Memòria tècnica del projecte per a la implementació de la xarxa LAN de l'empresa TECNOCAT

Gerard Baiget Pellicer
Administració de xarxes i sistemes operatius

Manuel Jesús Mendoza Flores

7 de juny de 2017

DEDICAT

Als meus pares, Per l'esforç, dedicació i paciència
Als meus fills, per els vostres somriures i petons diaris
A la meva dona, sense tu no hagués arribat tant lluny a la vida
T'estimo, us estimo

FITXA DEL TREBALL FINAL

Títol del treball:	*Memòria tècnica del projecte per a la implementació de la xarxa LAN de l'empresa TECNOCAT*
Nom de l'autor:	*Gerard Baiget Pellicer*
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 en Enginyeria informàtica*

Resum del Treball (màxim 250 paraules):

En aquest projecte s'abordarà una possible solució a la implementació des de zero d'una xarxa cablejada de telecomunicacions per a l'empresa TECNOCAT, tant per veu per com per dades, des del punt de vista d'una empresa consultora fictícia la qual hem anomenat NETing. Contempla tots els aspectes necessaris per l'anàlisi i futura execució d'una infraestructura de xarxa d'una gran empresa, analitzant les diferents casuístiques i aportant solucions concretes. Així doncs, els principals objectius d'aquest projecte són:

- Analitzar i entendre les mancances actuals del TECNOCAT i donar una solució mitjançant la implementació d'una xarxa cablejada pròpia de telecomunicacions
- Analitzar les diferents tecnologies en el mercat de la commutació, telefonia i seguretat i donar una solució per al seu desplegament funcional
- Oferir una solució de configuració dels equips d'accés dels usuaris per garantir un control sobre què es connecta a la xarxa

Abstract (in English, 250 words or less):

This project will address a possible solution to the implementation of a wired communications network for the TECNOCAT entrerprise, both by voice and data, from the point of view of a fictive consulting company that we have called NETing. It includes all the necessary aspects for the analysis and future execution of a network infrastructure of a large company, analyzing the different cases and providing concrete solutions. Thus, the main objectives of this project are:

• Analyze and understand TECNOCAT's current shortcomings and provide a solution through the implementation of her own wired comunications network

• Analyze the different technologies in the market for switching, telephony and security and provide a solution for their functional development

• Provide a solution for configuring user access equipment to ensure control over what connects to the network

Paraules clau (entre 4 i 8):

Consultoria
Xarxa
Connectivitat
Anàlisi
Solucions
Seguretat
veu
dades

Índex

1. Introducció

1.1 Context i justificació del Treball

La memòria tècnica de la implementació de la xarxa LAN per a l'empresa TECNOCAT és un projecte molt ambiciós que ha de dotar al centre amb una infraestructura de telecomunicacions d'últim nivell amb uns requeriments funcionals. Les empreses que vinguin a treballar al centre hauran de tenir totes les comoditats per poder desenvolupar els seus productes amb èxit, i una clau d'aquest èxit es tenir una infraestructura de xarxa eficient i segura.

Actualment les empreses que estan treballant a TECNOCAT no disposen d'un servei de telecomunicacions a l'alçada de les seves necessitats i, a més, han de contractar els serveis de veu i dades a empreses externes. Per tant, el que es vol aconseguir mitjançant aquesta memòria tècnica és donar una solució tecnològica al *pool* d'empreses que estiguin instal·lades al centre. Això permetrà a TECNOCAT:

- ser un referent tecnològic a la zona
- donar solucions personalitzades a les empreses
- atenció al client mitjançant un equip de treball *in-situ*
- augment de beneficis gràcies al pagament per ús dels serveis de telecomunicacions ofertats (sempre que TECNOCAT així ho vulgui)
- Donar un valor afegit a les empreses

És important esmentar que aquest projecte no pretén ser un pla estratègic, sinó un estudi extern, realitzat des del punt de vista d'una consultoria especialitzada (empresa que hem anomenat NETing) que ha de servir als administradors del TECNOCAT com a punt de partida per al pla estratègic.

Mitjançant la memòria tècnica es pretén donar una visió acurada de com haurien de ser els serveis de telecomunicacions d'un centre d'aquestes característiques.

1.2 Objectius del treball

Els objectius d'aquest projecte són diversos:

- Realitzar un projecte per a la implementació d'una xarxa LAN funcional
- Entendre les necessitats de les empreses tecnològiques
- Anàlisi de les diferents tecnologies del mercat
- Valoració econòmica de les diferents tecnologies
- Proposta arquitectònica de la infraestructura de veu i dades

En el projecte no es contemplen les següents solucions:

- Servidors de les empreses ubicats a sales que no siguin de les pròpies empreses
- CPD's dedicats a les empreses. Els CPD's o les sales de racks són d'ús exclusiu del Personal TIC del TECNOCAT
- DMZ's de les empreses
- Servei de Hosting
- Servei de DNS
- Servei WIFI per les empreses. Les empreses es podran posar la seva wifi pròpia a les seves instal·lacions mitjançant AP's.

Per tant, els requeriments del projecte del TECNOCAT són requeriments funcionals.

1.3 Enfocament i mètode seguit

Aquest projecte s'ha realitzat mitjançant un estudi inicial sobre la situació actual del TECNOCAT. Al no existir cap infraestructura física de telecomunicacions, el punt de partida ha estat la creació d'aquesta des de zero. Per dur a terme les diferents solucions, s'ha hagut d'entendre el funcionament del TECNOCAT i la seva projecció futura.

Un cop enteses les necessitats de l'empresa, es proposen les solucions que es creuen més adients per dotar el TECNOCAT d'una xarxa de comunicacions potent i fiable.

A l'annex s'ha adjuntat tota aquella informació que és necessària per el treball però no conforma el nucli del mateix.

1.4 Planificació del Treball

Per tal de dur a terme aquest projecte, han estat necessaris els coneixements d'assignatures cursades durant el grau, com ara Administració i gestió d'organitzacions i disseny de xarxes de computadors, entre d'altres.

Les tasques realitzades, segons la setmana, seran les següents:

<u>13 - 19 de març</u>

Es recopilarà tota la informació necessària per poder començar a desenvolupar el projecte del TECNOCAT. Caldrà saber quants edificis conformen el centre, creixement previst, tipus d'empreses que hi treballen, zones de treball i oci, tipus de material, definició de sales tècniques, tipus de cablejat, ...

20 - 26 de març

Es començarà a recopilar informació sobre les tecnologies de nivell 2 i nivell 3 que podrien ser una solució per el TECNOCAT.

27 de març - 2 d'abril

Es compararan les diferents tecnologies i equips de nivell 2. Finalment es seleccionarà una tecnologia amb el seu equip corresponent.

3 – 9 d'abril

Es compararan les diferents tecnologies i equips de nivell 3. Finalment es seleccionarà una tecnologia amb el seu equip corresponent.

10 – 14 d'abril

Es crearà una topologia de xarxa, connectant els diferents equips entre els diferents edificis, connexió de camins i equips redundants, tipus de velocitats de transmissió de dades, ...
Entrega de la PAC 2

15 – 23 d'abril

Es recopilarà tota la informació referent als tipus de telefonia i centraletes existents al mercat.

24 – 30 d'abril

Es donarà una solució d'infraestructura de veu, tant física com lògica. També s'orientarà del tipus de terminals a utilitzar.

1 – 7 Maig

Es definiran els tipus de protocols de dades, així com la qualitat de servei en les trucades.

8 – 14 Maig

Es definirà una solució en la configuració de les boques d'accés segons el dispositiu que es connecti.

15 – 19 Maig

Definició dels adreçaments de veu i dades

Entrega de la PAC 3

20 de maig – 7 de Juny

Finalització de la memòria i preparació de la presentació

	ACTIVITAT	INICI	FINAL	13 a 19/03	20 a 26/03	27/03 a 2/04	3 a 9/04	10 a 14/04	15 a 23/04	24 a 30/04	1 a 7/05	8 a 14/05	15 a 19/05	20/05 a 07/06
PAC 2	Recopilació d'informació: tipus edificis, sales reunions, usuaris totals, auditoris, tipus infraestructura física de LAN, ...	13 - març	19 - març											
	Selecció de material: electrònica de xarxa LAN equip de seguretat	20 - març	26 - març											
	comparativa equips de nivell 2 solució d'equip de nivell 2	27 - març	2 - abril											
	Comparativa equips de nivell 3 solució equip de nivell 3	3 - abril	9 - abril											
	Connexió equips de nivell 2 i 3	10 - abril	14 - abril											
PAC 3	Recopilació informació: tipus de centraletes electrònica de veu	15 - abril	23 -abril											
	Solució infraestructura de veu Tipus de terminals	24 - abril	30 - abril											
	Protocols de veu i dades	1 - maig	7 - maig											
	configuració de boques d'accès segons host	8 - maig	14 - maig											
	Tipus d'adreçaments LAN	15 - maig	19 - maig											
Entrega final	acabar la memòria Preparació de la presentació	20 - maig	7 - juny											

1.5 Breu sumari de productes obtinguts

El resultat obtingut ha estat una memòria tècnica "claus en mà" de com començar i acabar un projecte per a la implementació d'una xarxa LAN des de zero. Aquest projecte consta de 3 grans blocs:

- Anàlisi i solució de la infraestructura física que conformarà el TECNOCAT
- Anàlisi i solució de l'equipament de veu i dades
- Configuració lògica de la xarxa de veu i dades

1.6 Breu descripció dels altres capítols de la memòria

Com hem comentat al punt anterior, aquest projecte està basat en 3 grans blocs:

- Anàlisi i solució de la infraestructura física: un cop recopilada la informació actual del funcionament del TECNOCAT, es realitza un pla per dotar el TECNOCAT de cablejat vertical i horitzontal. Sense cablejat no es pot definir una infraestructura de telecomunicacions. També s'analitza la redundància entre els 3 edificis i la topologia de xarxa adient. Aquest bloc està conformat per els capítols 4, 5 i 6.
- Anàlisi i solució de l'equipament de veu i dades: S'analitzen acuradament els commutadors i els equips de nivell 2 i 3 actuals i es realitza una comparativa entre ells. També s'analitzen les futures solucions de veu actuals. Finalment s'escullen les solucions més idònies per donar servei al TECNOCAT. Aquest bloc el conformen els capítols 7, 8 i 10.
- Configuració lògica de la xarxa de veu i dades: S'analitzen els protocols importants de comunicació i seguretat tant de veu com de dades, es proposa un tipus d'adreçament i es dona una solució de configuració per les boques d'accés, diferenciant el tipus de host final que s'hi connecti. Podem trobar aquesta informació als capítols 9 i 10.

2. Introducció del projecte

2.1 Objecte

l'Objecte del present document es la realització d'una memòria tècnica de les opcions tecnològiques existents en el mercat actual per dotar al TECNOCAT d'una infraestructura de telecomunicacions pròpia.

2.2 Abast

L'abast d'aquest document inclou els següents elements:

- Selecció de l'equipament de dades, veu i seguretat
- Implementació de la infraestructura cablejada
- Configuració de les boques dels equips d'accés
- Disseny de la xarxa física i lògica de veu i dades
- *Best practices* per a la configuració dels equips
- Definició de polítiques de seguretat
- Definició de protocols importants de comunicacions

2.3 Destinataris

El present document ha estat elaborat per a ús del personal tècnic i de manteniment. Per al seu seguiment es requereix tenir coneixements mitjans de xarxes, així com estar familiaritzat amb l'entorn de xarxes d'àrea local i els equips de commutació associats.

3. Dades generals

- Direcció de l'empresa: Avinguda Berenguer IV, 08001 Barcelona
- Persona de contacte:
  Nom: Miquel Mas i Segarra
  Càrrec: Director tècnic
  Telèfon: 685 34 56 12
  E-mail: miquel.mas@tecnocat.cat

4. Situació Inicial

4.1 distribució física de les instal·lacions

El TECNOCAT disposa d'unes instal·lacions físiques ubicades al 22@ de Barcelona. El complex està format per 3 edificis adjacents, els quals s'hi desenvolupen diferents activitats relacionades amb les noves tecnologies. Els tres edificis són:

- Edifici Catalunya: destinat a oficines
- Edifici Ictineu: destinat a tallers i manipulació de materials
- Edifici CatLab: destinat a laboratoris

4.1.1 Edifici Catalunya

L'edifici Catalunya és l'edifici més gran dels 3 que conformen el TECNOCAT. Està format per 3 plantes de 31 oficines cadascuna, sumant un total de 93 oficines. Hi ha 26 oficines que són de 35 metres quadrats i 5 oficines que són de 70 metres quadrats, les quals estan destinades a empreses amb un número de treballadors més elevat. També hi ha destinades 3 sales tècniques on hi hauran d'anar els equips de l'electrònica de xarxa. A més, consta d'un auditori amb capacitat per unes 112 persones, un bar restaurant i la recepció principal del complex. L'edifici té un total d'uns 4200 metres quadrats, sumant totes les estàncies.

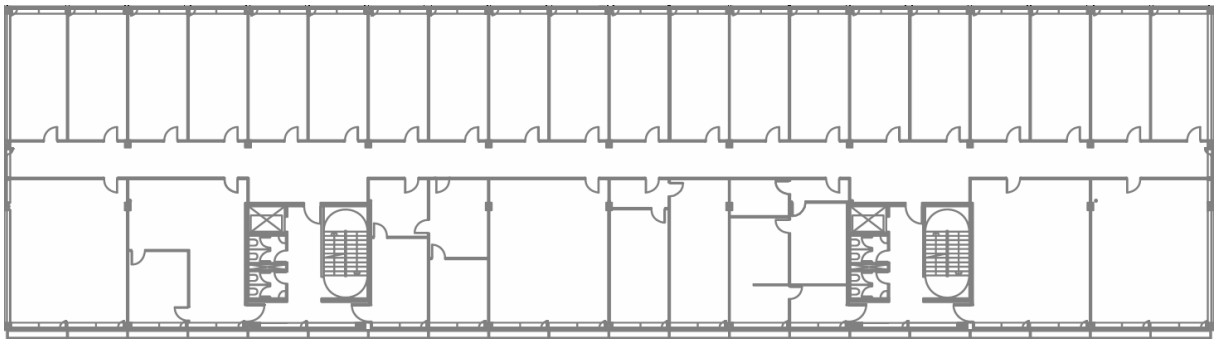

figura 4-1 Edifici Catalunya planta 0

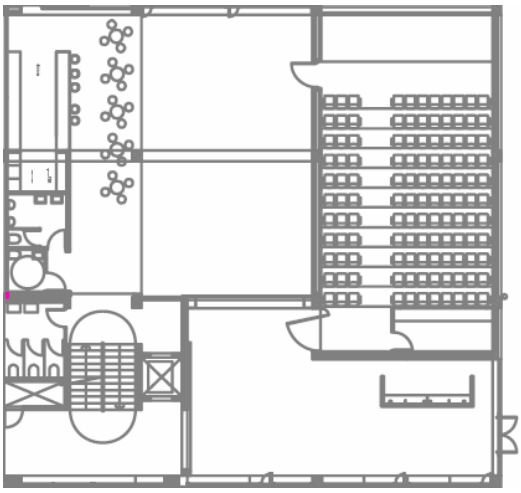

figura 4-2 Edifici Catalunya planta 0

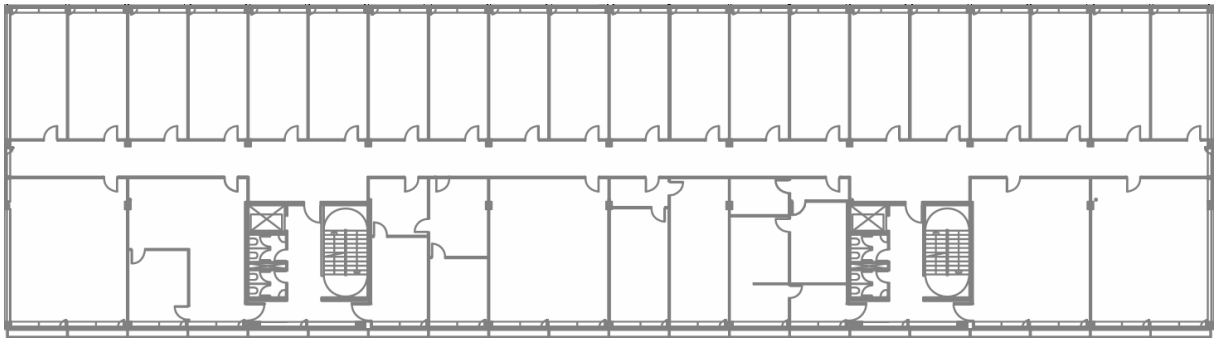

figura 4-3 Edifici Catalunya planta 1

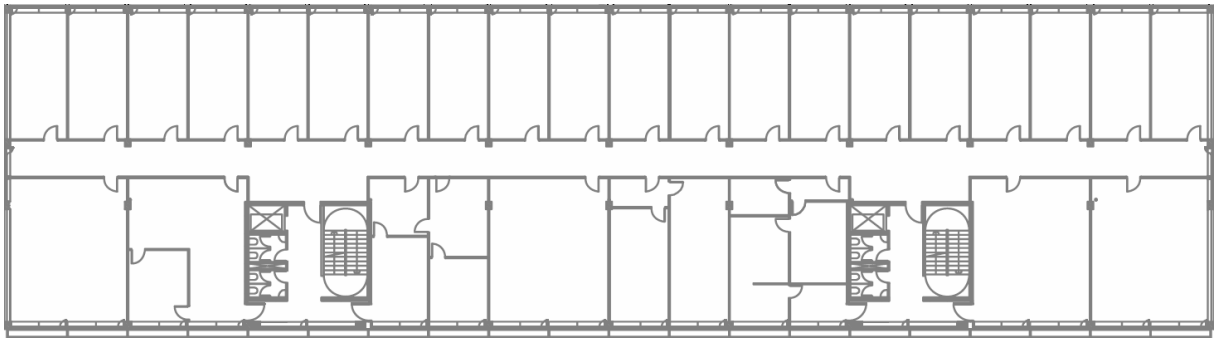

figura 4-4 Edifici Catalunya planta 2

4.1.2 Edifici Ictineu

L'edifici Ictineu és el segon edifici més gran del TECNOCAT i disposa de tallers ens els quals es poden manipular o fabricar materials. Consta d'una planta baixa amb tallers i una primera amb altells. Hi ha tallers de 35, 70 i 95 metres quadrats i altells de 15, 35 i 50 metres quadrats respectivament. També hi podem trobar 4 sales de reunions. L'edifici té un total d'uns 2000 metres quadrats. En aquest edifici és on hi ha destinat el CPD (Central Process Data) del TECNOCAT i la sortida cap a la WAN dels 3 edificis. S'ha escollit aquest edifici per dues raons, és l'edifici que queda al mig dels 3 i a més té la sala més apropiada per instaurar un centre de processament.

figura 4-5 Edifici Ictineu planta 0-1

4.1.3 Edifici CatLab

L'edifici CatLab és l'edifici més petit del TECNOCAT i allotja empreses que necessiten laboratoris per desenvolupar les seves activitats. A la planta 0 hi ha 13 laboratoris de 45 metres quadrats. A la planta 1 hi ha 11 laboratoris de mides compreses entre els 45, 90 i 135 metres quadrats. A més també es pot trobar un bar restaurant i varies zones comuns d'incubació. L'edifici té un total de 1750 metres quadrats. Consta d'una sala tècnica prevista per allotjar els equips de l'electrònica de xarxa.

