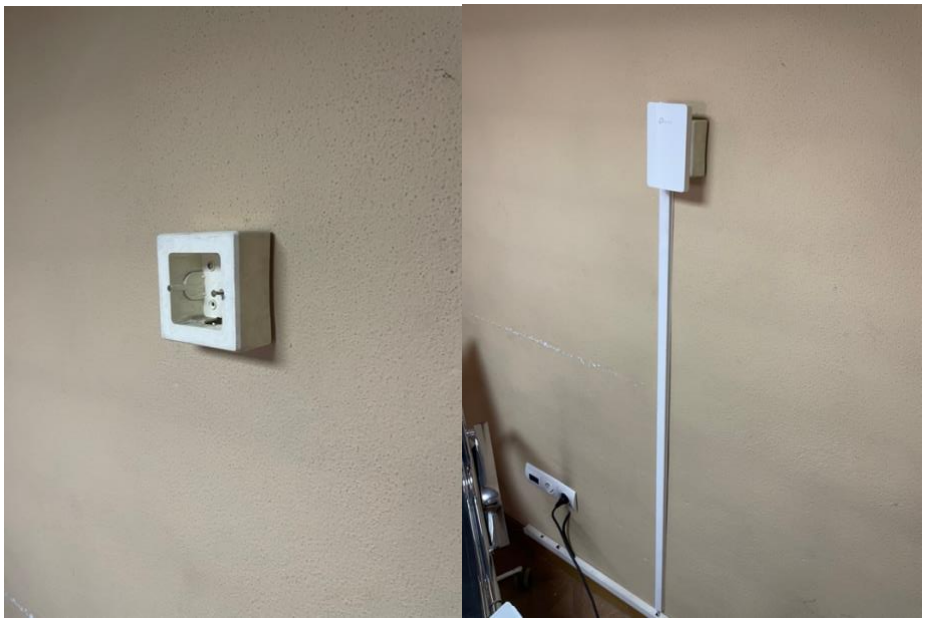
Per a l'oficina es passarà cable des de la sala de reunions on estarà el armari, fins a la sala de l'oficina on esta ubicat el PC-Oficina i el AP-Oficina.

Es compra una canaleta de plàstic per a cable on passaran el cables del PC i del AP i es fixa a la paret per a tindre una organització del cablejat i protegir-lo dels usuaris.

Il·lustració 80 - Cablejat Oficina

Muntatge AP-Oficina

Per al AP de l'oficina es recicla una caixa de connexions antiga ubicada al despatx. Per a segur protegint els cables, s'instal·la una canaleta que ix d'una creueta de la canaleta anterior.

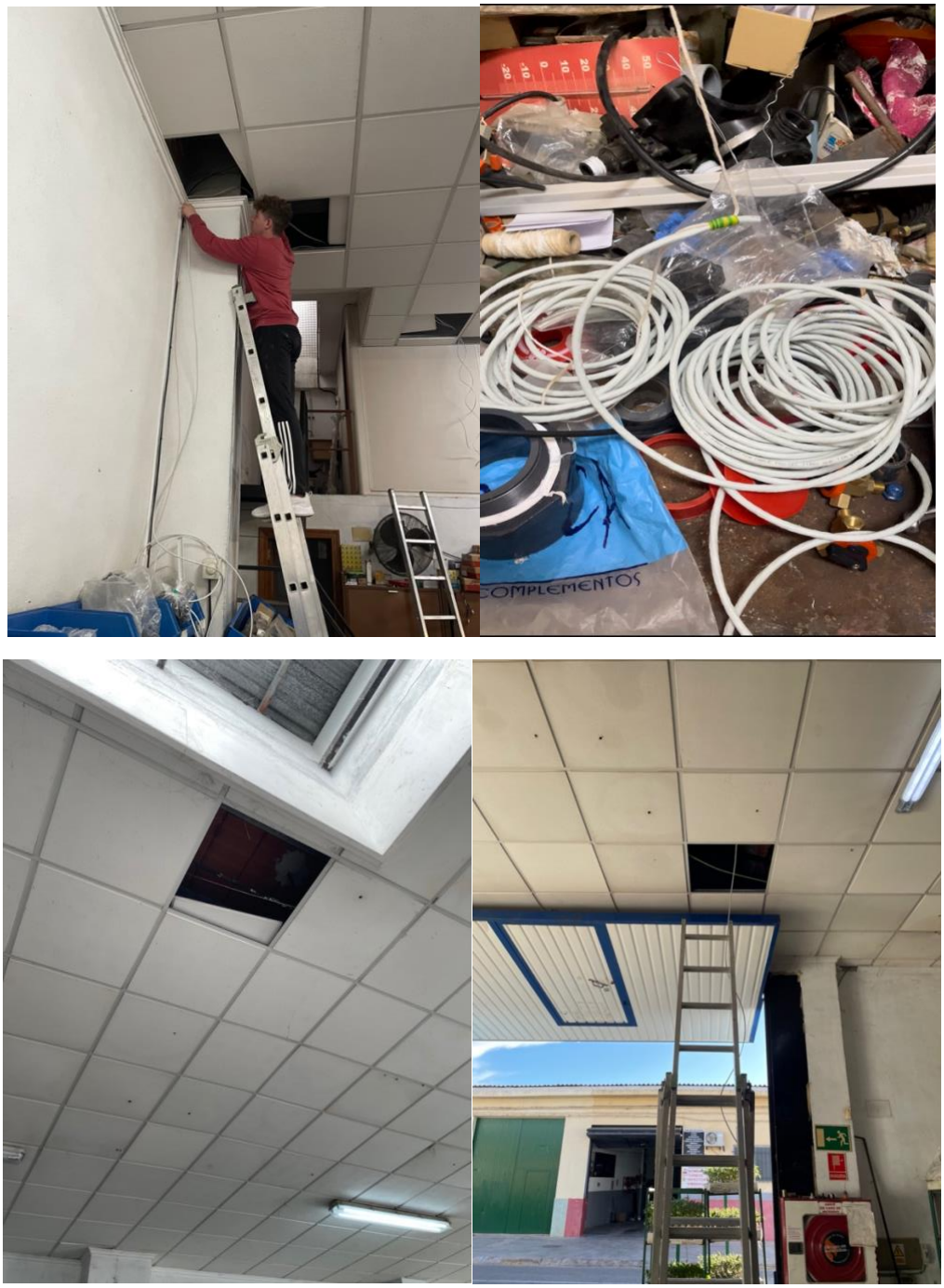


Il·lustració 81 - AP Oficina

Cablejat de tenda

El sostre de la tenda es de panels de algeps, els que ens facilita el distribuir cables al llarg de la superfície de la tenda, sense que estiguen a la visa i sense tindre que instal·lar mes canaletes a llarg de tota la tenda.

El procés es realitza llevant els panels amb l'ajuda d'una escala i amb un fil lligat a una tuberia de PVC i al altre extrem al cable Ethernet de la bobina. Es tracta de arrossegar la tuberia al llarg del sostre i obrir el panel on ha quedat parada.



Il·lustració 82 - Cablejat tenda

Instal·lació càmeres i AP Tenda

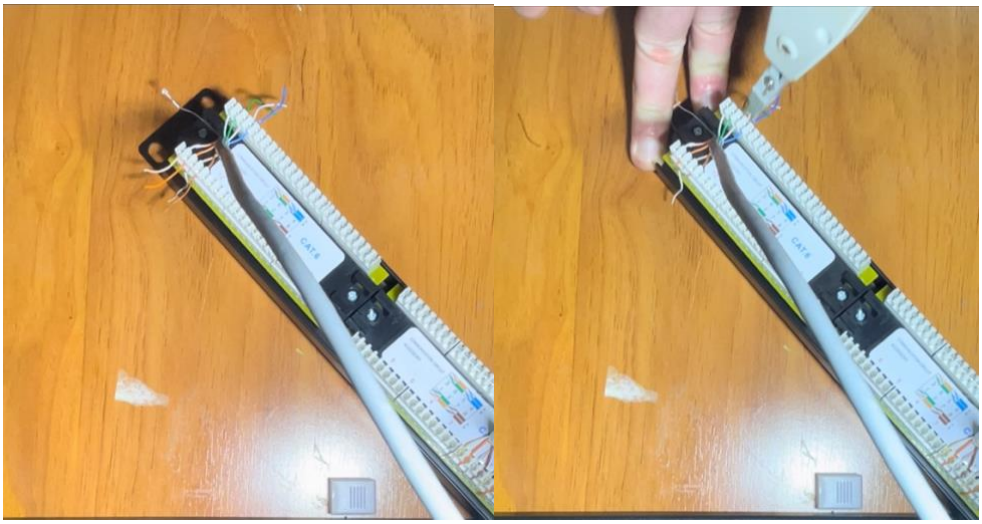
Una vegada passat el cable fins als punts on aniran les càmeres i el AP Tenda, caldrà fer un forat de uns 10mm de grossor, per a passar el cable Ethernet i un fixar les càmeres i el AP que comptem amb la seua "tornilleria".

Il·lustració 83 - Càmeres i AP Tenda

Patch panel

El Patch panel seguix un ordre en el qual es deuen connectar els 8 cables de coure que van al interior del cable Ethernet.

S'utilitza una ferramenta que inserta el cable a la clavilla al mateix temps que talla el sobrant per a que no quede el cable massa sobrant i puga generar interferències.



Il·lustració 84 - Instal·lació Patch panel

Armaris

Per als armaris i haurà que fixar els equips i el Patch panel, be siga amb safates o amb caragols (tornillos) especials per a armaris.

El armari de la oficina tindrà el seu Patch panel, el Router ISP, el Router TP-Link i el SW-Tenda. El armari tenda comptarà amb el mateix Patch panel amb el gravador CCTV i el SW-Tenda

A la part superior es sol connectar el Patch panel i des de ací es distribuixen els cables als diferents equips.

Il·lustració 85 - armaris muntats

Anàlisis Wireless

Una vegada realitzada la instal·lació dels dispositius de la xarxa es torna a realitzar un mapa de calor per a demostrar al client la milloria en quant a senyal wireless.

Il·lustració 86 - Mapa de calor final

Podem comprovar com no comptem amb zones de senyal en color grog com experimentàvem amb la xarxa wireless del ISP.

Valors obtinguts per zones:

- Blau verd: -35 dB o greater
- Ved oscur: --40 a -35 db
- Verd: -48 a -40
- Verd claret -56 a -48

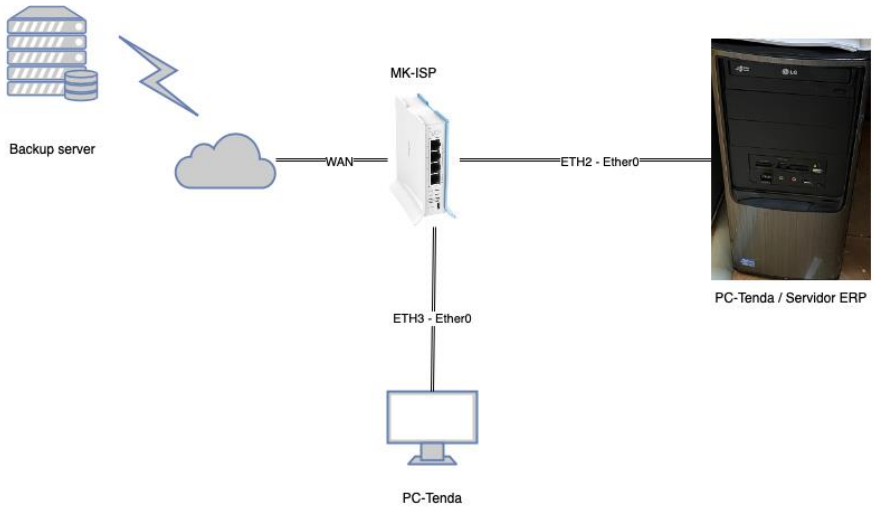
Hem aconseguit abastir de bona cobertura wireless a totes les instal·lacions de la empresa, situant la senyal de la xarxa wireless en valors superiors a -35dBm i en els pitjors casos superiors a -56dBm.

3.2 Disseny de sistemes

El disseny del sistemes, al igual que el de xarxes, estarà estructurat en dues parts, situació inicial, on es mostrarà la configuració actual del sistemes de la empresa i situació final, on es mostrarà els sistemes escollits per a la migració i la configuració realitzada.

3.2.1 Situació inicial

Aquest que es mostra es l'esquema actual de sistemes de l'empresa:



Il·lustració 87 - Esquema sistemes inicial

A l'empresa no es compta amb un servidor dedicat per a la instal·lació del ERP o amb cap tipus de software de gestió de dades. Actualment el ERP – WinOmega esta instal·lat al PC-Oficina, actuant com a servidor.

3.2.1.1 Servidor

L'equip es un ordinador de taula, amb Windows 10 x32 instal·lat. Els sistemes de Windows de 32 bits compten amb la limitacions com per exemple un màxim de 4GB de memòria RAM (Random Acces Memory).

