Optimització de les comunicacions LAN i WAN

Rubén Navarro Martínez
Grau d'Enginyeria Informàtica

Manuel Jesús Mendoza Flores

07/06/2017

FITXA DEL TREBALL FINAL

Títol del treball:	*Optimització de les comunicacions LAN i WAN.*
Nom de l'autor:	*Rubén Navarro Martínez*
Nom del consultor:	*Manuel Jesús Mendoza Flores*
Data de lliurament (mm/aaaa):	*06/2017*
Àrea del Treball Final:	*Administració de Xarxes i SO*
Titulació:	*Grau d'Enginyeria Informàtica*

Resum del Treball (màxim 250 paraules):

El treball pretén presentar una via d'optimització de recursos i costos, així com millorar la garantia d'estabilitat en relació a les connexions LAN i WAN d'una organització tipus amb seu central i una altre seu satèl·lit.

El document contindrà les diferents fases que hauria de tenir un projecte d'aquest tipus en una implantació real: presentació de tecnologies emprades, anàlisi de situació actual, proposta d'alternatives, selecció de solució final i la implementació de la solució (simulada en aquest cas).

Abstract (in English, 250 words or less):

This project looks for a possible route of optimization of resources and economic costs, to guarantee the stability of the LAN and WAN communications of an organization composed by headquarters and a branch located in another city.

The document contains the different phases that a project of this type would have: presentation of technologies used, analysis of the current situation, alternatives proposal, selection and implementation of the final solution (simulated in this case).

Paraules clau (entre 4 i 8):

SDWAN, DMVPN, Switching, Redundància, Optimització.

Índex

Llista de figures

1. Introducció

1.1 Context i justificació del Treball

Avui en dia les xarxes LAN són el motor i/o la base de qualsevol infraestructura TIC d'una organització. Tot i ser una part molt important, no se li dona el pes i la importància que haurien de tenir i, molt sovint, ens trobem amb organitzacions (de qualsevol mida i número de treballadors) que conten amb infraestructura de xarxa precària o, encara més preocupant, amb bona infraestructura però configurada de forma que no s'aprofita el gran potencial latent.

Una xarxa LAN multi seu i una WAN no aprovisionades i/o aprofitades correctament poden comportar els següents problemes:

- Gran exposició a talls de comunicació. Derivant en producció negativa segons l'impacte i sector de l'organització.
- Alts costos de comunicacions WAN derivats d'una optimització inexistent.
- Experiència d'usuari negativa versus el rendiment de les aplicacions corporatives.

Aquest treball, es basa en un escenari fictici però que respon a un model d'organització habitual que requereix de serveis de consultoria de xarxes per a fer una millora substancial de la xarxa interna, de les comunicacions entre seus i de l'optimització de la WAN.

El context del treball és el d'una organització la qual té tres seus: una central i dos més situades a un altre país. Tal i com s'ha indicat anteriorment, tot i ser un escenari fictici, podem trobar que moltes organitzacions responen a aquest esquema de seu central i satèl·lits en les quals les comunicacions estan centralitzades a la seu central.

Dins del projecte s'analitzaran i es buscaran solucions per tal de que les dues seus, Dieuze i París, contin amb unes comunicacions internes estables i redundades, amb una comunicació eficient entre seus (DMVPN) i amb un creixement exponencial de l'aprofitament de l'amplada de banda WAN (SDWAN).

1.2 Objectius del Treball

A continuació s'identifiquen els diferents objectius a assolir amb la realització d'aquest projecte:

- Garantir la redundància de connectivitat (LAN) per als elements que requereixin alta disponibilitat.
    - Disseny d'una topologia física redundada.
    - Reduir a mínims la possibilitat de que la fallada d'un element de xarxa comprometi la resta.
- Garantir l'aprofitament de les connexions entre seus.
    - Possibilitar la comunicació entre seus com si d'una xarxa interna es tractés mitjançant tecnologies dinàmiques d'establiment de xarxes IPSEC.
- Millorar el funcionament de la xarxa LAN tot evitant incidències derivades d'un no aprofitament de les possibilitats tecnològiques actuals.
- Reducció dels costos de WAN corporativa.
    - Aplicació de les últimes tecnologies disponibles per a migrar d'una WAN tradicional cap a una Intelligent WAN o Software Defined WAN.

1.3 Enfocament i mètode seguit

Aquest treball es podria dur a terme amb dues estratègies ben diferenciades:

- Reutilització de l'actual infraestructura afegint els nous elements necessaris segons els nous requisits.
- Renovació total de la infraestructura.

L'elecció vindrà donada a partir dels resultats de l'anàlisi de la infraestructura actual de l'organització, per tal de veure si un re-aprofitament és beneficiós no només a nivell de costos si no en funcions.

L'enfocament, però, serà el d'adaptar un producte existent al mercat actual de les comunicacions, en comptes de desenvolupar un nou producte.

El desenvolupament d'un nou producte comportaria unes despeses de temps i recursos que farien que el projecte no tingués una viabilitat econòmica possible.

1.4 Planificació del Treball

El projecte es divideix en les següents tasques:

- **Tasca 1:** Anàlisi tecnològic
  - **Sub-tasca 1:** Recollida inicial de dades.

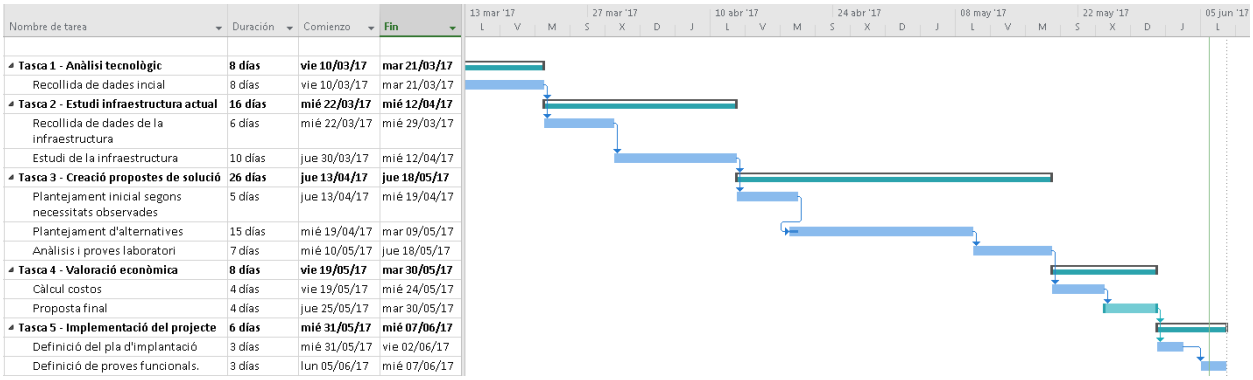
- **Tasca 2:** Estudi infraestructura actual.
  - **Sub-tasca 1:** Recollida dades infraestructura.
  - **Sub-tasca 2:** Estudi de la infraestructura actual.

- **Tasca 3:** Creació propostes de solució i/o canvi
  - **Sub-tasca 1:** Plantejament inicial segons les necessitats observades a les tasques 1 i 2.
  - **Sub-tasca 2:** Plantejament d'alternatives.
  - **Sub-tasca 3:** Proposta final

- **Tasca 4:** Valoració econòmica
  - **Sub-tasca 1:** Càlcul de costos per seu
  - **Sub-tasca 2:** Càlcul de costos total

- **Tasca 5:** Implementació del projecte.
  - **Sub-tasca 1:** Definició de pla d'implantació.
  - **Sub-tasca 2:** Definició proves funcionals.

Per a la planificació temporal, s'ha efectuat un diagrama de Gantt:



Nombre de tarea	Duración	Comienzo	Fin
Tasca 1 - Anàlisi tecnològic	**8 días**	**vie 10/03/17**	**mar 21/03/17**
Recollida de dades incial	8 días	vie 10/03/17	mar 21/03/17
Tasca 2 - Estudi infraestructura actual	**16 días**	**mié 22/03/17**	**mié 12/04/17**
Recollida de dades de la infraestructura	6 días	mié 22/03/17	mié 29/03/17
Estudi de la infraestructura	10 días	jue 30/03/17	mié 12/04/17
Tasca 3 - Creació propostes de solució	**26 días**	**jue 13/04/17**	**jue 18/05/17**
Plantejament inicial segons necessitats observades	5 días	jue 13/04/17	mié 19/04/17
Plantejament d'alternatives	15 días	mié 19/04/17	mar 09/05/17
Anàlisis i proves laboratori	7 días	mié 10/05/17	jue 18/05/17
Tasca 4 - Valoració econòmica	**8 días**	**vie 19/05/17**	**mar 30/05/17**
Càlcul costos	4 días	vie 19/05/17	mié 24/05/17
Proposta final	4 días	jue 25/05/17	mar 30/05/17
Tasca 5 - Implementació del projecte	**6 días**	**mié 31/05/17**	**mié 07/06/17**
Definició del pla d'implantació	3 días	mié 31/05/17	vie 02/06/17
Definició de proves funcionals.	3 días	lun 05/06/17	mié 07/06/17

Il·lustració 1: Diagrama de Gantt

Les tasques segons el diagrama es poden veure amb més detall a continuació:

Nombre de tarea	Duración	Comienzo	Fin
Tasca 1 - Anàlisi tecnològic	**8 días**	**vie 10/03/17**	**mar 21/03/17**
Recollida de dades incial	8 días	vie 10/03/17	mar 21/03/17
Tasca 2 - Estudi infraestructura actual	**16 días**	**mié 22/03/17**	**mié 12/04/17**
Recollida de dades de la infraestructura	6 días	mié 22/03/17	mié 29/03/17
Estudi de la infraestructura	10 días	jue 30/03/17	mié 12/04/17
Tasca 3 - Creació propostes de solució	**26 días**	**jue 13/04/17**	**jue 18/05/17**
Plantejament inicial segons necessitats observades	5 días	jue 13/04/17	mié 19/04/17
Plantejament d'alternatives	15 días	mié 19/04/17	mar 09/05/17
Anàlisis i proves laboratori	7 días	mié 10/05/17	jue 18/05/17
Tasca 4 - Valoració econòmica	**8 días**	**vie 19/05/17**	**mar 30/05/17**
Càlcul costos	4 días	vie 19/05/17	mié 24/05/17
Proposta final	4 días	jue 25/05/17	mar 30/05/17
Tasca 5 - Implementació del projecte	**6 días**	**mié 31/05/17**	**mié 07/06/17**
Definició del pla d'implantació	3 días	mié 31/05/17	vie 02/06/17
Definició de proves funcionals.	3 días	lun 05/06/17	mié 07/06/17

Il·lustració 2: Tasques segons temporalitat

1.5 Breu sumari de productes obtinguts

Aquest projecte tindrà com a producte final una solució, documentada, LAN/WAN aplicable al tipus d'organització de tres seus definida anteriorment.

Els documents del projecte seran la memòria i la presentació. El primer contindrà la informació d'anàlisi, propostes de solucions, solució escollida i una simulació de desplegament.

1.6 Breu descripció dels altres capítols de la memòria

La memòria del treball final de grau està composada pels diferents capítols següents:

- **Capítol 2:** Les Xarxes LAN/WAN corporatives.
  - Pretén fer un repàs conceptual del que són les xarxes LAN, WAN, MPLS i VPN. La seva relació global amb el projecte és la d'entendre les tecnologies sobre les quals parlarem en el desenvolupament del mateix.

- **Capítol 3**: Anàlisi tecnològic de l'organització.
  - Fa un repàs de la situació actual de l'organització, presenta el problema a resoldre amb la implantació del projecte.

- **Capítol 4:** Propostes de solució i/o canvi amb proposta final.
  - Presenta les alternatives per a solucionar el problema presentat al capítol anterior.
  - Proposa la solució final en base a un anàlisis tecnològic.

- **Capítol 5:** Valoració econòmica.
  - Conté la valoració econòmica de la implantació de la solució final proposada al capítol anterior.

- **Capítol 6:** Implementació del projecte.
  - Recull el pla d'implantació, una planificació de com s'hauria de fer el desplegament i de quines proves funcionals s'haurien de realitzar per validar l'acompliment del projecte.

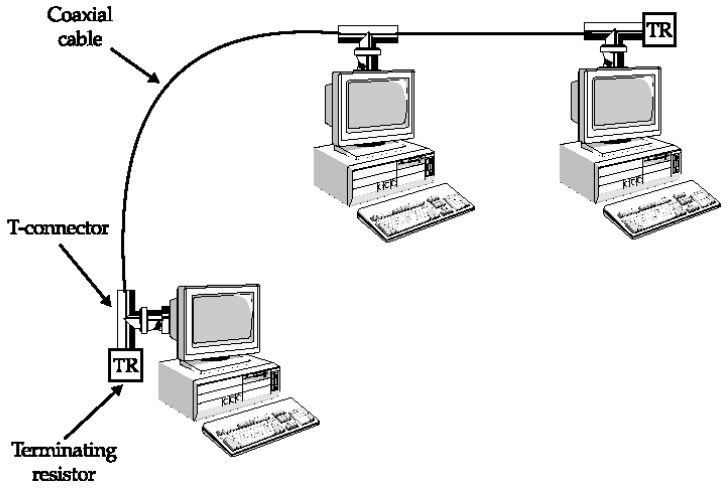
2. Les xarxes LAN/WAN corporatives

Les infraestructures de xarxa d'una organització varien segons la seva mida, si hi ha seus interconnectades, etc. Mentre que a nivell domèstic el més normal és tenir una petita xarxa local LAN i una sortida a internet o WAN, a nivell corporatiu ens trobem amb d'altres com MPLS, VPN IPSEC, etc.

2.1 Local Area Network

Les xarxes locals proporcionen accés als usuaris i als dispositius dins d'una mateixa localització, com per exemple una oficina. Al ser locals, l'amplada de banda és molt gran i és habitual avui dia trobar que els accessos es fan a 1Gbps i la interconnexió entre els diferents dispositius de xarxa puguin arribar fins als 40Gbps.

Antigament, aquestes connexions es realitzaven mitjançant cable coaxial i amb un esquema de connexió en cascada, la qual cosa provocava que la fallida d'una connexió, deixés sense connexió la resta d'elements.



Il·lustració 3: Xarxa LAN coaxial

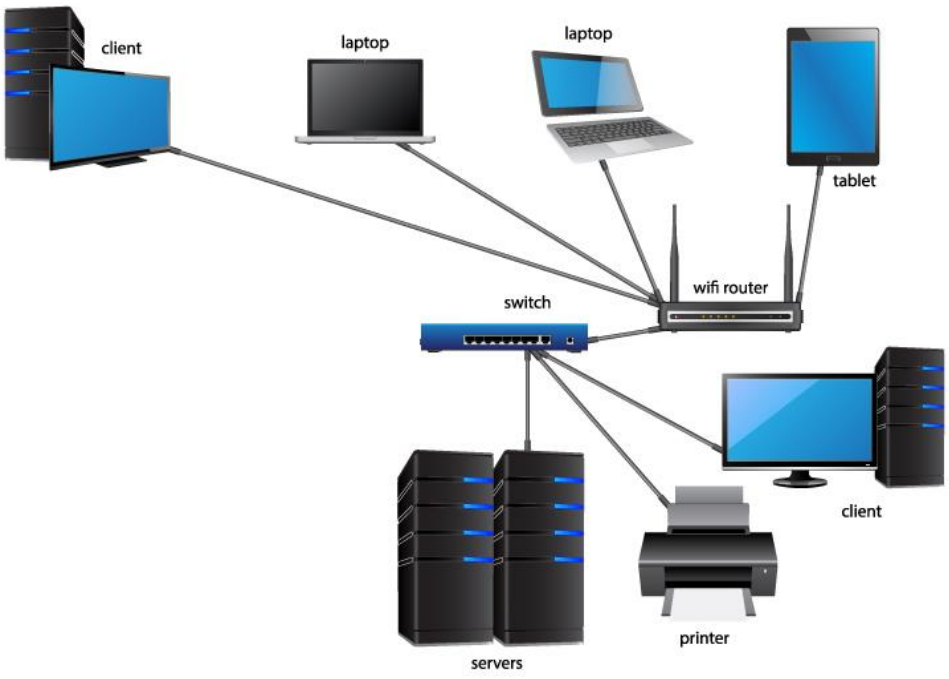
A l'actualitat els esquemes de connexió són més complexos, tot fent servir elements d'interconnexió o Switch (evolució del hub). A més, el coaxial va caure en desús i actualment s'utilitzen connexions de coure o fibra per a enllaços que requereixin més de 100 metres de distància o velocitats superiors a les suportades pel coure.

Per a la interconnexió de dispositius s'utilitzaven hubs i, des de fa temps, dispositius switch. Els primers van caure en desús ja que eren dispositius que feien la funció de multi connectar tots els dispositius de forma ineficient; transmetien la informació rebuda per un port a tota la resta. En canvi, els switchs, poden discernir cap a qui va la informació i enviar-la només pel port que correspon (excepte broadcast, multicast).

A les xarxes LAN trobem dues tecnologies de transmissió:

- **Ethernet:** connexió mitjançant cable. Format de la trama ethernet definit al IEEE 802.3 per a qualsevol tipus de cable emprat.

- **Wifi:** connexió sense cables recollida al estàndard IEEE 802.11. La connexió es fa mitjançant un punt d'accès o AP, el qual si està connectat a un switch. També es podria dir que amb aquesta tecnologia estaríem conformant una WLAN (Wireless LAN).

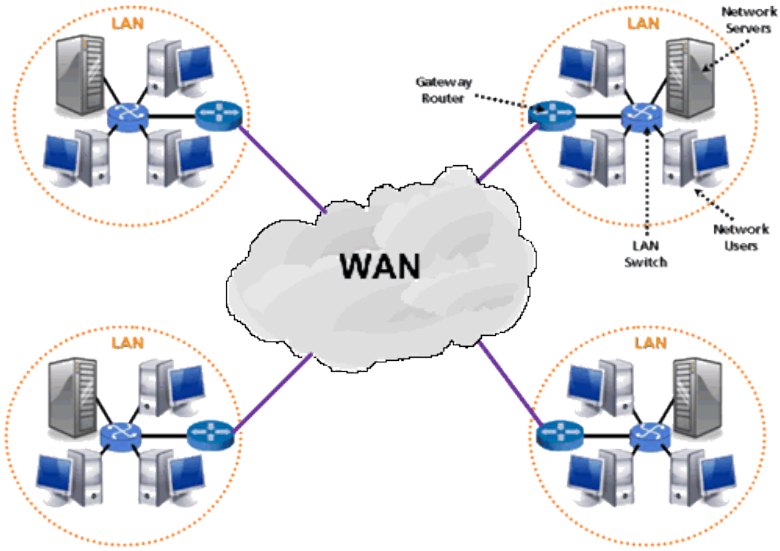


Il·lustració 4: Xarxa LAN amb connexions Ethernet i Wifi

Les xarxes LAN permeten grans velocitats però com hem dit, son xarxes locals que tenen limitació espacial. A més de no permetre la interconnexió de seus a no ser que aquestes estiguin en edificis contigus i la tirada de fibra sigui factible.