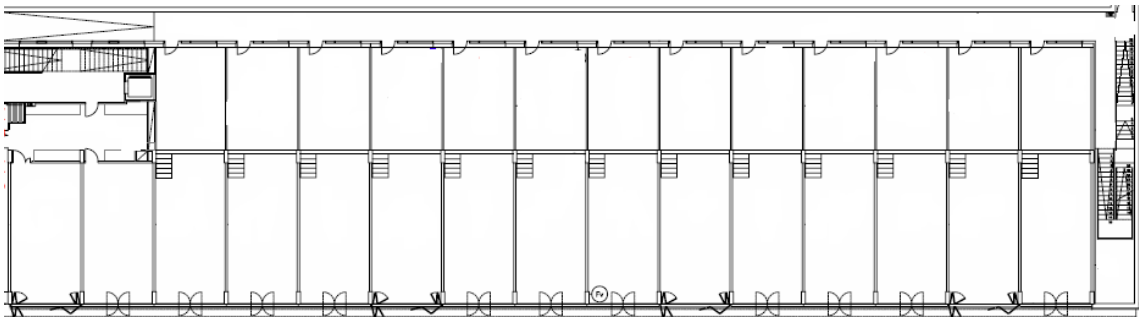

figura 4-6 Edifici LabCat planta 0

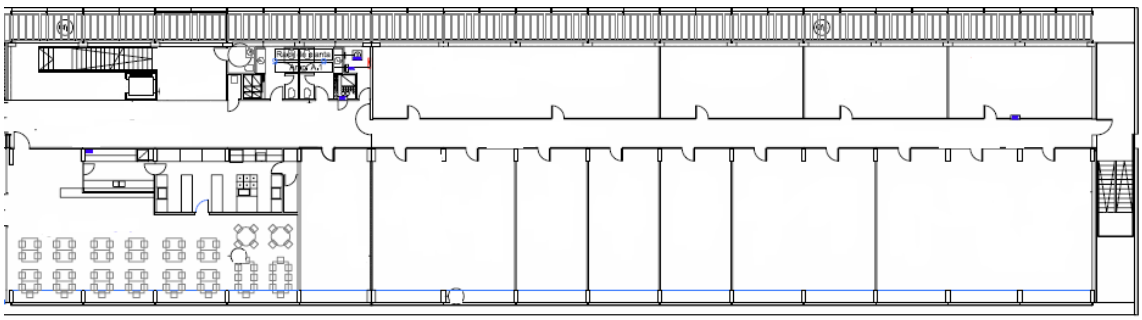

figura 4-7 Edifici LabCat planta 1

4.2 Entrada empreses

Quan una empresa entra a treballar per primera vegada al TECNOCAT es troba amb alguns obstacles i algunes mancances que cal resoldre.

4.2.1 Problemes

Els principals problemes que es troben les empreses per entrar al TECNOCAT són:

- Lentitud alhora de contractar un servei de veu i dades
- Manca de solucions a problemes tècnics
- Inversions inicials per adequar els espais
- Inversions posteriors en cas de creixement
- Manca de solucions a necessitats tècniques
- Falta de visibilitat davant de reptes tecnològics

4.2.2 Propostes d'implantació

A grans trets, es proposen una sèrie de propostes per dotar al TECNOCAT d'una infraestructura de telecomunicacions pròpia, fet que evitarà els problemes inicials que es troben les empreses.
Per poder disposar d'aquest servei, s'hauran de fer les següents actuacions

- Instal·lació de cablejat estructurat horitzontal i vertical
- Adequació sales tècniques i CPD
- Contractació ISP veu i dades
- Adquisició de l'equipament necessari per donar servei de veu, dades i seguretat
- Contractació d'un equip IT (intern o extern) per el manteniment preventiu i correctiu de la xarxa de veu i dades

5. Infraestructura dels edificis

5.1 Infraestructura física de la xarxa

Per adaptar la instal·lació de cablejat als requeriments físics d'equipament de veu i dades, es recomana utilitzar cablejat estructurat. Aquesta normativa regula la problemàtica de fer arribar el cablejat necessari a cadascun dels llocs de treball.

Dins de la normativa de cablejat estructurat, s'utilitza d'una banda el cablejat vertical per comunicar cadascuna de les plantes de l'edifici principal, i el cablejat horitzontal que determina les connexions entre l'electrònica de xarxa de la mateixa planta.

Per traçar les línies del cablejat vertical i comunicar les plantes entre si, s'ha d'optar per realitzar canalitzacions interiors a través de les zones comunes de l'edifici.

Per traçar les línies de cablejat horitzontal per cadascuna de les plantes es recomana fer-ho passar per el fals sostre. El cablejat haurà d'anar subjecte dins d'unes safates metàl·liques.

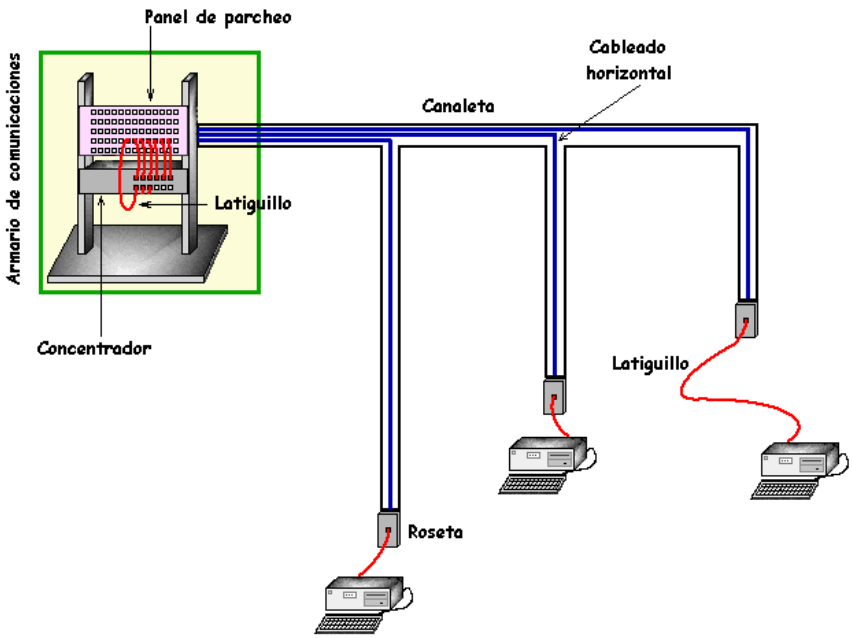

figura 5-1 Cablejat estructurat horitzontal

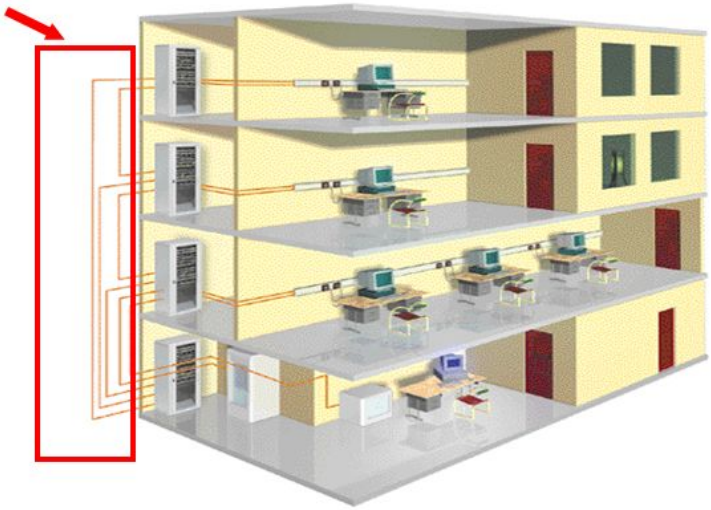

figura 5-2 Cablejat estructurat vertical

5.2 Infraestructura física dels edificis

Com hem comentat anteriorment, es distingeixen 2 tipus de cablejat estructurat, el cablejat horitzontal i el cablejat vertical:

- Cablejat horitzontal: Aquest cablejat connecta cadascun dels hosts amb la seva sala tècnica. Connecta cadascuna de les rosetes dels llocs de treball fins al seu *patch panel*, el qual està dins d'un *rack* de comunicacions on també hi ha l'electrònica de xarxa.

figura 5-3 punt de xarxa o roseta

figura 5-4 Patch panel

figura 5-6 Armari rack de 48U

- Cablejat vertical: és el que connecta les sales tècniques de l'edifici

5.3 Tipus de cablejat horitzontal

Els equips electrònics emeten senyals electromagnètics. Quan hi ha molts cables a prop uns d'uns altres, aquests poden interferir entre si. Aquesta interferència es coneix com "diafonia". La diafonia augmenta els errors i els paquets perduts (entre altres temes). Les versions més recents de cables redueixen l'impacte de la diafonia a través d'una varietat de mètodes, incloent blindatge millorat i disseny de cable retorçat.

5.3.1 Similituds entre els cables Cat5 i Cat6

Cal dir que tant els cables Cat5 com Cat6 utilitzen la mateixa peça final, és a dir, es poden "connectar" als mateixos ports. Les diferències entre cadascun d'aquests cables estan en les seves capacitats, així com els mètodes i materials utilitzats per crear-los. El que tots els cables tenen en comú es coneix com RJ-45, i és capaç de connectar qualsevol connector Ethernet en un ordinador, encaminador o un altre dispositiu similar. Ningú en la indústria espera que això canviï ràpid.

5.3.2 Cable Cat5

El cable Cat5 es divideix en dues categories diferents: Cat5 i Cat5I. Cat5 s'ha tornat obsolet en els últims anys a causa de les seves limitacions en comparació dels cables Cat5I i Cat6. Encara que el cable Cat5 pot manejar fins a 10/100 Mbps a un ample de banda de 100MHz (que abans es considerava bastant eficient), les noves versions de cables Cat són significativament més ràpides.

El cable Cat5I es va convertir en el cable estàndard fa uns 15 anys i ofereix un rendiment significativament millor que l'antic cable Cat5, incloent velocitats fins a 10 vegades més ràpides i una major capacitat per recórrer distàncies sense ser afectat per diafonia .

5.3.3 Cables Cat6 i Cat6A

Els cables Cat6 s'han utilitzat principalment com l'espina dorsal a les xarxes, en comptes de connectar les estacions de treball en sí mateixes. La raó d'això (més enllà del cost) és el fet que, mentre que els cables Cat6 poden manejar fins a 10 Gigabits de dades, aquest ample de banda es limita a 49,987 metres. Si es sobrepassa aquesta distància la velocitat baixarà a només 1 Gigabit (el mateix que Cat5I).

Cat6A és l'última iteració i utilitza una carcassa de plàstic excepcionalment gruixuda que ajuda a reduir encara més la diafonia. La major diferència entre els cables Cat6 i Cat6A és que Cat6A pot mantenir velocitats de 10 Gigabits pels 99,974 metres de cable Ethernet.

En el cas del TECNOCAT, optaríem per posar Cat6 a tot el recinte ja que les sales tècniques estan suficientment a prop dels llocs de treball i en cap cas es superarien els 100 metres de distància en els 3 edificis. A més, entenem que un ample de banda màxim de 10 Gb és més que suficient en els propers anys.

5.4 Tipus de cablejat vertical

Hi ha dos tipus de cables que s'utilitzen en el cablejat vertical, els cables monomode i els cables multimode. Tots dos tenen un conducte al centre anomenat nucli a través el qual la llum viatja en línia recta o rebotant en les parets del revestiment, un material òptic que fa rebotar la llum.

5.4.1 Cable de connexió monomode:

Té la peculiaritat que dins del seu nucli, la data viatja sense rebotar en les seves parets el que permet mantenir velocitats de transferència més altes. Les dades es transfereixen traçant una línia, per això no molts feixos de llum poden viatjar al mateix temps a través de les petites proporcions del seu conducte.

Les velocitats de transmissió de dades van de 1Gb a 10Gb i la distància de 5 a 10 quilòmetres. Per tant, per connectar instal·lacions separades (edificis, oficines, ...) s'utilitza la fibra monomode.

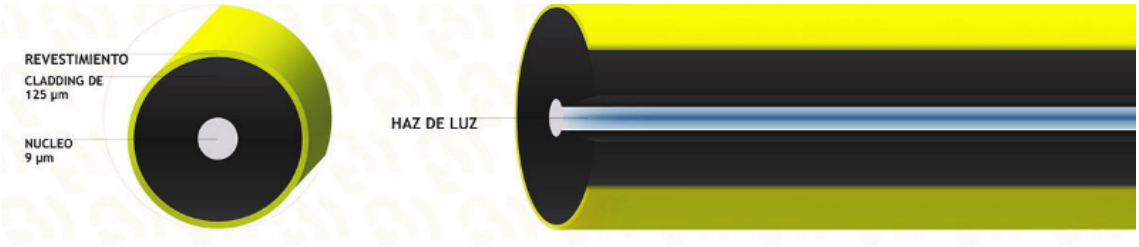

figura 5-7 exemple de fibra monomode

5.4.2 Cable de connexió multimode:

Aquesta és la fibra "domèstica" i en contrast amb la fibra monomode, permet que els feixos de llum rebotin en les parets del revestiment. Això provoca una major quantitat de feixos de llum viatjant al mateix temps a través del nucli. En comparació de la fibra monomode, el nucli de la multimode mesura des de 50 a 62.5 micròmetres, concedint més espai perquè la informació viatgi.

La fibra multimode pot arribar a velocitats Ethernet de fins a 100Gb, en canvi hi ha la limitació de la distància que en el cas que ens ocupa oscil·laria entre els 550 metres com a màxim.