Il·lustració 88 - Especificacions Servidor Actual

3.2.1.2 Gestió de dades

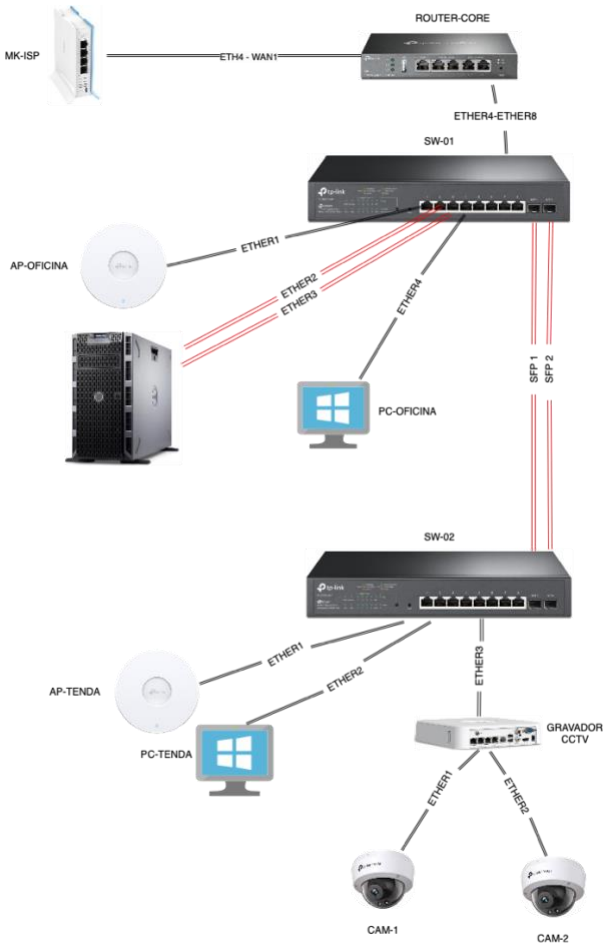
Actualment a l'empresa la gestió de dades esta sent "administrada" per un administrador extern, el qual fa anys va contractar un servei de Backup de la companyia MBO (Mast Backup Online) el qual genera copies de seguretat de les carpetes de treball dels programes WinOmega i ContaPlus únicament.

3.2.2 Situació final

Una vegada analitzada la part corresponent als sistemes de la empresa i anotades les carències i punts vulnerables com son la mala elecció del equip servidor, no tenir implementat cap sistema RAID al equip que proporció al menys una copia en casa de falla del propi disc i en conseqüència la pèrdua d'informació i l'atur de la productivitat de l'empresa, d'altra banda la redundància de ubicacions per a la gestió de les copies de seguretat.

3.2.2.1 Esquema proposat

Al disseny de xarxa ja proposat, afegiríem un nou element, el servidor. Aquest servidor albergaria tant el ERP WinOmega com un gestor de dades per a realitzar també en local les copies de seguretat diàries.



Il·lustració 89 - Esquema de sistemes final

Com s'aprecia al esquema, el servidor anirà connectat amb dos interfícies, formant així un failover per a tindre accés en cas de que una de les interfícies falle.

3.2.2.2 Servidor

El servidor de una empresa deu anar en funció de les necessitats d'aquesta. L'empresa comenta des de primer moment que els recursos econòmics son limitats per a tota la actualització de xarxa i sistemes, per tan s'aquirix un servidor "refurbished". Servidors de compra vendes autoritzats que els han revisat i han reparat qualsevol tipus de mal funcionament o que simplement son de segona ma.

Dell PowerEdge T620

Es un servidor de tipus torre i no de tipus rack, ja que els armaris son de 10 polzades i els servidors tipus rack es necessita un armari de 19".

Il·lustració 90 - Servidor Dell PowerEdge T620

Especificacions

Processador:

- CPU 1: Intel(R) Xeon(R) CPU E5-2690 v2 @ 3.00GHz E5 3000 MHz
- CPU 2: Intel(R) Xeon(R) CPU E5-2690 v2 @ 3.00GHz E5 3000 MHz

Memòria RAM:

Capacitat instal·lada 64GB

- DIMM A1 DDR-3 16.00 GB 1333 MHz
- DIMM A2 DDR-3 16.00 GB 1333 MHz
- DIMM A3 DDR-3 16.00 GB 1333 MHz
- DIMM A4 DDR-3 16.00 GB 1333 MHz

Memòria

- 2x Disc SAS de 600GB
- 4x Disc SSD de 500GB

Targetes de Xarxa

- Intel(R) Gigabit 2P I350-t LOM 1000Mbps (2 targetes de xarxa)

3.2.2.3 Alta disponibilitat

Per a garantir la integritat de les dades, es configura un sistema raid amb els discs del que disposa el servidor.

Il·lustració 91 - Discs al servidor

RAID

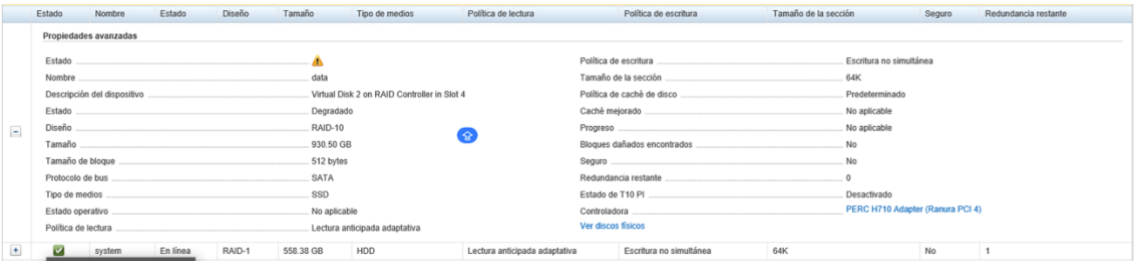
Es crea un sistema RAID 1 espill amb els discs SAS, aquest disc seran els que tindran instal·lats tant el host ESXi com totes les maquines virtuals que s'instal·len a ell, deixant-nos una capacitat de 558 GB al combinar els dos discs de 600 GB.

Si un dels disc falla, el altre entra en Backup de forma automàtica, permetent-nos reemplaçar el disc amb problemes en calent o "Hot Swap".

Per a la gestió de dades es crearà un RAID 10 (1 + 0) en els discs SSD, aquest seran exclusivament per a la escriptura dels fitxers de Backup de Veeam.

Il·lustració 92 - Disc SSD

Al crear el RAID 10 la capacitat passa a ser de 930GB. Es combinen els quatre SSD en grups de dos, pel que ens crea dos grups de tipus RAID 1 de 465 GB que després es combinen en un RAID 0 sumant les seues capacitats.



Il·lustració 93 - Resum RAID

3.2.2.4 Virtualització

A la empresa es decidix virtualitzar, d'aquesta manera tindrem el software ERP accessible a un servidor dedicat i amb els recursos necessaris per a que funcione sense problemes ni interrupcions.

El software de virtualització es VMware ESXi en la versió 7 degut a que el servidor no es compatible amb versions superiors.

L'elecció de ESXi ve donada per diverses raons, una de elles per la llicencia gratuïta que et faciliten a VMware per registrar-se a la seua web i altra raó per la fiabilitat amb la virtualització de maquines en entorns empresarials que ha demostrat al llarg dels anys.

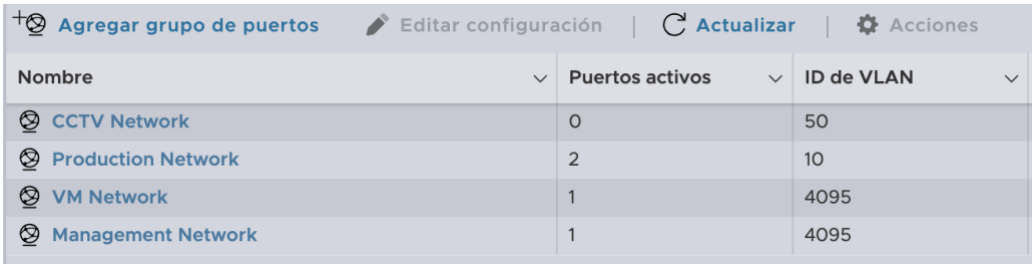
La instal·lació de ESXi es com qualsevol instal·lació de sistema operatiu a un equip final. Amb una memòria USB i un software de creació de "USB Boot" es carregarà la imatge ESXi.

Una vegada instal·lat al nostre servidor podrem accedir al entorn web que ens proporciona VMware.

Il·lustració 94 - Entorn web ESXi

Una vegada dins podrem gestionar les maquines virtuals que es desitgen instal·lar a la empresa.

El primer serà declarar les VLANs per a que el servidor es puga comunicar tant amb Producció (10) per al ERP com per a configurar les maquines en cas de necessitar-ho. Al ESXi la VLAN 4095 equival al mode trunk, d'aquesta forma aconseguim passar la VLAN de gestió.



Il·lustració 95 - VLAN ESXi

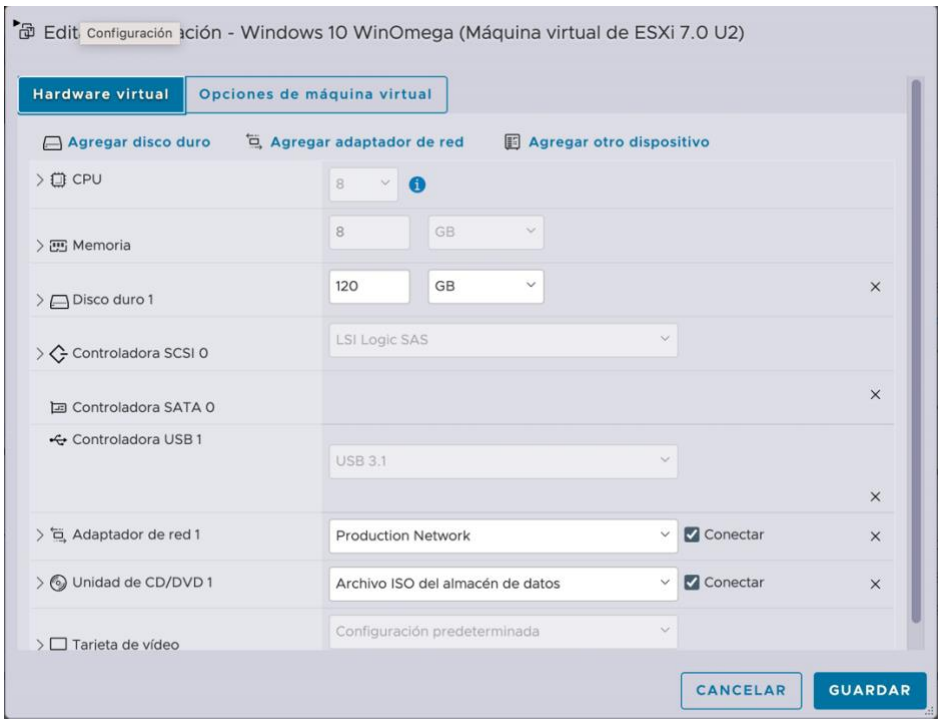
Servidor ERP

El servidor ERP actual estava ocupant una mitja de 120 GB de espai al disc dur del PC-Tenda, per tant seguint un poc amb les característiques i els requisits mínims mencionats a la web del distribuïdor de software, es crea una maquina virtual amb sistema operatiu Windows 10 de 64 bits per a millorar les prestacions del actual servidor de l'empresa.

La maquina tindrà una capacitat inicial de 120GB, que seran suficients ja que necessitem 50 per a Windows i altres 25GB per a WinOmega. No comptarà amb mes software.

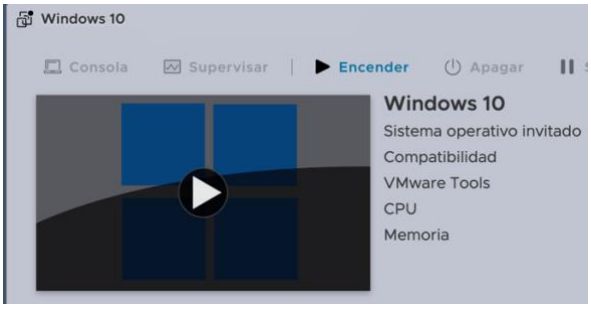
En quant a memòria RAM s'ampliarà de 2GB actuals a 8GB.

L'adaptador de xarxa s'ha de configurar a la xarxa Producció, per a que els equips de la tenda tinguen accés als recursos del ERP.



Il·lustració 96 - Especificacions ERP Virtualitzat

Una vegada configurades les especificacions, podrem arrancar la maquina virtual com si de un equip físic es tractara. Començarà aleshores el procés de instal·lació de Windows 10. Serà necessari crear un usuari al igual que quan adquirim un equip amb el sistema operatiu instal·lat o si el instal·lem nosaltres des de cero.



Il·lustració 97 - Maquina Virtual creada

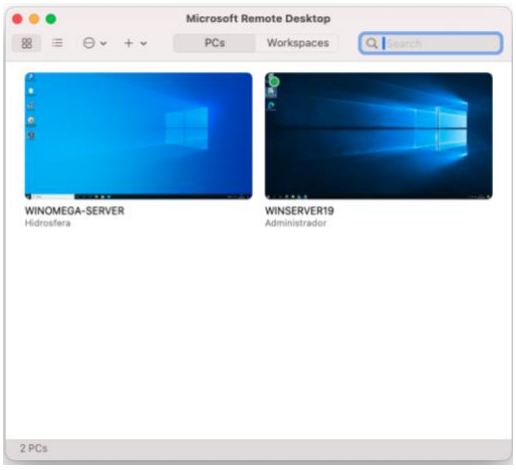
Una vegada finalitzat el procés de instal·lació la maquina es accessible a traves de la interfície gràfica de ESXi, per dificulta la feina per al treball diari ames de que es poc aconsellable donar-li el accés a servidor de virtualització al usuari final i mes si no te experiència prèvia amb aquests sistemes.