2.2 Wide Area Network

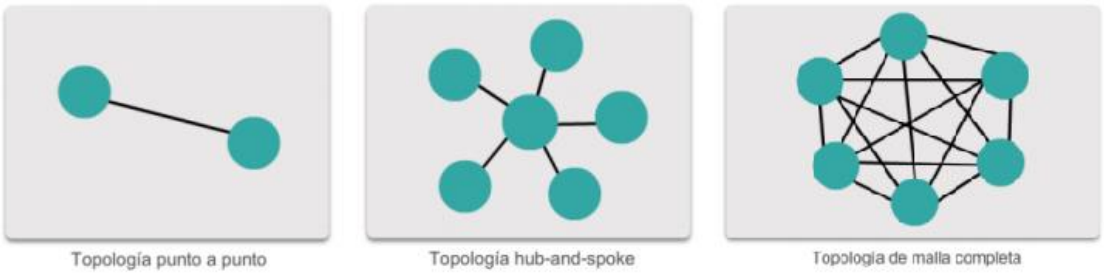
Una WAN es podria definir com una xarxa que uneix o interconnecta diferents LANs. Normalment, les xarxes WAN estan creades i mantingudes per els ISP (Internet Service Provider) per tal de donar connectivitat entre tots els seus clients i connectivitat cap a altres xarxes WAN d'altres ISP. Com ja sabem, internet és un conglomerat de xarxes interconnectades entre sí.



Il·lustració 5: Exemple de Xarxa WAN

A nivell d'usuari podríem definir la WAN com la sortida a internet. La xarxa necessària per poder connectar a recursos que són exteriors a la nostra LAN.

En el cas que ens ocupa, una WAN també es podria fer servir per interconnectar dues seus si utilitzem una topologia punt a punt o una seu central amb totes les seves subseus utilitzant topologies hub-and-spoke o de malla complerta:

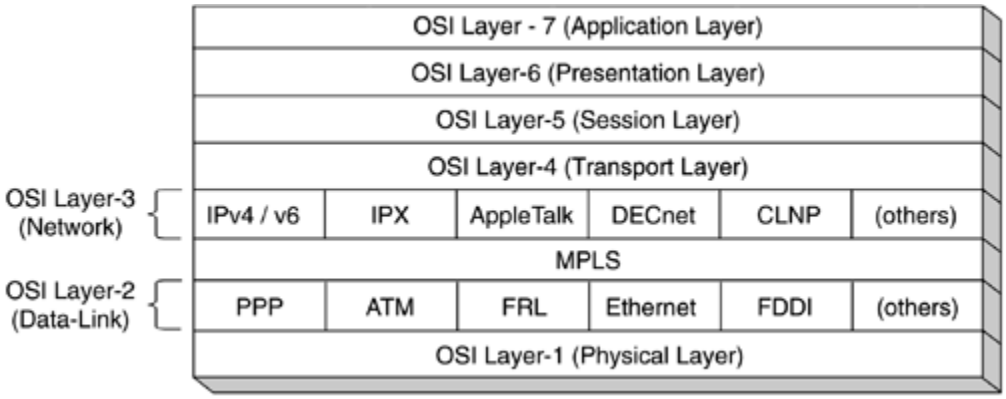


Il·lustració 6: Topologies WAN més comuns.

2.3 MPLS

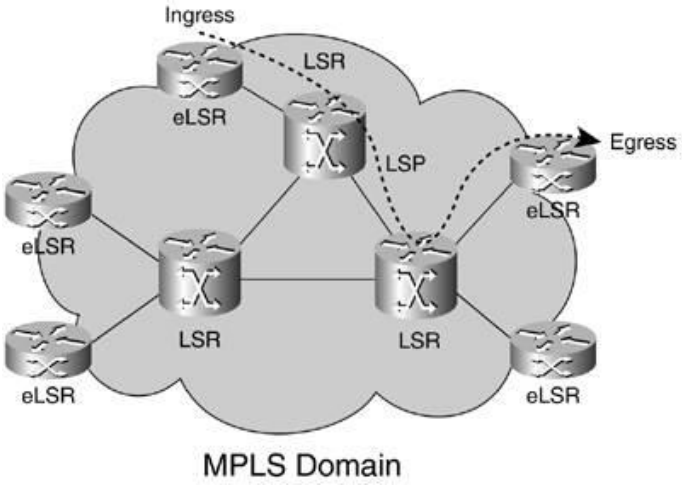
Les sigles MPLS, Multiprotocol Label Switching, defineixen el mecanisme de transport recollit al RFC 3031 desenvolupat per la IETF (Internet Engineering Task Force). [2]

Aquest protocol es situa entre la capa 2 i la capa 3 del model OSI, és a dir, entre la capa d'enllaç de dades i la capa de xarxa. Gràcies a això, les xarxes MPLS aporten la velocitat del forwarding a nivell 2 i el control del Routing.



Il·lustració 7: MPLS en el model OSI

El funcionament, com es desprèn de les seves sigles, es basa en l'ús d'etiquetes o més bé LSP (Label-Switched-Paths). El camí que un paquet ha de recórrer és assignat pels diferents punts LSR (Label Switched Router), els quals van creant el camí virtual i assignant les etiquetes pertinents per tal de que el següent LSR continuï el procés.



Il·lustració 8: Exemple de xarxa MPLS

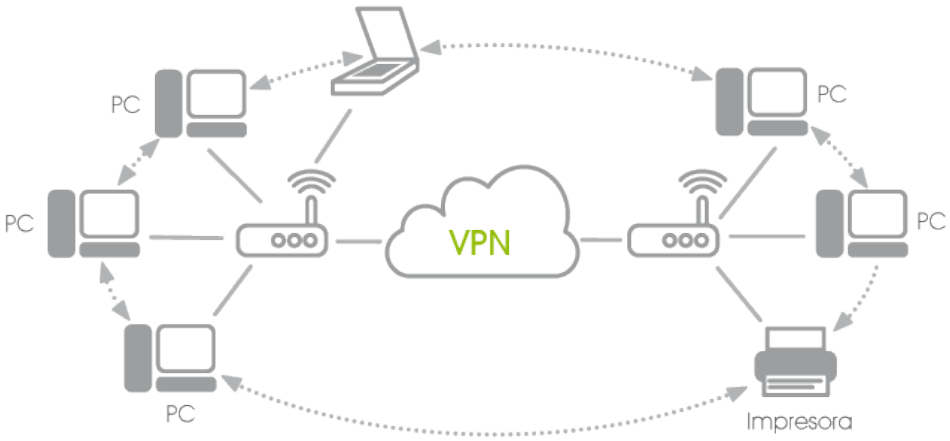
Aquestes etiquetes aporten eficiència des del punt de vista que és més ràpid mirar el contingut d'una etiqueta en comptes de processar la capçalera dels paquets i posteriorment enrutar segons les taules d'enrutament.

Es podria simplificar dient que una connexió MPLS permet crear una intranet/extranet entre dos punts a través d'internet com si d'una connexió de línia dedicada es tractés.

La utilització de MPLS en l'ambient corporatiu va comportar flexibilitat i escalabilitat en les xarxes entre seus ja que es poden incorporar nous punts o noves connexions sense necessitat de modificar la infraestructura existent. A més de la possibilitat d'incorporar QoS en les comunicacions corporatives; fet important amb l'aparició de la VoIP i la necessitat de QoS que aquesta tecnologia demanda en un medi compartit.

2.3 VPN i VPN L2TP/IPSEC

Una VPN és una xarxa privada virtual que permet fer una extensió segura de la xarxa LAN sobre una xarxa WAN que pot ser dedicada o pública. Permeten unificar l'adreçament ip de dues seus, tal i com permet les MPLS, però amb un cost menor. [5]

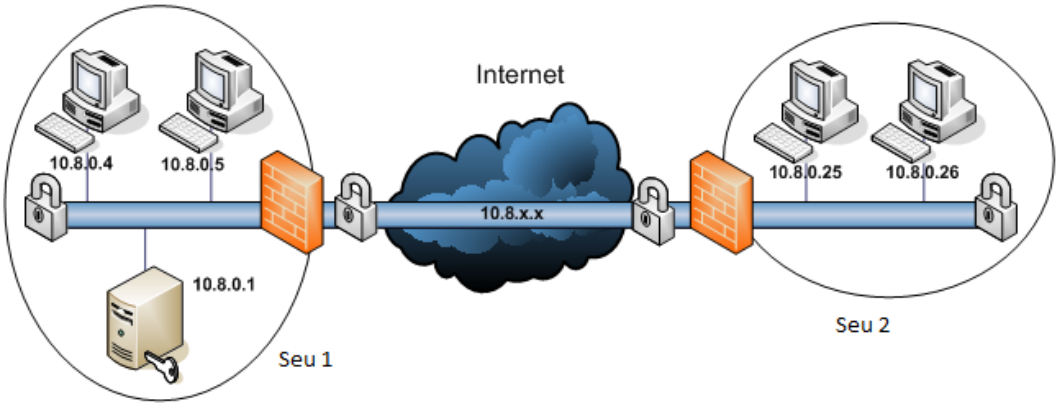


Il·lustració 9: VPN entre dues seus

Precisament la possibilitat de muntar una VPN sobre una línia segura dedicada punt a punt o sobre una línia pública del ISP (tan fàcil com tenir internet a cada seu amb un adreçament públic de ip fixa) és el que fa necessari l'aparició de les VPN IPSEC que no deixen de ser una VPN amb seguretat.

Les L2TP/IPSEC implementen un conjunt de protocols criptogràfics que permeten:

- Assegurar el flux de paquets. Es comprova la integritat de les dades i encapsula les dades dos vegades.
- Garantir la autenticitat de les comunicacions.
- Establir diferents paràmetres d'encriptació. Fins a 256 bits. [4]



Il·lustració 10: Exemple VPN IPSEC entre dues seus

A la imatge anterior es pot veure dues xarxes LAN independents físicament amb un mateix adreçament ip, gràcies a la utilització d'un túnel VPN L2TP/IPSEC. Les dades viatgen per internet encriptades, per tant no poden ser interceptades i/o desxifrades.

3. Anàlisi tecnològic de l'organització

Per tal de garantir l'acompliment dels objectius fixats, primerament és necessari situar-se en el context de l'empresa a la qual va dirigida. Començant per una recollida de dades exhaustiva la qual reculli totes les dades de l'estructura tecnològica actual.

3.1 L'organització

El projecte es centra en una organització multinacional fictícia dedicada al món del subministrament de peces auxiliars per automoció, la qual té les següents tres seus:

Il·lustració 11: Seus en el mapa

- Seu central: Ubicada a Parets del Vallès, Barcelona, Espanya.
- Seu satèl·lit 1: Ubicada a Dieuze, França
- Seu satèl·lit 2: Ubicada a París, França

Per simplificar la identificació, nombrarem i ens referirem a l'organització, d'ara en davant, com a PecesCotxe S.A.

PecesCotxe, inicialment només tenia la seu central de Parets del Vallès, però en els darrers últims 10 anys, fruit del fort increment de demanda del sector, s'ha expandit passant a conformar les tres seus descrites anteriorment.

L'esmentada expansió va esdevenir en la necessitat d'adaptar la xarxa LAN tot ampliant cap a una MPLS corporativa. Com es pot despendre de la necessitat d'aquesta xarxa, un requisit principal era la possibilitat d'interconnexió entre seus de forma transparent.

Poc a poc amb el pas del temps i el creixement de la producció, les necessitats de caudal o amplada de banda han anat creixent, fins arribar a un punt que s'ha plantejat la necessitat de buscar alternatives d'optimització WAN i/o d'interconnexió entre seus per reduir costos.

Finalment, en els darrers mesos, han sofert talls de producció a la seu central fruit de la caiguda dels equips que fan switching a nivell de CORE.

3.2 Xarxa LAN

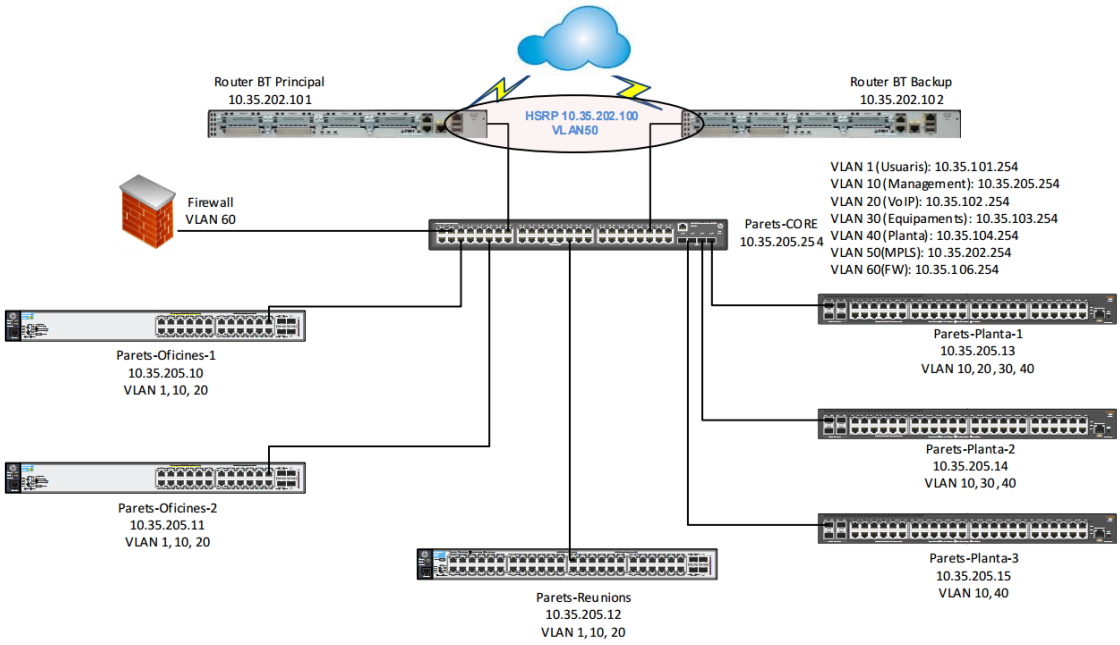
PecesCotxe S.A va renovar fa 4 anys la infraestructura de xarxa LAN de totes les seus. Van contemplar diverses opcions i fabricants, per finalment optar cap a una solució de switching conformada per equips HP Commware (H3C) i HPE Aruba Procurve.

La renovació no va contemplar realment un re-disseny de la xarxa sinó que es va limitar a una substitució d'elements de xarxa i canviar les connexions de coure entre switch a fibra.

A continuació es recull la informació respectiva a la LAN de cadascuna de les tres seus: esquema de xarxa, inventari d'equips i l'ús que se li dona a la mateixa.

3.2.1 LAN seu central

La seu central té una xarxa LAN que interconnecta les oficines, sales de reunions, la planta de producció, el Firewall, el switch de CORE i els routers de sortida MPLS:



Il·lustració 12: Topologia LAN Seu Central

**Les fibres són multimode; no es supera la distància màxima de transmissió.*
*** Els switch no tenen habilitat STP*.

En el moment de la renovació de xarxa, es va proveir la zona de planta de producció amb equips switch que conten amb uplinks de 10GB mentre que la zona d'oficines i sales de reunions es fan els enllaços amb coure a 1GB.

3.2.1.1 Inventari

A la següent taula es detallen les dades dels switch que conformen la LAN:

NOM	MODEL	IP	PORTS*
Parets-CORE	HP 5130 JG976A	10.35.205.254	48Gigabit Ethernet 4 SPF+ 10G
Parets-Oficines-1	HP 2530 J9773A	10.35.205.10	24Gigabit Ethernet POE+
Parets-Oficines-2	HP 2530 J9773A	10.35.205.11	24Gigabit Ethernet POE+
Parets-Planta-1	HP 2540 JL355A	10.35.205.13	48Gigabit Ethernet 3 SPF+ 10G
Parets-Planta-2	HP 2540 JL355A	10.35.205.14	48Gigabit Ethernet 1 SPF+ 10G
Parets-Planta-3	HP 2540 JL355A	10.35.205.15	48Gigabit Ethernet 1 SPF+ 10G
Parets-Reunions	HP 2530 J9775A	10.35.205.12	48Gigabit Ethernet

**Els ports de fibra només s'enumeren si es conta amb el corresponen transceiver al switch; és a dir, si es funcional sense comprar addicionals.*

Per a la proposta de possibles canvis, és necessària la relació de ports lliures, ocupats i ampliables en cadascun dels equipaments:

NOM	OCUPATS	LLIURES	AMPLIABLE
Parets-CORE	6x1GB coure 3 SFP+	42x1GB coure 1 SFP+	No
Parets-Oficines-1	22x1GB coure	2x1GB coure	Si, capacitat per a 4 SFP 1G
Parets-Oficines-2	21x1GB coure	3x1GB coure	Si, capacitat per a 4 SFP 1G
Parets-Planta-1	18x1GB coure 3 SFP+	30x1GB coure	Si, capacitat per a 1 SFP+ 10G
Parets-Planta-2	35x1GB coure 1 SFP+	13x1GB coure	Si, capacitat per a 3 SFP+ 10G
Parets-Planta-3	21x1GB coure 1 SFP+	27x1GB coure	Si, capacitat per a 3 SFP+ 10G
Parets-Reunions	40x1GB coure	8x1GB coure	Si, capacitat per a 4 SFP 1G

3.2.1.2 Usos de la LAN a la seu Central

En aquest apartat recollim què està connectat a cada switch, així com què hi ha a la LAN que s'hagi de tenir en compte per l'anàlisi de possibles millores; servidors, que es fa amb ells i que fluxos de comunicació hi ha entre els diferents elements.

De l'esquema de xarxa s'extreuen 4 zones de switching diferenciades:

- Switch Core:

  Té com a funció ser l'element encaminador de tota la LAN, interconnectar els dos routers de MPLS i connectar el Firewall.
  Si aquest element cau, tota la comunicació de la seu es veu afectada.

- Switch Oficines:

  Aquests equipaments s'utilitzen per a la connexió a la xarxa d'equips pc portàtils i sobretaula a 1GB.
  A més, es connecten telèfons Avaya 4600 series que alimenten mitjançant el POE ja que no disposen d'alimentadors a xarxa de corrent.