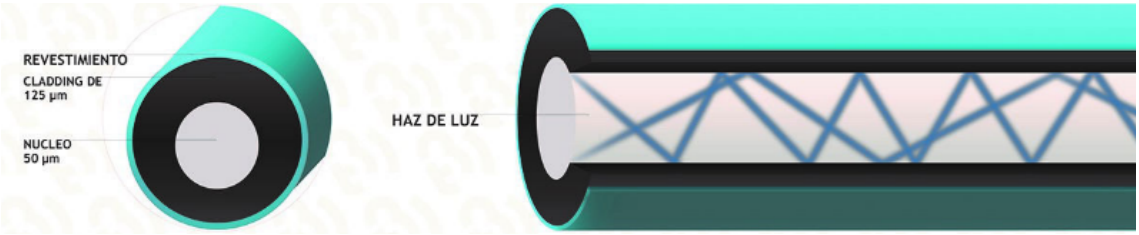

figura 5-8 exemple de fibra multimode

A continuació podem observar un exemple de connectivitat vertical que uniria els 3 edificis:

- Connexió entre equips del mateix edifici: fibra multimode
- Connexió entre els 3 edificis: fibra monomode

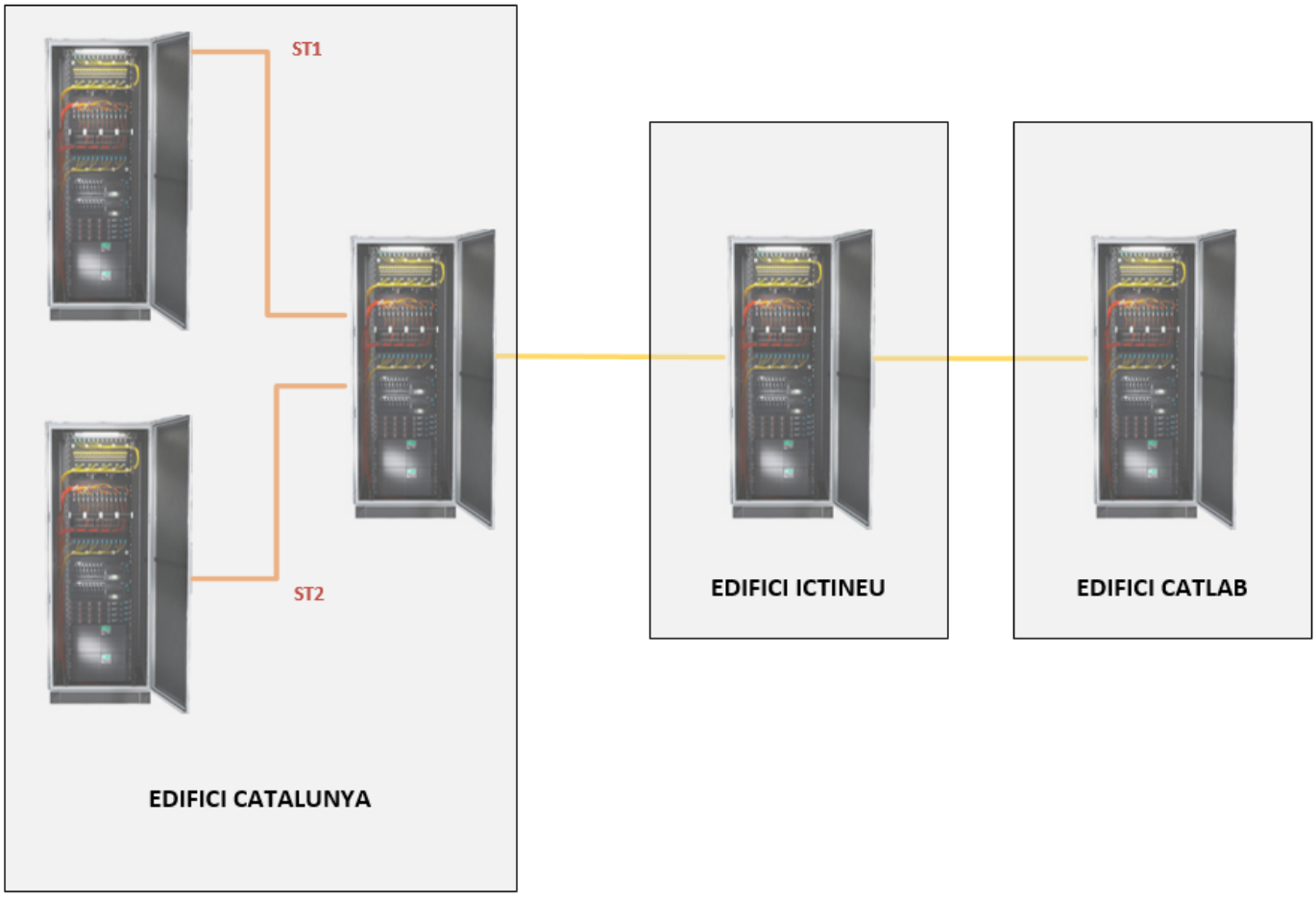

figura 5-9 connexió entre edificis

6. Topologia de xarxa

6.1 Disposició física de la xarxa

Existeixen diferents topologies o disposicions físiques de xarxa, però en el cas del TECNOCAT ens basarem en les 2 que més s'ajusten a les seves característiques estructurals.

6.1.1 Topologia en estrella

Una xarxa en estrella és una xarxa en la qual les estacions estan connectades directament a un punt central i totes les comunicacions s'han de fer mitjançant aquest.

Donat la seva transmissió, una xarxa en estrella té un node central actiu que normalment té els mitjans per prevenir problemes relacionats amb el ressò.

S'utilitza sobretot per a xarxes locals. La majoria de les xarxes d'àrea local que tenen un encaminador (router), un commutador (switch) o un concentrador (hub) segueixen aquesta topologia. El node central en aquestes seria el encaminador, el commutador o el concentrador, pel qual passen tots els paquets.

Avantatges:

- Té dos mitjans per prevenir problemes.
- Permet que tots els nodes es comuniquin entre si de manera convenient.
- Es poden aprofitar tots els enllaços sense crear bucles *etherchannel*

Desavantatges

- Si el node central falla, tota la xarxa es desconnecta.
- És costosa, ja que requereix més cable que la topologia Bus i anella

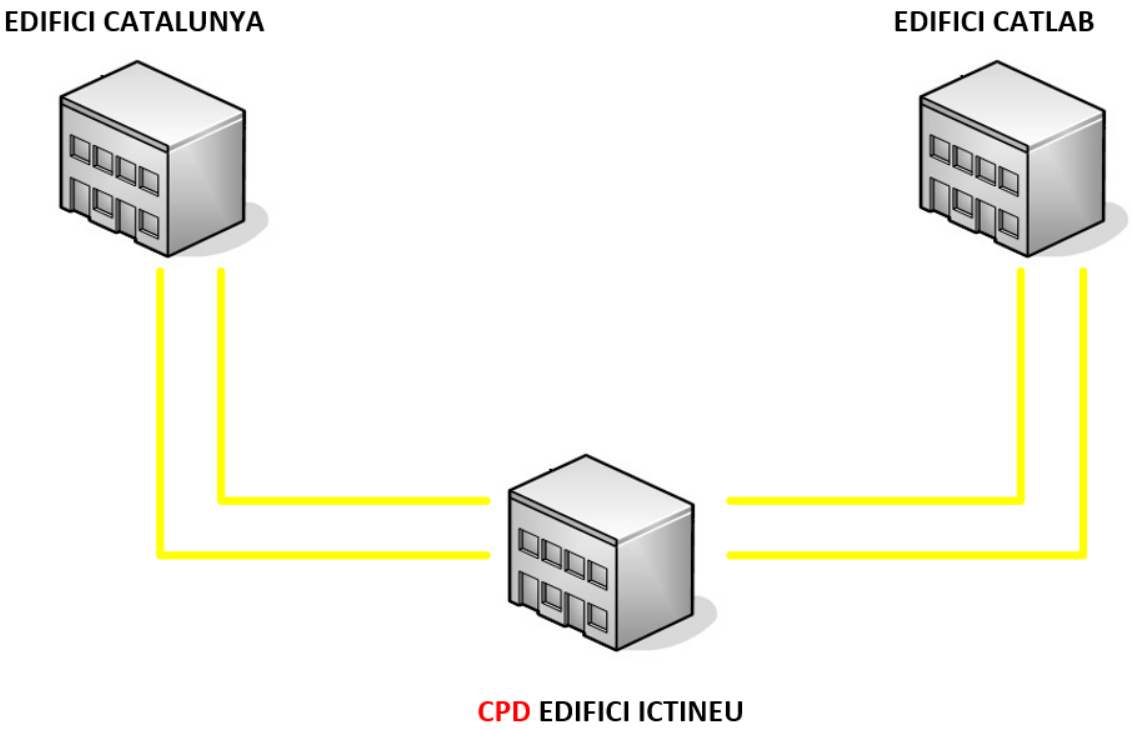

figura 6-1 topologia en estrella

6.1.2 Topologia en anella

Cada equip està connectada a la següent i l'última està connectada a la primera. Si cau un enllaç la informació es deriva cap a l'altre costat. Si afegim un segon enllaç entre edificis (veure figura 6-2) podríem estar parlant d'una topologia en anell redundada o de malla.

Avantatges:

- Simplicitat d'arquitectura. Facilitat de creixement.

Desavantatges:

- Un dels enllaços quedarà blocat per *STP* i la informació passarà únicament per l'enllaç actiu.

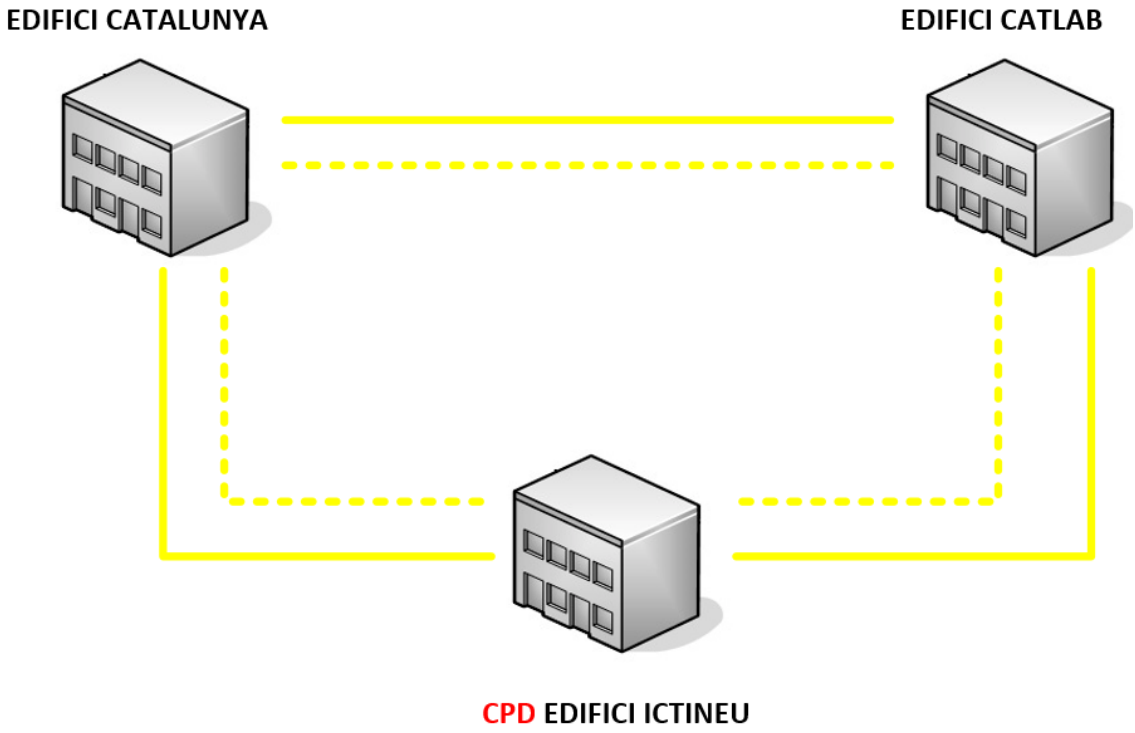

figura 6-2 topologia en anell/topologia en anell redundat/topologia en malla

Finalment, la disposició de xarxa que veiem més adient i que creiem que s'hauria d'implantar a la futura xarxa del TECNOCAT és la topologia en estrella. Els motius són els següents:

- Redundància total de xarxa
- És més econòmica que la opció en anell redundat i que en malla
- Aprofitament dels enllaços cap al node central mitjançant(Etherchannel)
- Facilitat de gestió
- És la més utilitzada per els principals fabricants de commutadors

6.2 Topologia jeràrquica de xarxa

La jerarquia té molts beneficis en el disseny de les xarxes i ens ajuda a fer-les més predictibles. En si, definim funcions dins de cada capa, ja que les xarxes grans poden ser extremadament complexes i incloure múltiples protocols i tecnologies; així, el model ens ajuda a tenir un model fàcilment comprensible d'una xarxa i per tant a decidir una manera apropiada quina configuració aplicar.

Aquest model està proposat per Cisco Systems i distingeix 3 capes lògiques dins d'un model jeràrquic:

6.2.1 Access Layer (Capa d'accés):

La capa d'accés de la xarxa és el punt en el qual cada usuari es connecta a la xarxa. Aquesta és la raó per la qual la capa d'accés s'anomena a vegades capa de lloc de treball, capa d'escriptori o d'usuari. Els usuaris així com els recursos als quals aquests necessiten accedir amb més freqüència, estan disponibles a nivell local. El tràfic ambdues direccions de recursos locals està confinat entre els recursos, *switchs* i usuaris finals. En la capa d'accés podem trobar múltiples grups d'usuaris amb els seus corresponents recursos. En moltes xarxes no és possible proporcionar als usuaris un accés local a tots els serveis, com a arxius de bases de dades, emmagatzematge centralitzat o accés telefònic al Web. En aquests casos, el tràfic d'usuaris que demanden aquests serveis es desvia a la següent capa del model: la capa de distribució.

6.2.2 Distribution Layer (Capa de distribució):

La capa de distribució marca el punt mig entre la capa d'accés i els serveis principals de la xarxa. La funció primordial d'aquesta capa és realitzar funcions com ara encaminament, filtrat i accés a WAN.

En un entorn com en el que ens trobem, la capa de distribució abasta una gran diversitat de funcions, entre les quals figuren les següents:

- Servir com a punt de concentració per accedir als dispositius de capa d'accés.
- Encaminar el trànsit per a proporcionar accés als departaments o grups de treball.
- Segmentar la xarxa en múltiples dominis de difusió / multidifusió.
- Proporcionar serveis de seguretat i filtrat.

La capa de distribució pot resumir-se com la capa que proporciona una connectivitat basada en una determinada política, atès que determina quan i com els paquets poden accedir als serveis principals de la xarxa. La capa de distribució determina la forma més ràpida perquè la petició d'un usuari (com un accés al servidor d'arxius) pugui ser remesa al servidor. Una vegada que la capa de distribució ha triat la ruta, envia la petició a la capa de nucli. La capa de nucli podrà llavors transportar la petició al servei apropiat.

6.2.3 Core Layer (Capa de nucli):

La capa de Core o nucli s'encarrega de desviar el trànsit el més ràpidament possible cap als serveis apropiats. Normalment, el tràfic transportat es dirigeix o prové de serveis comuns a tots els usuaris. Aquests serveis es coneixen com a serveis globals o corporatius. Alguns d'aquests serveis poden ser correu electrònic, l'accés a Internet o la videoconferència. Quan un usuari necessita accedir a un servei corporatiu, la petició es processa al nivell de la capa de distribució. El dispositiu de la capa de distribució envia la petició de l'usuari al nucli. Aquest es limita a proporcionar un transport ràpid fins al servei corporatiu sol·licitat. El dispositiu de la capa de distribució s'encarrega de proporcionar un accés controlat a la capa de nucli.

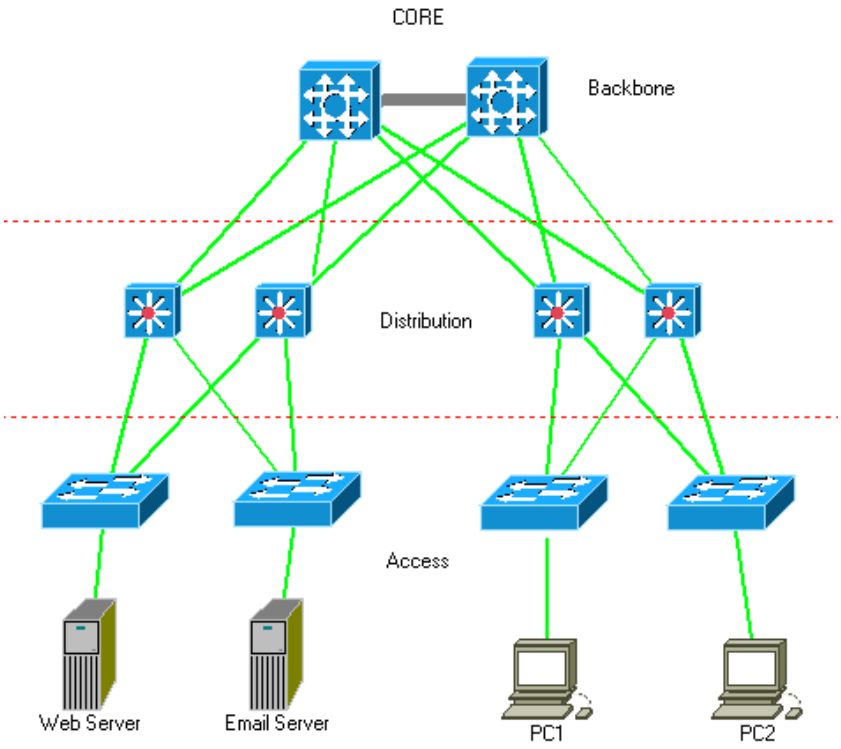

figura 6-3 exemple de model jeràrquic de xarxa segons Cisco

Un cop definit el model jeràrquic que s'hauria d'implantar per connectar les diferents sales tècniques que conformen el TECNOCAT, es conformen els tipus de commutadors que aniran a cada edifici:

Edifici Catalunya

capa d'accés: segons volum d'usuaris
capa de distribució: 2 equips
capa de nucli: cap equip

Edifici Ictineu

capa d'accés: segons volum d'usuaris
capa de distribució: 2 equips
capa de nucli: 2 equips

Edifici CatLab

capa d'accés: segons volum d'usuaris
capa de distribució: 2 equips
capa de nucli: cap equip

A la següent il·lustració es pot observar un exemple de com podria ser la topologia jeràrquica del TECNOCAT, suposant que:

- Segons les instal·lacions dels edificis, les dues sales tècniques i el mateix CPD del TECNOCAT tindran equips d'accés.
- Els equips estaran redundats per, com a mínim, 2 camins.