Il·lustració 98 - ERP a la consola ESXi

Per tant, el primer pas a realitzar, serà habilitar el accés a l'equip a traves de l'escriptori remot de Windows.

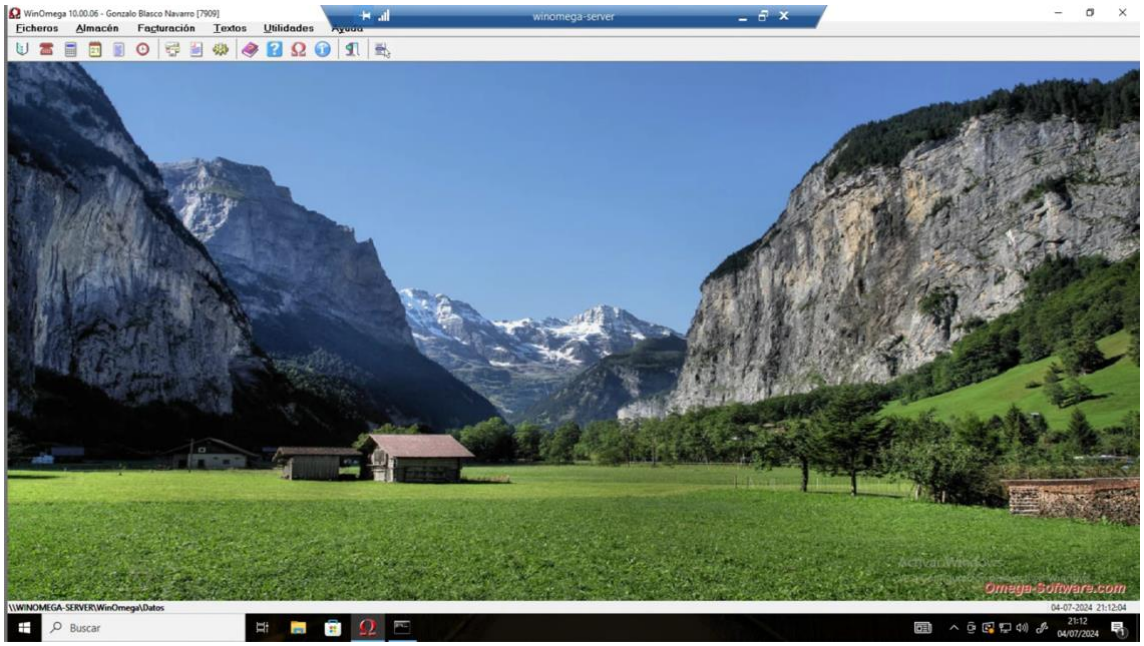
Il·lustració 99 - Habilitat escriptori remot

Una vegada tenim habilitat el accés, podrem gestionar el servidor ERP des de el nostre equip sense necessitat d'accedir a la consola del servidor ESXi amb el software de Microsoft Remote Desktop.



Il·lustració 100 - Microsoft Remote Desktop

Quan accedir amb l'escriptori remot ens trobem amb l'entorn de Windows i el ERP però instal·lats en remot, fent-lo així accessible des de qualsevol lloc a traves de la VPN.



Il·lustració 101 - Escriptori remot ERP

3.2.2.5 Gestió de dades

Per a gestionar les dades, s'ha escollit el software Veeam degut a les 10 carregues de treball gratuïtes en la seua versió CE.

Aquest s'instal·larà sobre un Windows Server 2019 Standard, pensant també en un futur, per a proporcionar el accés als equips i a la xarxa wireless amb usuaris Active Directory.

Servidor Veeam

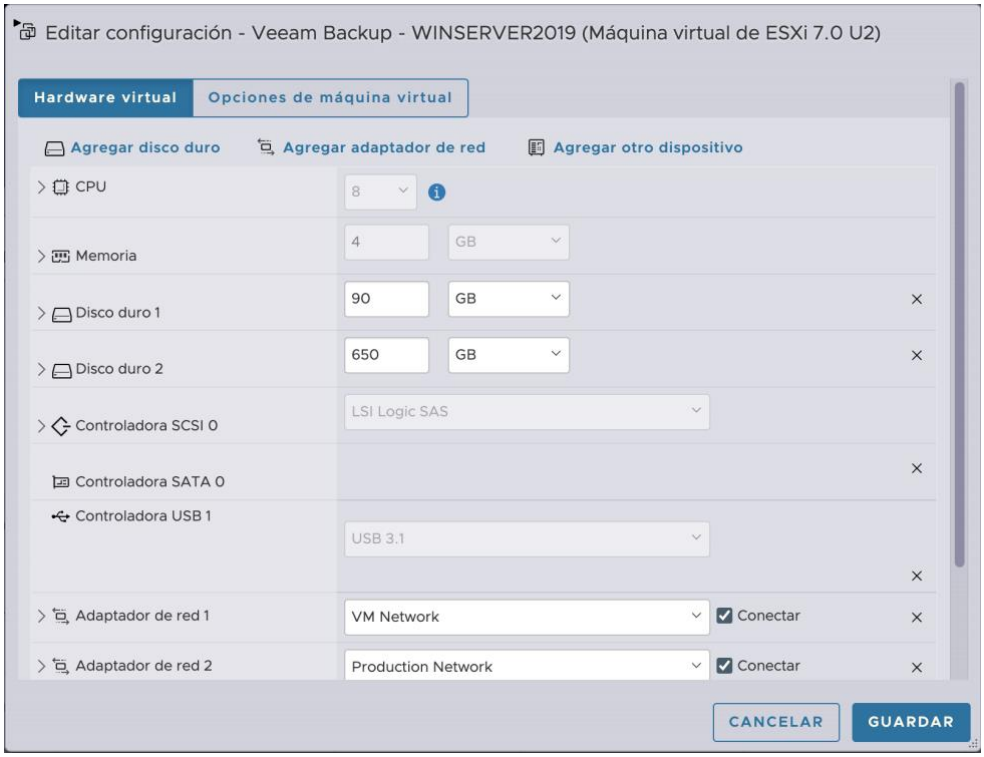
Es realitzarà el procés semblant amb el servidor ERP, creant una maquina virtual amb els requisits necessaris per a al software Veeam.

La diferencia amb la maquina del ERP es que aquesta comptarà amb un altre volum diferent al del sistema operatiu, serà a aquest volum on s'emmagatzemaran les copies de seguretat creades pel software Veeam.

Especificacions

La maquina virtual es crea amb 90 GB per a sistema operatiu i 650 GB per a emmagatzemament de dades.

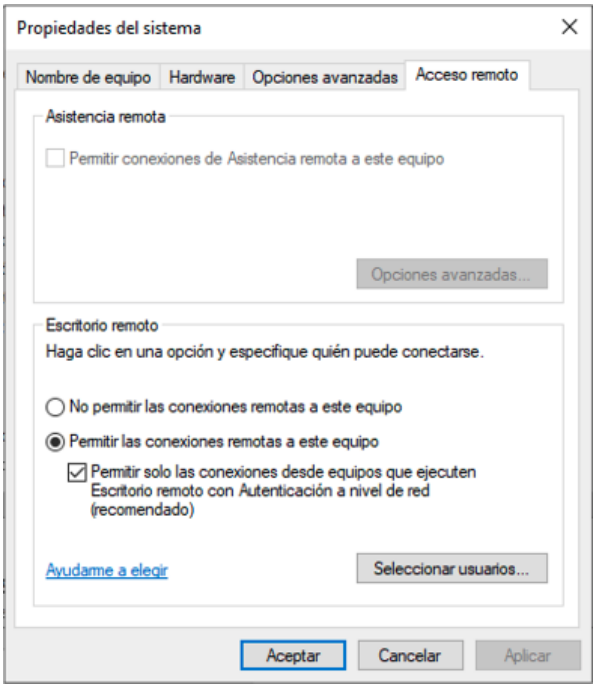
Tindrà dos adaptadors de xarxa, un a la VLAN 10 per a poder crear les copies de seguretat dels fitxers de la xarxa de producció i altra en la VLAN 99 per al seu manteniment i gestió per part del administrador.



Il·lustració 102 - Especificacions Veeam

Arrancarem la maquina virtual, per a començar amb la instal·lació del Windows Server 2019 al igual que hem fet amb el servidor ERP. Una vegada finalitzat el procés de instal·lació, habilitarem l'accés per escriptori remot.

Al ser diferent sistema operatiu, l'accés remot es configura a la pestanya de propietats del sistema.



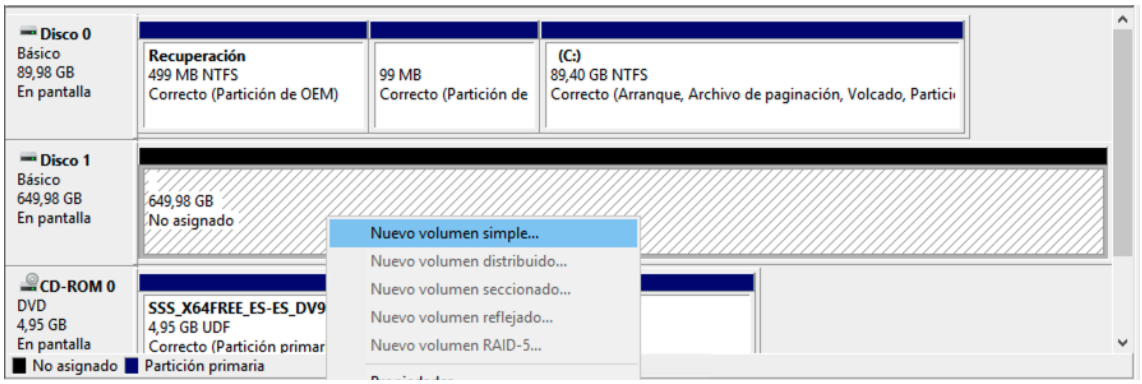
Il·lustració 103 - Escriptori remot Veeam

Una vegada habilitat l'escriptori remot podrem accedir a la maquina virtual des de qualsevol equip de la xarxa o des de el exterior sempre que estigam connectats via VPN.

Il·lustració 104 - Escriptori remot Veeam

Preparació del sistema operatiu

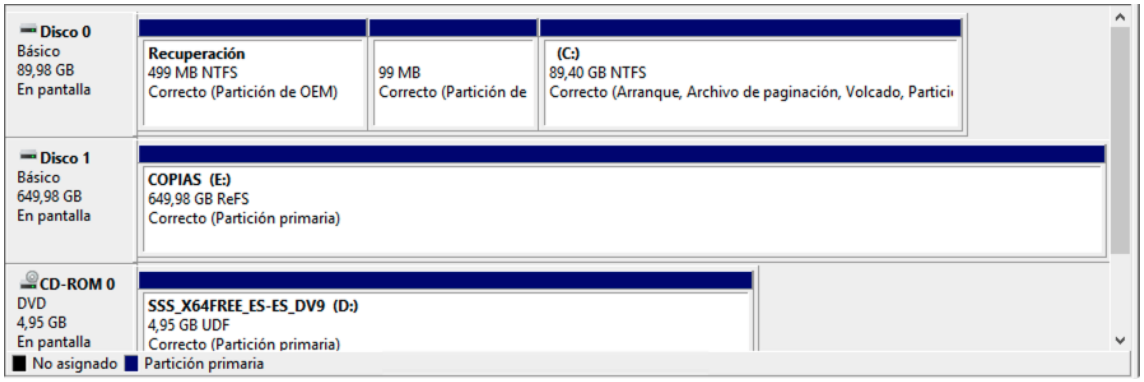
Al instal·lar el sistema operatiu estem obligats a formatar el disc on va a crear-se la partició del sistema, però el segon disc connectat al servidor es quede per reconèixer, per tant haurem de donar-li format.



Il·lustració 105 - Creació de Volum

Per al cas de Veeam es recomana crear un volum simple de tipus ReFS o Resilient File System. És un sistema d'arxius desenvolupat per Microsoft, introduït per primera vegada amb Windows Server 2012. Va ser dissenyat per a superar les limitacions dels sistemes d'arxius anteriors, com NTFS (New Technology File System), i oferir major resiliència, escalabilitat i rendiment en entorns d'emmagatzematge moderns.

El sistema ReFS utilitza un mecanisme de sumes de verificació per a detectar i corregir automàticament la corrupció de dades en temps real.

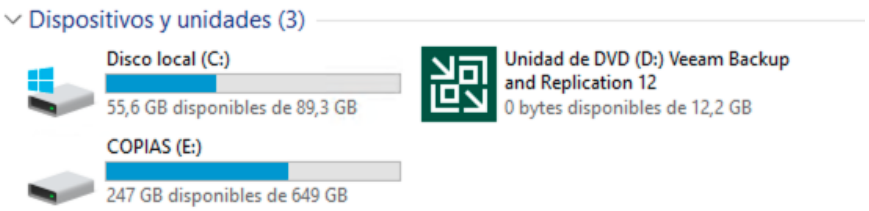


Il·lustració 106 - Volum ReFS

Configuració de Veeam Backup & Replication CE

El software de Veeam es pot aconseguir de la seua pagina web a traves del enllaç: https://www.veeam.com/es/products/free/backup-recovery.html

La descarrega te format ISO pel que deurem de carregar-la a la maquina virtual com un CD i executar el programa



Il·lustració 107 - Veeam ISO

El software treballa amb el que es coneixen com a Jobs o tasques, al ser llicencia gratuïta ens permet crear fins a 10, per al nostre cas nomes seran necessàries dos.