- Switch Reunions:

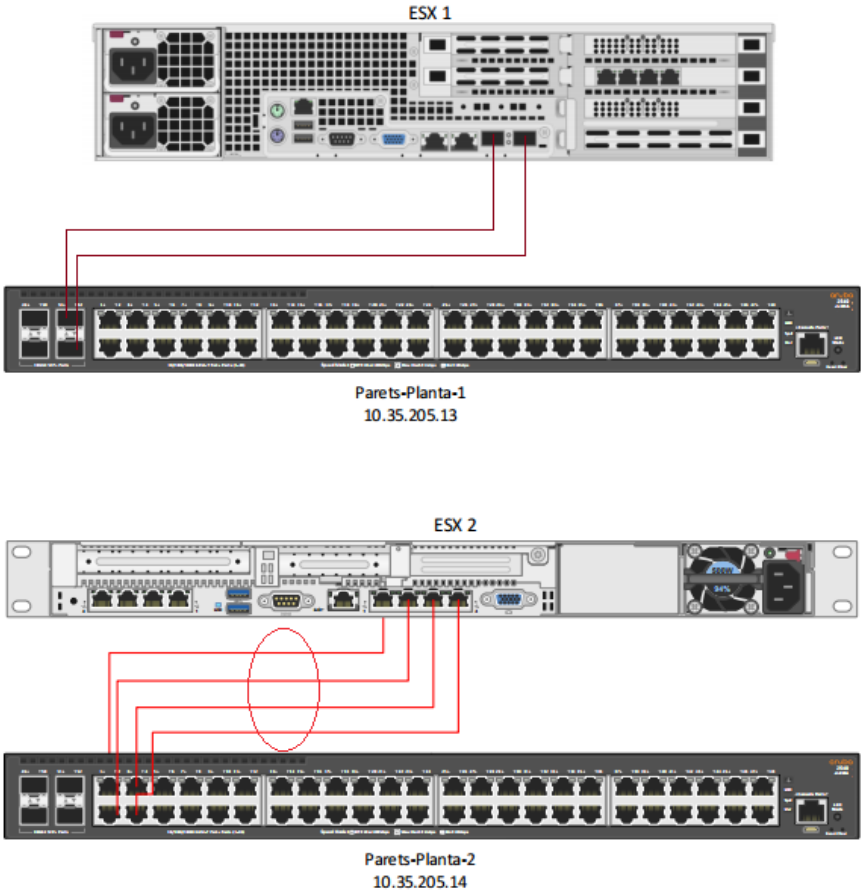
  Hi ha 3 sales de reunions les quals conten, cadascuna, amb un PC, un projector i un sistema de vídeo-conferència. A més, cada sala de reunions té 10 punts de xarxa Ethernet addicionals.

- Switch Planta:

  Aquests equipaments són els encarregats de connectar a la xarxa les màquines de producció automatitzades (PLC), els diferents rellotges de marcat pel control horari del personal, petites estacions de treball, la centraleta telefònica Avaya i dos servidors ESX que conformen l'entorn VMWARE per a servidors (tots els servidors són virtuals) connectats de la següent forma:

  - Servidor ESX 1 connectat a switch Parets-Planta-1 mitjançant 2x10GB de fibra.

  - Servidor ESX 2 connectat a switch Parets-Planta-2 mitjançant una agregació de ports dinàmica LACP formada per 4 ports de coure a 1GB (aquest servidor no compta amb interfícies de fibra).



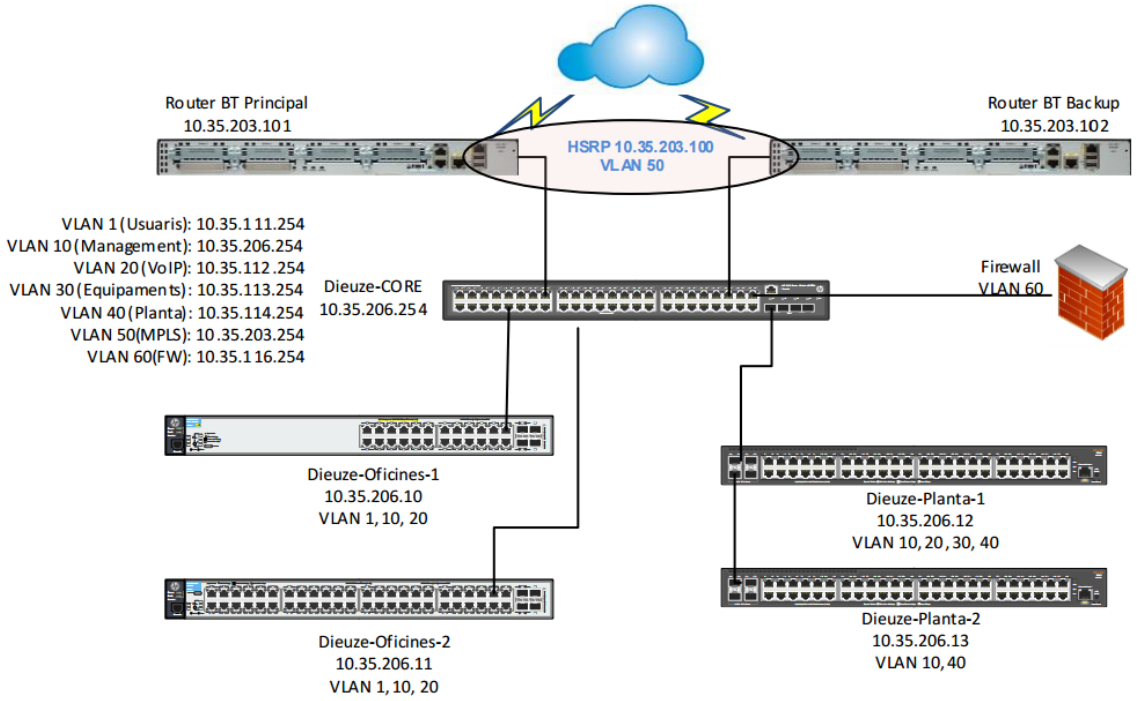
Il·lustració 13: Connexió servidors ESX a Switch de planta

Els principals fluxos de comunicació són:

- Navegació d'internet, que es produeix dels switch d'oficines i planta (WindowsUpdate i aplicatius servidors), cap a CORE i posterior Firewall.
- Telefonia. La centraleta Avaya està connectada a un switch de planta i es produeix comunicació entre els telèfons (switch oficines) i aquesta. La centraleta és local, no es comparteix amb altres seus.
- Rellotges d'horari treballadors. Connectats a switch de planta i es comuniquen amb un servidor virtual de sincronització.
- Correu. El servidor Microsoft Exchange de correu està a la plataforma VMWARE i és el servidor central de correu; les altres dues seus tenen la entrada/sortida de correu a través d'aquí.
- Servidor de Fitxers. La seu compta amb un Fileserver on es centralitzen tots els documents comuns entre seus.
- Màquines o PLC. Les màquines de la planta de producció es comuniquen amb dos servidors virtuals que les controlen.

3.2.2 LAN seu Dieuze

La seu de Dieuze és molt similar a la seu central tret del nombre de switch en planta i la inexistència de switch de reunions al no haver-hi aquests emplaçaments:



Il·lustració 14: Topologia LAN Dieuze

**Les fibres son multimode; no es supera la distància màxima de transmissió.*
*** Els switch no tenen habilitat STP.*

Els uplinks, com en el cas de la central, son a 10GB de plantes a CORE i de 1GB coure d'oficines a CORE.

3.2.2.1 Inventari

A la següent taula es detallen les dades dels switch que conformen la LAN:

NOM	MODEL	IP	PORTS
Dieuze-CORE	HP 5130 JG976A	10.35.206.254	48Gigabit Ethernet 1 SPF+ 10G
Dieuze-Oficines-1	HP 2530 J9773A	10.35.206.10	24Gigabit Ethernet POE+
Dieuze-Oficines-2	HP 2530 J9775A	10.35.206.11	48Gigabit Ethernet
Dieuze-Planta-1	HP 2540 JL355A	10.35.206.12	48Gigabit Ethernet 1 SPF+ 10G
Dieuze-Planta-2	HP 2540 JL355A	10.35.206.13	48Gigabit Ethernet 1 SPF+ 10G

**Els ports de fibra només s'enumeren si es conta amb el corresponen transceiver al switch; és a dir, si es funcional sense comprar addicionals.*

La relació de ports lliures, ocupats i ampliables en cadascun dels equipaments és la següent:

NOM	OCUPATS	LLIURES	AMPLIABLE
Dieuze-CORE	5x1GB coure 1 SFP+	42x1GB coure	Si, capacitat per a 3 SFP+ 10G
Dieuze-Oficines-1	16x1GB coure	8x1GB coure	Si, capacitat per a 4 SFP 1G
Dieuze-Oficines-2	35x1GB coure	13x1GB coure	Si, capacitat per a 4 SFP 1G
Dieuze-Planta-1	26x1GB coure 1 SFP+	12x1GB coure	Si, capacitat per a 3 SFP+ 10G
Dieuze-Planta-2	23x1GB coure 1 SFP+	25x1GB coure	Si, capacitat per a 3 SFP+ 10G

3.2.2.2 Usos de la LAN a Dieuze

Els usos són gairebé els mateixos que a la central:

- Switch Core:
  En aquest cas també és l'element encaminador de la xarxa i també és l'element que **al fallar deixa tota la seu sense comunicacions.**

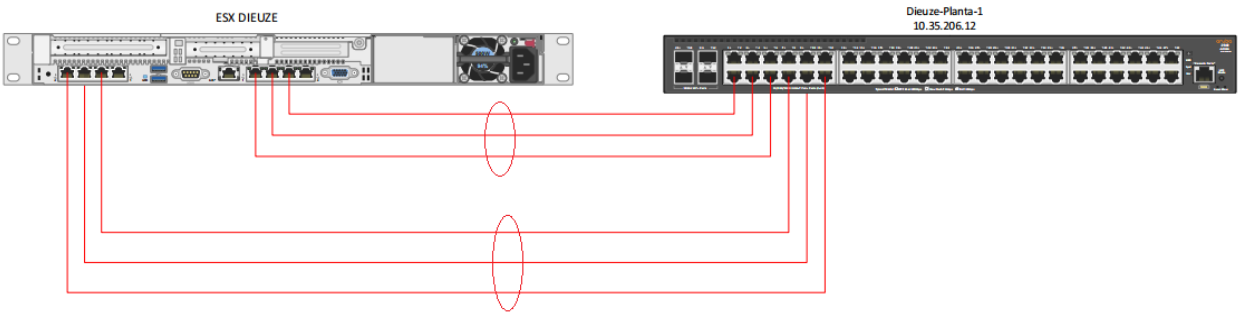
- Switch Oficines:
  Aquí també connectem portàtils i equips de sobretaula amb coure a 1GB, però la diferencia es que en alguns casos s'utilitza el switch del propi telèfon Avaya 4600 per a donar servei al PC.

Il·lustració 15: Connexió PC a LAN mitjançant switch telèfon Avaya

- Switch Planta:
  Com en la central, aquí es connecten els PLC, els rellotges de marcat de control horari, algunes estacions de treball, la centraleta telefònica Avaya i la plataforma VMWARE.

  Encara que en aquest cas només es compta amb un servidor ESX el qual es connecta de la següent forma:

  - Servidor ESX connectat a switch Dieuze-Planta-1 amb dos agregacions de ports LACP formades per 3 ports de coure a 1GB cadascuna.



Il·lustració 16: Connexió servidor ESX Dieuze a switch planta

Els principals fluxos de comunicació són:

- Navegació d'internet, que es produeix dels switch d'oficines i planta (WindowsUpdate i aplicatius servidors), cap a CORE i posterior Firewall.

- Telefonia. Comunicació entre la centraleta i els telèfons Avaya, una connectada a switch planta i els altres a switch oficines. Com en el cas anterior, la centraleta no es comparteix, és local.

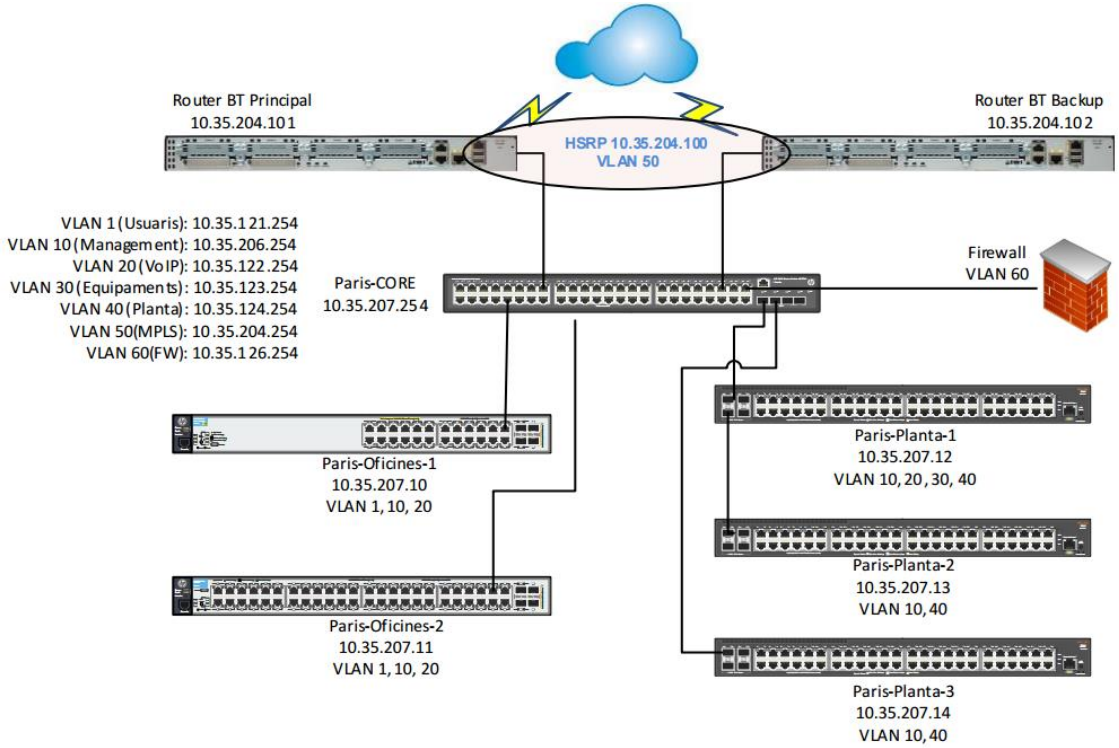
- Rellotges d'horari treballadors. També connectats a switch de planta i es comuniquen amb un servidor virtual de sincronització.

- Correu. El **servidor de correu està centralitzat** a la seu central, per tant, a la LAN els correus arriben des de la MPLS.

- Màquines o PLC. Les màquines de la planta de producció es comuniquen amb dos servidors virtuals que les controlen i estan a la plataforma VMWARE.

3.2.3 LAN seu París

Aquesta seu té el mateix esquema que les anteriors i la mateixa configuració de uplinks; coure a 1GB per oficines i planta a 10GB SFP+:



Il·lustració 17: Topologia LAN París

**Les fibres son multimode; no es supera la distància màxima de transmissió.*
*** Els switch no tenen habilitat STP*.

3.2.3.1 Inventari

A la següent taula es detallen les dades dels switch que conformen la LAN:

NOM	MODEL	IP	PORTS
Paris-CORE	HP 5130 JG976A	10.35.207.254	48Gigabit Ethernet 2 SPF+ 10G
Paris-Oficines-1	HP 2530 J9773A	10.35.207.10	24Gigabit Ethernet POE+
Paris-Oficines-2	HP 2530 J9775A	10.35.207.11	48Gigabit Ethernet
Paris-Planta-1	HP 2540 JL355A	10.35.207.12	48Gigabit Ethernet 2 SPF+ 10G
Paris-Planta-2	HP 2540 JL355A	10.35.207.13	48Gigabit Ethernet 1 SPF+ 10G
Paris-Planta-3	HP 2540 JL355A	10.35.207.14	48Gigabit Ethernet 1 SPF+ 10G

**Els ports de fibra només s'enumeren si es conta amb el corresponen transceiver al switch; és a dir, si es funcional sense comprar addicionals.*

La relació de ports lliures, ocupats i ampliables en cadascun dels equipaments és la següent:

NOM	OCUPATS	LLIURES	AMPLIABLE
Paris-CORE	5x1GB coure 2 SFP+	42x1GB coure	Si, capacitat per a 2 SFP+ 10G
Paris-Oficines-1	20x1GB coure	4x1GB coure	Si, capacitat per a 4 SFP 1G
Paris-Oficines-2	31x1GB coure	17x1GB coure	Si, capacitat per a 4 SFP 1G
Paris-Planta-1	32x1GB coure 1 SFP+	16x1GB coure	Si, capacitat per a 2 SFP+ 10G
Paris-Planta-2	28x1GB coure 1 SFP+	20x1GB coure	Si, capacitat per a 3 SFP+ 10G
Paris-Planta-3	29x1GB coure 1 SFP+	19x1GB coure	Si, capacitat per a 3 SFP+ 10G

3.2.3.2 Usos de la LAN a París

Com en el cas de Dieuze, els usos són els mateixos fent alguna petita variació:

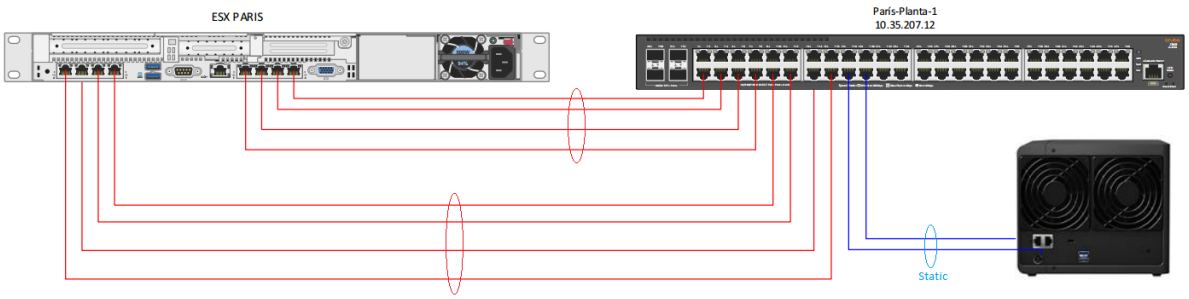
- Switch Core:
  De igual forma actua com element encaminador de la xarxa i és l'element que **al fallar deixa tota la seu sense comunicacions.**

- Switch Oficines:
  Aquí també connectem portàtils i equips de sobretaula amb coure a 1GB, però, com en el cas de la seu central, tots els telèfons i pcs estan connectats amb un port de xarxa individual per a cadascun; no s'utilitza la funció de switch dels telèfons Avaya.