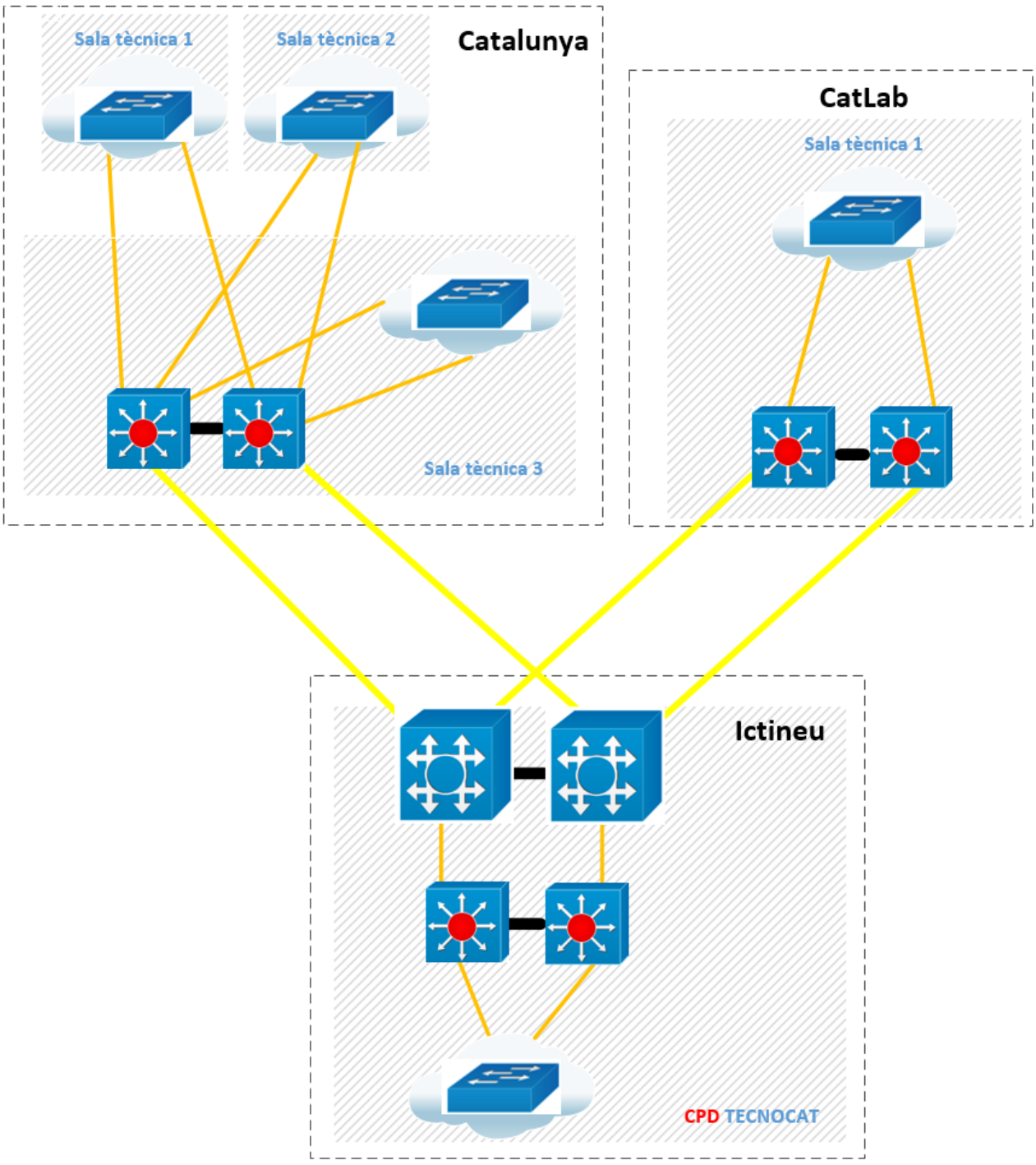

figura 6-4 exemple de model jeràrquic de xarxa del TECNOCAT

7. Equipament de nivell 2

7.1 Principals fabricants

Existeixen diferents tipus de fabricants segons les necessitats de cada client. Per dotar al TECNOCAT amb una infraestructura de xarxa adequada, s'han escollit els fabricants més importants del moment en la fabricació de commutadors de nivell 2:

- Cisco Systems
- HP
- Huawei

Aquests fabricants dominen el mercat mundial de la commutació, com es pot observar en la següent figura:

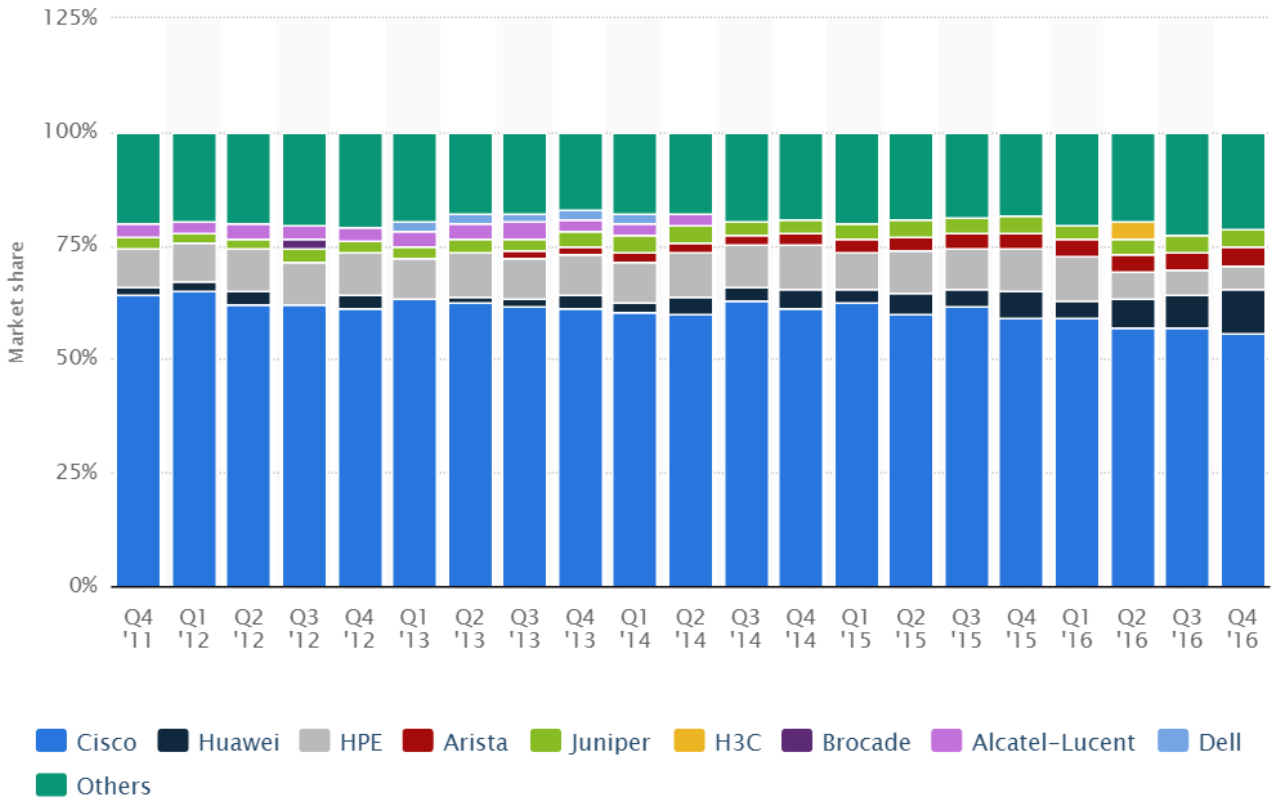

figura 7-1 principals fabricants de commutadors de xarxa

7.1.1 Cisco Systems

Actualment Cisco Systems és l'empresa líder del sector, el qual s'emporta més del 50% dels beneficis mundials en la fabricació d'equipament. Podríem dir que a dia d'avui no té rival. Si ens fixem en la figura 7-1 però, en els últims anys hi ha una lleugera tendència a la baixa, per la forta competència que té.

Fortaleses

- Suport a l'usuari
- Documentació
- Certificacions
- varietat de productes
- estandarditzat en la majoria d'empreses grans
- Qualitat dels productes

Debilitats

- cost elevat dels productes
- protocols de comunicacions propietaris

7.1.2 HP

Hewlett-Packard és una de les 3 companyies més importants en equipament de commutació a nivell mundial. Mitjançant la compra d'empreses del sector, com ara 3com, ha aconseguit entrar de ple en aquest món. No hi ha una previsió a curt termini de que pugui fer-li ombra a Cisco, però poc a poc s'està veient que els productes de *networking* que desenvolupa són de gran qualitat.

Fortaleses

- Proveïdors
- Preu estandarditzat
- Qualitat dels productes
- Documentació

Debilitats

- La gamma alta de productes té un cost elevat
- Dificultat d'administració
- Migració més lenta

7.1.3 Huawei

Huawei és el fabricant que més beneficis ha obtingut en els últims anys. De fet, un dels fets de que Cisco hagi tingut un retrocés en la venta d'equipament és degut a Huawei. El preu dels seus productes fa que tinguin un fort creixement en empreses de països emergents.

Fortaleses

- Preu baix
- Facilitat d'ús
- Gran creixement mundial

Debilitats

- Qualitat del producte poc contrastada
- Poca implantació a Catalunya
- Baix suport a l'usuari
- Pocs proveïdors

7.2 Models de commutadors de xarxa

Segons ens ha comunicat l'administració del TECNOCAT, la ocupació màxima prevista de tots els espais rondaria els 800 - 1000 usuaris. Partint d'aquesta premissa, els equips de commutació que recomanem segons model jeràrquic són els següents:

7.2.1 Commutadors de xarxa en la capa d'accés

Cisco Systems

Es proposa el switch Catalyst 2960x-48 stack. Els commutadors de la sèrie 2960x són de configuració fixa, apilables, commutadors de Gigabit Ethernet que proporcionen accés de classe empresarial per a aplicacions de campus i sucursals. Permeten operacions de negocis escalables, segurs i energèticament eficients amb serveis intel·ligents i una àmplia gamma de tecnologies avançades del programari de la IOS de Cisco.

figura 7-2 Catalyst 2960x-48G

HP

Es proposa el switch HP 3Com 5130-48G. La sèrie HPE 5130 inclou commutadors Gigabit Ethernet que suporten encaminaments STATIC i RIP, serveis diversificats i reenviament IPv6, a més de proporcionar quatre ports Ethernet de 10 Gigabits (10GbE). La tecnologia única de teixit intel·ligent resistent (IRF) crea un teixit virtual administrant diversos switchs com un únic dispositiu lògic, el que augmenta la resistència, el rendiment, la disponibilitat de la xarxa i redueix la complexitat operacional.

Aquests commutadors proporcionen accés Gigabit Ethernet i poden utilitzar-se a la vora d'una xarxa o per connectar clústers de servidors en centres de dades petits. Alta disponibilitat, simplicitat d'administració i polítiques de control de seguretat integrals estan entre les característiques clau que distingeixen aquesta sèrie.

figura 7-3 HP 3Com 5130-48G

Huawei

Es proposa el switch Huawei S1720-52GWR-4X . Switchs d'accés Ethernet d'última generació que estalvien energia per a petites i mitjanes empreses. El disseny avançat del maquinari optimitza la utilització de l'ample de banda i suporta l'expansió senzilla d'un sol commutador d'accés a xarxes d'arbre, estrella o anell a mesura que canvien les necessitats. Disponible en una àmplia gamma de versions no gestionades i gestionades per SNMP o web, que proporcionen de 8 a 48 ports.

Fàcils d'instal·lar i mantenir, els switchs Huawei S1700 combinen alta fiabilitat amb riques funcions d'administració i seguretat per ajudar els clients a crear xarxes segures, fiables i d'alt rendiment.

Figura 7-4 Huawei S1720-52GWR-4X

7.2.2 Commutadors de xarxa en la capa de distribució

Cisco Systems

Es proposa el switch Catalyst 3850-12S. El Cisco Catalyst 3850 Series és la pròxima generació de classe empresarial Ethernet apilable i d'accés i agregació de switchs de capa multigigabit Ethernet que proporcionen una convergència total entre cablejada i sense fils en una sola plataforma. Compta amb Unified Access Data Plane (Uadp) i circuit integrat (ASIC). Gran convergència de dades gràcies a la nova i millorada tecnologia de Cisco StackWise-480.

Els commutadors de la sèrie Cisco Catalyst 3850 suporten els estàndrards IEEE 802.3 en Power over Ethernet Plus (PoE +), alimentació a través d'Ethernet (Cisco UPOE), mòduls de xarxa modulars i reemplaçables al camp, interfícies d'enllaç descendent RJ45 i basats en fibra, i ventiladors redundants. Amb velocitats que arriben als 10 Gbps, els Cisco Catalyst 3850 multigigabit poden suportar velocitats sense fils actuals i de pròxima generació i estàndards (Incloent 802.11ac Wave 2) en la infraestructura de cablejat existent.

Figura 7-5 Catalyst 3850-12S

HP

Es proposa el switch HPE 5700. La sèrie de commutadors HPE FlexFabric 5700 proporciona una porta oberta per a l'expansió de la xarxa empresarial mitjançant l'addició de capacitat amb commutació local i suport L2 / Light L3. Les millores de IRF per a les configuracions spine / leaf, simplifiquen la gestió de la xarxa i amplien la connexió de servidor. Capacitat de recuperació i facilitat de gestió vénen de la mà amb el FlexFabric 5700. Al mateix temps
que IRF redueix les complexitats de gestió fins a un 88%, també ofereix <50 ms de temps de convergència.

Figura 7-6 HPE 5700 40xSFP+ - 2xQSFP+

Huawei

Es proposa el switch Huawei S5720-32x. Tecnologia avançada en un switch Gigabit resistent, per a accés o agregació fiable i fàcil d'administrar en xarxes de campus empresarials. Els ports d'enllaç a 10 Gb permeten capacitats completes de processament de serveis, i la tecnologia iStack intel·ligent proporciona escalabilitat fàcil.
Basats en la propera generació de processadors d'alt rendiment de Huawei i en la Plataforma de Encaminament Versàtil (VRP), els switchs S5720-EI ofereixen mides de taules més grans i capacitats de processament de maquinari més altes que els commutadors similars.

Figura 7-7 Huawei S5720-32X

7.2.3 Commutadors de xarxa en la capa de nucli

Cisco Systems

Es proposa el model Cisco Catalyst C6840-X. És ideal per a aquells que volen introduir serveis de 10G a xarxes troncals de campus petits o mitjans. Aquesta plataforma única ofereix densitat de ports de 10G, funcionalitat IPv4 / IPv6 completa i funcionalitat MPLS / VPLS amb mides de taules grans (fins a 256.000 entrades FIB) i més de 15 anys de les millors característiques de la seva classe. Amb un conjunt complet de L2 / L3, virtualització, seguretat, multidifusió, IPv6, visibilitat d'aplicacions, operacions intel·ligents i serveis de mitjans enriquits, el Cisco Catalyst 6800-X ofereix capacitats sense precedents en el primer dia. Aquesta plataforma també funciona amb la mateixa arquitectura que el Cisco Catalyst 6500 i per tant ofereix estabilitat amb el programari del sistema operatiu provat.

El xassís de la sèrie Cisco Catalyst 6840-X ofereix una elasticitat integrada mitjançant la redundància de la font d'alimentació 1 + 1, una sola safata de ventilador extraïble amb quatre ventiladors redundants i el suport per al sistema de commutació virtual (VSS), la qual limita el temps d'inactivitat de la xarxa i assegura la productivitat, satisfacció del client i rendibilitat.

Figura 7-8 Catalyst C6840-X

HP

Es proposa el Switch HPE Flexfabric 5930. La serie 5930 proporciona funcions avançades i alt rendiment en una arquitectura de commutador de centre de dades per la part superior del bastidor. El 5930, que consta de un commutador d'1U de 32 ports 40 GbE QSFP +, una versió modular de 2 ranures amb 2 ports 40 GbE i una versió modular de 4 ranures, ofereix alta densitat en un espai reduït. El IRF de 9 unitats redueix les complexitats de la gestió en fins a un 88%, alhora que ofereix <50 ms de temps de convergència.

Figura 7-9 HPE Flexfabrix 5930

Huawei

Es proposa el switch model S7703 16p. Aquesta sèrie compta amb múltiples serveis d'enrutament a 10 GE i és escalable per a grans xarxes de campus.

El disseny modular, la gestió unificada d'usuaris i les característiques de seguretat integrals fan que el commutador S7700 sigui ideal per a xarxes petites i grans. El disseny Super Virtual Fabric (SVF 2.0) i el clustering CSS proporcionen escalabilitat i un gran ample de banda per a serveis que tinguin una necessitat més gran.