Job per al servidor ERP

Esta tasca serà l'encarregada de crear copies de la maquina virtual ERP. Es plantejarà de la següent forma:

- Es crearà un Backup incremental cada dia a les 20:45 menys els diumenges
- El Backup d'inici serà complet i es farà de forma incremental durant el propers 5 dies.
- Al sèptim dia es realitzarà un altre Backup complet i els propers 5 dies es realitzarà un Backup incremental.
- La política de retenció serà de 14 dies, pel que fins que no es completen dos períodes de 14 dies, 28 en total, no s'eliminaran els primers 14 dies.
- Es configurarà una política GFS (Grandfather-Father-Son) per Backup a llarg termini.
- Es configuraran notificacions de correu electrònic per a assegurar-nos que les copies de seguretat es realitzen de forma correcta.

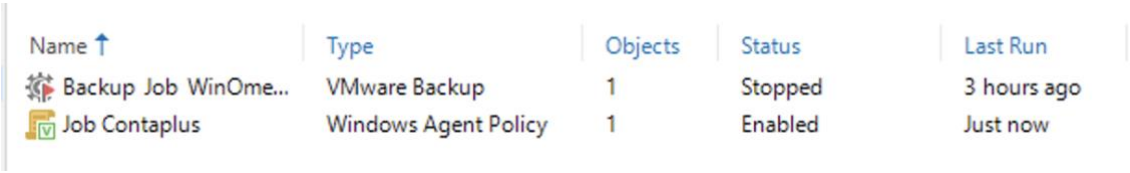
Job per al PC-Tenda

El PC-Tenda compta amb el programa de comptabilitat i finances Contaplus, es ací on l'empresa porta el control del saldo total, de les factures pagades de clients i proveïdors o les que estan per pagar.

Esta tasca serà l'encarregada de fer copies de la carpeta de treball del programa ContaPlus. Es plantejarà de la següent forma:

- Es crearà un Backup incremental cada dia a les 20:45 menys els diumenges
- El Backup d'inici serà complet i es farà de forma incremental durant el propers 6 dies.
- Al octau dia es realitzarà un altre Backup complet i els propers 6 dies es realitzarà un Backup incremental.
- La política de retenció serà de 14 dies, pel que fins que no es completen dos períodes de 14 dies, 28 en total, no s'eliminaran els primers 14 dies.

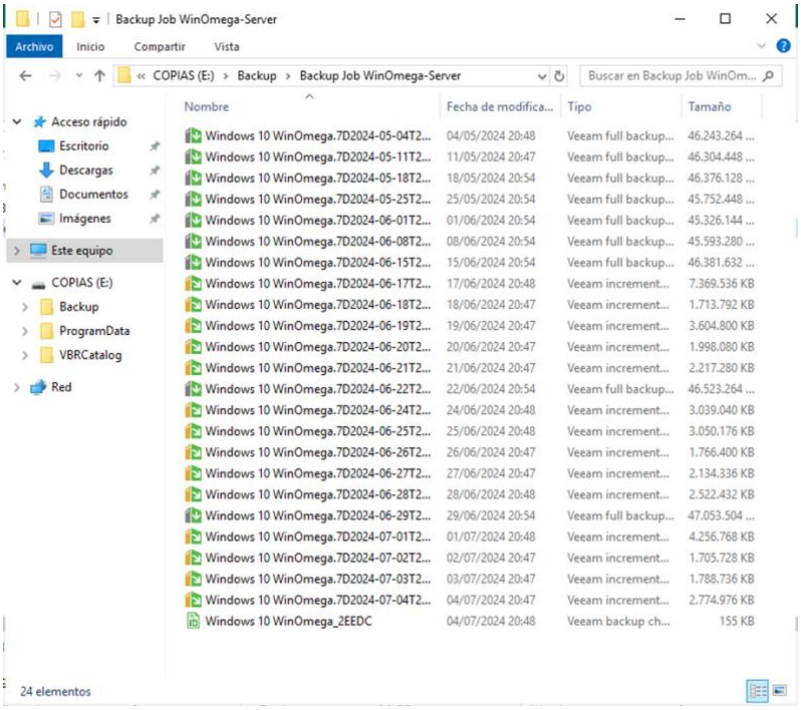
A la pestanya de Job podrem veure les nostres dos tasques de Backup.



Name	Type	Objects	Status	Last Run
Backup Job WinOme...	VMware Backup	1	Stopped	3 hours ago
Job Contaplus	Windows Agent Policy	1	Enabled	Just now

Il·lustració 108 - Resum tasques Backup

Es pot diferenciar entre la copia de tipus VMware, que esta dedicada a maquines virtuals i la copia de Windows Agent, orientada a equips individuals.



Il·lustració 109 - Fitxers de backup ERP

Primeres 7 línies: política retenció de 8 setmanes llarg termini.
Línia 8 a 12: Backup incremental diari.
Línia 13: Backup total de la setmana.
Línia 7 a 19: Política de retenció de 14 dies. (S'eliminaran quan la següent política de 14 dies es complete).
Línia 20 a fi: Inici de política de retenció de 14 dies

4. Conclusions i futures línies de treball

L'objectiu d'aquest treball de fi de grau era aconseguir una solució a una necessitat real de una empresa que buscava millorar els seus sistemes TIC, tant la xarxa de la empresa com el que coneguem com a sistemes.

Per a aconseguir aquest objectiu comencem sempre escoltant les necessitats del client. Durant unes primeres reunions es decidix tot el que va a fer falta per a dur a terme el projecte i s'acorda quin es el pressupost total.

Una vegada posades d'acord les dos parts, comença la part del disseny. Va ser necessari buscar equips de xarxa, com Router, Switch, AP que s'ajusten al pressupost del client complint amb les necessitats reals de la xarxa.

També serà necessari buscar un servidor per a virtualitzar el software ERP en el que es treballa a diari a l'empresa que estiga en bones condicions, ja que un dels nous se passaria per complet del pressupost del client.

La connectivitat física dels equips de l'empresa era un punt important a tenir en compte, mai abans havia realitzat cap instal·lació de cable de xarxa o semblant per tant no tenia cap tipus de practica ni experiència. Cabia la possibilitat de contractar un electricista encarregat de fer aquesta tasca, però amb l'ajuda del client em vaig decidir a fer-ho pel meu conter i baix la meua responsabilitat, resultant ser un poc tediós en alguns moments però sentint-me realitzat i acabant sent un èxit total en la instal·lació.

La xarxa es dissenya amb equips de la sèrie gama TELECO de TP-Link per el SDN OMADA de gestió de dispositius, que facilita realment la feina alhora de configurar equips existents o de adoptar-ne de nous.

A la part de sistemes el software ESXi em resulta bastant familiar degut a que ha estat present a la carrera com a les practiques, pel que em facilita la feina i no necessite de manuals de fabricant ni guies de configuració

En quant a la gestió de dades, no coneixia el software Veeam i ha resultat sent la gran sorpresa d'aquest TFG, es un software que requerix de molt poques hores de aprenentatge i facilita molt la feina en quan a la restauració de fitxers però sobretot de maquines virtuals es tracta.

Com a futures millores, esta planificat adquirir un NAS de la marca Synology, per a implementar un Job al Veeam que ens cree un Backup a casa del client, connectat per VPN. D'aquesta manera prevenir qualsevol pèrdua de dades per fallades del servidor o per catàstrofes naturals com puga ser un incendi a l'oficina.

Queda pendent ampliar espai al servidor per a millorar les polítiques de retenció.

I per últim la ampliació de la xarxa CCTV amb la instal·lació de mes càmeres de seguretat.

5. Bibliografia

Atenuació Wireless. (2022). *Syscomblog.com*. https://www.syscomblog.com/2022/09/cuales-son-los-tipos-de-atenuacion-wi.html

Omada SDN Controller User Guide. (s/f). Tp-link.com. https://www.tp-link.com/us/user-guides/omada-sdn-software-controller/

RAID. (2019). MercadoIT. https://www.mercadoit.com/blog/analisis-opinion-it/niveles-de-almacenamiento-de-datos-raid-5-y-raid-6/

SDN. (2021). Huawei. https://info.support.huawei.com/info-finder/encyclopedia/en/SDN.html

Veeam Backup and Replication CE. (2020, diciembre 30). Youtube. https://www.youtube.com/watch?v=XuFo4pmv9Mk

VLAN. (2022). Huawei.com. https://forum.huawei.com/enterprise/es/VLAN-en-Ethernet/thread/667232489518809088-667212890693840896

Wi-Fi. (2023). Wavlink.com. https://www.wavlink.com/en_us/article/details/WiFi_6_Technical_Features.html

6. Annexos

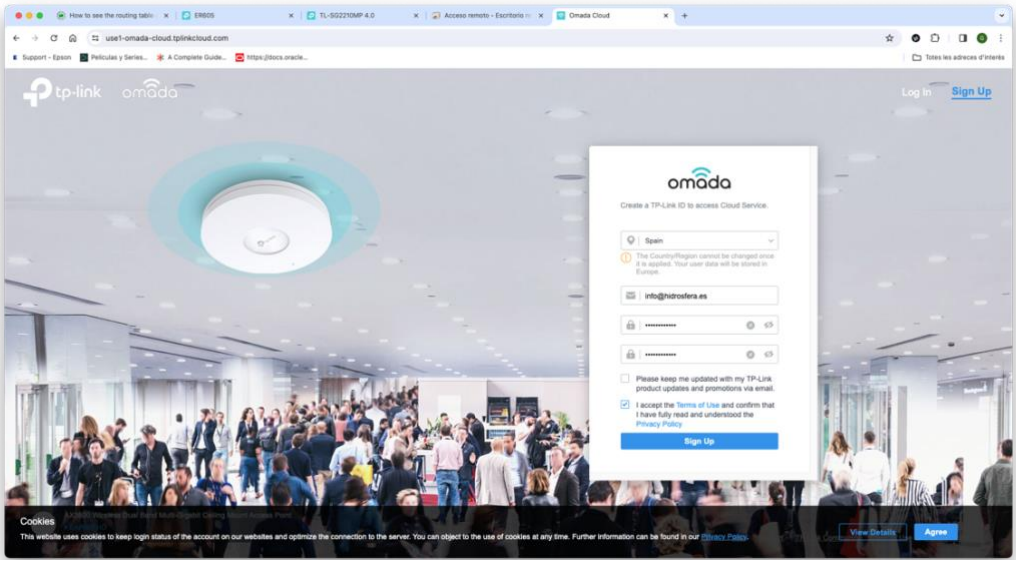
6.1 Configuració Controller Omada

Per configurar els equips escollirem el mode controlador que mencionava als fonaments teòrics, lo principal serà connectar el OC a internet (Omada Controller), per açò connectarem al nostre Router IPS, el Router ER605 al port WAN, un dels Switch al Router i finalment el Controller a un dels ports PoE del switch.

El que necessitem es que el Router comence a entregar direccions IP, ja que per defecte, te el servidor DHCP habilitat.

Per a accedir al seu entorn web serà necessari registrar-se en la web de Omada cloud:

https://use1-omada-cloud.tplinkcloud.com



Il·lustració 110 - Registre Usuari Omada

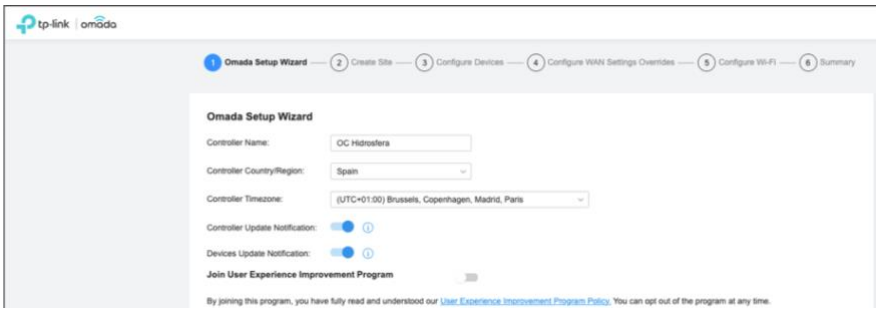
Una vegada registrats i fet el login, deurem registrar el OC200 al nostre conter de Omada. Si es la primera vegada que configurem un controlador, ens obrirà una guia rapida de configuració en la que ens demanarà que el nostre OC estiga connectat a internet:

Il·lustració 111 - Afegir OC

Una vegada connectat a internet el controlador OC, deixarà de parpellejar el LED superior “cloud”. Es ara quan emparellarem el OC mitjançant la seua MAC address.

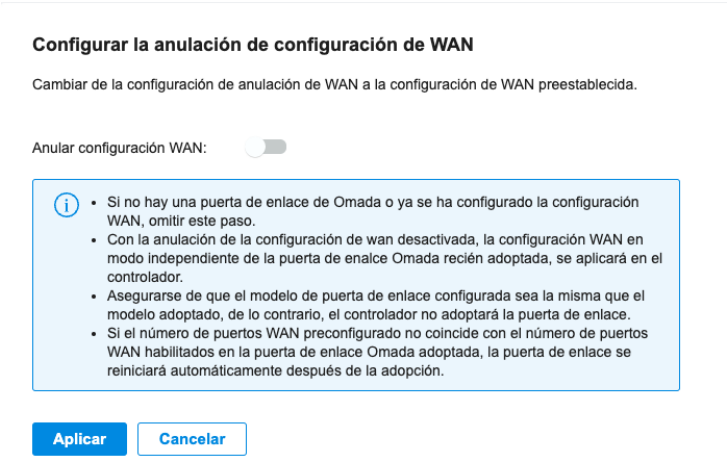
Il·lustració 112 - Emparellar OC

Seguint amb el assistent de configuració, el primer pas serà dona-li nom al controlador, establir una localització i una zona horària fonamental per a la recollida de notificacions (logs) del sistema.