- Switch Planta:
  Situació a mirall de Dieuze, excepte que en aquesta seu a més de tenir un servidor ESX, tenen un NAS Synology:

  - Servidor ESX connectat a switch Paris-Planta-1 amb dos agregacions de ports LACP formada per 4 ports de coure a 1GB cadascuna.

  - NAS Synology DS416 connectat a switch Paris-Planta-1 amb una agregació estàtica (NAS no soporta LACP) de dos ports de coure a 1GB.



Il·lustració 18: Connexió servidor ESX i NAS a switch planta

Els principals fluxos de comunicació són:

- Navegació d'internet, que es produeix dels switch d'oficines i planta (WindowsUpdate i aplicatius servidors), cap a CORE i posterior Firewall.

- Telefonia. Comunicació entre la centraleta i els telèfons Avaya, una connectada a switch planta i els altres a switch oficines. Com en el cas anterior, la centraleta no es comparteix, és local.

- Rellotges d'horari treballadors. També connectats a switch de planta i es comuniquen amb un servidor virtual de sincronització.

- Correu. El **servidor de correu està centralitzat** a la seu central, per tant, a la LAN els correus arriben des de la MPLS.

- Màquines o PLC. Les màquines de la planta de producció es comuniquen amb dos servidors virtuals que les controlen i estan a la plataforma VMWARE.

- NAS. Aquesta seu té un NAS que a més es **compartit amb Dieuze**. S'utilitza com a servidor de fitxers i la comunicació a la LAN es produeix entre switch oficines i planta, i entre switch planta i CORE quan la petició de fitxers ve de Dieuze.

3.3 MPLS

Com hem indicat anteriorment, PecesCotxe SA té contractada, amb British Telecom, una MPLS per a la comunicació entre seus. **Les comunicacions es troben centralitzades a Parets del Vallés**, és a dir, les comunicacions corporatives entre les seus de Francia (el que no sigui navegació), sempre passen per la seu central.

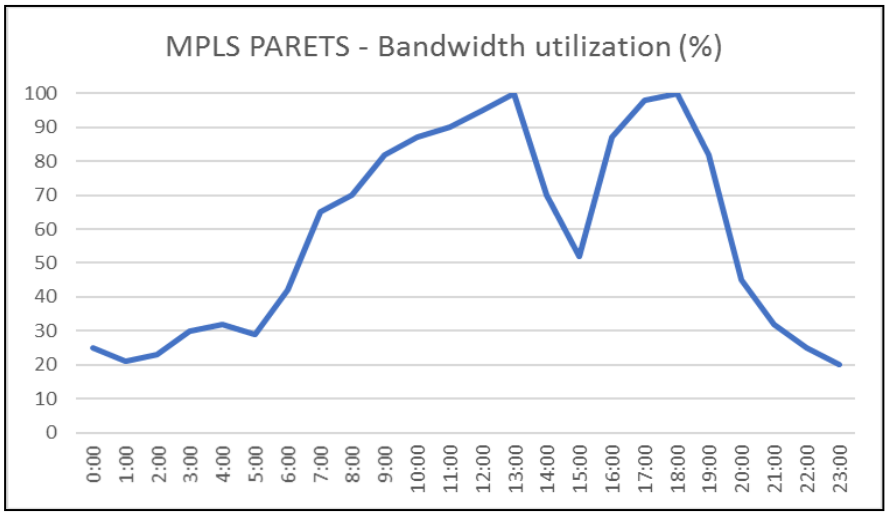
A continuació es mostra una taula on es referencia les diferents línies amb la velocitat contractada i el cost associat:

LINIA	VELOCITAT	COST MENSUAL
Seu central	30Mbps	650 euros
Dieuze	15 Mbps	400 euros
París	15 Mbps	400 euros

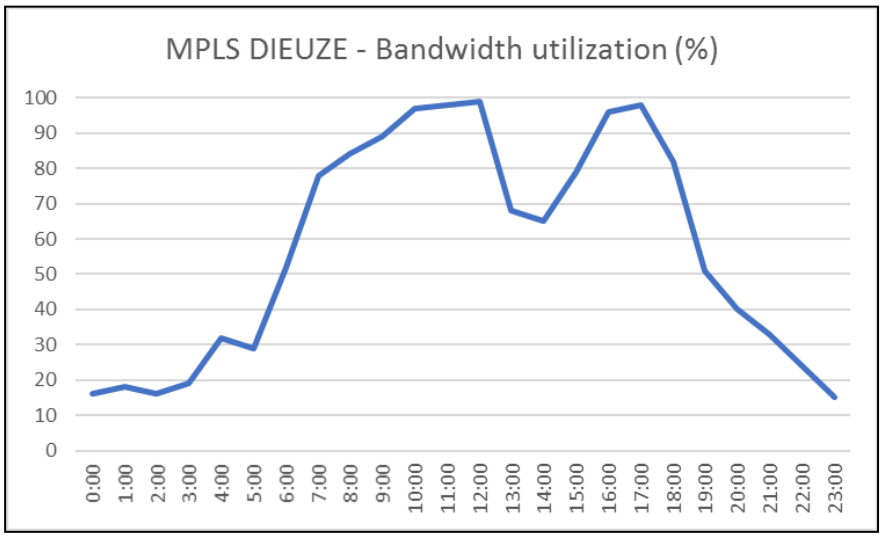
A nivell de redundància, com es pot veure en els esquemes LAN, cada una de les seus té 2 routers del proveïdor configurats amb HSRP per tal de tenir una ip virtual que és alhora el default gateway del switch de CORE.

Les velocitats de totes tres línies s'han anat ampliat segons ha sigut necessari, però durant els últims mesos les gràfiques d'estadístiques de consum mostren que s'hauria d'ampliar aquestes velocitats, amb el sobre cost afegit, ja que la utilització mitja ronda el 85-90% del caudal de les mateixes (en hores d'oficina); arribant fins i tot a la saturació en moments puntuals.

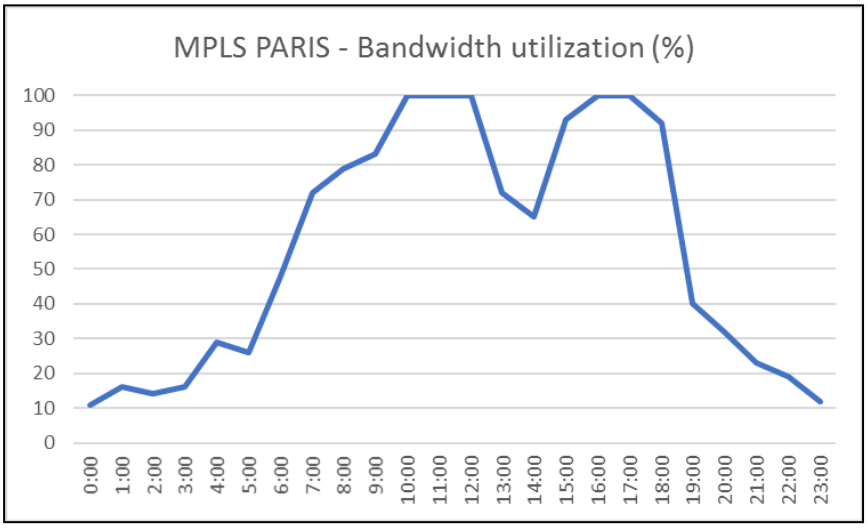
A continuació es mostren les gràfiques d'amplada de banda consumida per seu en un dia laborable amb un volum de feina habitual. Les dades són extrapolables al que succeeix la resta de dies de la setmana.



Il·lustració 19: Gràfic utilització MPLS Parets del Vallès



Il·lustració 20: Gràfic utilització MPLS Dieuze

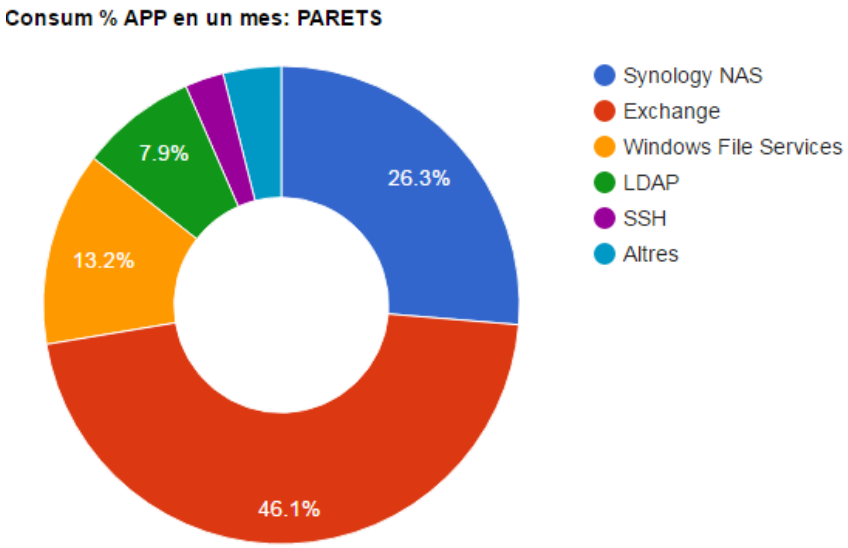


Il·lustració 21: Gràfic utilització MPLS París

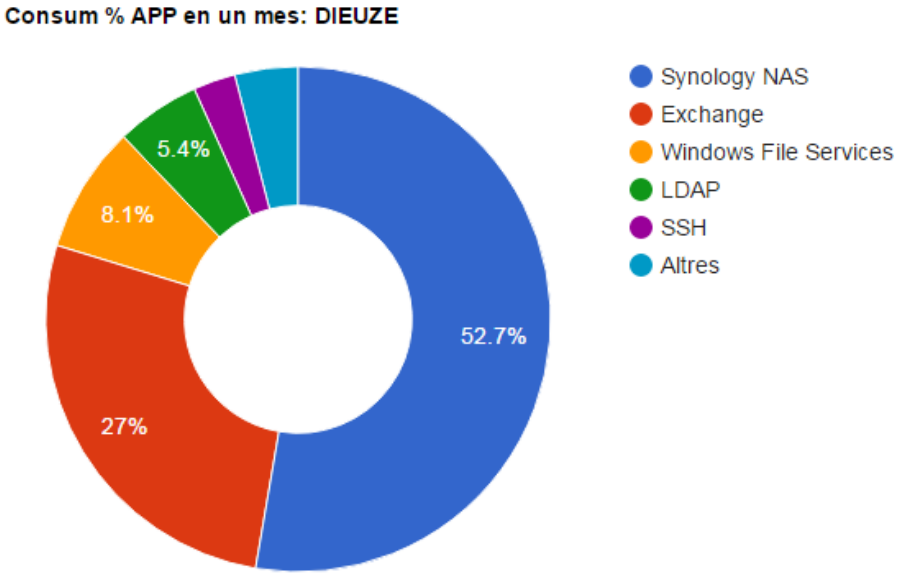
Les directrius provinents de la direcció de PecesCotxe SA van encaminades a l'estalvi de costos de MPLS i no veuen viable el continuar incrementant el caudal; fet derivat de l'alt cost de les línies.

3.3.1 Anàlisis Netflow

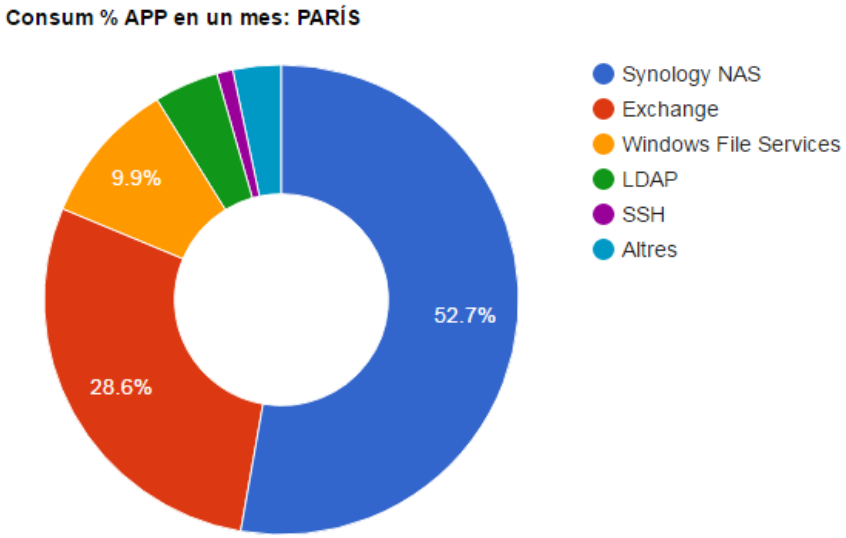
El proveïdor, British Telecom, té Netflow configurat als routers Cisco que té instal·lats cada seu. No contem amb accés a la plataforma de recol·lecció, però si hem obtingut uns gràfics representant la recol·lecció de dades d'ús, per veure què i com s'està consumint l'ample de banda de la MPLS:



Il·lustració 22: Gràfic Netflow consum bw per app a Parets



Il·lustració 23: Gràfic Netflow consum bw per app a Dieuze



Il·lustració 24: Gràfic Netflow consum bw per app a París

Dels gràfics anteriors, s'extreu que el dispositiu Synology, situat a París, **consumeix més de la meitat de la capacitat de la MPLS** en les dues seus satèl·lit: aproximadament 7,9 Mbps dels 15Mbps contractats.

A més, el fet de que tota comunicació entre Dieuze i París, passi per la central de Parets, fa que aquesta també es vegi afectada amb un impacte del 26% del caudal contractat.

La resta de dades amb volum refereixen a:

- **Exchange:** al tenir el servidor de correu en Parets, les seus han de consumir ample de banda per anar a descarregar/enviar correus.

  Es tracta d'un percentatge important de tràfic degut a que es la principal via de comunicació amb proveïdors i clients.

- **Windows File Services:** aquest tràfic es degut a que els servidors de PLC locals en cada seu, es sincronitzen mitjançant fitxers compartits entre sí o dit d'una altra forma, amb la utilització de Shared Folders.

- **LDAP:** bàsicament es tracta de l'autenticació d'usuaris del Active Directory al trobar-se els controladors de domini a Parets.

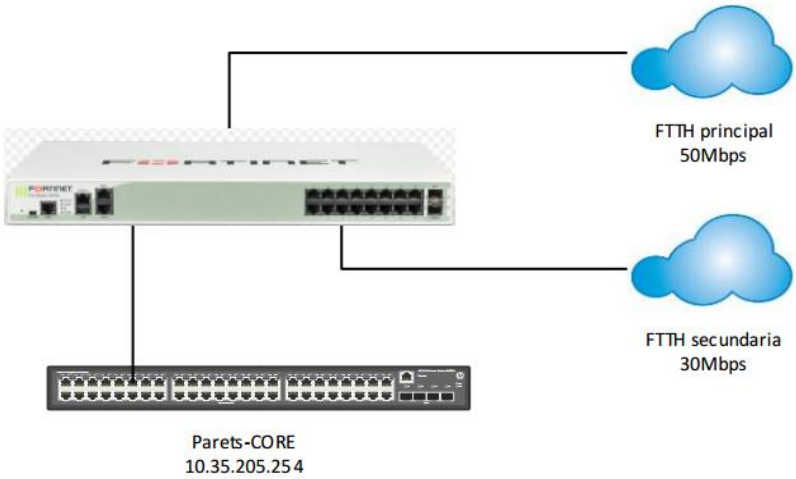
3.4 Xarxa WAN

Totes tres seus surten a internet de forma local però amb la diferència de que les seus satèl·lit tenen una única sortida cadascuna i la seu central a Parets del Vallès compta amb dues línies per navegació.

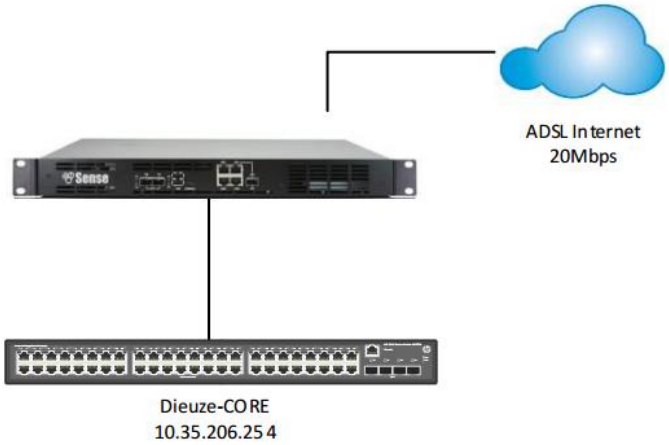
Les WAN estan controlades per un Firewall Pfsense en les dues seus franceses, mentre que a Parets del Vallès es va substituir per un Firewall Fortigate 200B quan es va incorporar la segona línia WAN: amb motius de fer balanceig de càrrega entre línies (WAN Load Balancing) ja que en el moment de la implantació no es suportava aquesta funcionalitat amb Pfsense. La sortida es fa mitjançant routers Cisco 2951 a totes tres seus.

Des de PecesCotxe s'indica que **no hi ha problemes de WAN en les seus franceses**, però, en canvi, a Parets es troben amb què la utilització d'internet no és la desitjada i sovint arriben a saturar totes dues fibres amb descarregues, streaming d'àudio, etc. **Tot i així, la política a seguir no és la de bloquejar, si no buscar prioritzar la navegació lícita per sobre de l'oci dels treballadors.**

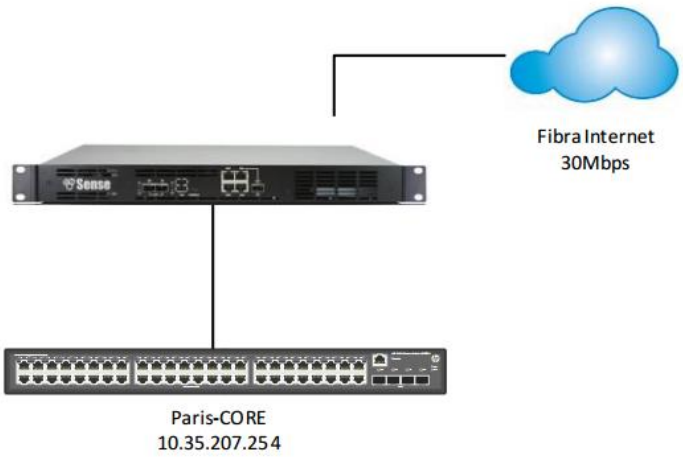
A continuació es mostra la topologia WAN de les seus conjuntament amb les respectives sortides i velocitats:



Il·lustració 25: Topologia WAN Parets del Vallès



Il·lustració 26: Topologia WAN Dieuze



Il·lustració 27: Topologia WAN Paris

Durant la recollida de requisits de la WAN, **es recopilen les següents necessitats per a la seu de Parets:**

- Si una línia cau, que no hi hagi tall de comunicacions WAN.
- Que es continuï fent balanceig de carrega entre les dues FTTH.
- S'ha d'aplicar QoS per tal de garantir un ample de banda mínim per a la navegació HTTP i HTTPs considerada corporativa.
    - Es considera corporativa la que no està categoritzada com a web de contingut sexual, jocs, social media i/o armes.
- El tràfic de streaming d'àudio, vídeo i descarregues, no es prohibirà però haurà de ser de com a màxim el 10% de l'ample de banda contractat.