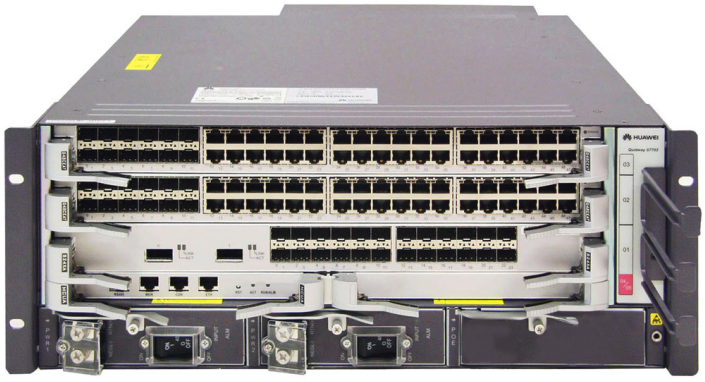

Figura 7-10 Huawei S7703

7.2.4 Preus dels diferents commutadors de xarxa

A continuació es detallen els preus (sense IVA) dels dispositius de xarxa que s'han presentat al punt anterior com a futuribles equips de l'electrònica de xarxa del TECNOCAT:

- **Preu dels dispositius de la capa d'accés:**

Marca	Model	Preu unitari
Cisco Systems	Catalyst 2960x-48G	4.543 €
HP	3Com 5130-48G	3.639 €
Huawey	S1720-52GWR-4X	2.456 €

- **Preu dels dispositius de la capa de distribució:**

Marca	Model	Preu unitari
Cisco Systems	Catalyst 3850 12S	4.105 €
HP	HPE 5700	4.509 €
Huawey	S5720-32x	2.738 €

- **Preu dels dispositius de la capa de nucli**

Marca	Model	Preu unitari
Cisco Systems	Catalyst C6840-X	10.675 €
HP	HPE Flexfabric 5930	13.385 €
Huawey	S7703 16p	11.222 €

7.3 Solució escollida de nivell 2

Donat que el TECNOCAT a de ser un referent tecnològic a la zona, s'han escollit els 3 fabricants més importants del moment. Aquests fabricants tenen un gran volum de negoci a nivell mundial ja que els seus productes són de gran fiabilitat. D'aquests 3 fabricants però, n'hi ha un que destaca sobre la resta, Cisco. El fet que s'emporti més del 50% del mercat mundial no és casual. Per tant, creiem que la infraestructura de xarxa de nivell 2 del TECNOCAT hauria de ser amb els commutadors del fabricant Cisco. Algunes de les raons són:

- Facilitat d'administració
- Gràcies als seus certificats, els administradors de xarxa tenen un coneixement molt ampli de la solució a gestionar
- lideratge internacional
- Importants empreses catalanes treballen amb aquest fabricant
- Qualitat dels seus equips àmpliament contrastada
- Ampli suport tècnic darrera
- Durabilitat dels equips
- Molts administradors de xarxa coneixen el seu funcionament
- Gran ventall de partners i proveïdors a Catalunya
- Fiabilitat
- Escalabilitat
- Àmplia comunitat a internet darrera
- Manteniment durador
- Relació qualitat – preu
- Extensa gamma de productes

Per les capes d'accés i de distribució s'ha optat per els commutadors estàndard del fabricant, és a dir, equips potents i fiables amb un rendiment contrastat entre el tractament de paquets i d'ample de banda. A més, són una evolució de les seves respectives famílies (2960 f/e i 3750) respectivament.

En el cas de l'equip Core, hem optat per proposar una arquitectura pensada plenament per campus i que és una evolució de la família 6500 però amb unes dimensions i preu molt inferiors. Aquest equip porta una supervisora molt potent (Supervisora 2T) que té una capacitat de 960 Gbps i una capacitat de *switching* de 80 Gbps. Però el que realment veiem diferencial i important en un equipament tant bàsic són paràmetres com la memòria, CPU i *buffer* per evitar pèrdua de paquets i garantir la latència.

Finalment comentar que les solucions de *switching* de Cisco ofereixen una experiència de xarxa d'alta qualitat als usuaris connectats, això augmenta la productivitat i satisfacció dels usuaris. També brinden un màxim temps d'activitat, alta capacitat de processament d'implementació ràpida, un millor accés i operacions automatitzades.

7.4 Connexions entre els diferents equips

A continuació es veuen les diferents connexions que hi es podrien dur a terme per inter-connectar els diferents equips de xarxa:

Equips d'accés Catalyst 2960x:

connexió entre ells: mode *stack-wise.*
connexió cap a la capa de distribució: 2 *etherchannels* de 1 Gb cadascun de fibres multimode, sumant un ample de banda cap a la capa de distribució de 2Gb.

Equips de distribució Catalyst 3850:

connexió entre ells: mode *stack-wise.*
connexió cap a la capa de nucli: 2 *etherchannels* de 10 Gb cadascun mitjançant fibres monomode (excepte en el cas de l'edifici Ictineu), sumant un ample de banda cap a la capa de distribució de 20Gb.

Equips CORE Catalyst 6800:

connexió entre ells: VSS.

7.5 Esquema de nivell 2 amb electrònica de xarxa Cisco:

En la següent il·lustració podem observar la solució Cisco de nivell 2 proposada al TECNOCAT:

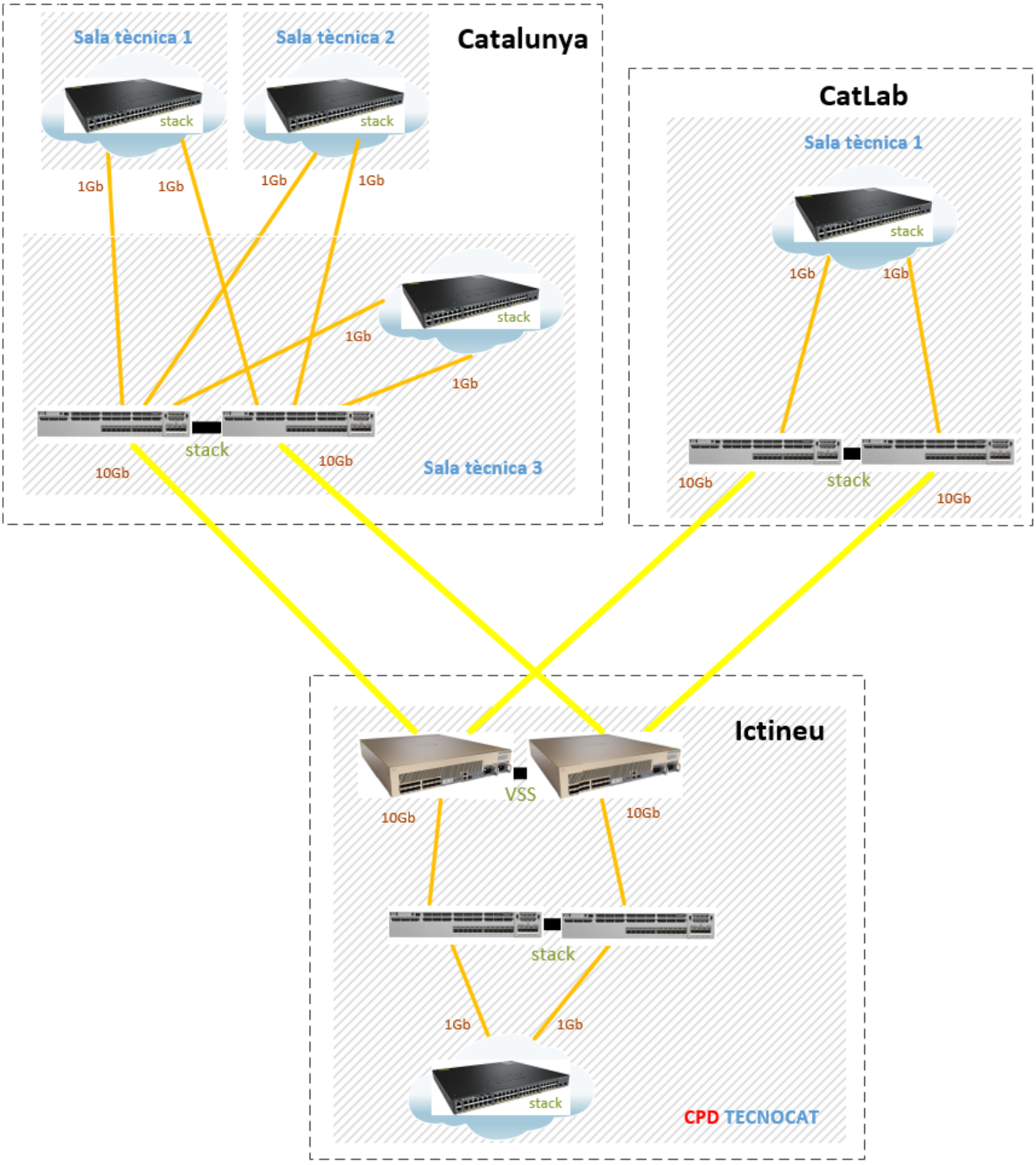

Figura 7-11 Solució Cisco de nivell 2

8. Equipament de seguretat (nivell 3)

8.1 Tipus de firewalls

Per poder determinar quin equip de seguretat és el més adequat per donar servei a les empreses del TECNOCAT, haurem de diferenciar entre 2 maneres diferents de funcionament dels firewalls:

8.1.1 Firewalls Tradicionals

Un firewall tradicional inclou un dispositiu que és capaç de controlar el trànsit d'entrada o sortida.

Molts tallafocs tradicionals es limiten a usar només les capes 2 a 4 del model OSI i només poden realitzar un seguiment del trànsit basant-se en aquesta informació.

Altres característiques comunes d'un tallafocs tradicional inclouen suport per a traducció d'adreces de xarxa (NAT), traducció d'adreces de ports (PAT) i acabament de xarxes privades virtuals (VPN), a més de poder oferir un alt nivell de disponibilitat i rendiment.

8.1.2 Next Generation Firewalls (NGF)

Els tallafocs de pròxima generació integren tres actius clau: capacitats de tallafocs empresarials, un sistema de prevenció d'intrusions (IPS) i control d'aplicacions. Els *NGFW*s aporten context addicional al procés de presa de decisions del tallafocs proporcionant-li la capacitat de comprendre els detalls del trànsit d'aplicacions web que passa a través d'ell i prendre mesures per bloquejar el trànsit que pugui explotar vulnerabilitats.

Els tallafocs de pròxima generació combinen les capacitats dels tallafocs tradicionals, inclosos el filtrat de paquets, la traducció d'adreces de xarxa (NAT), el bloqueig d'URL i les xarxes privades virtuals (VPN), amb funcionalitat i característiques de qualitat de servei (QoS) que tradicionalment no es troben en productes tallafocs. Aquests inclouen la prevenció d'intrusions, la inspecció SSL i SSH, la inspecció profunda de paquets i la detecció de malware, així com el coneixement de les aplicacions. Les capacitats específiques de l'aplicació estan dissenyades per impedir el creixent nombre d'atacs d'aplicació que tenen lloc en les capes 4-7 del model OSI.

Donades les característiques del TECNOCAT, creiem que l'equip de seguretat a implantar hauria de ser un firewall tipus NGF. Els tallafocs de pròxima generació s'han desenvolupat per necessitat en els entorns informàtics actuals, on els atacs de malware han crescut en sofisticació i intensitat i han trobat formes d'aprofitar les debilitats dels tallafocs tradicionals.

On els tallafocs tradicionals han caigut és en la seva incapacitat per inspeccionar la càrrega de dades dels paquets de la xarxa i la seva falta d'intel·ligència granular per distingir diferents tipus de trànsit web. Amb la majoria del tràfic de xarxa utilitzant protocols web, els tallafocs tradicionals no poden distingir entre aplicacions de negoci legítimes i atacs, per la qual cosa o permeten tot el trànsit o el deneguen. A més, un NGF no afecta a la latència de la xarxa, que és un dels motius perquè es va crear.

El fet de disposar d'una tecnologia com aquesta, permetrà al TECNOCAT oferir un plus de seguretat i donar valor afegit a les empreses que s'instal·lin.

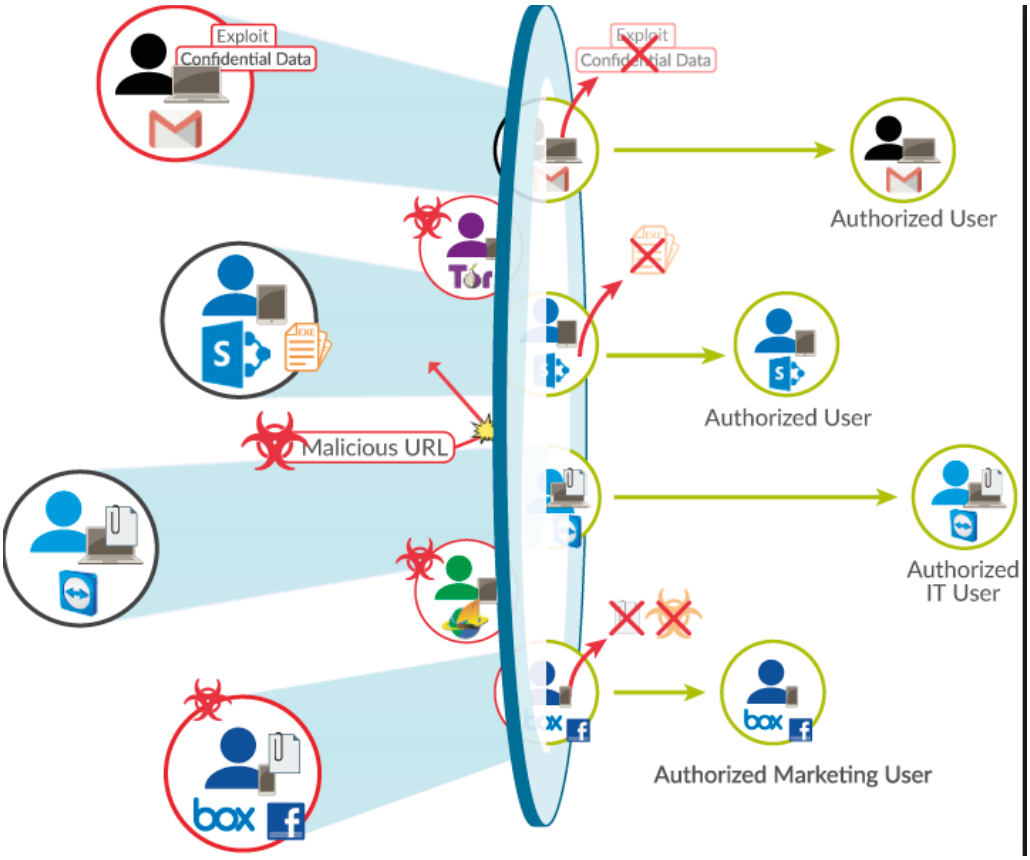

Figura 8-1 exemple de funcionament d'un NGF

8.2 Principals fabricants

A diferència dels dispositius de nivell 2, el mercat d'equips de seguretat està molt més ajustat, no hi ha un fabricant líder. Per tant, l'elecció de l'equip de seguretat ha de ser un dispositiu capaç de diferenciar-se de la resta, ha de reunir unes característiques especials que el distingeixin i el fagin únic. Aquestes característiques han de donar el valor afegit que el TECNOCAT busca i que les empreses que s'instal·lin puguin treballar amb total seguretat.

Per poder determinar quins fabricants podrien encaixar en el projecte del TECNOCAT, ens hem basat en els fabricants líders d'equips de NGF:

Figura 8-2 Fabricants líders fins l'abril de 2015

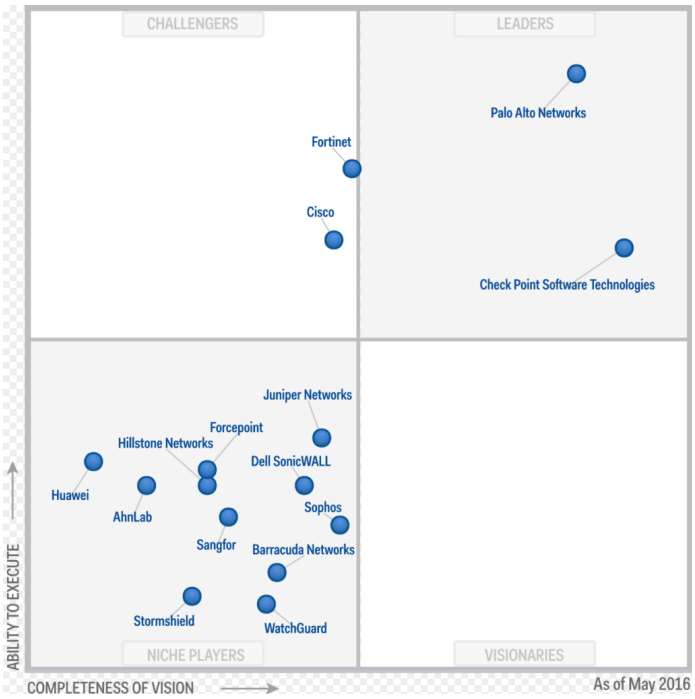

Figura 8-3 Fabricants líders fins maig de 2016

8.2.1 Check Point Software Technologies

Proporciona un paquet complet de solució NGFW amb tots els seus fulls de programari inclosos amb una única llicència. No obstant això, no proporciona controls de dispositius mòbils o control de la xarxa Wi-Fi sense necessitat d'adquirir un producte de Check Point diferent.

El programari s'integra amb Active Directory per a la identitat de l'usuari i el punt final, el que permet als administradors personalitzar les polítiques de seguretat granulars. Check Point també ofereix la possibilitat d'educar els usuaris en temps real. UserCheck és un sistema de seguretat que apareix en forma de finestra quan l'usuari viola la política de seguretat. La finestra explica la violació i guia les accions a realitzar a l'usuari. Aquest programari també permet als usuaris proporcionar informació als administradors.

Fortaleses

- Ofereix tallafocs d'alta qualitat i característiques UTM en un dispositiu fàcil d'administrar.
- Proporciona una ruta de desplegament ràpida i un baix cost de capacitació per als clients existents de Check Point .
- Gestió multi-dispositiu opcional sense necessitat de servidor extern.
- Encaminament dinàmic disponible a un cost addicional.

Debilitats

- L'estructura externa dels equips (chassis) no és de bona manipulació.
- Rendiment inferior a les expectatives.
- Llicències cares

8.2.2 Paloalto Networks

Va ser el primer fabricant a oferir tallafocs de pròxima generació i el primer a reemplaçar la classificació de trànsit basada en ports amb el coneixement de les aplicacions. Els productes de la companyia es basen en un motor de classificació conegut com App-ID. App-ID identifica les aplicacions utilitzant diverses tècniques, incloent desxifrat, detecció, descodificació, signatures i heurístiques. Els ID d'aplicació individuals per a una aplicació donada poden confiar en qualsevol combinació d'aquestes tècniques en un sol paquet, el que permet al motor identificar totes les versions d'una aplicació, així com totes les plataformes en què s'executa l'aplicació. App-ID, com a nucli dels tallafocs de Palo Alto, està sempre en execució, pel que pot identificar quan una aplicació realitza una funció, com una transferència d'arxius, i pot aplicar la política a

aquesta funció específica. La companyia també assenyala que App-ID és extensible, de manera que a mesura que noves tècniques estiguin disponibles, poden ser incorporades en el motor de classificació.