Il·lustració 113 - Assistent pas 1

El pas mes important i el únic que precisa de comprensió del assistent de configuració es aquest, si volem restaurar el Router TP-Link i que el assistent el “auto-configure”, marcarem aquesta opció. Si pel contrari ja l’hem configurat de forma manual, ja siga amb obtenció de IP de forma dinàmica o amb usuari PPPoE, la deixarem des-habilitada.

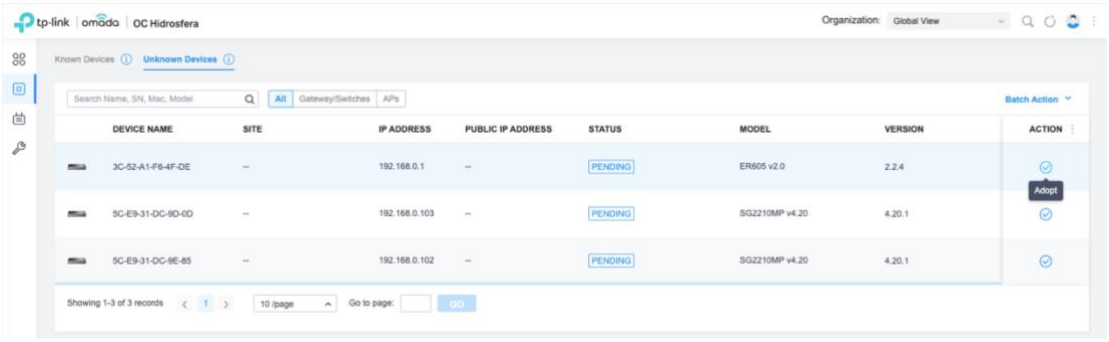


Il·lustració 114 - Anul·lació de configuració de WAN

6.2 Adoptar equips

Adoptar equips ens permet equips nous o equips amb configuració, convertir-los en membres de la nostra organització i així aconseguir unificar la gestió al nostre controlador Omada.

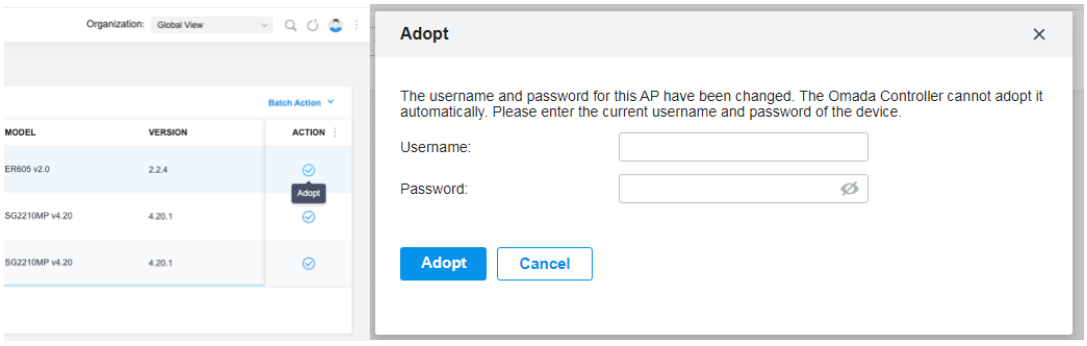
Sempre que el controlador tinga equips al abast que es puguen adoptar, els mostrarà a la pestanya de dispositius desconeguts amb l'estat **pendent** i com a acció podrem adoptar.



Il·lustració 115 - Equips per adoptar

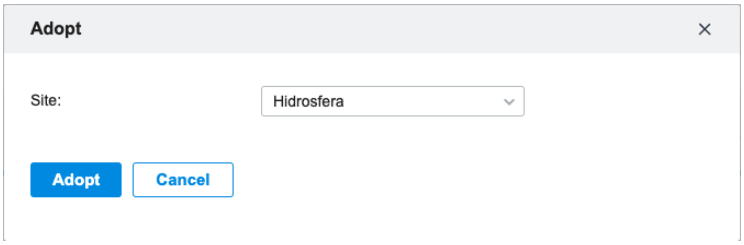
Adoptar un equip

Per a adoptar un equip deurem de fer clic a la icona de la dreta on es mostra **adopt** i, si es necessari, posar el usuari i contrasenya per defecte admin/admin.



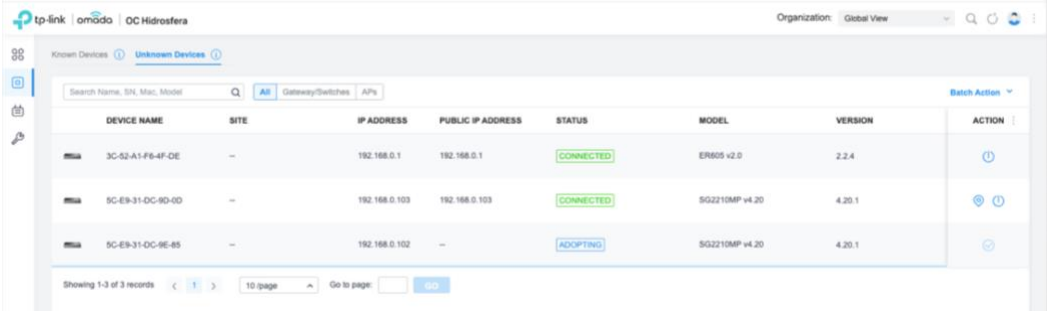
Il·lustració 116 - Adoptar un equip

Els afegirem a un Site o lloc, ja que amb el mateix controlador podríem configurar mes de un Site en les oficines



Il·lustració 117 - Adoptar Site

Si no hi ha cap error durant el procés d'adopció deuríem de veure al nostre panel els equips com a **connectats.**



Il·lustració 118 - Equips adoptats

Des d'aquest moment, els equips passen a treballar baix la gestió del controlador Omada i si tractem d'accedir a ells via web ens mostraran un missatge d'error.

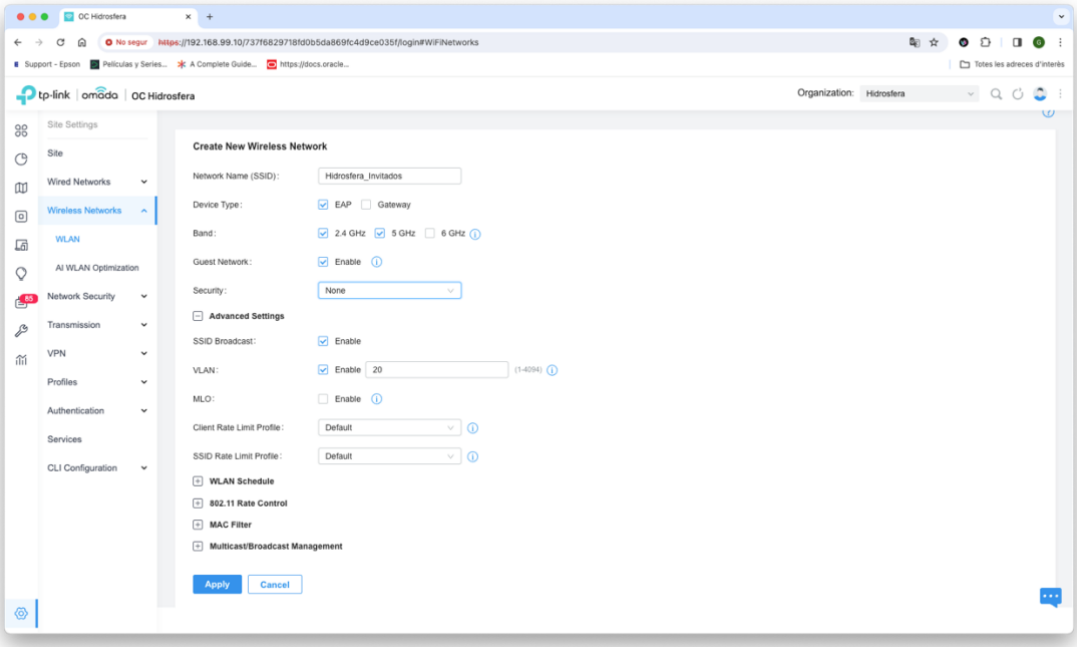
Il·lustració 119 - Equips controlats per OC

6.3 WLAN Convidats

La WLAN (Wireless Local Area Network) de convidats serà una xarxa wireless oberta, però al connectar-se a ella els usuaris deuran de autenticar amb unes credencials facilitades per l'empresa, que els limitarà el tràfic en quan a temps, velocitat de carrega i descarrega o algun altre tipus de restricció. Aquesta tècnica d'autenticació es coneguda com a Hotspot o portal captiu.

Els passos per a la seua configuració son els següents:

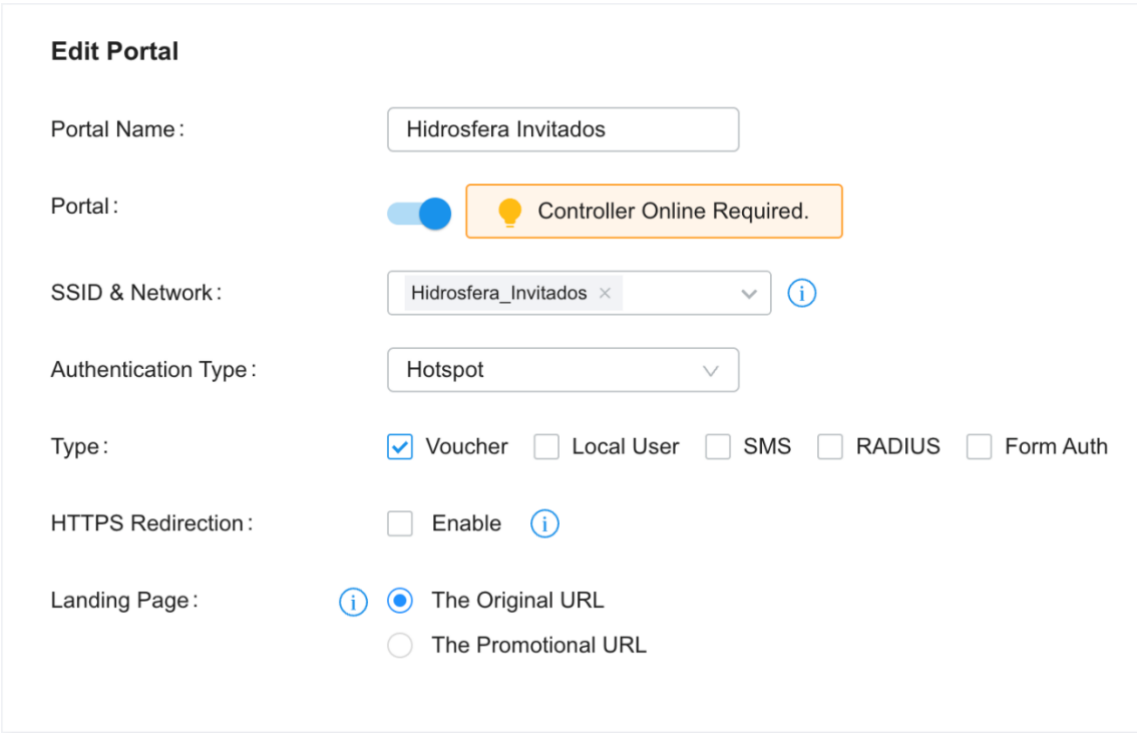
- Al la secció **Wireless Networks** crearem una nova xarxa wireless, que tindrà com a SSID "Hidrosfera_Invitados".
- Direm que aquesta xarxa treballarà als equips de tipus EAP a les bandes 2.4GHz, 5GHz i 6Ghz.
- Al habilitar la casella "Guest Network" els AP s'encarregaran de aïllar la xarxa wireless de la resta de la xarxa, evitant així que qualsevol persona aliena a la xarxa tinga accés als recursos d'aquesta.
- La deixarem sense seguretat en un primer moment, vindrà configurada pel Hot Spot.
- Per últim indicarem a quina VLAN pertany amb el VLAN ID, açò ens assignarà IP del Pool (rang) de la VLAN 20.