3.4 Conclusions

Després de l'anàlisi de dades fet anteriorment, s'identifiquen els següents problemes i/o punts de millora als que aquest projecte ha de donar resposta:

- **LAN a totes les seus:**
  - Necessitat de redundar els switch de CORE per evitar que una caiguda d'aquest, afecti a tota la seu.
  - Revisió dels camins entre els switch de oficines i planta; no existeix redundància de camins.
  - Garantir que si un switch de planta cau, la plataforma VMWARE continuï operativa.

- **MPLS a totes les seus:**
  - Alleugerir la càrrega de les línies de les MPLS per tal de no necessitar l'ampliació de l'amplada de banda de les mateixes.

- **WAN a la seu central**:
  - Donar solució a la voluntat de prioritzar el tràfic WAN corporatiu, vers el no desitjable, a la seu central.
  - Tenir backup de línia en cas de caiguda d'una de les dues fibres.
  - Aplicar QoS al tràfic corporatiu.
  - Aplicar perfils de Maximum Bandwith per a la resta de tràfic.

Finalment, PecesCotxe remarca la importància d'oferir una solució que aprofiti al màxim possible la infraestructura actual i minimitzi la necessitat d'adquirir nous equipaments.

4. Propostes de canvi i solució final

Segons l'anàlisis tecnològic actual i les conclusions del mateix, es presenten a continuació les diferents propostes de canvi relacionades amb la LAN, MPLS i WAN de cadascuna de les tres seus.

4.1 Canvis LAN

Tal i com hem vist en l'anàlisi tecnològic de la organització, quan es va renovar la xarxa no es va promoure la necessitat de tenir redundància de connexions per evitar que la caiguda d'un sol cable o d'un equipament, provoqui la caiguda global de comunicacions a una seu.

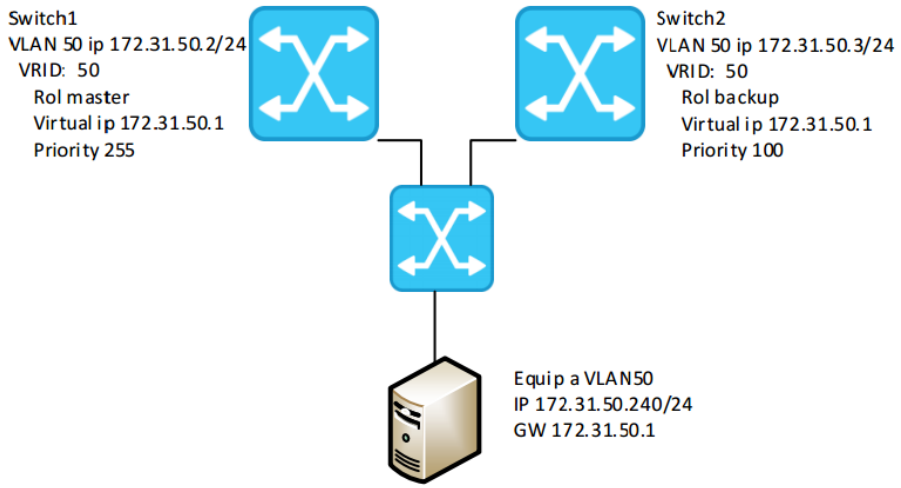
Per a la confecció de les propostes, s'han tingut en compte les premisses de intentar aprofitar el material existent, i, en cas de ser necessari la compra de nous equipaments, que aquests tinguin el menor cost possible.

4.1.1 Stacking vs VRRP

Amb la intenció de tenir redundància de CORE, plantegem dues possibilitats:

- Comprar una unitat idèntica addicional i fer Stack, tot aprofitant que els switch HP H3C ho permeten només comprant un cable.
- Substituir el CORE per una parella de switch de capa 3 i fer un VRRP per a cadascuna de les VLAN o xarxes que ha d'encaminar.

VRRP o Virtual Router Redundancy Protocol:
Es resumeix com a un protocol de redundància basat en la utilització d'una porta d'enllaç virtual en comptes de la ip d'un router o switch capa 3 físic.[8]



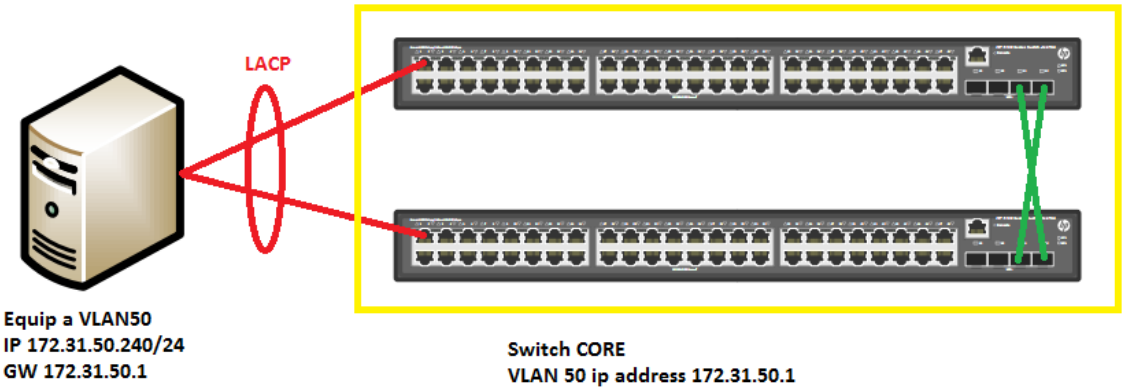
Il·lustració 28: Esquema conceptual funcionament VRRP

Si observem la imatge anterior, podem veure com tenim dos switch de capa 3 els quals tenen dues ips configurades per a la VLAN 50; una que podríem considerar física, i una virtual. A més, establim el rol de master/backup per a que preferiblement sigui la adreça MAC del master la respongui a la petició ARP dels equips que la seva porta d'enllaç apunti a la virtual ip.

Es pot fer entre switch de diferents fabricants, fet que aporta gran flexibilitat alhora de fer configuracions redundades.

Stacking

La tecnologia de stacking permet unir físicament més d'un switch per a obtenir un únic switch lògic:



Il·lustració 29: Exemple de stack de 2 membres amb enllaç LACP

A la imatge veiem com dos switch s'uneixen mitjançant dos cables de stack (pot ser amb un cable o més d'un) per acabar formant un únic switch lògic de CORE amb una ip a la VLAN 50.

L'equip està connectat amb dos cables, un a cada switch físic, formant un agregat LACP. Com s'aprecia, la porta d'enllaç de l'equip es la ip del switch lògic en la seva VLAN.

Al configurar el stack, definim un sistema de pesos/prioritats per definir qui és preferiblement el master del stack. Aquest master serà el que respondrà a la petició ARP amb la seva MAC i serà qui encamini la comunicació de l'equip.

El fabricant HP anomena IRF, Intelligent Resilient Framework, com a tecnologia de stacking per als switch de la gama H3C Commware; els utilitzats en CORE i planta de les 3 seus.

Elecció de tecnologia:

Un dels avantatges de fer un stack en comptes de VRRP, és que acabem tenint diversos switch com si fossin un de sol. Això permet que s'administri tot el stack des de un sol pla de control i que puguem fer **agregació d'enllaços entre diferents membres.** Aquesta última premissa, és important tenir-la en compte alhora d'oferir HA (alta disponibilitat) en entorns VMWARE.

Habitualment els servidors físics que fan de host ESX tenen dos switch integrats en comptes de tenir targetes de xarxa convencionals. Aquests switch es poden connectar cadascun a un switch diferent i d'aquesta forma tenir la seguretat de que en el cas de caiguda d'un switch de planta el ESX continuï donant servei; sempre i quan a nivell de VMWARE s'hagi configurat correctament.

Si es té un stack, es simplifica la tasca de tenir HA en l'entorn virtual, ja que podem fer que el servidor ESX tingui el seu switch1 connectat amb un agregat LACP el qual està format per ports membres de dos o més switch de planta diferents. Sense fer configuracions addicionals en VMWARE, s'aconsegueix que encara que falli un switch de planta i un switch del servidor ESX, la infraestructura estigui disponible.

D'altra banda hem de tenir en compte que normalment fer una implantació amb VRRP per als switch de capa 3 és més econòmic que no pas fer un stack ja que els dispositius preparats per a fer-ho tenen un sobre-cost associat.

No obstant, en els tres escenaris tenim connexions de 10GB amb SFP+, la qual cosa fa que els switch de capa 3 amb SFP+ tinguin un cost molt elevat i l'opció de canviar el CORE per 2 nous switch tingui un impacte econòmic molt més elevat que no pas comprar una unitat addicional (en cada seu) i fer un stack.

Pels motius abans esmentats, **es considera que la millor opció per a PecesCotxe és la de implementar stack IRF** amb els switch HP H3C Commware existents.

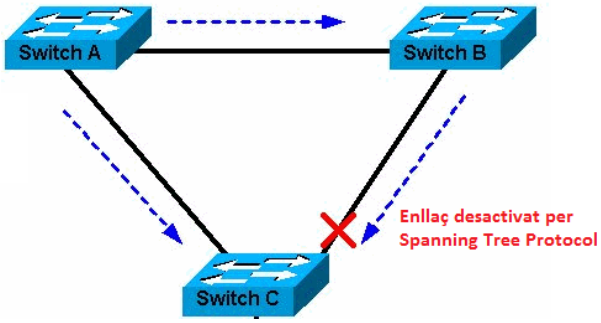
4.1.1 STP vs RSTP

Durant la recollida de dades, es fa palesa de la no existència de configuració STP als switch de totes tres seus. Si més no, al no tenir camí redundants, no és un requisit necessari.

Com hem vist al punt 4.1, una de les millores de la LAN passa per crear camins redundants entre switch i, per tant, és obligatori tenir un mecanisme de control que activi/desactivi camins i així evitar bucles de comunicacions.

STP

Spanning Tree Protocol és un protocol de xarxa de nivell 2 el qual gestiona tots els bucles existents en una xarxa; entenem bucles com a existència de més d'un camí per arribar a un mateix lloc, per exemple:



Il·lustració 30: Esquema funciona STP amb enllaços redundants

El Switch A pot arribar al Switch C desde dos camins, un més directe que no pas l'altre. Per defecte es basa en calcular el port arrel, on determinarà quin és el switch "core" de la xarxa i a partir d'aquí, calculant el cost administratiu d'enllaç, habilitatarà l'enllaç de menor cost i la resta els bloquejarà.

RSTP

Evolució del STP, com les seves sigles indiquen (Rapid STP) es millora en gran mida el temps de convergència quan un enllaç falla. En el STP passen fins a 50 segons, mentre que en el RSTP un port pot passar de DISCARDING a FORWARDING en pocs segons. [13]

Elecció de tecnologia:

Totes dues tecnologies servirien per possibilitar els camins redundants a la LAN, però **es considera que la millor opció passa per habilitar RSTP en tots els switch de la LAN** i així tenir un temps de convergència o recuperació de la xarxa molt menor; fet que deriva en talls de comunicació gairebé imperceptibles.

4.1.3 LAN seu Central

A la seu central es proposa com a solució els següents canvis:

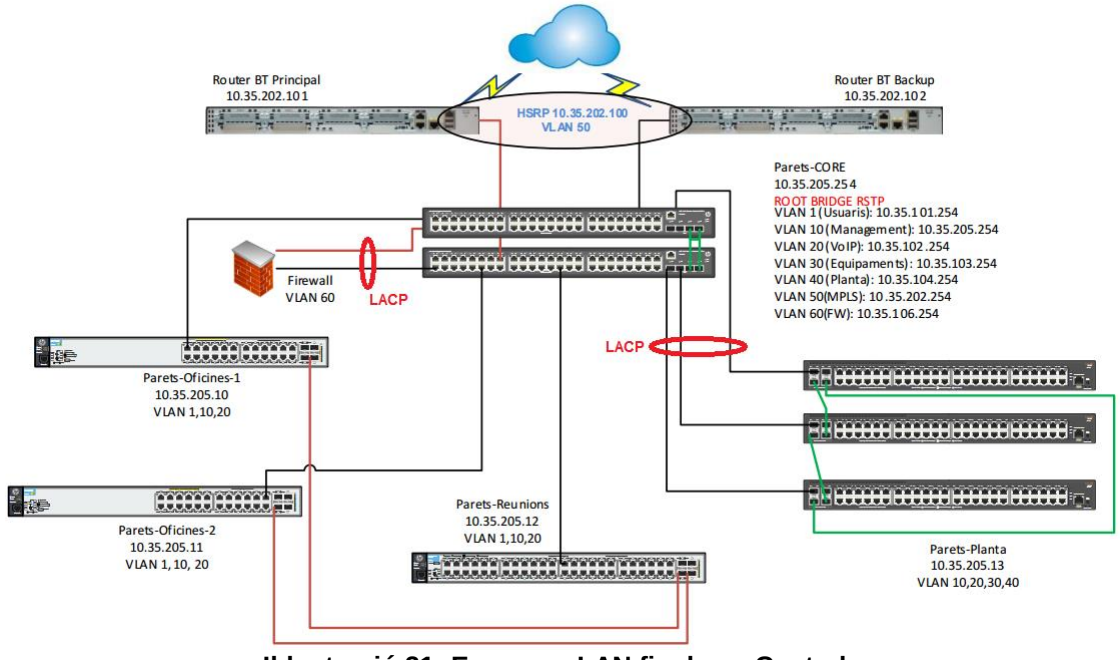
- Adquirir un nou equip HP H3C 5130 per a fer un stack IRF de CORE
  - Si cau un CORE, no afecta el global de les comunicacions.
  - Connectarem el Firewall Fortigate amb un agregat LACP per oferir redundància a la sortida WAN i els routers de MPLS estaran connectats cadascun a un membre del stack.

- Fer un stack IRF amb els 3 switch de planta
  - Possibilitarà el crear un agregat LACP dels servidors ESX amb 2 switch en el cas del ESX1 i de 3 switch en el cas del ESX2. Per tant, s'acompleix el requeriment de HA per a VMWARE.
  - Es crearà un agregat LACP amb els 3 enllaços existents per redundar els camins cap al CORE.

- Connectar oficines amb Reunions mitjançant fibra a 1GB
  - Aquests 3 switch només estan units al CORE per un cable de coure cadascun. Si aquest cable falla, tot el switch cau. Amb l'addicció d'aquestes fibres, obtenim redundància de camins.

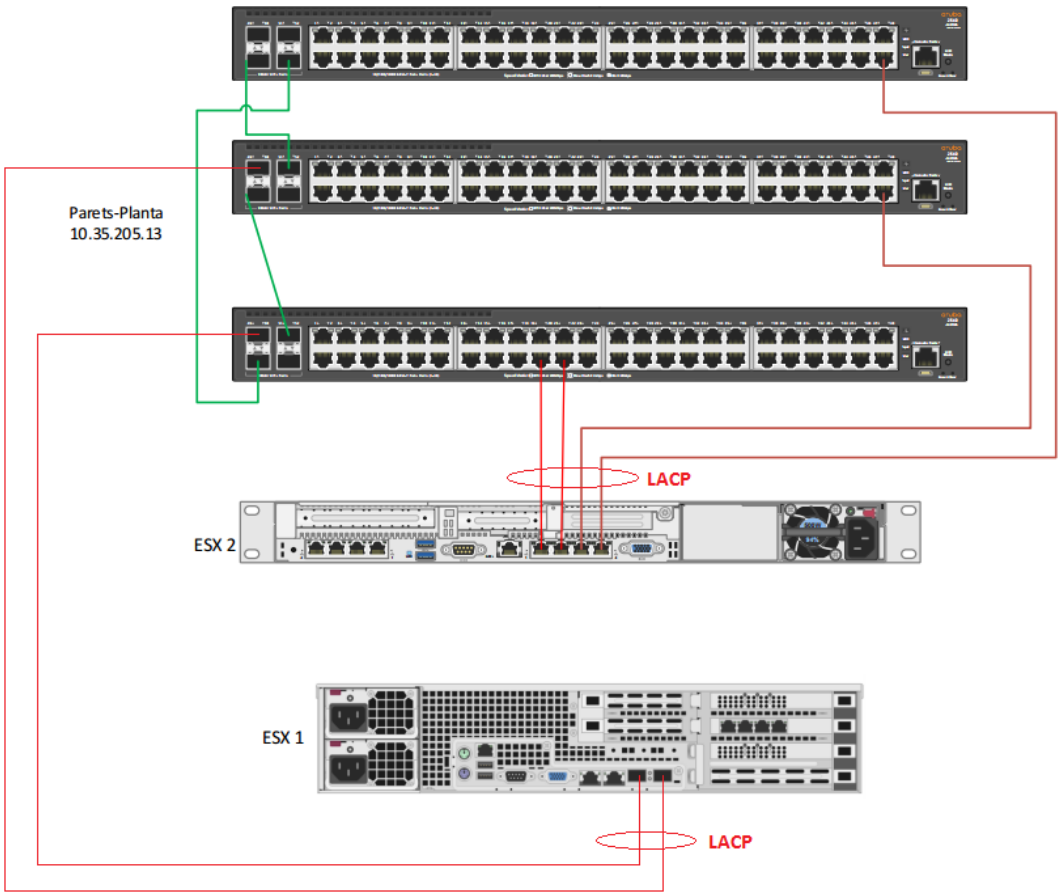
- Configurar RSTP en tots els switch
  - Habilitar el protocol RSTP en tots els switch i establir que el root bridge RSTP és el CORE.
  - Habilitar BPDU Guard en els ports dels switch d'accés que no interconnectin amb altres switch.