Fortaleses

- Rang de fins a 700 aplicacions controlades
- No hi ha llicencies per usuari, per el que surt més econòmic que altres fabricants
- Integració d'un mateix *appliance* de funcions firewall + IPS + antivirus + filtratge url
- Eina Wildfire de prevenció de malware i exploits
- Software de gestió versàtil

Debilitats

- Actualitzacions diàries que poden provocar que alguns serveis deixin de funcionar
- Calen coneixements elevats de la plataforma per estar molt protegit
- Manteniment car

8.3 Models de dispositius de seguretat

Segons indicàvem al punt 7.2, un cop el TECNOCAT estigui en una ocupació màxima, aquesta rondaria les 800 - 1000 persones. Parlant tècnicament, això significa que es podrien connectar entre 800 i 1000 ordinadors simultàniament (en el millor dels casos) més altres dispositius com ara connexions d'impressores, tauletes, dispositius mòbils, ... Necessitem doncs, que l'equip de seguretat en qüestió pugui suportar un volum de tràfic d'aquestes dimensions.

Check Point Software Technologies

Es proposa el model Checkpoint 5600. D'entre les funcionalitats més rellevants, incorpora seguretat web en temps real, protecció de la informació, protecció contra amenaces i prevenció contra extracció de la informació. El 5600 és Una passarel·la de seguretat de pròxima generació d'1U amb una ranura d'expansió per a més capacitat. També conté ventiladors redundants, opcions redundants per a la font d'alimentació i disc dur de 240Gb.

La optimització de seguretat del 5600 ofereix prevenció d'amenaces en el món real per protegir els actius i els entorns crítics.

Figura 8-4 Checkpoint 5600

Palo Alto

Es proposa el model PA-3020. Aquest equip gestiona els fluxos de trànsit de xarxa utilitzant processament i memòria dedicats a les xarxes, seguretat, prevenció i gestió d'amenaces. L'element de control és el PAN-OS, un sistema operatiu específic de seguretat que nativament classifica i gestiona tot el tràfic, incloses les aplicacions, amenaces i contingut i després vincula aquest trànsit a l'usuari, independentment de la ubicació o el tipus de dispositiu. Els elements de negoci s'utilitzen com a base de les pròpies polítiques de seguretat, que dona com a resultat una visió clara de seguretat i una reducció en el temps de resposta a incidents. Treballa amb 2 sistemes diferents separats, el sistema de gestió per els administradors i el sistema on està la configuració, d'aquesta manera s'obté un rendiment més elevat.

Figura 8-4 PA-3020

8.3.1 Preus dels equips de seguretat

A continuació es detallen els preus (sense IVA) dels equips de seguretat que s'han presentat al punt anterior com a futuribles dispositius de nivell 3 del TECNOCAT. Els preus són amb les seves respectives llicències:

Marca	Model	Preu unitari
Check Point Software Tech	Checkpoint 5600	20.112 €
Palo Alto Networks	PA-3020	14.403 €

8.4 Solució escollida de nivell 3

A dia d'avui, Checkpoint i Palo Alto són els líders mundials en la venta de firewalls de pròxima generació. Van començar el seu lideratge de mercat a partir de l'any 2014. Són equips molt estables, eficaços i amb unes capacitats robustes. Un dels inconvenients de Checkpoint és l'elevat preu dels seus productes i la seva arquitectura blade de programari, que ofereix moltes opcions a la carta, a vegades masses. Palo Alto està creixent d'una manera exponencial, però per contra també ofereix productes a preus elevats i els seus equips no tenen un ecosistema robust.

Les dues solucions proposades són semblants, però hi ha algunes diferències importants. La gamma de productes Checkpoint estan encarats cap a la total protecció de l'usuari. Segons el centre de recerca tecnològica Gartner[1], Checkpoint és l'empresa de NGF que detecta més atacs a nivell mundial. Palo Alto, a part d'oferir seguretat d'alt nivell per a l'usuari, gràcies a la seva extensa base de dades, ofereix 3 productes essencials repartits en 3 llicències: servei d'antivirus, *Application and threats* i el sistema de detecció de malware anomenat w*ildfire.* Checkpoint també ofereix aquests productes (excepte wildfire que no el té integrat) però repartits en més llicències, les quals són més cares, to depenent de les necessitats dels clients.

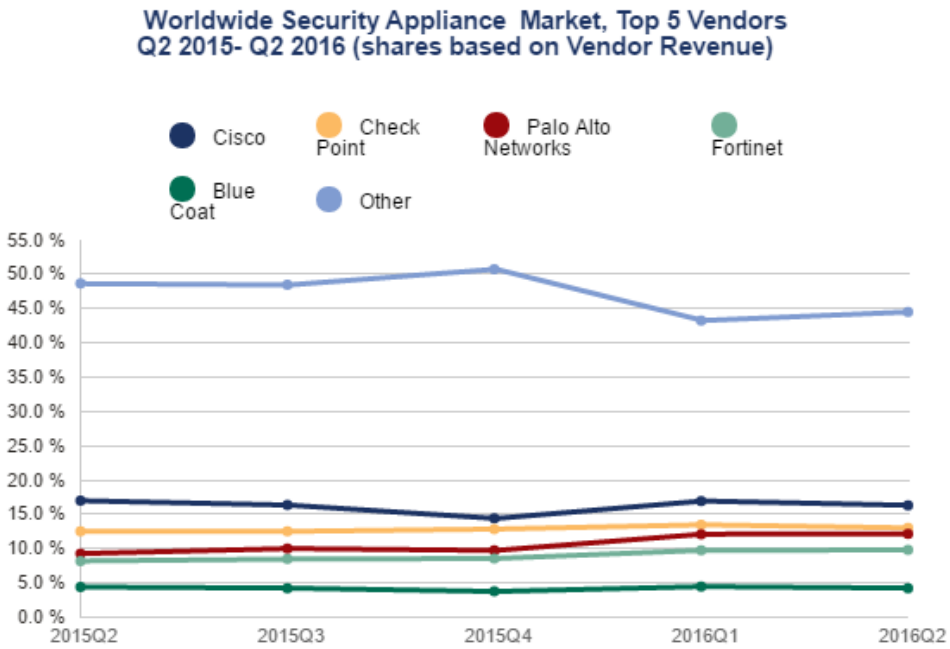

Figura 8-5 mercat d'equips de seguretat a nivell mundial

Top 5 Vendors, Worldwide Security Appliance Revenue, Market Share, and Growth, Second Quarter of 2016 (revenues in US$ millions)					
Vendor	**2Q16 Revenue**	**2Q16 Market Share**	**2Q15 Revenue**	**2Q15 Market Share**	**1Q16/1Q15 Growth**
Cisco	$449	16.3%	$441.64	17.0%	1.6%
Check Point	$358	13.0%	$325.53	12.5%	10.0%
Palo Alto Networks	$334	12.1%	$241.38	9.3%	38.2%
Fortinet	$270	9.8%	$213.35	8.2%	26.4%
Blue Coat	$117	4.2%	$114.69	4.4%	1.9%
Other	$1,224	44.5%	$1,264.60	48.6%	-3.2%
Total	**$2,751**	**100%**	**$2,601.19**	**100%**	**5.8%**
Source: IDC Worldwide Quarterly Security Appliance Tracker Q2 2016, September 14, 2016					

Figura 8-6 facturació mundial d'equips de seguretat fins setembre 2016

Donades les semblances entre les dues tecnologies, per a l'elecció del dispositiu de seguretat ens hem basat en dues premisses clau, el preu del producte i la integració dins la xarxa del TECNOCAT. Palo alto té un preu inferior i ofereix una gamma de serveis molt semblants a Checkpoint. També entenem que les característiques de l'ús de la xarxa del TECNOCAT seran, a part de seguretat, serveis a les empreses instal·lades. Aquest fet és important, ja que si es volgués, permetria oferir a les empreses paquets de seguretat i amb Palo alto es podria ajustar més el preu. Per tant, entenem que el dispositiu que més encaixara dins la xarxa del TECNOCAT és Palo Alto. A continuació, fem referència a alguns dels motius d'aquesta elecció:

- Preu inferior dels equips
- Preu inferior en llicències
- Gamma de serveis molt semblants a Checkpoint
- Sistema de gestió PANOs àgil, robust i entendible
- Empreses catalanes treballen i confien en els seus productes
- Oferta de *partners* elevada
- Sistema de gestió únic
- Actualitzacions constants de serveis i versions de software
- Operabilitat
- Facilitat d'integració dins d'una organització
- Marca contrastada
- Sistema Wildfire únic en detecció de *malware*
- plataformes de gestió i d'informació separades

8.5 Connexió cap al Core 6800

La connexió cap al Core del TECNOCAT es podria realitzar mitjançant una connexió de 10 Gb mitjançant fibres multimode, suficient per no provocar un coll d'ampolla en cas de tenir un 100% d'activitat al centre.

8.6 Exemple de proposta de nivells 2 i 3 del TECNOCAT

En la següent il·lustració podem observar les solucions de nivell 2 i 3 proposades:

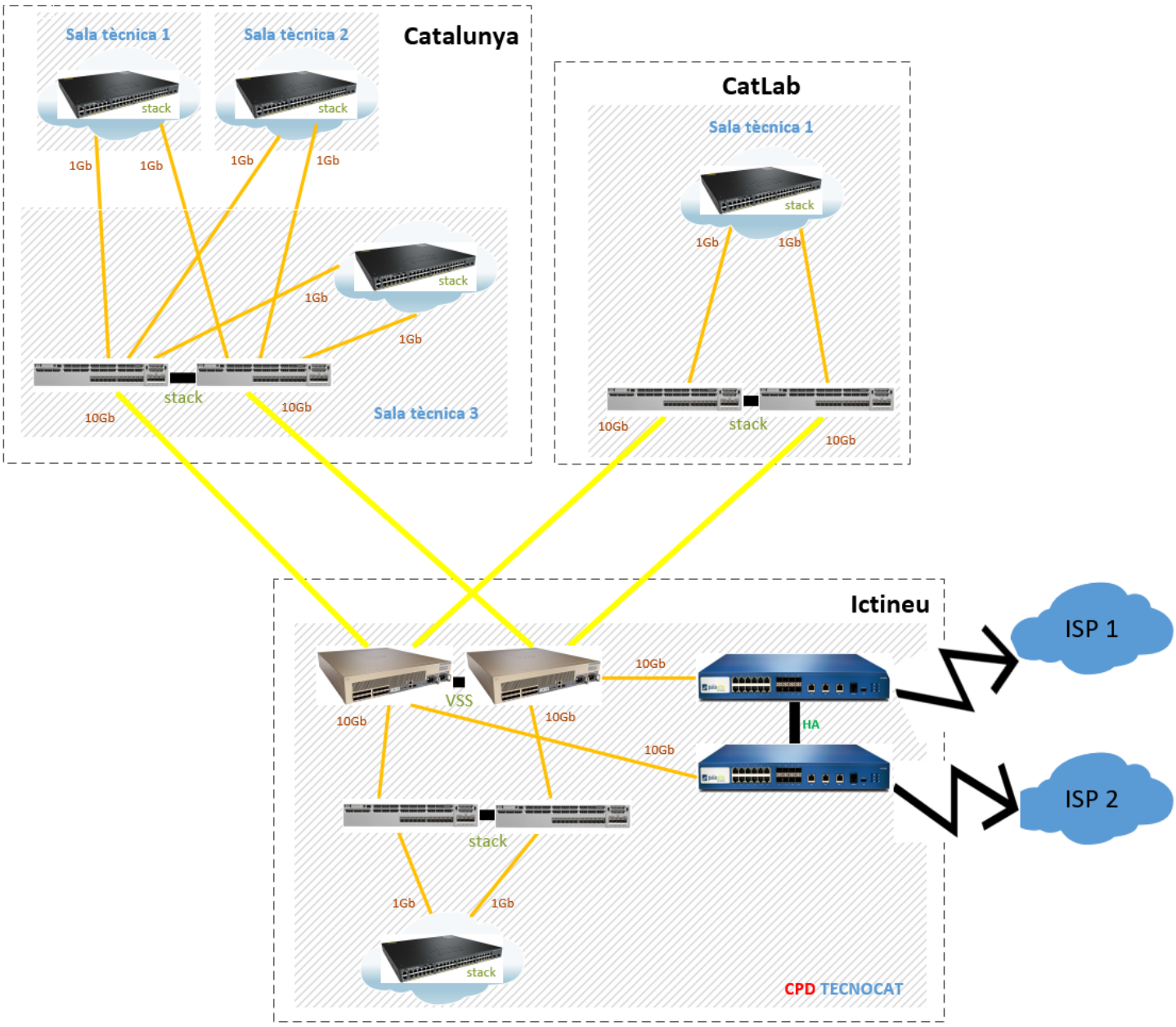

Figura 8-7 solució de xarxa de nivell 2 i 3

8.7 Connexió cap al ISP

S'aconsella fermament disposar de 2 ISP's diferents en cas de fallida en algun d'ells, d'aquesta manera s'aconsegueix una bona redundància cap a Internet. Per calcular l'ample de banda necessari, ens basarem en una fórmula matemàtica molt simple, **AB = G*Q**, on:

AB = Ample de banda a contractar
N = Quantitat d'usuaris que es connectaran a Internet
G = Ample de banda que garantirem a cada usuari
Q = quantitat de persones que poden utilitzar Internet simultàniament

Es recomana realitzar el càlcul en hores punta, per exemple a l'entrada de les empreses per el matí, que es quan s'engeguen les màquines i més demanda hi haurà d'ample de banda.

9. Nivell lògic de la xarxa de dades

Tal i com s'ha descrit anteriorment els requeriments de xarxa són funcionals. En aquest apartat es donarà un tipus de solució per a la connexió de les diferents empreses que conformin el TECNOCAT.

9.1 Connexió de les empreses

La solució per a la connexió de les diferents empreses passarà per la configuració de *Vlans*. Cada *Vlan* doncs serà una empresa i no es podran veure entre elles. Aquestes *Vlans* tindran associada la seva subxarxa, màscara, porta d'enllaç i el DHCP (no es configurarà un servidor DNS en el TECNOCAT, s'haurà de configurar en el DHCP de cada empresa un DNS alié). Aquesta configuració s'haurà de posar al firewall (nivell 3) i s'hauran de passar les *Vlans* de cada empresa fins a la seva connexió final (*access layer* - nivell 2).

Degut a la idiosincràsia del TECNOCAT en el que cada empresa es correspon a una vlan diferent i que només es troba en una ubicació, no es recomana la utilització del protocol VTP ja que les vlans seran molt reduïdes a nivell d'implantació. Per tant, es recomana la configuració dels dispositius en vtp mode transparent, és a dir, amb una configuració estàtica de vlans on es configurin a tots els switchos del mateix rack totes les vlans d'aquell rack, els ports d'uplink es configurin en mode trunk i en l'equipament de distribució es filtrin les vlan's que s'enviïn a cada rack mitjançant els *allowed vlan* en els ports d'uplink que correspongui. Per exemple, si tenim un empresa ubicada a l'edifici Ictineu no té cap sentit configurar la seva Vlan als altres 2 edificis.

Altrament, també es recomana que el CORE 6800 del TECNOCAT tingui la prioritat root spanning-tree més baixa que la resta d'equips de l'electrònica de xarxa, d'aquesta manera els equips amb STP a la xarxa crearan un camí redundant central i no un altre amb menys redundància.

9.1.1 Adreçament de les empreses

La subxarxa que es configuraria seria amb adreçament de Classe C, per exemple 192.168.**0**.0/24 on el tercer octet serà el diferenciador de cada empresa. Exemple de configuració d'una empresa:

Nom empresa/Vlan: **empresa A**
Id Vlan: **2**
xarxa: 192.168.**2**.0/24
màscara: 255.255.255.0
Porta d'enllaç: 192.168.**2**.254

Nom empresa/Vlan: **empresa B**
Id Vlan: **3**
xarxa: 192.168.3.0/24
màscara: 255.255.255.0
Porta d'enllaç: 192.168.3.254

Cada empresa doncs, tindrà 253 ip's disponibles per al seu ús. Es reservarà un espai fora del DHCP (excluded DHCP) de 14 ip's per si les empreses hi volen posar dispositius com impressores, servidors locals, NAS, etc:

Rang DHCP: 192.168.**X**.1-239
Excluded DHCP: 192.168.**X**.240.253

Com hem comentat anteriorment, no es contempla la solució d'implementació d'un servidor DNS al TECNOCAT però es proposen els següents servidors els quals acostumen a ser estables:

Google: 8.8.8.8; 8.8.4.4
Telefónica: 194.179.1.101
CSUC: 84.88.84.88

Per a la sortida a internet de les empreses s'haurà de contractar al proveïdor d'internet un *pool* d'ips públiques. La sortida es farà mitjançant NAT de la xarxa de cada empresa a la seva ip pública. Es proposa que cada empresa surti per la mateixa ip pública a l'exterior (pool VLAN):

Nom empresa/Vlan: **empresa C**
Id Vlan: **4**
xarxa: 192.168.4.0/24
màscara: 255.255.255.0
Porta d'enllaç: 192.168.4.254
Exemple d'ip pública: 81.89.61.4

9.2 Protocols importants a configurar en les boques d'accés

9.2.1 PORTFAST

Quan es connecta un dispositiu a la xarxa, en una Vlan amb *spanning tree*, el port abans d'estar operatiu passa per diferents estats fins a estar operatiu, és a dir, fins a posar-se en *forwarding*. Durant aquest període que pot arribar a ser de fins a 45 segons el port no és operatiu i potser el dispositiu final ha intentat iniciar algun servei de xarxa, com pot ser la petició DHCP.