Il·lustració 120 - WLAN Convidats

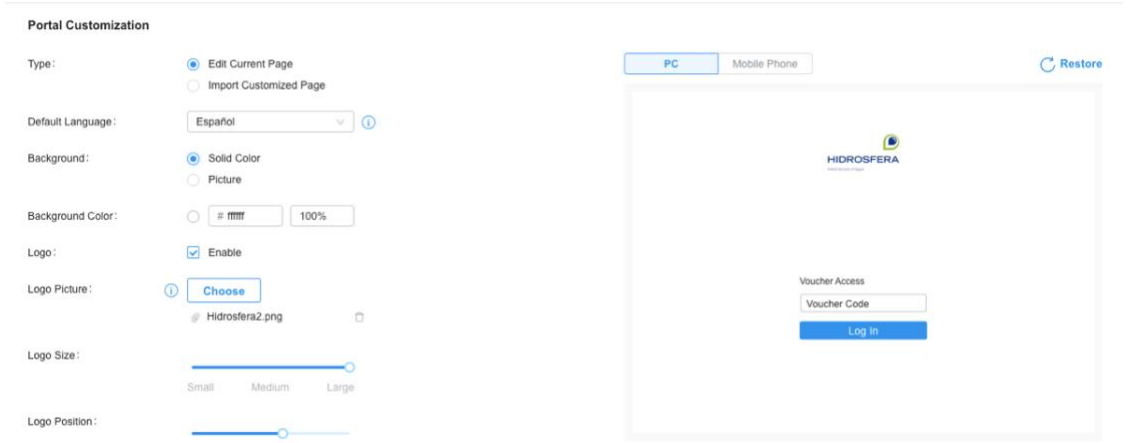
Ens dirigirem al apartat Portal, ubicat en la pestanya de configuracions del controlador, a la secció de **authentication**, crearem un Portal amb el nom de referencia i li indicarem sobre quin SSID treballarà.

L'autenticació serà de tipus HotSpot i el tipus Voucher, es a dir tiquets.



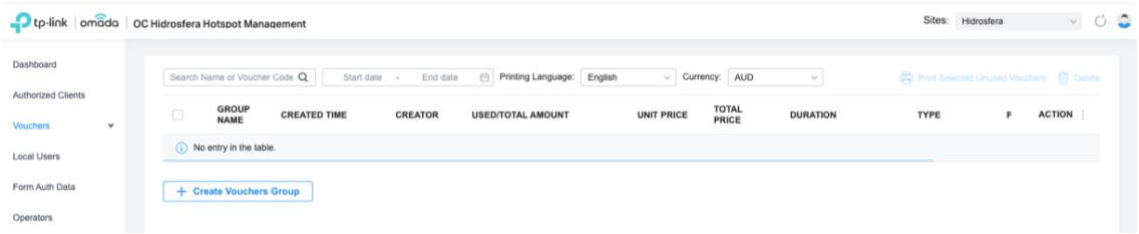
Il·lustració 121 - Portal Captiu WLAN Convidats

El portal captiu ens permet personalitzar-lo de manera que els usuaris sàpiguen que estan connectant-se a la xarxa corporativa i inspire així també cert grau de confiança i professionalitat.



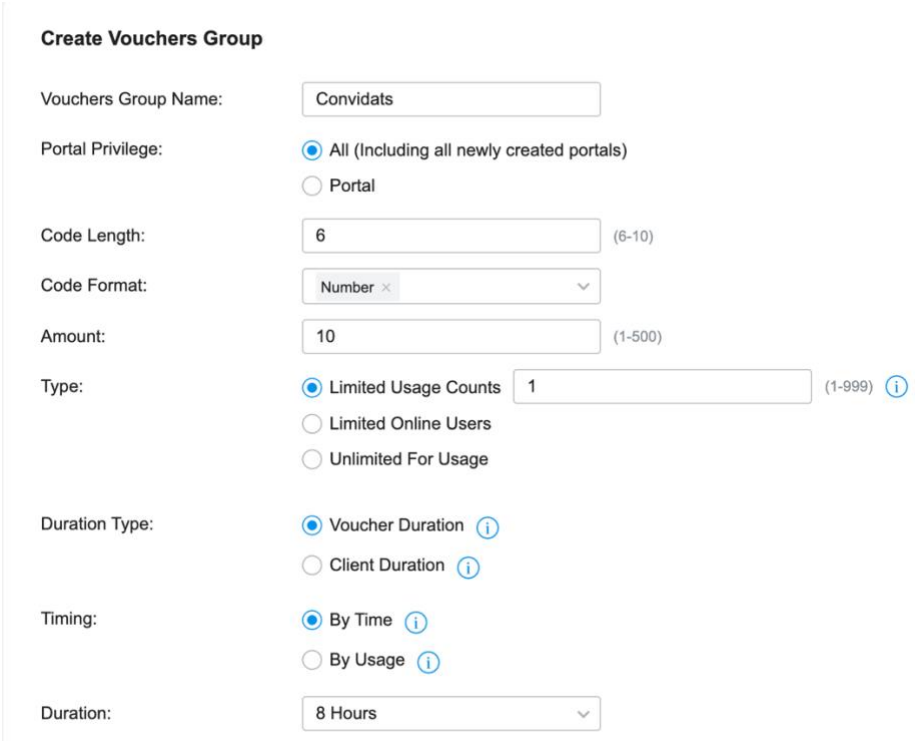
Il·lustració 122 - Disseny portal captiu

Per últim quedarà crear els tiquets que es repartiran quan un client, comercial o convidat en general, desitge connectar-se a la xarxa wireless. Açò permetrà al encarregat de tenda o empleat de l'oficina proporcionar accés a la xarxa, sense tindre que facilitar les credencials de la xarxa wireless de producció, mantenint així la seguretat de la xarxa i la segmentació i sense tindre que recordar o consultar les credencials de usuari.



Il·lustració 123 - Creació de Vouchers

- Assignarem un nom de identificació al grup de tiquets.
- Com sols tenim un portal captiu seleccionem ALL.
- Escollim el nombre de dígits que tindrà el tiquet generat.
- Podem escollir entre un codi numèric o un codi de alfabètic.
- La quantitat de tiquets que volem generar.
- Tipus de us: Nombre de usos per codi, Nombre de usuaris per codi o il·limitat.
- Duració: Per client o per tiquet
- Temps de duració: Per minuts, hores, dies o per data de us.



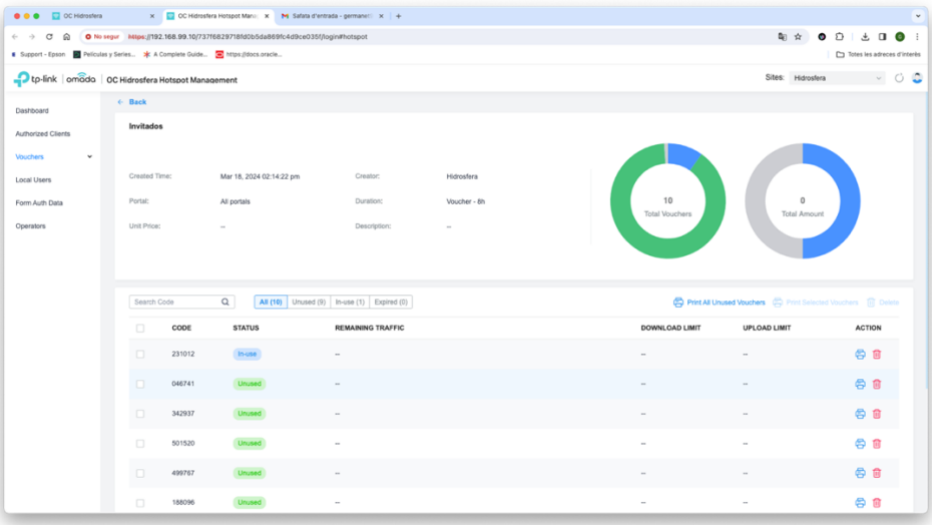
Il·lustració 124 - Parametres dels Vouchers

Una vegada creats els podrem visualitzar o imprimir per a tindre'ls mes accessibles.

046741 Válido por 8h Cuenta de uso limitado 1 Validación: 2024-03-20 -- 2025-03-20	**342937** Válido por 8h Cuenta de uso limitado 1 Validación: 2024-03-20 -- 2025-03-20

Il·lustració 125 - Format Voucher

Al panel de control tindrem una visió de cada un dels tiquets i de si estan en us, han sigut utilitzats o estan sent utilitzats en aquest mateix moment i poder ampliar la concessió de dispositius

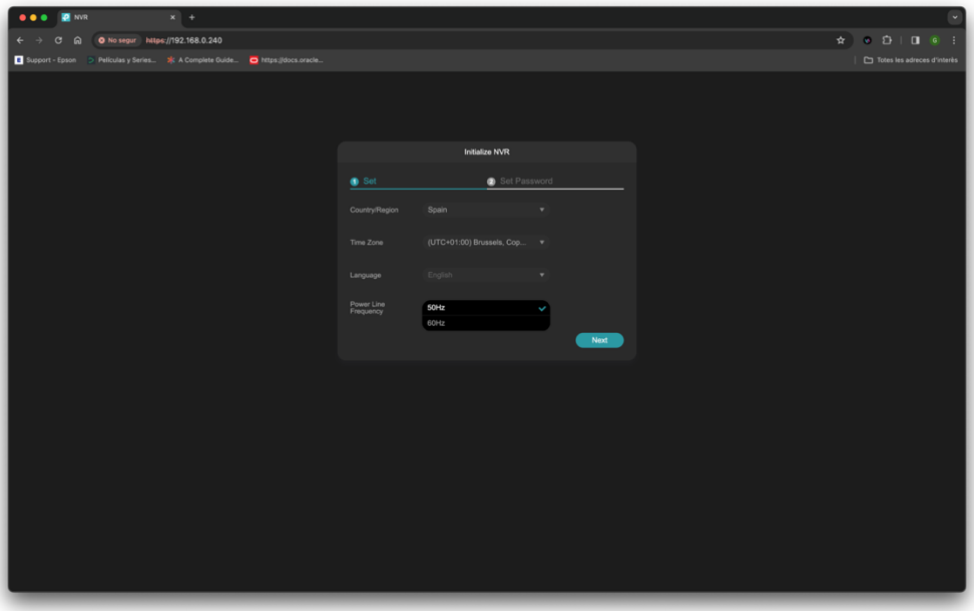


Il·lustració 126 - Gestió Voucher

6.4 CCTV

El CCTV ve configurat per dos parts, la configuració del gravador i la adopció de les càmeres.

El gravador es configura a traves de la IP per defecte que ens proporciona el fabricant accedint a la URL http://192.168.0.240

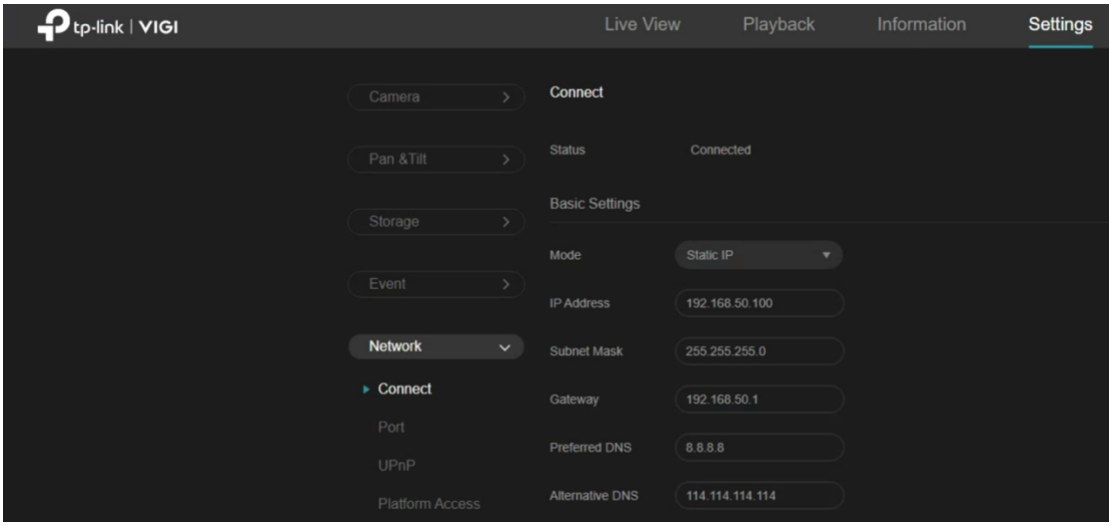


Il·lustració 127 - Assistent config CCTV

Una vegada configurada la ubicació i la data, ens sol·licitarà que creem una contrasenya.

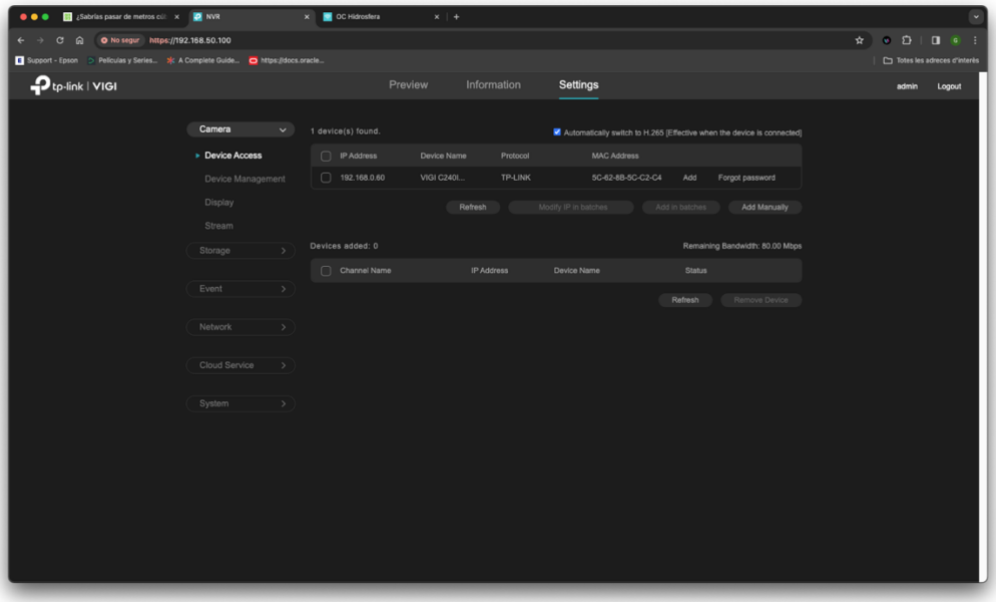
Quan finalitzem els primers passos de configuració amb l'assistent podrem assignar-li una direcció IP per a incloure'l a la xarxa corresponent.