A continuació es mostra l'esquema general final després dels canvis. En verd els enllaços de stack i en vermell els nous enllaços o modificacions:



Il·lustració 31: Esquema LAN final seu Central

Finalment, la connexió de VMWARE es modificarà seguint el següent esquema:



Il·lustració 32: Connexions ESX amb switch de planta en stack

Com hem esmentat anteriorment, amb aquest muntatge tenim redundància de camins i HA per a la plataforma de VMWARE amb només una combinació de caigudes de switch que ocasiona pèrdua de connectivitat amb el ESX1:

Switch stack#1	Switch stack#2	Switch stack#3	ESX 1	ESX 2
✗	✓	✓	✓	✓
✓	✗	✓	✓	✓
✓	✓	✗	✓	✓
✗	✗	✓	✓	✓
✗	✓	✗	✓	✓
✓	✗	✗	✗	✓

4.1.4 LAN Dieuze

A la seu de Dieuze es proposa dur a terme accions semblants a la seu central però adaptant a les condicions de fibres de uplink i tenint en compte que no hi ha switch de reunions:

- Adquirir un nou equip HP H3C 5130 per a fer un stack IRF de CORE.
  - Redundància de CORE.
  - Els routers de MPLS estaran connectats cadascun a un membre del stack i el Firewall PFSense anirà connectat amb un LACP de 2 membres; un a cada switch.

- Fer un stack IRF amb els 2 switch de planta.
  - El servidor ESX té dos switch de 4 ports cadascun. Connectarem cada switch del servidor als dos membres del stack, de tal forma que tindrem HA encara que falli un switch del stack i un switch del servidor a la mateixa vegada.

- Nou enllaç SFP+ entre switch Dieuze-Planta-2 i CORE:
  - Amb l'esquema existent, si el switch Dieuze-Planta-1 cau, totes les comunicacions de planta cauen.

    Es proposa fer una tirada d'un enllaç de fibra a 10GB per tal de connectar el switch Dieuze-Planta-2 al CORE.

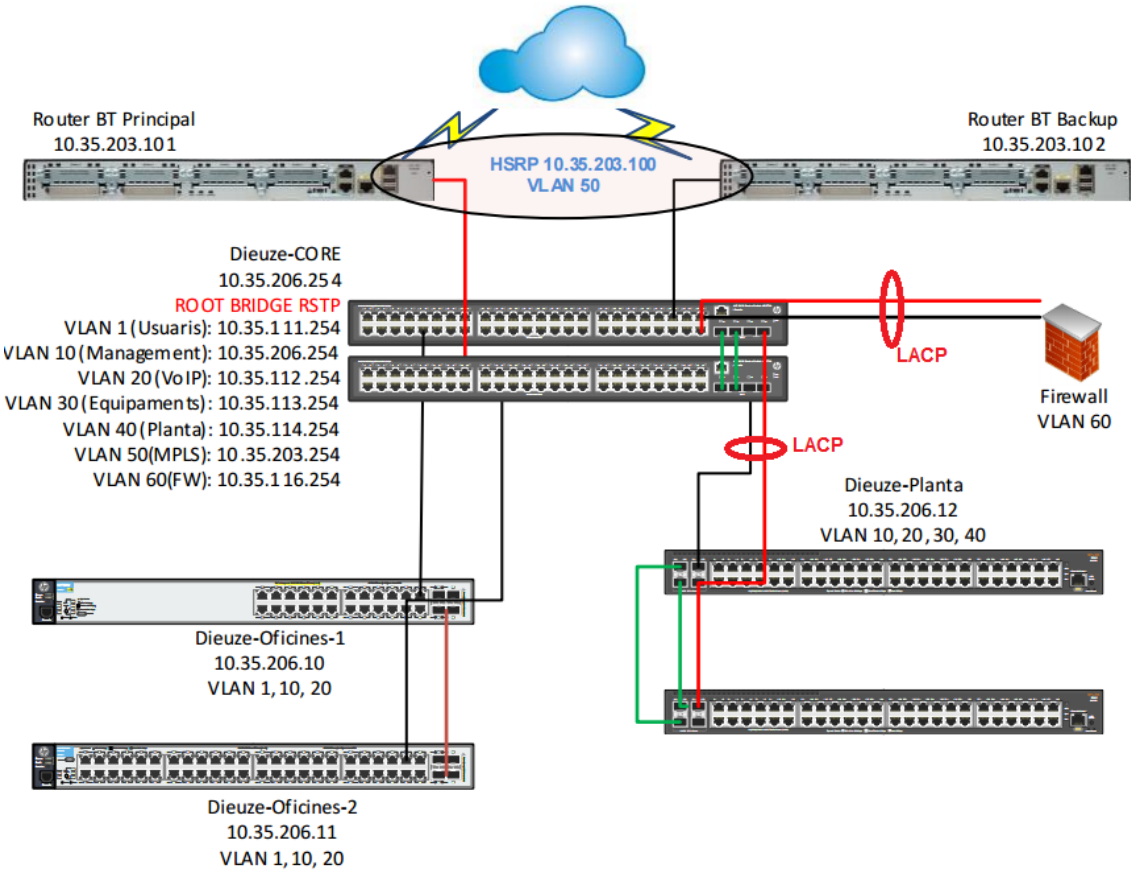
  - El nou enllaç i el ja existent entre CORE i switch Dieuze-Planta-1, conformaran un agregat de ports dinàmic LACP.

- Connectar els dos switch de oficines mitjançant fibra a 1GB:
  - Aquests 2 switch només estan units al CORE per un cable de coure cadascun. Si aquest cable falla, tot el switch cau. Amb l'addicció d'aquestes fibres, obtenim redundància de camins.

- Configurar RSTP en tots els switch
  - Habilitar el protocol RSTP en tots els switch i establir que el root bridge RSTP és el CORE.

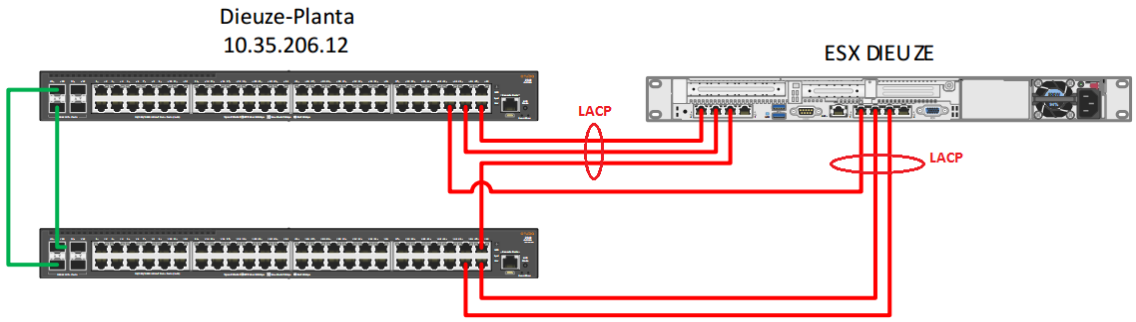
  - Habilitar BPDU Guard en els ports dels switch d'accés que no interconnectin amb altres switch.

A continuació es mostra l'esquema general final després dels canvis. En verd els enllaços de stack i en vermell els nous enllaços o modificacions:



Il·lustració 33: Esquema LAN final seu Dieuze

A nivell de ESX, la connexió quedarà feta segons el següent esquema:



Il·lustració 34: Connexió ESX amb switch de planta en stack

Amb aquestes connexions, pot fallar qualsevol dels dos switch, per separat, sense que hi hagi afectació al servei de plataforma VMWARE:

Switch stack#1	Switch stack#2	ESX DIEUZE
✗	✓	✓
✓	✗	✓

4.1.5 LAN París

En aquesta seu continuem amb l'esquema seguit per a les altres dues tenint en compte les situacions particulars de la mateixa com són la existència de un ESX i del NAS Synology el qual té gran importància per a les seus Franceses.

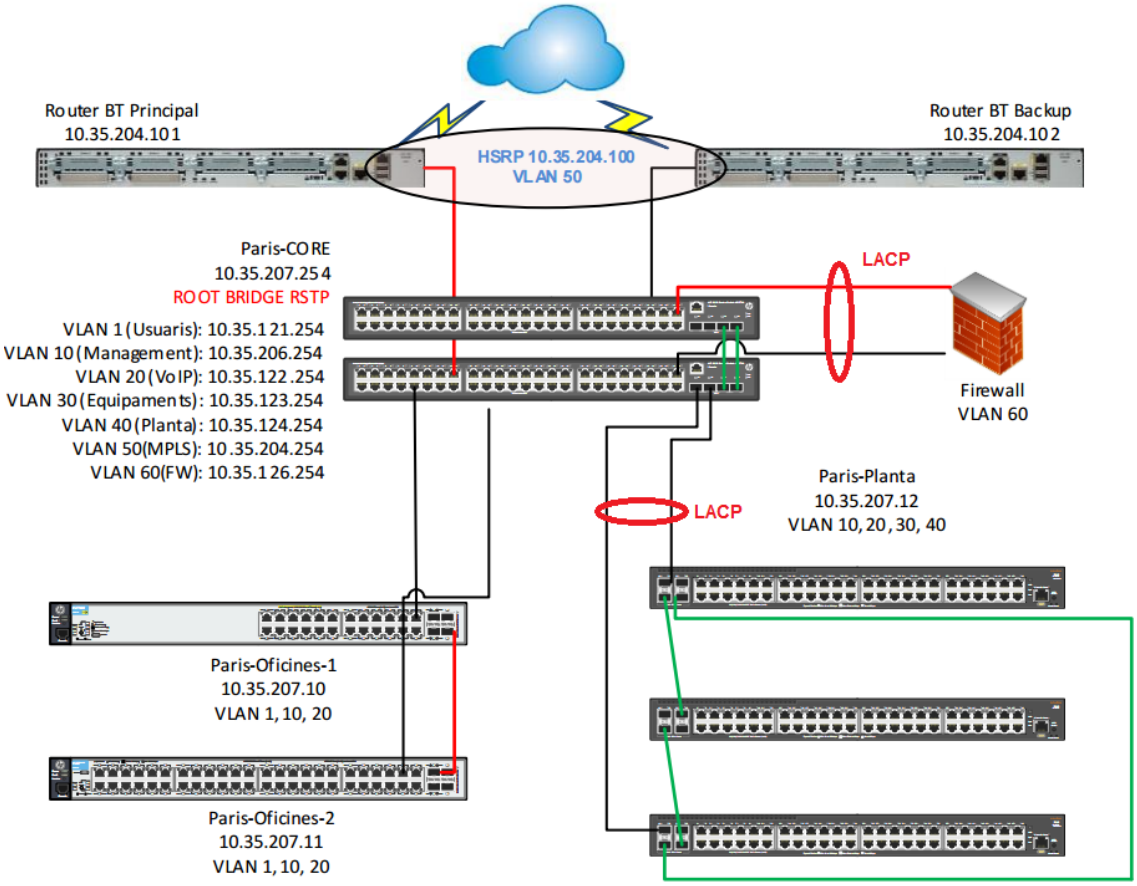
- Adquirir un nou equip HP H3C 5130 per a fer un stack IRF de CORE.
    - Redundància de CORE.
    - Els routers de MPLS estaran connectats cadascun a un membre del stack i el Firewall PFSense anirà connectat amb un LACP de 2 membres; un a cada switch.

- Fer un stack IRF amb els 3 switch de planta.
    - El servidor ESX té dos switch de 4 ports cadascun. Connectarem cada switch del servidor als dos membres del stack, de tal forma que tindrem alta disponibilitat encara que falli un switch del stack i un switch del servidor a la mateixa vegada.
    - Respecte al NAS Synology, connectat a un switch, canviarem un dels cables per a que estigui connectat a dos membres del stack.

- Connectar els dos switch d'oficines mitjançant fibra a 1GB
    - Com en el cas de Dieuze, obtenim redundància de camins.

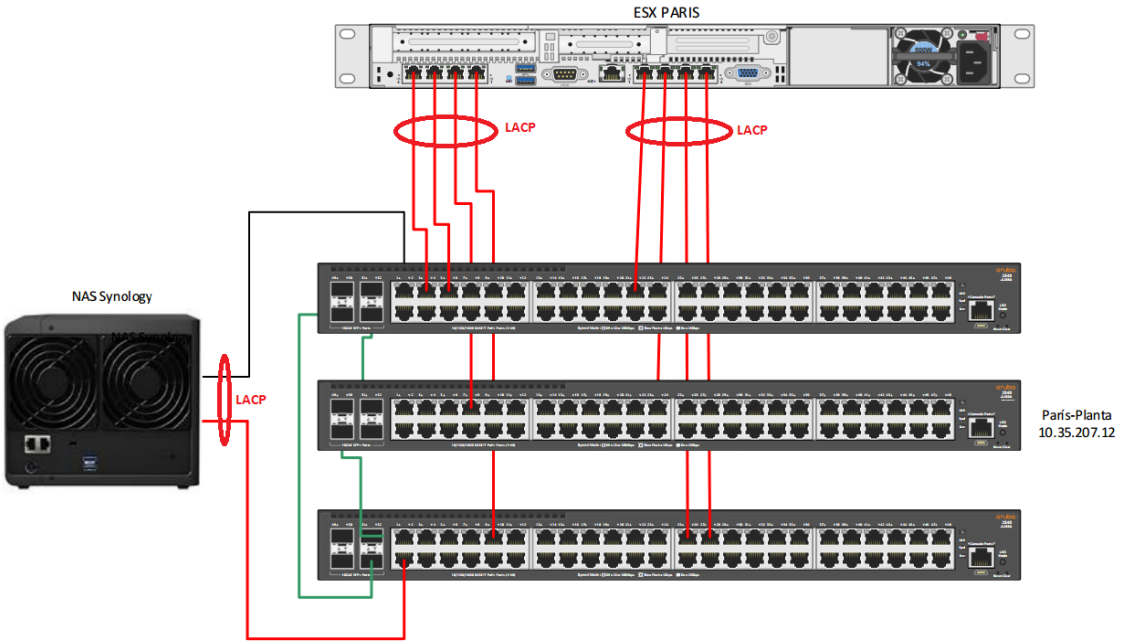
- Configurar RSTP en tots els switch
    - Habilitar el protocol RSTP en tots els switch i establir que el root bridge RSTP és el CORE.
    - Habilitar BPDU Guard en els ports dels switch d'accés que no interconnectin amb altres switch.

A continuació es mostra l'esquema general final després dels canvis. En verd els enllaços de stack i en vermell els nous enllaços o modificacions:



Il·lustració 35: Esquema LAN final seu París

Les connexions del servidor ESX i l'equip NAS Synology seguirà el següent esquema:



Il·lustració 36: Connexions ESX i NAS Synology amb stack switch de Planta

Amb aquest esquema tenim HA per a la plataforma VMWARE encara que caiguin dos switchs alhora. En canvi, el NAS només té dos interfícies, per tant, si cau el switch stack#1 i #3, el NAS quedaria sense connexió:

Switch stack#1	Switch stack#2	Switch stack#3	ESX	NAS
✗	✓	✓	✓	✓
✓	✗	✓	✓	✓
✓	✓	✗	✓	✓
✗	✗	✓	✓	✓
✗	✓	✗	✓	✗
✓	✗	✗	✓	✓

4.2 MPLS

De l'anàlisi de la situació tecnològica actual, s'extreu que en relació a la MPLS, hi ha un problema de consum d'ampla de banda relacionat amb el NAS Synology que està situat a la seu de París.

El tràfic d'aquest dispositiu suposa el 50% de l'ampla de banda contractat a Dieuze i a París, i el 25% en el cas de la seu central. Davant el requisit de no poder augmentar aquests amples de banda, es proposa que la comunicació del NAS entre seus sigui a través de la WAN.

Es descarta la possibilitat de publicar a internet el NAS i que aquest sigui accedit sense xifrar les comunicacions. Per tant, ja que es disposa de routers Cisco a les sortides WAN, tenim dues alternatives: Túnels VPN IPSEC Hub and Spoke o una VPN Multipunt o Dynamic Multipoint VPN.

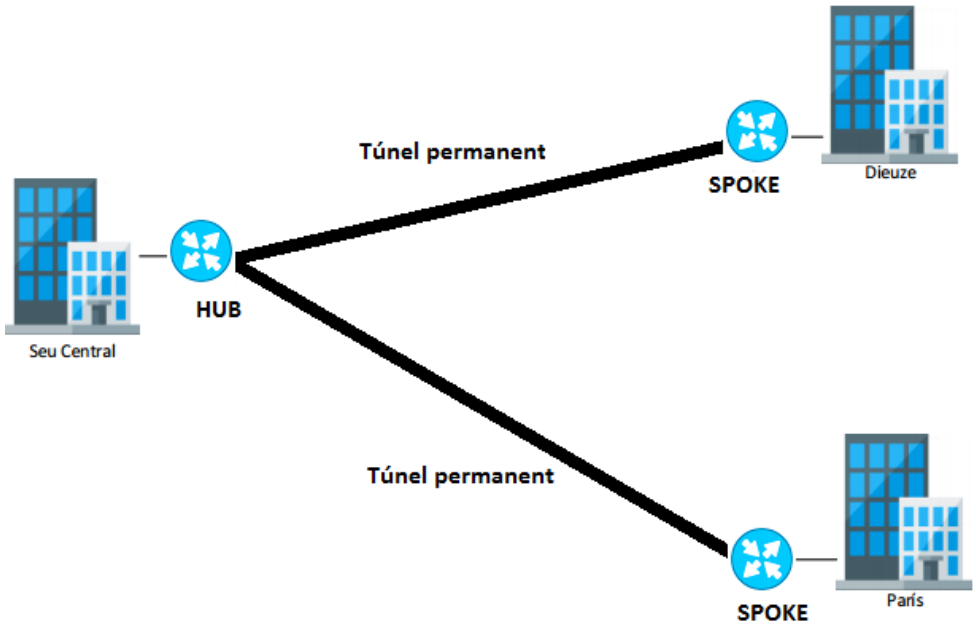
4.2.1 VPN Hub and Spoke vs DMVPN

En el cas de que l'escenari només tingués dues seus, el més adient seria fer una VPN Site-to-Site entre les dues seus. Al tenir tres seus, tenim dues possibilitats:

- **VPN IPSEC Hub and Spoke:**

  Aquesta topologia de VPN es basa en l'existència d'un node central o HUB, que en aquest cas seria la seu de Parets, i els Spokes que serien les seus de Dieuze i París.

  Tota comunicació sobre la VPN entre Dieuze i París, passaria primer pel HUB; la seu central:



Il·lustració 37: Topologia vpn hub and spoke

Veient l'esquema es pot veure que es podria fer un altre túnel entre París y Dieuze, deixant així 3 túnels site-to-site en comptes de fer una estructura Hub-and-spoke.