Per evitar la problemàtica comentada, es recomana configurar els ports on sapiguem que es connectin dispositius finals amb aquesta opció perquè el pas a *forwarding* sigui automàtic. Aquesta opció mai ha de configurar-se a ports de connexió amb altres switchos.

9.2.2 BPDUGUARD

Tal com s'ha comentat anteriorment, quan es configura un port com portfast, s'aplica una funcionalitat per accelerar la posada en servei d'un port físic, però aquest port segueix estant dins d'un domini de spanning tree, per tant, si arribessin BPDUs a aquest port les processaria com a tal. És a dir, podríem provocar un canvi de topologia en el domini de STP. Per evitar això podem usar BPDUGuard en conjunció amb Portfast.

Aquesta funcionalitat controla la recepció de BPDUs en el port, on no s'espera que existeixin aquest tipus de trames ja que, tal com s'ha indicat anteriorment, únicament ha de configurar-se portfast en ports on es connectin dispositius finals d'usuari. Quan es rep una trama d'aquest tipus, es bloqueja el port com a mecanisme de seguretat per evitar qualsevol problemàtica que es pugui produir ja que s'entén que el que estem connectant en el port no és d'acord amb la seva configuració.

9.2.3 ROOTGUARD

Aquesta funcionalitat el que produeix és que si rep un BPDU en el port on està activada on s'indiqui que un switch connectat a aquell port està intentant ser el root bridge ja que informa d'una prioritat més baixa es deshabilitarà el port.

9.2.4 PORT SECURITY

En la mida del possible i per a poder disposar d'un control del que es connecta a la xarxa del TECNOCAT es recomana l'aplicació d'aquesta característica als ports d'accés. Aquesta característica permet aprendre les adreces MAC connectades a cada port de la xarxa i permet únicament a aquestes adreces MAC comunicar-se a través de tal port. Si un altre dispositiu amb una altra adreça MAC intenta comunicar-se a través del port, port-security deshabilitarà el port i si es segueix la recomanació de gestió dels missatges traps SNMP i syslog es podrà generar una alarma que produeixi una notificació a l'administrador de la xarxa respecte el bloqueig del port. Cal tenir en compte que la implantació d'aquesta característica comporta assumir un increment en la gestió de l'accés de nous dispositius dins de la xarxa.

Per defecte, el funcionament d'aquesta característica és permetre únicament una adreça MAC en cada port, que serà la primera que es connecti, i si es connecta una nova adreça MAC el port es desactivarà. Per suposat, aquestes opcions son modificables fins arribar a poder suportar fins a 132 adreces MAC en un port i escollir l'acció a prendre quan hi hagi una violació de la regla configurada, sent aquestes opcions deshabilitar el port, avís a l'administrador de la xarxa o permetre únicament el tràfic de les MAC registrades com a correctes.

9.3 Configuració de dades a les boques d'accés per a cada empresa

9.3.1 Usuari amb switch

Aquests ports son d'accés a usuaris que conectaràn un switch local que no serà de la xarxa del TECNOCAT. Es recomana la següent configuració:

interface GigabitEthernet X/Y
switchport access vlan <vlan_dades_ID>
switchport mode access
spanning-tree rootguard

9.3.2 Usuari amb pc

Aquests ports son d'accés a usuaris que només tenen connectat un PC, impressora, ... Es recomana la següent configuració:

interface GigabitEthernet X/Y
switchport access vlan <vlan_dades_ID>
switchport mode access
switchport port-security
spanning-tree portfast
spanning-tree bpduguard enable

9.4 Seguretat

Tal i com s'ha comentat anteriorment, les diferents empreses no es podran veure entre elles. Per dur a terme aquesta configuració s'hauria de crear una zona al *firewall* (zona empreses) on estiguessin totes les empreses i una regla que prohibís la seva visibilitat.

Tots els equips que conformen l'electrònica de xarxa del TECNOCAT hauran d'estar aïllats de les empreses. Es proposa crear una altre zona al firewall (zona gestió) on estiguin tots els equips que conformin els dispositius de xarxa del TECNOCAT, com ara els commutadors de xarxa, firewall, dispositius de xarxa sense fils, ... En aquesta zona només haurien de tenir accés els administradors de la xarxa. Es proposa una xarxa amb adreçament privat. Exemple de configuració de la xarxa de gestió:

Nom Vlan: **gestio**
Id Vlan: **15**
xarxa: 10.0.0.0/24
màscara: 255.255.255.0
Porta d'enllaç: 10.0.0.254

9.5 Exemple de connexió LAN d'una empresa

En la següent il·lustració s'observa la connexió d'una empresa connectada a la xarxa del TECNOCAT:

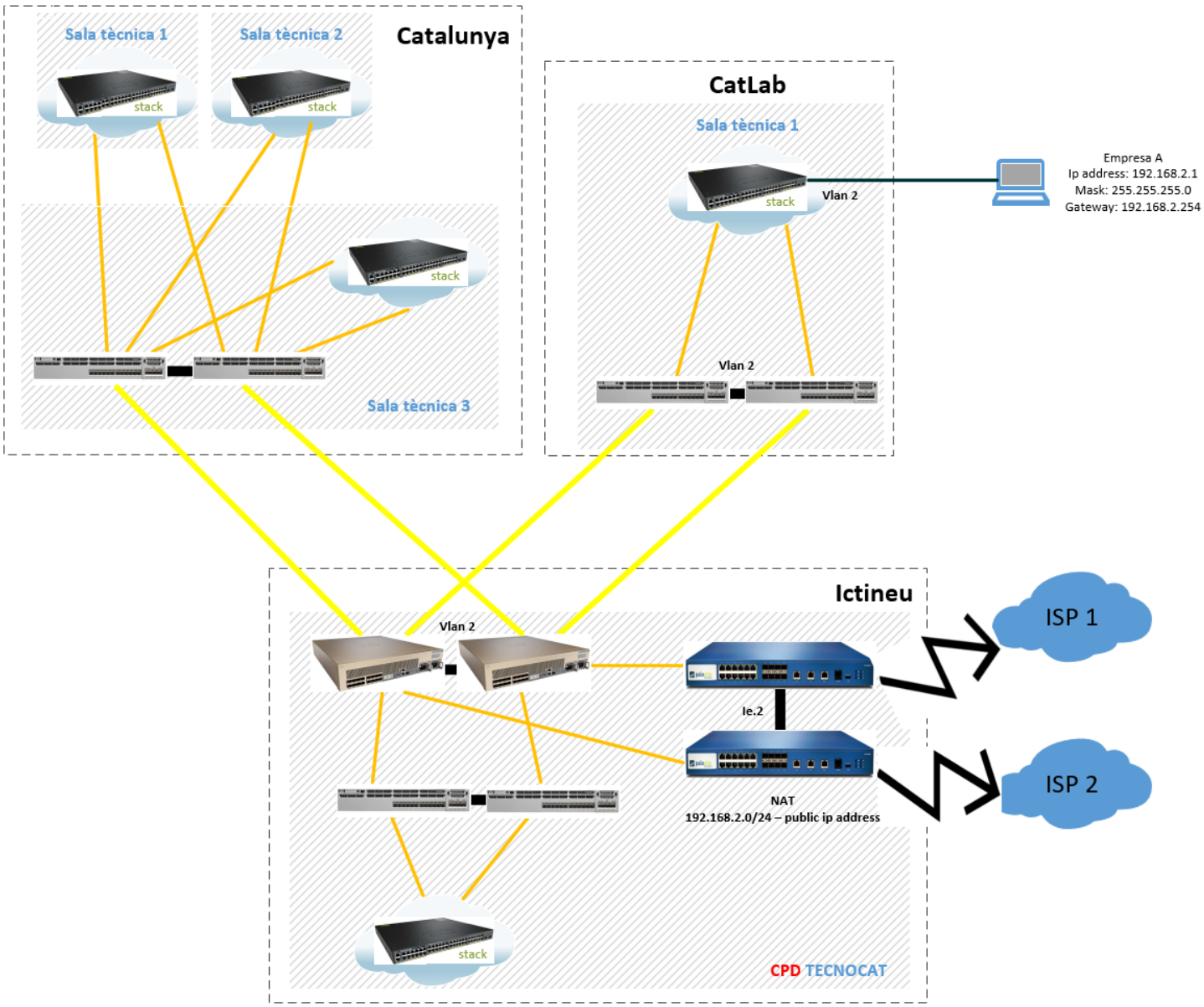

Figura 9-1 exemple de connexió d'una empresa a la xarxa del TECNOCAT

10. Equipament de Veu

El món de les telecomunicacions és cada vegada més complex. En el cas del TECNOCAT, intentarem explicar les diferents tecnologies que estan darrere dels sistemes de telefonia fixa perquè puguem entendre de què ens estan parlant i valorar el què convé.

Actualment hi ha tres tecnologies sobre les quals realitzem les nostres trucades, la telefonia digital, la telefonia analògica i la veu IP. Aquestes tecnologies poden combinar-se entre si quan emetem una trucada, ja que totes les xarxes es combinen per fer possible la comunicació amb qualsevol altre telèfon del món. No obstant això, per a fer aquest anàlisi ens centrarem en les línies que ens arriben a la nostra oficina, com connectem la nostra centraleta a les línies i conèixer els terminals que s'han d'utilitzar.

10.1 Tipus de Telefonia

10.1.1 Telefonia Digital

Es tracta d'un estàndard pel qual diverses comunicacions poden transmetre's en format digital (uns i zeros) alhora a través dels cables de telèfon tradicionals (el parell de coure tradicional). Forma part de la Xarxa Digital de Serveis integrats (RDSI), i es basen en un protocol digital que permet proporcionar una àmplia gamma de serveis, tant de veu com de teleserveis i altres tipus. Aquesta tecnologia permet una major capacitat de transmissió, on veu i dades poden viatjar alhora. En general té una capacitat de 128kbps tant per a pujada com per a baixada i d'aquí surten els dos canals de veu de 64kbps. A continuació veiem les principals característiques d'una línia RDSI:

- Línies RDSI (BRI), permeten 2 comunicacions simultànies a través de 2 canals de 64 Kbps, per a veu o dades.
- Cada canal suposa una numeració (DDI) amb la qual ens poden cridar i emetre trucades, no obstant això es sol configurar en centraleta per usar un de principal per identificar-se en les trucades sortints, o saltar a altres nombres en la recepció de trucades si el principal està comunicant.
- Les línies RDSI (PRI), permeten fins a 30 comunicacions simultànies a través de 30 canals de 64 Kbps, per a veu o dades.
- Majoritàriament utilitzada al mercat empresarial.
- Major qualitat de so que les analògiques (codec G-711) ja que no hi ha sorolls ni interferències.

10.1.2 Telefonia Analògica

Aquestes línies pertanyen a la Xarxa de telefonia commutada (RTC o RTBC) i bàsicament estan pensades per a transmissió de veu, encara que poden també transportar dades, per exemple en el cas del fax o de la connexió a Internet ADSL. Es basa en un cable de dos fils fins de coure pel qual es transmet un senyal elèctric que es converteix en ones de so. Aquestes ones són les que transmeten la veu quan parlem per telèfon. Característiques:

- Permeten una sola comunicació per línia contractada
- Majoritàriament utilitzada al mercat residencial
- Cada línia va sota un nombre identificador, o DDI geogràfic

10.1.3 Telefonia IP

Una línia IP en realitat no és més que un canal de veu on la trucada es transmet per la xarxa d'Internet, connectant un dispositiu SIP o centraleta amb el proveïdor VoIP. En general s'usa l'estàndard SIP per a les trucades VoIP i el nombre de canals és tan gran com ens permeti l'ample de banda i ens ofereixi el nostre proveïdor de telefonia VoIP. No existeixen per tant línies físiques IP, sinó que són les connexions de dades (fibra òptica, ADSL, LAN…) que ens permeten realitzar aquest tipus de trucades. Característiques línia IP:

- No depenem de línies físiques sinó d'una infraestructura de xarxa, per la qual cosa pràcticament no hi ha limitacions en la quantitat de converses simultànies
- Els números de telèfon s'allotgen en el núvol del nostre operador de telecomunicacions. Podem usar tants nombres com vulguem contractar, i del lloc geogràfic que vulguem (conforme normatives i disponibilitat). Així, podem usar una línia IP amb un smartphone, estant en qualsevol part del món, i usar múltiples números de contacte (Barcelona, París, Madrid…).
- Al no dependre d'unes línies físiques podem crear una xarxa unint múltiples ubicacions.
- Podem aconseguir una qualitat HD en les trucades segons l'operador i equips que tinguem.

10.2 Tecnologia escollida en telefonia

Avui dia el sistema telefònic d'una empresa que vulgui funcionar de forma eficient es basa en solucions informàtiques que són més flexibles, barates i potents que una central telefònica.

Donat el volum d'usuaris que pot tenir en un futur el TECNOCAT i el tipus d'entorn, l'opció de telefonia escollida es la veu ip. Utilitzant els protocols de xarxa, l'anomenada Veu sobre IP (VoIP) permet integrar els equips informàtics amb el sistema telefònic per dotar d'unes prestacions increïbles a qualsevol empresa. Alguns dels motius d'aquesta elecció són els següents:

- Escalabilitat: sense límit de creixement
- Estalvi de costos: En utilitzar la connexió a Internet, podem prescindir de línies addicionals, que tenen un cost mensual elevat. A més el sistema permet utilitzar l'operador de veu IP que més ens interessi a cada moment, aconseguint estalvis de fins al 90% en el consum telefònic.
- Llibertat en l'elecció de l'operador: Només és necessari disposar de connexió a Internet. Ens és igual quin operador doni el servei. Les trucades a la xarxa telefònica es configuren per utilitzar qualsevol operador de VoIP, amb l'objectiu d'aprofitar les tarifes més barates.
- Llibertat en l'elecció d'equips: A diferència de les centraletes basades en maquinari, no hi ha l'obligació a utilitzar telèfons ni aparells d'una marca concreta, tenint així una gamma molt més àmplia d'opcions.
- Integració amb SmartPhones: Si l'empresa utilitza smartphones, es pot utilitzar la quota de dades o una xarxa wifi per fer i rebre trucades a través de la centraleta IP. Des del smartphone podem saber quins usuaris estan operatius.

10.3 Tipus de centraletes de veu

10.3.1 Centraleta IP al núvol

Les centraletes IP al núvol (Virtual IP voice) són centraletes en les quals l'operador de telefonia IP és el responsable d'allotjar-la en els seus servidors, del seu manteniment i del correcte funcionament. L'empresa només ha de connectar els telèfons IP a Internet perquè les trucades passin a través de la centraleta virtual. Els operadors de telefonia IP cobren a les empreses quotes mensuals per aquest servei.

La centraleta virtual està allotjada en el núvol i conté tota la configuració del sistema telefònic de l'empresa. Les extensions es connecten a la centraleta virtual a través d'Internet, per la qual cosa és possible que treballadors que es troben en diferents localitzacions geogràfiques estiguin connectats a la mateixa centraleta. L'operador de telefonia IP s'encarrega de l'engegada, programació, manteniment, seguretat i resolució d'incidències de la centraleta virtual. Les característiques més importants són:

- Allotjada en Internet i connectada amb la xarxa telefònica
- Les extensions es connecten a la centraleta a través d'Internet
- El servei es contracta a un Operador de telefonia IP que inclou:
  - Línies telefòniques
  - Numeració telefònica
  - Tarifes de trucades
- Inclou el manteniment i suport
- Inclou un panell de configuració *online* de la centraleta

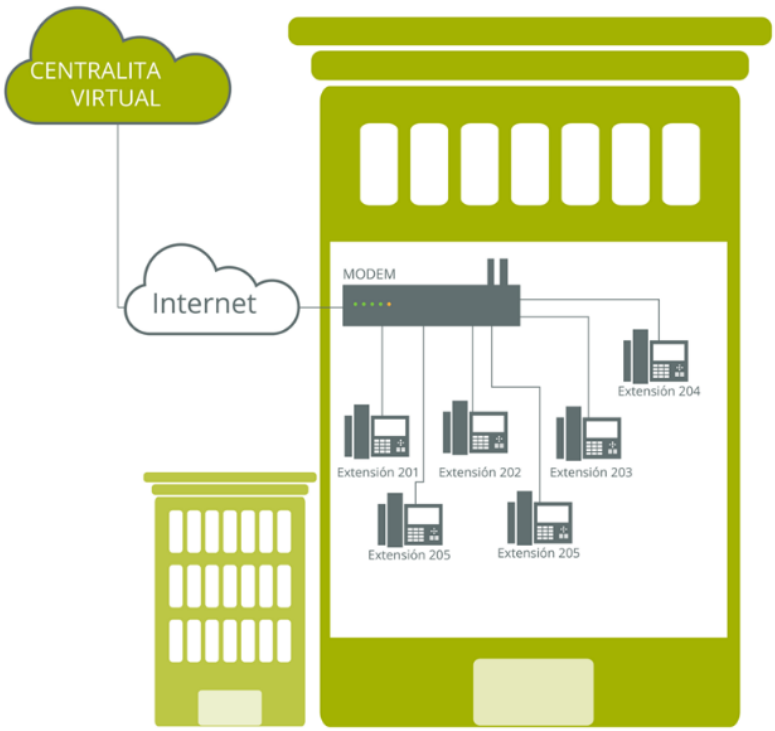

Figura 10-1 Exemple de connexió a una centraleta IP al núvol

10.3.2 Centraleta IP física

La centraleta IP física és un dispositiu físic que s'instal·la dins de l'empresa i a la qual es connecten les extensions per cables o a través de la xarxa interna. Perquè la centraleta IP tingui línia telefònica és necessari contractar el servei de SIP trunk o troncal SIP amb un operador de telefonia IP, al que es connecta a través d'Internet.