Es convenient posar una IP estàtica per a sempre ser accessible apuntant a la mateixa direcció per a facilitat les coses al usuari final.



Il·lustració 128 - IP fixa CCTV

Per últim sols caldrà afegir les càmeres connectant-les al gravador i esperant a que les reconega.



Il·lustració 129 - Panel gestió càmeres

Al moment d'afegir-les podrem fer-ho modificant la IP o afegir-la amb la IP que ha agafat amb el servidor DHCP de la VLAN 50 en aquest cas.

Il·lustració 130 - Càmera per adoptar

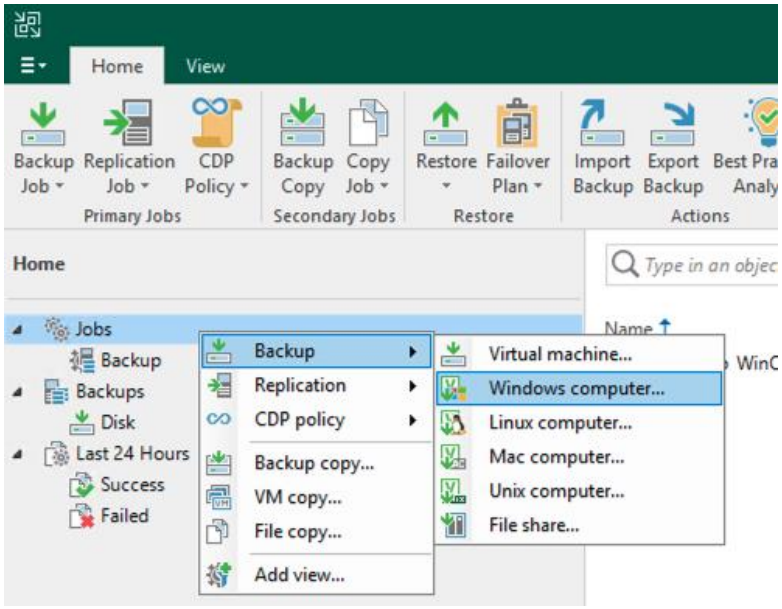
Una vegada emparellades podrem canviar-li el nom i altres paràmetres de configuració de vídeo i àudio

Il·lustració 131 - Càmeres adoptades

6.5 Creació tasca Backup Veeam

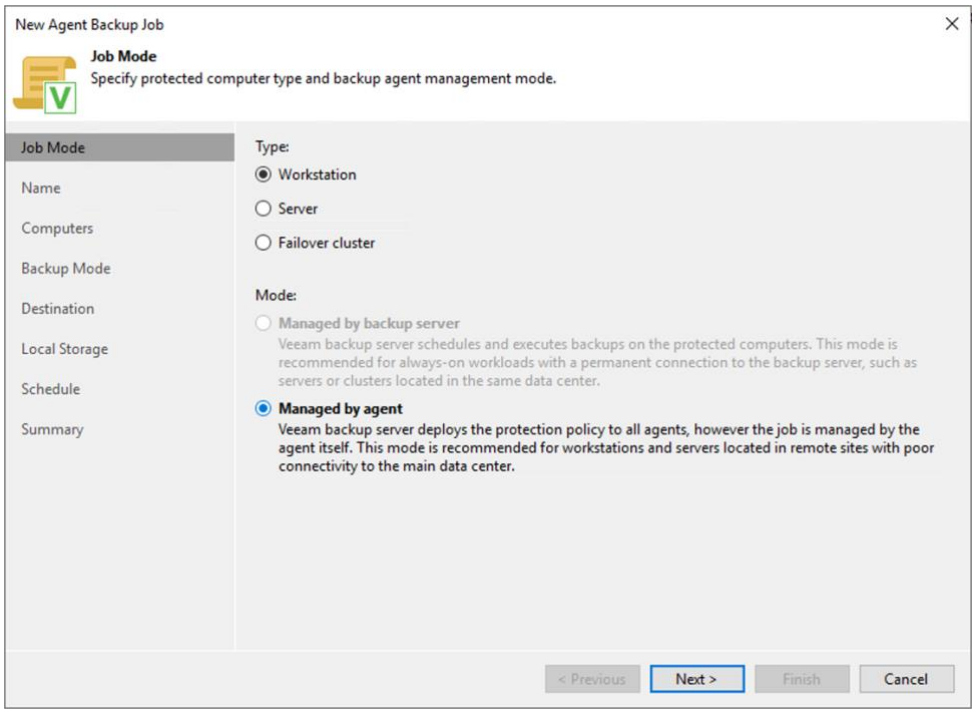
Este punt mostrarà el procés de creació d'una tasca de Backup per a un equip Windows.

El primer pas es dirigir-nos a la pestanya de Jobs, i les opcions de Backup, escollir Windows computer.



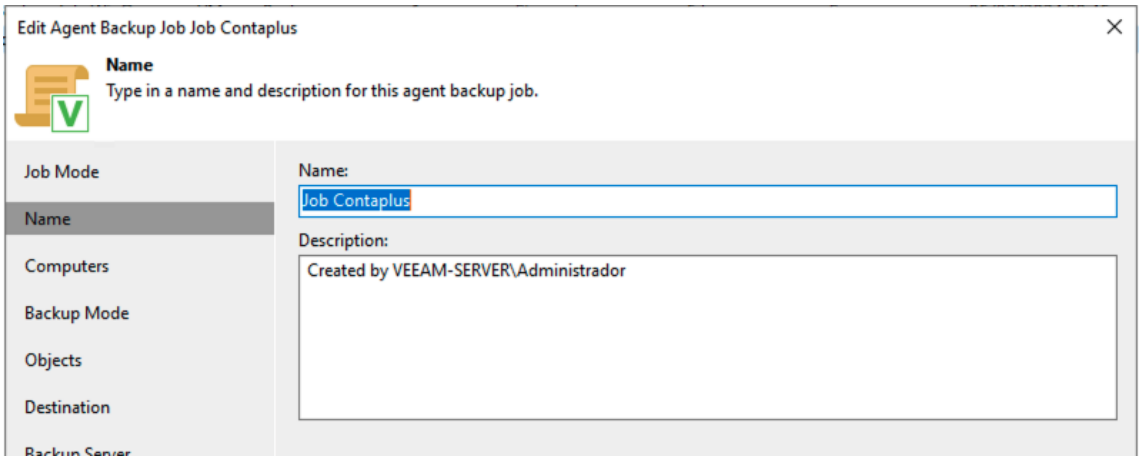
Il·lustració 132 - Job (1)

Se'ns obrirà el assistent de configuració de Jobs. Seleccionarem la opció Workstation ja es tracta d'un equip de treball individual.



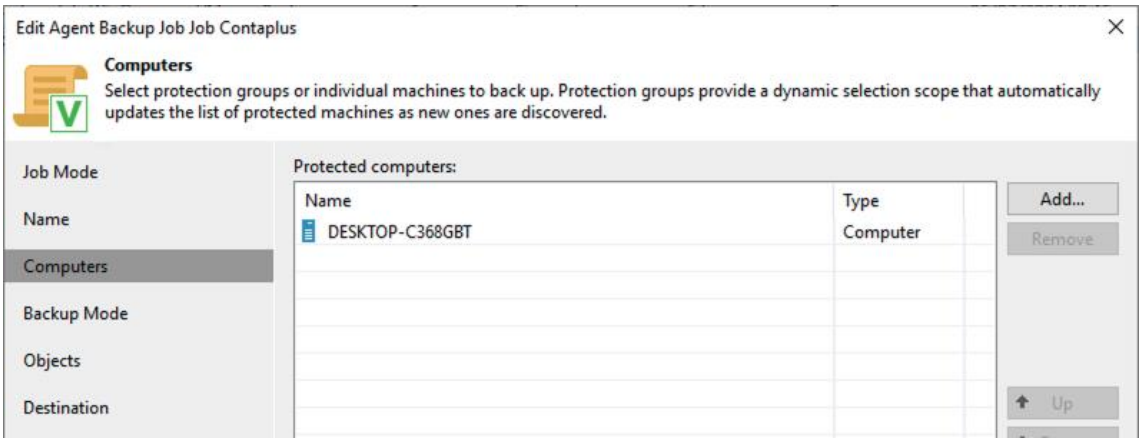
Il·lustració 133 - Job (2)

Assignarem un nou que identifique fàcilment al Job que estem creant.



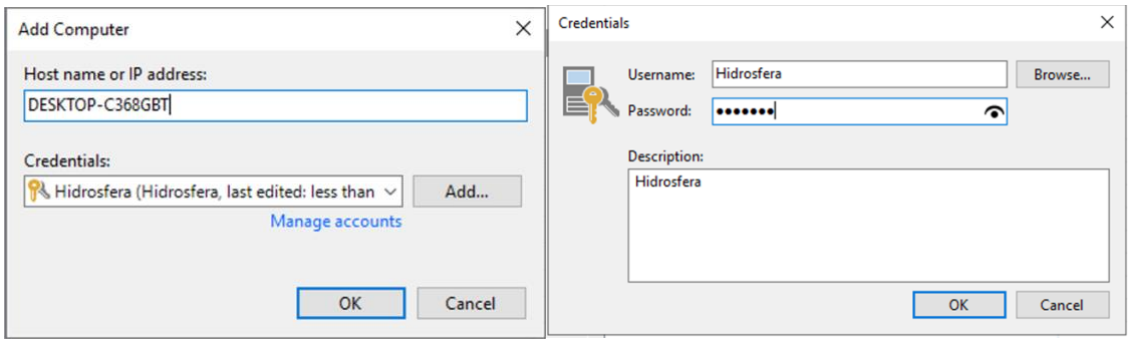
Il·lustració 134 - Job (3)

El següent punt haurem d'afegir el ordinador al que anem a connectar-nos per a realitzar les copies de seguretat



Il·lustració 135 - Job (4)

Afegirem un ordinador ja siga per IP o per nom de equip. Si 'equip va tindre una IP estàtica podrem afegir-lo per IP, pel contrari si l'equip rep IP a traves de DHCP serà convenient associar-lo amb el nom del equip.

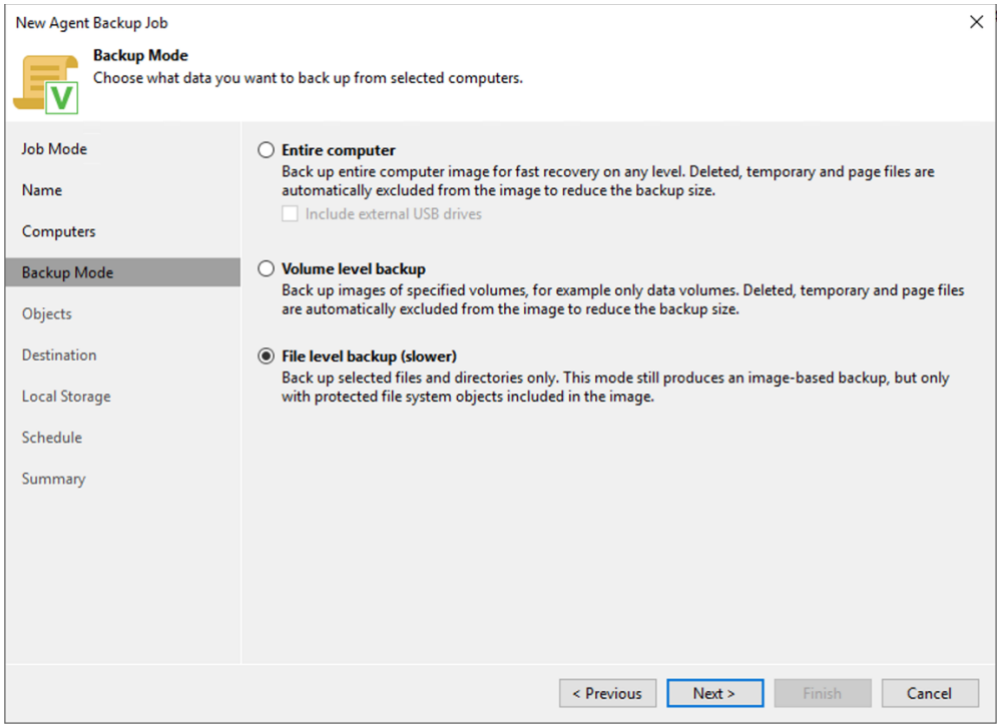


Il·lustració 136 - Job (5)

Caldrà afegir unes credencials de usuari del equip que estem tractant de afegir i que aquest usuari tinga permisos de administrador.

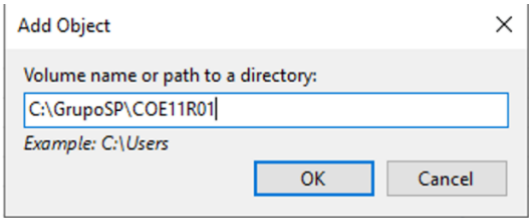
El mode Backup indica quina de part del ordinador volem fer una copia de seguretat. Podent escollir entre:

- **Entire Computer**: Ordinador complet
- **Volume level backup**: Volums específics ja que podem comptar amb volum de sistema i volum de dades.
- **File level backup**: El escollit en aquesta guia ja que ens permet copiar una ruta concreta, ja siga una carpeta de treball d'un programa o la carpeta de baixades del nostre equip.