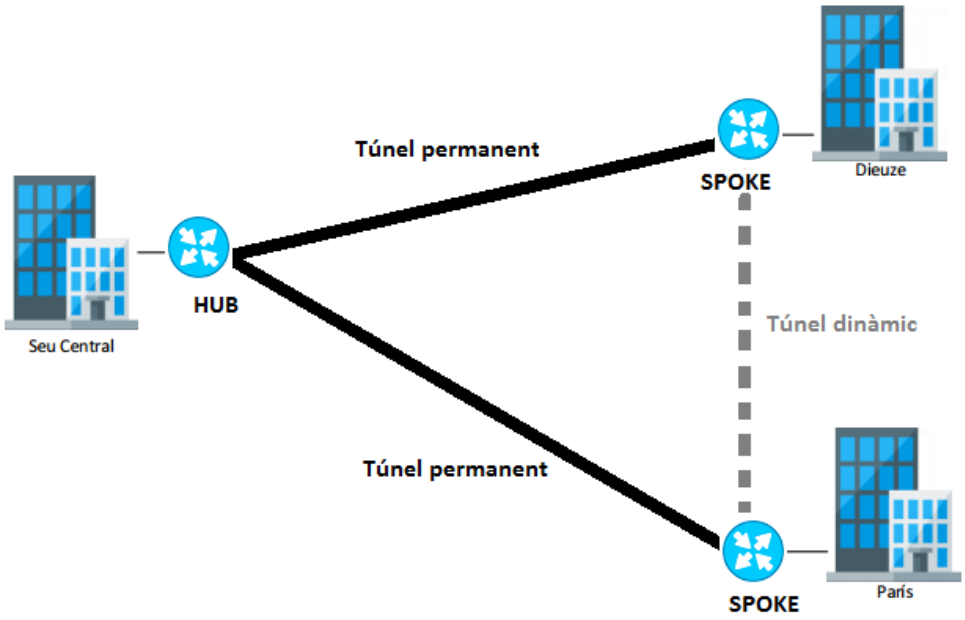
Aquesta opció es descarta ja que cada túnel ipsec té el seu adreçament privat, i això comportaria que en un escenari de 3 túnels site-to-site, tindríem també 3 adreçaments privats que farien a la vegada que el troubleshooting davant d'un problema de xarxa es dificultés en gran mesura; fet derivat de la utilització de 3 NATS diferents (segons el túnel) per al dispositiu NAS Synology.

- **DMVPN:**

La tecnologia VPN Multipunt, primerament només suportada a routers Cisco i, darrerament, en multitud de dispositius basats en UNIX, permet establir túnels dinàmics en el moment que sigui necessari.

En l'escenari de PecesCotxe, tindríem que tenim dos túnels estàtics, per exemple, de Parets a Dieuze i de Parets a París, però a més, en el moment que Dieuze i París es vulguin comunicar directament, s'estableix un túnel VPN amb encapsulament GRE entre ells.

Aquest dinamisme és gràcies a que DMVPN implementa NHRP o Next Hop Routing Protocol, i Multipoint GRE [3]. Quan un spoke vol comunicar-se amb un altre spoke (Dieuze amb París), el primer paquet s'envia al HUB (Parets) juntament amb un requeriment NHRP demanant la ip de l'altre spoke. Quan el spoke que inicia la comunicació rep la resposta de NHRP, construeix el túnel directament cap a l'altre spoke:



Il·lustració 38: Topologia vpn entre seus amb DMVPN

4.2.2 Solució MPLS proposada

Analitzant les dues alternatives, tenim que amb la utilització de VPN Hub-and-spoke tornem a tenir, com en el cas de la MPLS actual, un esquema de comunicacions (en aquest cas només el NAS), que es troba centralitzat en un punt, cosa que fa que comunicacions entre les dues seus satèl·lits, acabin consumint ample de banda de la seu central. **Tot i que és una solució viable, no és la millor, i per tant, queda descartada.**

Per tant, **es proposa la implantació de DMVPN en els routers Cisco 2951 de les tres seus** per tal de tenir un tràfic eficient alhora de consulta al NAS des de qualsevol de les tres seus, i a més, tenir les comunicacions segures mitjançant túnels GRE.

Finalment, tenint en compte l'anàlisi NetFlow de les línies MPLS a l'apartat 3.3.1, **el problema de saturació d'amples de banda MPLS a les tres seus, quedarà resolt** ja que s'alliberen 7,9 Mbps de mitjana en cadascuna de les línies MPLS.

4.3 Solució WAN

La solució WAN per a la seu central de Parets està basada en l'aprofitament de l'equip Fortigate 200B existent a la seu, ja que aquest permet aplicar regles, perfils, etc, que donin com a resultat el funcionament que s'espera.

Aquesta capacitat d'operar sobre la WAN més enllà del Routing, si no tenint una capacitat lògica i decisiva segons el que està succeint en aquell moment o el que s'ha definit prèviament, es defineix com SDWAN o Software Defined WAN (Intelligent WAN per a Cisco).

Amb SDWAN tenim la possibilitat de aplicar QoS sobre un tràfic si va a un destí concret, si és un protocol o un altre, donar amples de banda màxims per a certs destins/aplicacions/protocols, etc. Tenim un control total sobre el que es fa a la WAN, cosa que amb una solució WAN convencional, només podrem tenir definides rutes estàtiques que derivin el tràfic segons les ips/xarxes destí.

A més, amb SDWAN podem mesurar la latència, la pèrdua de paquets i el jitter de cadascuna de les línies WAN per determinar en qualsevol moment quina és la millor línia per la qual fer sortir la comunicació.

Si més no, també es podria aplicar SDWAN no només per a la sortida WAN si no per al conjunt WAN+MPLS, i d'aquesta forma treballar també sobre quin tràfic enviem a la MPLS. En el cas de PecesCotxe no és necessari ja que cap tipus de navegació es produeix per la MPLS i solament hi ha tràfic entre seus i l'entrada de correu corporatiu.

A continuació es presenta la proposta per donar resposta a cada un dels requisits de la organització respecte a la WAN de Parets:

Requisit	Solució
Si cau una línia, que no es tallin les comunicacions	Es configura un Health Check al Fortigate cap a les dues línies FTTH. En el cas que el Health Check falli a una de les línies, automàticament i sense tenir en compte la resta de regles, el tràfic es redirigeix a l'altre línia.
Tenir balanceig entre les dos línies de FTTH	Es manté el muntatge actual on les dues línies físiques estan connectades mitjançant una interfície virtual anomenada Wan Link Load Balance . Aquesta interfície fa balanceig actiu entre les dues WAN tenint en compte l'origen i destí de la comunicació.
Streamings àudio/vídeo i descarregues P2P limitades al 10% del BW	S'aplicarà un Traffic Shapping de 8 Mbps (10% del BW total) com a perfil de sortida per a aplicacions de streaming i P2P.
Aplicar QoS al tràfic corporatiu	S'aplicarà perfils de QoS i perfils de navegació segons categories per tal de garantir que les categories que es consideren corporatives, tinguin una qualitat de servei juntament amb un ample de banda garantit.

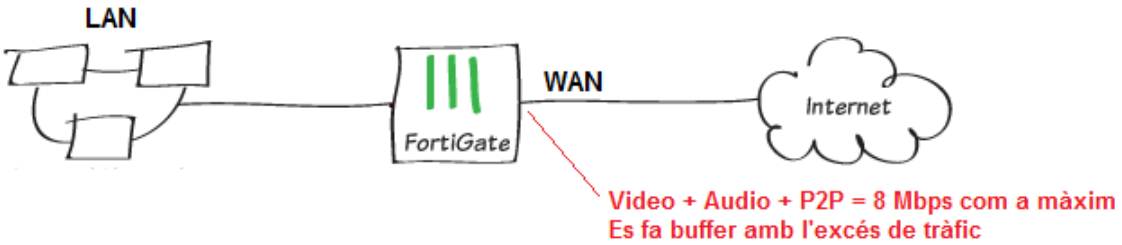
Amb l'aplicació de Traffic Shapping, limitem a que com a màxim tots els fluxos de comunicació entre la LAN i la WAN, que siguin Streamings o P2P, utilitzaran 8 Mbps.

D'altra banda, l'aplicació de QoS al tràfic corporatiu, respon a la necessitat de garantir un ample de banda mínim per al tràfic que es considera lícit. És necessari aplicar aquest QoS ja que amb l'anterior Traffic Shapping limitem descarregues, etc, però no altres tipus de tràfic que no sigui aquest o HTTP/HTTPS.

En resum, la consecució dels requisits de WAN passen per la re-configuració de l'equipament actual Fortigate 200B.

Proposta de Traffic Shaping

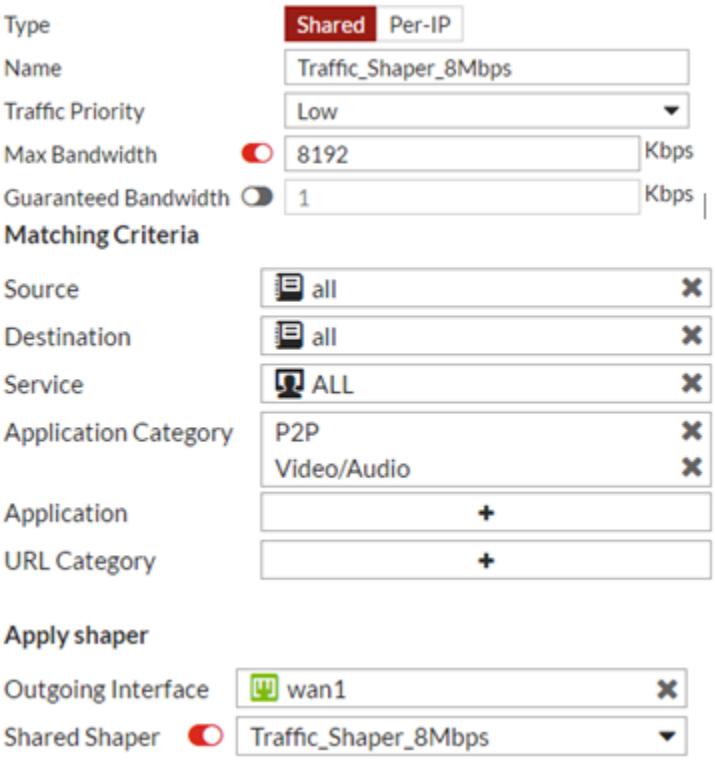
Tal i com hem indicat anteriorment, es pretén fixar un ample de banda màxim del 10% per a tràfic de àudio/vídeo i P2P. Tenint en compte que tenim un total de 80 Mbps entre les dues fibres, s'haurà d'aplicar un Traffic Shaping de 8 Mbps per aquestes comunicacions.



Il·lustració 39: Traffic shaping Fortigate

Aquest Traffic Shaping es fa d'entrada i de sortida i per a tots els usuaris, és a dir, s'utilitza el concepte de Shared Shaper de Fortigate que és aplicar-ho a tot el tràfic que passa pel Firewall, tant d'entrada com de sortida, i per a tothom.

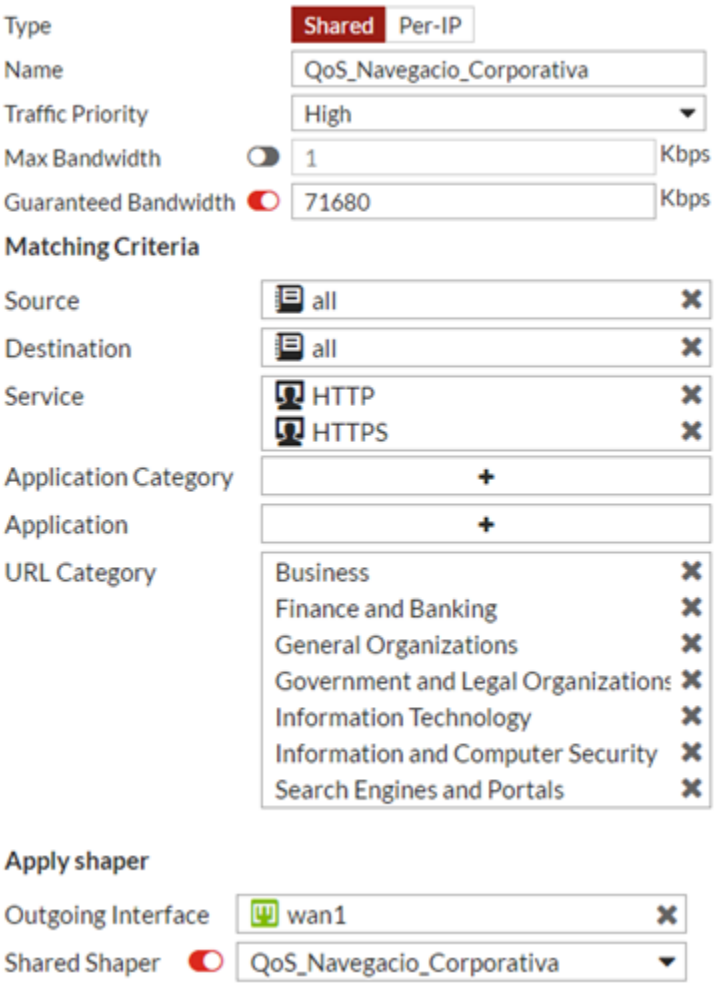
A més, es podria garantir un ample de banda mínim, però no ens interessa, per tant, es proposa aplicar un ample de banda màxim de 8192 Kbps per a les categories d'aplicacions Àudio/Vídeo i P2P [10]:



Il·lustració 40: Configuració traffic shaping al Fortigate

Proposta de QoS

Per a l'aplicació de QoS farem servir l'equipament Fortigate, però aquí ens trobem amb que el fabricant no anomena QoS com a tal la funcionalitat que ho permet, si no que es relaciona amb el concepte de Traffic Shaping amb un ample de banda garantit:



Il·lustració 41: Configuració QoS al Fortigate

La política anterior de Traffic-Shaping ens permet tenir el QoS que es demana a l'organització ja que el Firewall prioritzarà el tràfic HTTP i HTTPS cap a les categories de navegació definides.

Com es pot veure a la imatge (il·lustració 41), es proposa garantir 70Mbps per al tràfic de navegació corporativa. Tenint en compte que tenim 80Mbps totals i que apliquem un màxim de 8Mbps per al no corporatiu, tindríem un marge de 2Mbps per a tràfic "no controlat".

El concepte d'ample de banda garantit es refereix a que davant d'una congestió de la WAN, el Firewall descartaria la resta de tràfic per tal de poder donar servei HTTP/HTTPS corporatiu fins a 70Mbps. Si la navegació no necessita tot l'ample de banda garantit, aquest passa a estar lliure per a la resta de tràfic.

5. Valoració econòmica

A continuació es detallen els diferents costos referits a l'adquisició del material necessari per a la implantació de la solució, així com els associats a les hores tècniques necessàries per a assolir-ho.

Els preus de hardware són directes de fabricant, sense tenir en compte possibles descomptes que s'apliquen depenen del partner que executi la compra.

- **Hardware:**

ITEM	#	UNITARI	TOTAL
Seu central			
HP 5130 JG976A	1	4.627 €	4.627 €
Cable DAC 0,65m JH693A	2	184 €	368 €
Cable DAC 1,2m JH694A	3	195 €	585 €
SFP LC SX Trans. J4858C	4	223 €	892 €
Cable OM3 10m LC-LC	2	14,62 €	29,24 €
Cable UTP CAT6 1,5m	1	2,42 €	2,42 €
Dieuze			
HP 5130 JG976A	1	4.627 €	4.627 €
Cable DAC 0,65m JH693A	2	184 €	368 €
Cable DAC 1,2m JH694A	2	195 €	390 €
SFP LC SX Trans. J4858C	2	223 €	446 €
SFP+ LC SR Trans. J9150A	1	928 €	928 €
Cable OM3 2m LC-LC	4	7,80 €	31,20 €
Cable UTP CAT6 1m	1	2,30 €	2,30 €
París			
HP 5130 JG976A	1	4.627 €	4.627 €
Cable DAC 0,65m JH693A	2	184 €	368 €
Cable DAC 1,2m JH694A	3	195 €	585 €
SFP LC SX Trans. J4858C	2	223 €	446 €
Cable OM3 5m LC-LC	1	12,68 €	12,68 €
Cable UTP CAT6 1m	1	2,30 €	2,30 €

Cost total del material [12]: 19337,14 euros + IVA

- **Cost tècnic:**
  La segona part de la valoració econòmica correspon al cost humà/tècnic d'executar les tasques d'instal·lació del nou hardware, cablejat, configuració nous equips, re-configuració existents, etc.

CONCEPTE	H.	UNITARI	TOTAL
Seu central			
Re-configuració Fortigate FFHH	2	95 €	190 €
Configuració nou HP5130	2	50 €	100 €
Configuració STACK Planta i CORE en FFHH	3	95 €	285 €
Configuracions Agregats LACP	1	95 €	95 €
Cablejat fibra nous enllaços	4	50 €	200 €
Connexió nous enllaços	1	95 €	95 €
Proves de connectivitat i HA	1,5	50 €	75 €
Re-configuració router Cisco	0,75	95 €	71,25 €
Proves WAN i VPN	1	50 €	50 €
Dieuze			
Configuració nou HP5130	2	50 €	100 €
Configuració STACK Planta i CORE en FFHH	3	95 €	285 €
Configuracions Agregats LACP	1	95 €	95 €
Cablejat fibra nous enllaços	3,5	50 €	175 €
Connexió nous enllaços	1	95 €	95 €
Proves de connectivitat i HA	1,5	50 €	75 €
Re-configuració router Cisco	0,75	95 €	71,25 €
Proves VPN	1	50 €	50 €
París			
Configuració nou HP5130	1	50 €	50 €
Configuració STACK Planta i CORE en FFHH	3	95 €	285 €
Configuracions Agregats LACP	0,5	95 €	95 €
Cablejat fibra nous enllaços	2	50 €	100 €
Connexió nous enllaços	1	95 €	95 €
Proves de connectivitat i HA	1,5	50 €	75 €
Re-configuració router Cisco	0,75	95 €	71,25 €
Proves VPN	1	50 €	50 €

Cost total tècnic: 2928,75 euros + IVA

Per entendre la valoració, s'ha de tenir en compte:

- No es comptabilitza la fase de disseny de la solució.
- El preu hora serà de 50€ + IVA per a les accions portades a terme en horari laboral i de 95€ + IVA les que, per la seva naturalesa impliquin talls de comunicació, es facin fora d'horari laboral i/o de forma nocturna quan el tall tingui el mínim impacte possible en la productivitat de la organització.