Il·lustració 137 - Job (6)

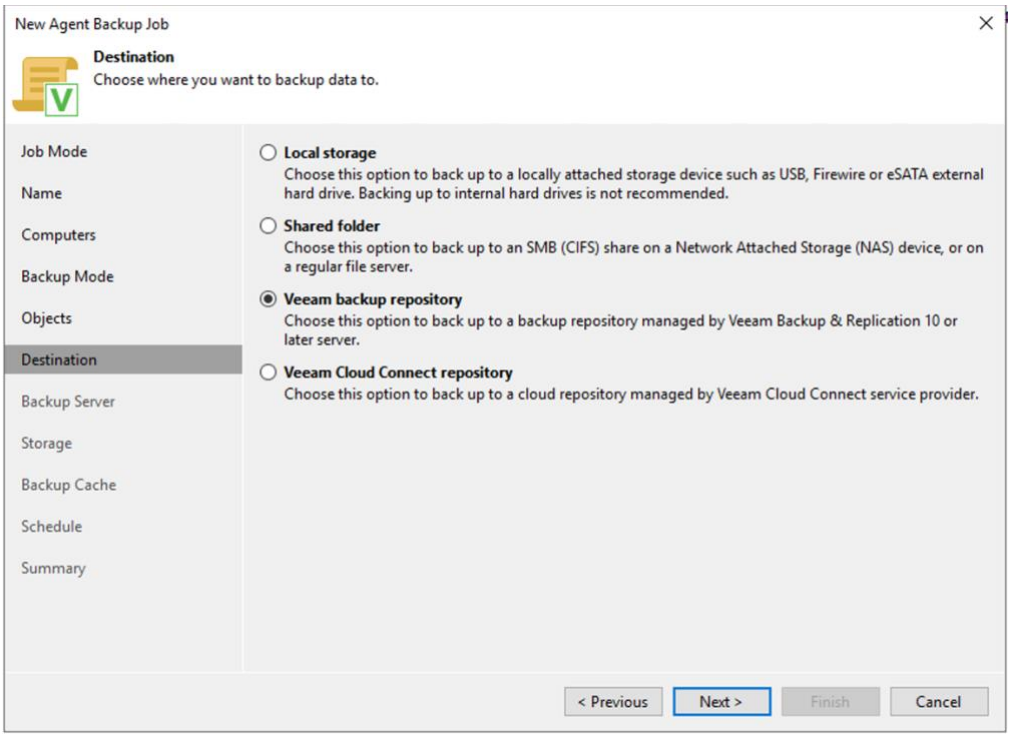
En este exemple es copia la carpeta de treball del software ContaPlus



Il·lustració 138 - Job (7)

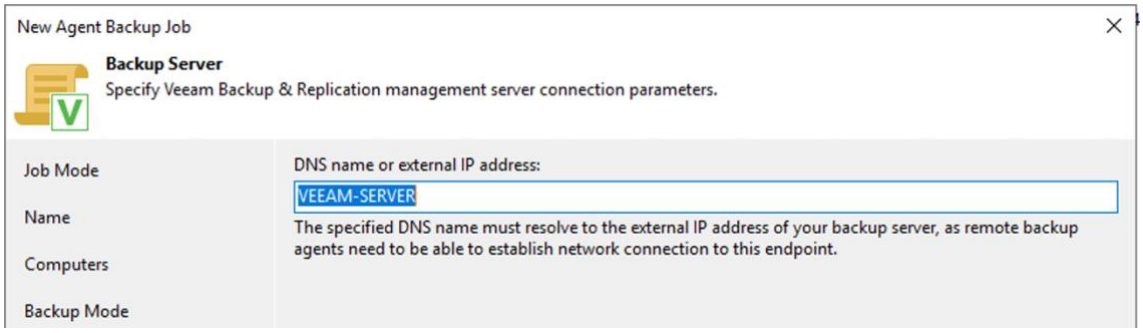
El destí fa referencia on es guardarà la copia una vegada realitzada:

- Equip local on estem realitzant la copia
- Carpeta compartida, NAS, SMB
- Veeam repository – Servidor Veeam
- Veeam Cloud – Servidor Veeam en el nuvol



Il·lustració 139 - Job (8)

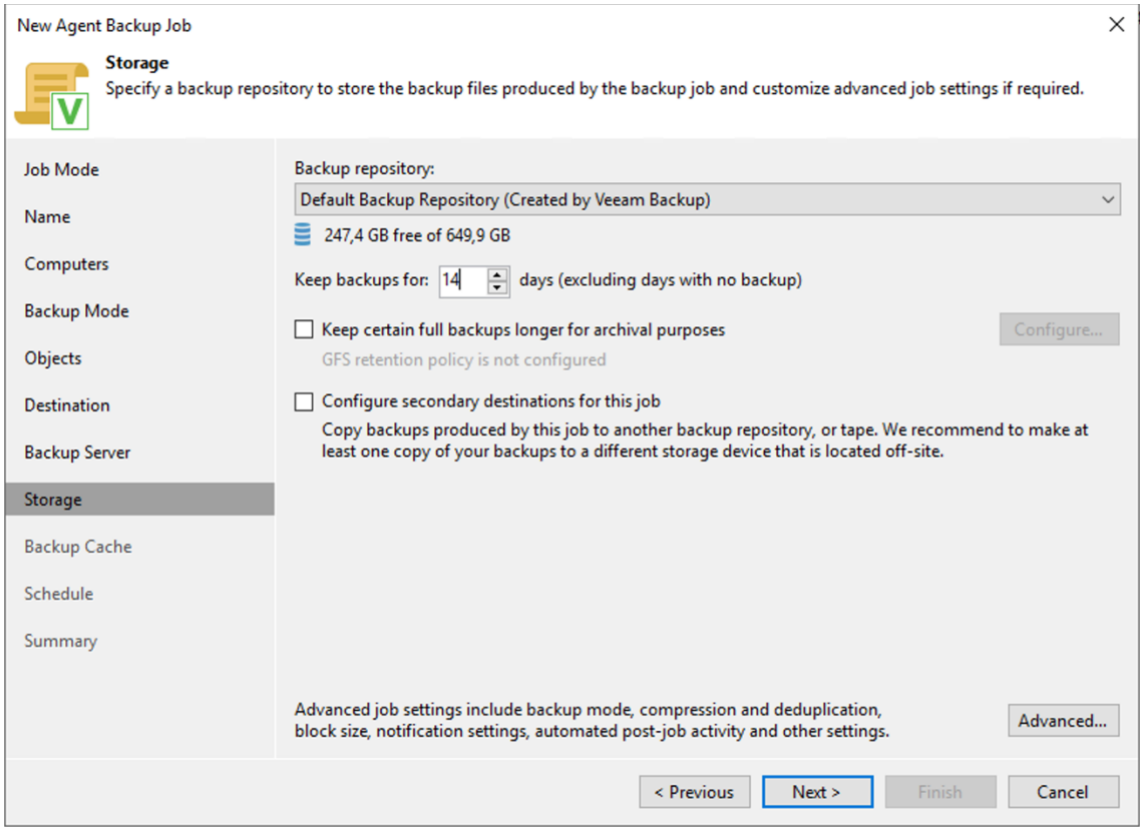
Al escollir la opció Veeam Backup Repository em de fer referencia al nom del propi servidor Veeam (Windows Server 2019).



Il·lustració 140 - Job (9)

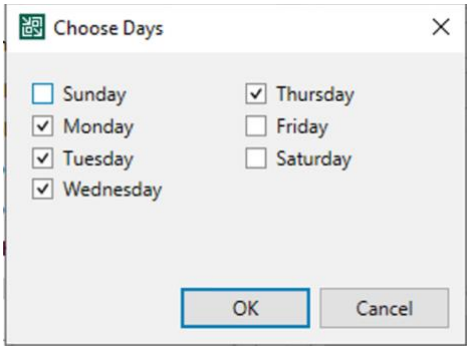
Podria donarse el cas que tinguérem altre servidor Veeam en local encarregat sols de emmagatzemar les copies i per tant podríem fer referencia a ell.

Política de retencions, en el cas de la copia de seguretat del software ContaPlus, es configurarà per a que es quede emmagatzemada durant 14 dies. Açò crearà una copia completa de la carpeta i anirà fent-la de manera incremental fins al dia 14 que la tornarà a fer completa, serà ara quan començarà el cicle de nou. Una vegada completat el segon cicle, podrà eliminar la primera copia completa.



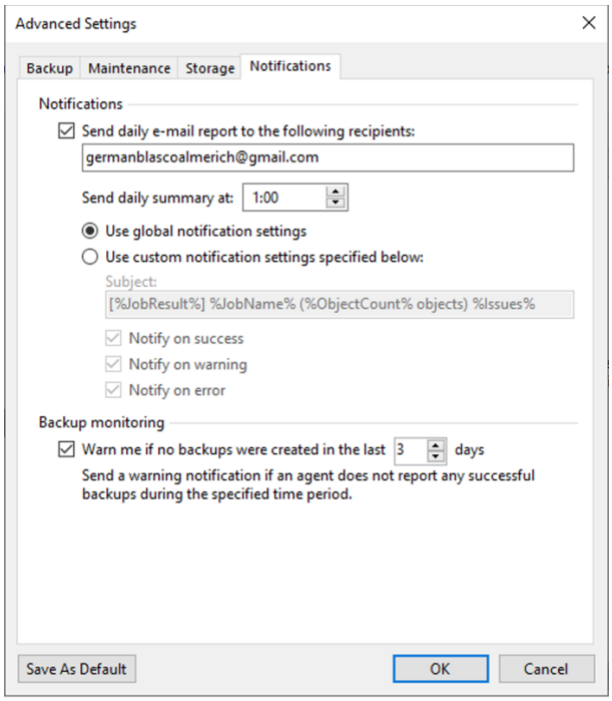
Il·lustració 141 - Job (9)

El Job s'executarà els dies seleccionats degut a que la persona responsable de facturació esta únicament de dilluns a dijous a l'empresa, llevant així carrega de treball a la xarxa.



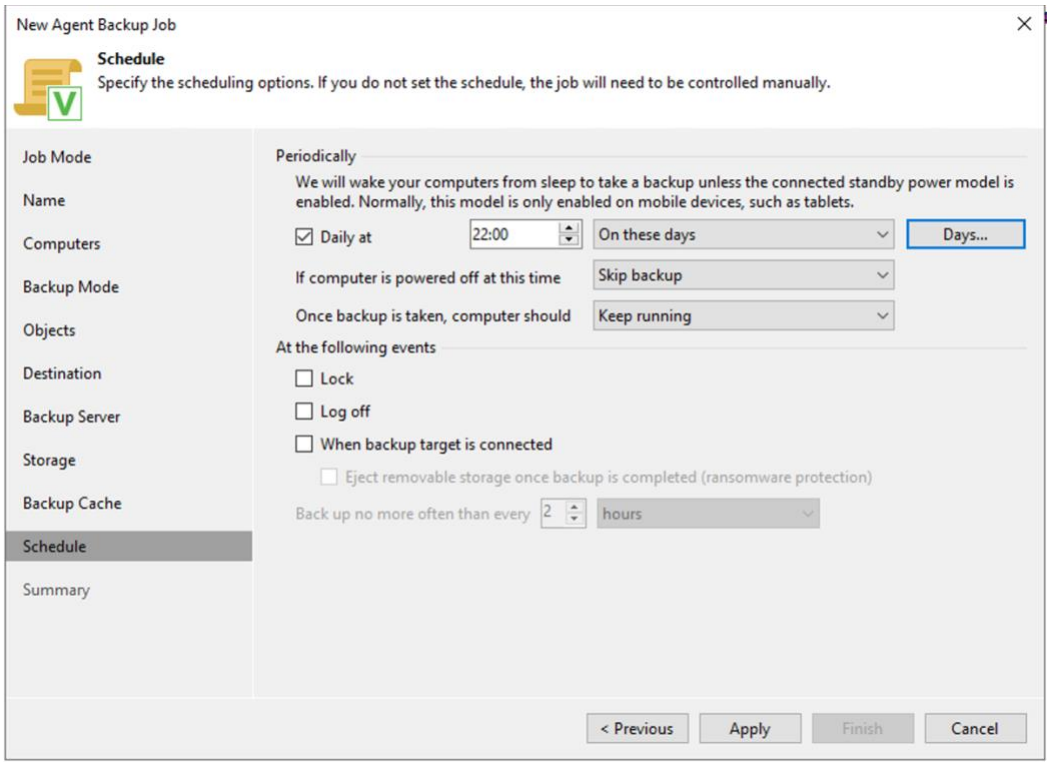
Il·lustració 142 - Job (10)

A al menú avançat de configuració, podem escollir que ens notifiquen cada vegada que es realitze una copia de seguretat i que ens notifique si fa X dies que no s'ha realitzat



Il·lustració 143 - Job (11)

Per ultim indicarem a quina hora es realitzaran les tasques. Es recomanable fer-ho en horaris fora de oficina degut a que solen ocupar un gran ampli de banda i poden arribar a dificultar les tasques del dia a dia.



Il·lustració 144 - Job (12)