- **Resum de costos:**

Segons hem calculat, l'execució d'aquest projecte tindria un cost de:

- Hardware: 19337,14 € + IVA
- Mà d'obra: 2928,75 € + IVA

COST TOTAL D'EXECUCIÓ: **22.265,89 €UROS + IVA**

6. Implementació del projecte

En el present apartat, es presenta la proposta d'implantació de projecte, recollint les tasques necessàries, i les proves funcionals que es consideren necessàries per garantir que el projecte respon a les necessitats de l'organització.

6.1 Seu central

A la seu central, s'han de fer canvis tant de LAN com de WAN. Els canvis no representen tall de comunicacions en la seva totalitat, però si que hi ha canvis a realitzar que no es poden dur a terme sense tallar momentàniament.

Per aquest motiu, es presenta el recull de tasques juntament amb la indicació de si comporta tall de comunicacions o no:

#	TASCA	TALL
1	Configuració dels perfils de QoS i Traffic Shaping en Firewall Fortigate	**Possible***
2	Configuració VPN multipunt a router Cisco de la seu	No
3	Cablejar i configurar enllaç fibra Reunions amb Oficines	No
4	Afegir cable UTP i configurar LACP al Firewall i CORE	**Si**
5	Configuració de nou switch H3c HP5130	No
6	Configuració i connectar IRF (stack) de CORE	**Si**
7	Configuració i connectar IRF (stack) de Planta	**Si**
8	Configurar LACP entre switch stack de Planta i CORE	**Si**
9	Canviar connexions routers BT MPLS per a estar connectat cadascun a un switch de CORE	No**
10	Configuració RSTP en tots els switch de la LAN	**Possible*** **

**En el moment d'aplicar els nous perfils, a les polítiques de navegació, es pot produir un micro-tall a les comunicacions o un reinici de les sessions TCP/UDP actives.*

***Encara que canviem connexions de routers BT, al estar configurats amb HSRP, podem desconnectar un d'ells, per canviar-ho de switch, i les comunicacions continuar funcionant ja que el switch crida a la ip virtual de HSRP.*

****La configuració de RSTP no ha de representar un tall considerable si no un possible micro-tall de comunicacions ja que ha de convergir la topologia de xarxa.*

Amb motiu de voler garantir que la configuració realitzada és funcional i que el comportament de la solució és el desitjat, s'indiquen les següents proves funcionals o de validació:

1. **Prova:** Descàrrega de fitxer a través de xarxa P2P.
   Valida: Traffic Shaping limita a 8Mbps la descarrega.

2. **Prova:** Prova de navegació corporativa a URL de categoria definida a la proposta de QoS tot descarregant un fitxer. En paral·lel es fa una descarrega d'un fitxer per FTP.
   Valida: Política de QoS on la navegació corporativa ha de tenir garantit un caudal de 70Mbps; descarrega de fitxer corporatiu té preferència sobre la descarrega de FTP.

3. **Prova:** Apagar un switch de CORE.
   Valida: Redundància de camins i no caiguda de xarxa davant la caiguda d'un equip de CORE.

4. **Prova:** Desconnexió del cable UTP que connecta Parets-Reunions amb el CORE i desconnexió d'un enllaç d'oficines amb CORE.
   Valida: Entre oficines/reunions-CORE tenim 3 enllaços, es verifica que la caiguda de fins a 2 cables, no talla les comunicacions.

5. **Prova:** Apagar el switch planta stack #1 i #2.
   Valida: Els dos servidos ESX continuen sent accessibles.

6. **Prova:** Desconnexió de 2 dels 3 ports que conformen el LACP entre Planta i CORE. Verificació de que els tres switch que conformen el stack de planta poden contactar amb el CORE.
   Valida: Redundància davant caiguda parcial de fibres de planta a CORE mantenint comunicacions.

7. **Prova:** Una vegada estiguin les tres seus configurades; verificar que la VPN entre seus funciona.
   Valida: Es valida la configuració DMVPN en router Cisco. Caldrà en les altre seus veure si el túnel entre elles s'estableix de forma dinàmica.

Finalment, tot i no ser considerada una prova, s'haurà de revisar les dades de Netflow mensuals, proporcionades per BT, per tal de comprovar que la descentralització del tràfic de NAS ha tingut l'efecte desitjat en el descens del tràfic de MPLS.

6.2 Seu Dieuze

En el cas de Dieuze, els canvis són a nivell de LAN amb les següents tasques:

#	TASCA	TALL
1	Configuració VPN multipunt a router Cisco de la seu	No
2	Cablejar i configurar enllaç fibra entre Oficines i Oficines 2	No
3	Afegir cable UTP i configurar LACP al Firewall i CORE	**Si**
4	Configuració de nou switch H3c HP5130	No
5	Configuració i connectar IRF (stack) de CORE	**Si**
6	Configuració i connectar IRF (stack) de Planta	**Si**
7	Configurar LACP entre switch stack de Planta i CORE	**Si**
8	Canviar connexions routers BT MPLS per a estar connectat cadascun a un switch de CORE	No
9	Configuració RSTP en tots els switch de la LAN	**Possible**

Les proves funcionals a dur a terme són:

1. **Prova:** Apagar un switch de CORE.
   Valida: Redundància de camins i no caiguda de xarxa davant la caiguda d'un equip de CORE.

2. **Prova:** Desconnexió del cable UTP que connecta Oficines 1 amb CORE. Repetir prova desconnectant, aquest cop, el UTP d'Oficines 2.
   Valida: Entre oficines -CORE tenim 2 enllaços, es verifica que la caiguda d'un enllaç no afecta a les comunicacions.

3. **Prova:** Apagar el switch planta stack #1 i posteriorment repetir prova apagant el #2 mentre que el #1 està actiu.
   Valida: Els ESX Dieuze continua accessible encara que caigui un switch de planta.

4. **Prova:** Desconnexió d'un port LACP entre Planta i CORE. Verificació de que els switch que conformen el stack poden contactar amb el CORE.
   Valida: Redundància camins entre Planta i CORE.

5. **Prova:** Quan estiguin les tres seus amb DMVPN configurades; establir comunicació amb NAS de París i veure que s'estableix un túnel dinàmicament gràcies a la configuració realitzada.
   Valida: Es valida la configuració DMVPN en router Cisco.

6.2 Seu París

La seu de París és un escenari molt semblant a Dieuze, tot i tenir les seves particularitats:

#	TASCA	TALL
1	Configuració VPN multipunt a router Cisco de la seu	No
2	Cablejar i configurar enllaç fibra entre Oficines i Oficines 2	No
3	Afegir cable UTP i configurar LACP al Firewall i CORE	**Si**
4	Configuració de nou switch H3c HP5130	No
5	Configuració a planta LACP amb NAS Synology	**Si***
6	Configuració i connectar IRF (stack) de CORE	**Si**
7	Configuració i connectar IRF (stack) de Planta	**Si**
8	Configurar LACP entre switch stack de Planta i CORE	**Si**
9	Canviar connexions routers BT MPLS per a estar connectat cadascun a un switch de CORE	No
10	Configuració RSTP en tots els switch de la LAN	**Possible**

**Es produirà un tall de comunicacions amb el NAS durant el canvi de configuració que passa per configurar l'enllaç existent i el nou cable en LACP.*

Les proves funcionals a dur a terme són:

1. **Prova:** Apagar un switch de CORE.
   Valida: Redundància de camins i no caiguda de xarxa davant la caiguda d'un equip de CORE.

2. **Prova:** Desconnexió del cable UTP que connecta Oficines 1 amb CORE. Repetir prova desconnectant, aquest cop, el UTP d'Oficines 2.
   Valida: Entre oficines -CORE redundància camins.

3. **Prova:** Apagar dos switch de Planta (indiferent quins son) i validar que el ESX de París continua sent accessible.
   Valida: El ESX de París no es veu afectat davant la caiguda de 2 switch de planta.

4. **Prova:** Apagar el switch planta stack #1 i stack #2 i verificar el NAS.
   Valida: el NAS continua accessible sempre que no caigui el switch stack #3.

5. **Prova:** Desconnexió d'un port LACP entre Planta i CORE. Verificació de que els switch que conformen el stack poden contactar amb el CORE.
   Valida: Redundància camins entre Planta i CORE.

7. Conclusions

Durant la realització d'aquest treball, he après nous conceptes com les VPN multipunt dinàmiques i les línies WAN definides per software. A més, he profunditzat en altres temes que, tot i no ser nous conceptes, només havia vist superficialment com és el STP i el stacking.

En quan a la planificació, la mateixa no ha sigut complerta al 100%, sobretot en quan a l'entrega de la PAC 2, ja que va ser insuficient, incomplint els marges temporals fixats per mi mateix a l'inici del projecte. Això ha fet que l'entrega de la PAC3 hagi sigut molt justa, tot i que crec que s'han assolit les fites marcades.

En relació al paràgraf anterior, he de dir que m'ha sorprès la dificultat que representa gestionar un projecte d'inici a fi, tot definint les tasques, sub-tasques i temps necessari per a cada fita. Fet d'això, he après que és tant important o més, la feina de gestió vers la de implantació; tenir una visió global del conjunt és un handicap que fins ara no havia hagut d'enfrontar-me.

Si parlem dels objectius proposats, crec que han sigut assolits i, fins i tot, ampliats, ja que entre la proposta inicial (PAC1) i la final (PAC2), hi ha tot una sèrie d'afegits que comportaven una major dedicació i treball. Per tant, crec que els objectius han sigut àmpliament assolits.

Finalment, m'agradaria dir que si aquest projecte el portés a terme a la vida real, afegiria un sistema de monitorització dels elements de xarxa. Crec que seria l'element que faria un projecte d'optimització LAN/WAN al 100%.

8. Glossari

- **DAC:** cable de fibra, amb connectors SFP, a 10GB que serveix per a fer STACK en switch HP H3C.

- **SFP/SFP+:** Small Form-factor Pluggable Transceptor. És un connector gigabit (SFP) o Ten-GigabitEthernet (SFP+) que permet connectar, per exemple, un cable de fibra al port d'un switch.

- **LC**: Lucent Technologies Connector, és un connector terminal òptic. Es fa servir per a permetre la connexió d'un cable de fibra a SFP/SFP+.

- **QoS**: Quality of Service. Concepte que s'aplica en relació a la capacitat de garantir que certa comunicació tindrà la qualitat mínima necessària pel seu bon funcionament.

- **GRE**: Generic Routing Encapsulation és un protocol per a l'establiment de túnels segurs a través d'internet.

- **NAS**: Network Attached Storage. Dispositiu d'emmagatzematge accessible en xarxa.

- **LACP**: Link Aggregation Control Protocol. Agregació dinàmica de ports físics. Permet la distribució de càrrega d'una comunicació entre diferents ports físics conformant un port lògic.

- **ESX**: S'anomena així als servidors que tenen el rol de suportar la plataforma de màquines virtuals (hypervisor) del fabricant VMWARE.

- **VLAN**: Virtual LAN, mètode per a tenir xarxes lògiques, diferenciades una de l'altre, dins de la mateixa xarxa física.

- **STP**: Spanning Tree Protocol. Protocol de xarxes de nivell 2 que proporciona la capacitat de gestionar bucles a topologies de xarxa les quals tenen enllaços redundants.

- **RSTP**: Rapid Spanning Tree Protocol. Evolució del STP; redueix el temps de convergència de la topologia de xarxa quan es produeix un canvi en la mateixa.

- **Traffic Shaping**: Mecanisme de control del tràfic d'una xarxa amb la finalitat d'evitar la sobrecarrega de la mateixa.

- **BDPU:** Bridge Protocol Data Units, son trames ethernet que contenen informació del protocol STP.

- **BPDU Guard:** Mecanisme de protecció per rebutjar les BPDU que es rebin en un determinat port. Serveix per evitar un canvi de topologia de STP si es connecta un switch a un switch d'accés.

9. Bibliografia

[1] Computer Networking – A Top-Down Approach
Autor: James F.Kurose / Keith W. Ross
Editorial: Pearson Education Limited
Edició: 6ta edició, 2013, England

[2] Multiprotocol Label Switching. Disponible a:
https://es.wikipedia.org/wiki/Multiprotocol_Label_Switching
Accedit el 11/03/2017

[3] DMVPN. Disponible a:
https://supportforums.cisco.com/es/blog/12882846
Accedit el 11/03/2017

[4] IPSEC. Disponible a:
https://es.wikipedia.org/wiki/IPsec
Accedit el 11/03/2017

[5] Virtual Private Network. Disponible a:
https://en.wikipedia.org/wiki/Virtual_private_network
Accedit el 12/03/2017

[6] Fortigate 200B DataSheet:
http://www.fortigate.cz/upload-sys/produkty2/file/10/fgt200b-ds.pdf
Accedit el 15/04/2017

[7] Fortinet CookBook 5.4. Disponible a:
http://docs.fortinet.com/d/fortigate-the-fortigate-cookbook-5.4
Accedit el 15/04/2017

[8] Stacking vs Chassis. Disponible a:
http://discover.vology.com/blog/technology-categories/networking/stacking-vs-chassis-access-switch-solutions/
Accedit el 29/04/2017

[9] QoS, calidad del Servicio. Disponible a:
https://es.wikipedia.org/wiki/Calidad_de_servicio
Accedit el 29/04/2017

[10] Limiting Traffic with Traffic shaping: Disponible a:
http://cookbook.fortinet.com/traffic-shaping-bandwidth-54/
Accedit el 29/04/2017

[11] IRF Configuration Guide. Disponible a:
http://www.h3c.com.hk/Technical_Support___Documents/Technical_Documents/Switches/H3C_S12500_Series_Switches/Configuration/Operation_Manual/H3C_S12500_CG-Release7128-6W710/02/201301/772606_1285_0.htm
Accedit el 16/05/2017

[12] HP Online Networking configurator. Disponible a:
http://h17007.www1.hpe.com/us/en/networking/products/configurator/
Accedit el 18/05/2017

[13] STP vs RSTP. Disponible a:
https://cciethebeginning.wordpress.com/2008/11/20/differences-between-stp-and-rstp/
Accedit el 26/05/2017

[14] VLAN Redes virtuales. Disponible a:
http://es.ccm.net/contents/286-vlan-redes-virtuales
Accedit el 27/05/2017

10. Annex: configuració stack IRF

A continuació es detalla tot el procés de configuració d'un stack IRF [11] de tres membres (el cas més complex del projecte):

1er pas: Activar el IRF als tres switch i definir les prioritats:

Switch Membre 1	
system-view irf member 1 priority 32 irf auto-update enable save quit reboot y	Amb aquestes comandes habilitem la capacitat d'actualitzar la taula de membres IRF i assignem una prioritat a aquest membre.

Switch MIembre 2	
system-view irf member 1 renumber 2 y irf auto-update enable quit reboot y **#Esperar reinici i fer:** System-view irf member 2 priority 16 save	El membre 2 i els següents, requereixen un reinici previ a l'assignació de prioritat, ja que fins que no es produeix el reinici, el membre no adquireix el número de membre assignat diferent a 1. Com es pot veure, el número de prioritat més alt, correspon a la prioritat més alta. Si després d'això fem un display interfases, veurem que ara s'anomenen Gi 2/0/x on el primer número indica el membre de IRF.

Switch MIEMBRO3
system-view irf member 1 renumber 3 y irf auto-update enable quit reboot y **#Esperar reinici i fer:** System-view irf member 3 priority 8 save

2on pas: Decidir quines interfícies físiques de 10GB utilitzarem pel IRF

Switch Membre 1
interface Ten-GigabitEthernet 1/0/51 interface Ten-GigabitEthernet 1/0/52
Switch Membre 2
interface Ten-GigabitEthernet 2/0/51 interface Ten-GigabitEthernet 2/0/52
Switch Membre 3
interface Ten-GigabitEthernet 3/0/51 interface Ten-GigabitEthernet 3/0/52

3er pas: Des habilitar les interfícies seleccionades

Switch Membre 1
System-view interface Ten-GigabitEthernet 1/0/51 shutdown interface Ten-GigabitEthernet 1/0/52 shutdown
Switch Membre 2
System-view interface Ten-GigabitEthernet 2/0/51 shutdown interface Ten-GigabitEthernet 2/0/52 shutdown
Switch Membre 3
System-view interface Ten-GigabitEthernet 3/0/51 shutdown interface Ten-GigabitEthernet 3/0/52 shutdown

4t pas: Crear els IRF-PORT tenint en compte:

Switch Membre 1	
IRF PORT 1/1	Interface Ten-gigabitEthernet 1/0/51
IRF PORT 1/2	Interface Ten-gigabitEthernet 1/0/52
Switch Membre 2	
IRF PORT 2/1	Interface Ten-gigabitEthernet 2/0/51
IRF PORT 2/2	Interface Ten-gigabitEthernet 2/0/52
Switch Membre 3	
IRF PORT 3/1	Interface Ten-gigabitEthernet 3/0/51
IRF PORT 3/2	Interface Ten-gigabitEthernet 3/0/52

Switch Membre 1
System-view Irf-port 1/1 port group interface Ten-GigabitEthernet 1/0/51 irf-port 1/2 port group interface Ten-GigabitEthernet 1/0/52
Switch Membre 2
System-view Irf-port 2/1 port group interface Ten-GigabitEthernet 2/0/51 irf-port 2/2 port group interface Ten-GigabitEthernet 2/0/52
Switch Membre 3
System-view Irf-port 3/1 port group interface Ten-GigabitEthernet 3/0/51 irf-port 3/2 port group interface Ten-GigabitEthernet 3/0/52

5é pas: Habilitar les interfases físiques dedicades al IRF

Switch Membre 1
System-view interface Ten-GigabitEthernet 1/0/51 undo shutdown interface Ten-GigabitEthernet 1/0/52 undo shutdown quit save
Switch Membre 2
System-view interface Ten-GigabitEthernet 2/0/51 undo shutdown interface Ten-GigabitEthernet 2/0/52 undo shutdown quit save
Switch Membre 3
System-view interface Ten-GigabitEthernet 3/0/51 undo shutdown interface Ten-GigabitEthernet 3/0/52 undo shutdown quit save

6é pas: Fer la connexió física amb els cables DAC seguint el següent esquema:

7é pas: Activar la detecció de nous membres IRF per tal de que es formi el stack de switch:

Switch MIEMBRO1
System-view irf-port-configuration active
Switch MIEMBRO2
System-view irf-port-configuration active
Switch MIEMBRO3
System-view irf-port-configuration active

8é pas: En el pas anterior es reiniciaran els switch, formaran el stack i ja estarà la configuració completada. No obstant, ho verificarem amb les següents comandes:

#: display irf
#: display irf topology