En la centraleta IP es programa la configuració i extensions del sistema telefònic i l'operador de telefonia IP únicament dóna el servei de connexió a la xarxa telefònica i la numeració.

L'empresa és la responsable de l'engegada, programació, manteniment, seguretat i resolució d'incidències de la centraleta IP. Les característiques més importants són:

- Aparell físic / maquinari dins de l'empresa connectada a la xarxa telefònica a través d'Internet
- Les extensions es connecten a través de la xarxa interna o per cable a la centraleta IP
- És necessari contractar un SIP Trunk amb un operador de telefonia IP, que inclou:
    - Connexió a la xarxa telefònica (PSTN)
    - Numeració telefònica
    - Tarifes de les trucades
    - L'empresa és la responsable del seu manteniment i redundància

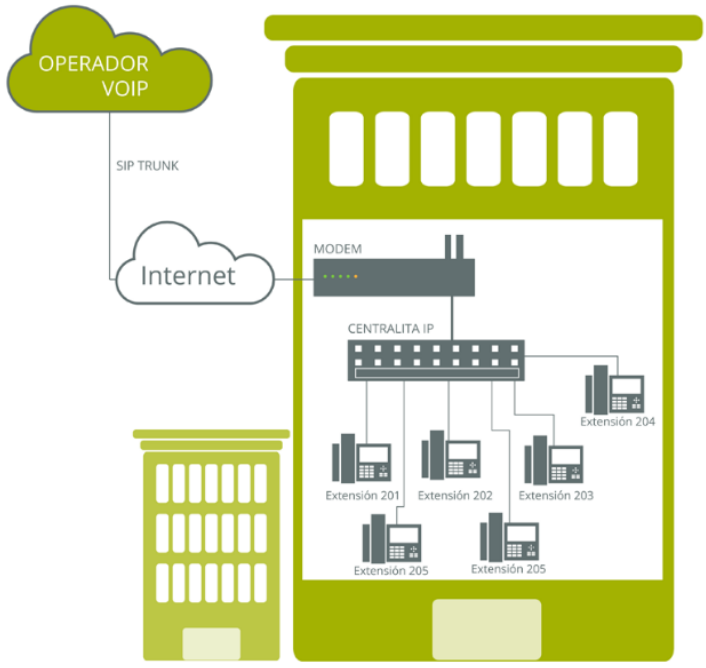

Figura 10-2 Exemple de connexió a una centraleta IP física

10.4 Solució de centraleta escollida

A continuació s'observen alguns dels elements a tenir en compte a l'hora d'escollir el tipus de centraleta:

	Centraleta al núvol	Centraleta física
Cost Inicial	baix	alt
Cost mensual	mitjà	baix
Cost manteniment	gratis	alt
Costos d'expansió	baix	alt
Programació centraleta	Inclosa	No inclosa
Dificultat programació	Mitjana/baixa	Alta
Manteniment	Inclòs	No inclòs
Actualitzacions	Incloses	No incloses
Necessari tècnic a l'empresa	No	Sí
Funcionalitats	Altes	Altes
Preu trucades	Econòmiques	Econòmiques
Flexibilitat geogràfica	Total	No
Seguretat	Elevada	Segons coneixements tècnic
Allotjament	Núvol	Empresa
Connexió extensions	Internet/xarxa local	Xarxa local
Serveis a contractar amb operador VoiP	Centraleta virtual	Troncal SIP
Responsable Configuració	Operador telefonia IP	Empresa
Manteniment	Operador telefonia IP	Empresa
Resolució incidències	Operador telefonia IP	Empresa
Extensions	Preu per unitat/servei	Es creen a la centraleta IP
Coneixements tècnics necessaris	No	Si
Límits d'ampliació	No	Si

Figura 10-3 Diferències entre centraleta al núvol i centraleta física

- Si parlem del desemborsament inicial veiem que:

Centraleta al núvol

Compra de telèfons
Contractació del servei

Centraleta IP física

Compra de telèfons
Compra de la centraleta IP
Contractar els serveis d'un instal·lador
Contractar el servei de SIP trunk

- Si parlem dels costos mensuals veiem que:

Centraleta al núvol

Quota mensual baixa
Trucades telefòniques
Sense costos de manteniment

Centraleta IP física

Quota mensual inferior
Trucades telefòniques
Possibles costos de manteniment

- Si parlem dels costos de manteniment veiem que:

Centraleta al núvol

Cap, inclòs dins del servei

Centraleta IP física

Impredictibles, dependrà de les modificacions i ampliacions necessàries i de les incidències que puguin sorgir

Les dues solucions de telefonia IP són molt valides a l'hora de dotar el TECNOCAT d'una infraestructura de veu, tot dependrà de les necessitats que es tinguin. Si ens basem en els costos, la telefonia cap al núvol és la més econòmica. Si el que volem es tenir un control total de la nostra infraestructura de veu, la opció més viable es tenir la centraleta dins l'empresa.

Si mirem el total de prestacions, busquem el seu valor afegit i observem els costos per part de les dues centraletes, el sistema que més encaixaria dins del TECNOCAT es la centraleta IP al núvol, la qual recomanaríem per:

- Inversió inicial mínima
- Programació i manteniment a càrrec de l'operador de telefonia IP
- Seguretat a càrrec de l'operador de telefonia IP
- Flexibilitat geogràfica
- Afegir nous números, extensions o canals és senzill i ràpid
- Sense límits d'ampliació
- trucades entre seus gratuïtes
- En cas de pèrdua de connexió a Internet o d'electricitat el teu operador de telefonia IP pot redirigir les trucades a línies de backup
- Accés remot a la configuració de la centraleta
- Usuari per empresa per consultar el seu consum
- Reports trucades
- No cal ser un tècnic per dur la gestió de la telefonia ip

10.5 Tipus de terminals

Es recomana adquirir terminals que portin incorporada la opció de switch per poder connectar un ordinador al mateix terminal. D'aquesta manera aprofitem una mateixa connexió a la roseta del terra per passar-hi 2 dispositius. En la següent il·lustració es pot observar un exemple de telèfon amb aquesta funcionalitat:

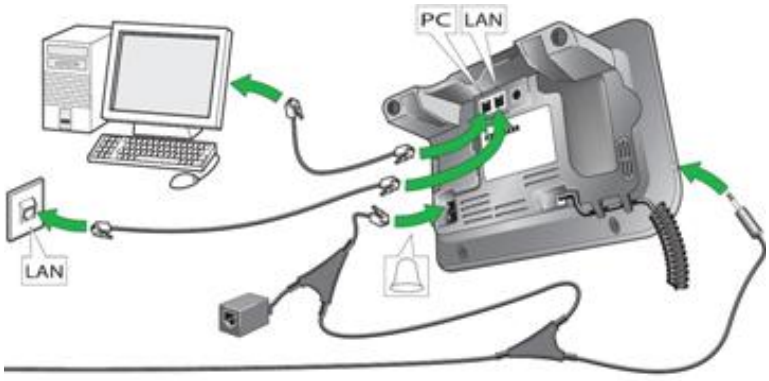

Figura 10-4 Exemple de terminal amb una entrada LAN i una per a pc

10.6 Protocols de veu importants a configurar en les boques d'accés

10.6.1 Qualitat de Servei

Per poder garantir una bona qualitat de servei a la veu ip, es recomana aplicar la següent política als equips d'accés:

```
policy-map policyQoS
        class mapQoS
        set dscp ef
class class-default
        set dscp default
```

10.7 Tipus d'adreçament

El tipus d'adreçament proposat va en funció de cada edifici, es proposa el següent:

Vlan Edifici Ictineu: **telefonia Ictineu**
Id Vlan: **601**
xarxa: 172.16.0.0/23
màscara: 255.255.254.0
Porta d'enllaç: 172.16.1.254

Vlan Edifici Ictineu: **telefonia Catalunya**
Id Vlan: **602**
xarxa: 172.16.2.0/23
màscara: 255.255.254.0
Porta d'enllaç: 172.16.3.254

Vlan Edifici Ictineu: **telefonia CatLab**
Id Vlan: **603**
xarxa: 172.16.4.0/23
màscara: 255.255.254.0
Porta d'enllaç: 172.16.5.254

10.8 Configuració de veu per a usuari amb telefonia

10.8.1 Usuari amb telefonia

Aquests ports s'han de configurar a les boques d'accés on s'hi connectarà un telèfon ip el qual tindrà la funció de switch per poder-hi connectar un telèfon. Es proposa la següent configuració:

interface GigabitEthernet X/Y
switchport trunk native vlan <vlan_dades_ID>
switchport trunk allowed vlan <vlan_dades_ID>, <vlan_veu_ID>
switchport mode trunk
switchport port-security
switchport port-security maximum 2
switchport port-security aging time 1
srr-queue bandwidth share 10 10 60 20
queue-set 2
priority-queue out
mls qos trust cos
spanning-tree portfast
spanning-tree bpduguard enable
service-policy input policyQoS

10.9 Exemple de connexió d'un terminal ip a la xarxa del TECNOCAT

En la següent il·lustració s'observa la connexió d'un terminal IP a la xarxa del TECNOCAT:

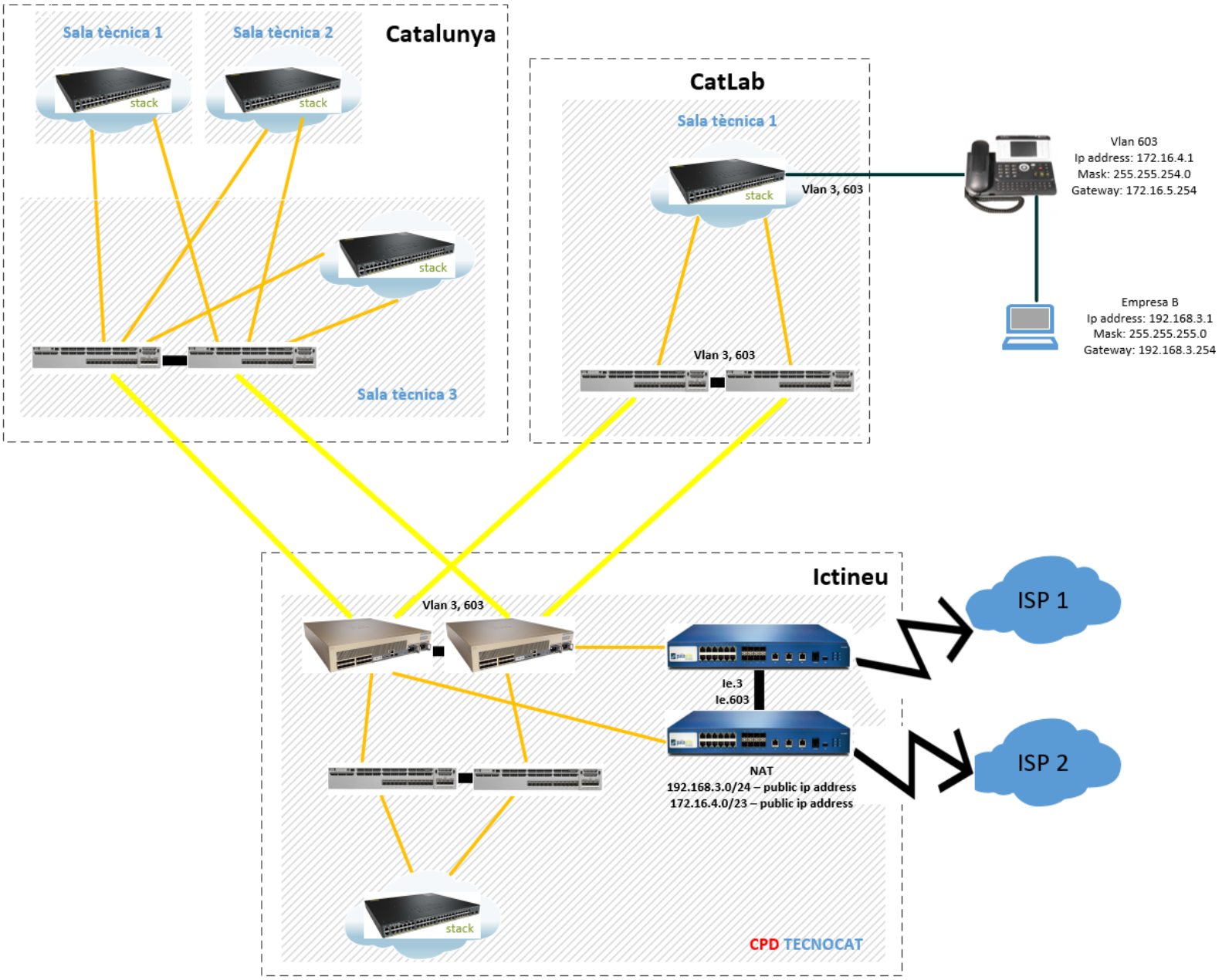

Figura 10-5 exemple de connexió d'un terminal Ip a la xarxa del TECNOCAT

11. Conclusions

La intenció del present Treball final de Grau és aportar una possible solució a la implementació d'una xarxa cablejada de telecomunicacions per a l'empresa TECNOCAT, tant per veu per com per dades, des del punt de vista d'una empresa consultora fictícia la qual hem anomenat NETing. Aquest projecte contempla tots els aspectes necessaris per l'anàlisi i futura execució d'una infraestructura de xarxa d'una gran empresa, analitzant les diferents casuístiques i aportant solucions concretes. Així doncs, els principals objectius d'aquest projecte han estat:

- Analitzar i entendre les mancances actuals del TECNOCAT i donar una solució mitjançant la implementació d'una xarxa cablejada pròpia de telecomunicacions
- Analitzar les diferents tecnologies en el mercat de la commutació, telefonia i seguretat i donar una solució per al seu desplegament funcional
- Oferir una solució de configuració dels equips d'accés dels usuaris per garantir un control sobre què es connecta a la xarxa

Les problemàtiques que es poden trobar en planificar un projecte de nova execució (des de zero) com el plantejat en aquest TFG és que no es tindrà el 100% de la informació des del principi, ja que la compra d'equipament variarà segons la demanda dels usuaris. Per exemple, com major nombre d'usuaris, major nombre d'equips d'accés i terminals de telefonia. S'haurà doncs de realitzar un dimensionament de la infraestructura amb un marge de tolerància ampli que podria implicar un dimensionament no ajustat a la realitat final.

Un cop avançava el projecte, s'han hagut d'eliminar alguns apartats proposats inicialment, com el desplegament wifi a les zones comuns dels edificis i una eina de monitorització per tenir visibilitat sobre la xarxa LAN. Aquests apartats no s'han inclòs ja que un cop analitzat l'abast s'ha comprovat que era molt ampli, sobretot en la dotació d'una infraestructura de xarxa sense fils en les zones comuns del TECNOCAT. A canvi s'han afegit apartats com ara els tipus de protocols de telecomunicacions i una possible solució en les boques d'accés dels usuaris. Així, ens hem pogut centrar més en la part més tècnica de la xarxa cablejada del centre. S'ha aconseguit doncs desplegar un projecte molt acurat amb diferents solucions de propostes físiques i lògiques, també econòmiques. Per tant, no s'ha seguit al peu de la lletra el pla de treball entregat a la PAC1.

Sobre la valoració econòmica dels dispositius es podria haver definit un pressupost més acurat, sobretot en la part dels equips de seguretat. Per

exemple, es podrien haver valorat els preus de les diferents llicències que es poden contractar, com ara el filtratge web (url filtering), *Wildfire*, *Threat Prevention*, ...

Altrament, cadascun dels apartats podria constituir en si mateix un projecte concret.

12. Glossari

- **LAN** *Local Area Network:* és una xarxa de computadores que abasta un àrea reduïda a una casa, un departament o un edifici.
- **CPD** *Central Process Data*: instal·lació on hi resideixen els sistemes informàtics com ara commutadors, encaminadors i servidors.
- **DNS** *Domain Name Server*: assigna els noms de domini a les adreces IP i la localització dels servidors de correu electrònic.
- **Commutador (switch)**: dispositiu de xarxa que permet agrupar un conjunt de dispositius Ethernet mitjançant un mateix segment de xarxa. És un dispositiu més sofisticat que un hub ja que guarda en memòria les direccions MAC dels equips.
- **ISP** *Internet Service Provider*: empresa subministradora d'accés a Internet.
- **Patch panel** [2]: panell de connexions on va a raure tots els cables d'un cablejat estructurat.
- **Armari Rack**: armari on es posaran els equips de xarxa i els patchs panels.
- **Encaminador (router)** [3]: dispositiu de xarxa que envia els paquets de dades entre xarxes de commutadors i que pertany al nivell 3 de l'OSI.
- **Concentrador (hub)** [4]: dispositiu de xarxa que permet agrupar un conjunt de dispositius Ethernet mitjançant un mateix segment de xarxa.
- **Etherchannel** [5]: tecnologia desenvolupada per Cisco que permet l'agrupació lògica de diferents enllaços físics.
- **STP** *Spanning Tree Protocol*: protocol de xarxa de capa 2 del model OSI que analitza i evita els possibles bucles que es puguin presentar.
- **WAN** *World Area Network*: xarxa de comunicacions a nivell mundial.
- **Core**: equip central d'una xarxa de comunicacions.
- **Stack**: Tecnologia que permet agrupar diferents dispositius físics en 1 de lògic.

- **RIP** *Routing Information Protocol* [6]: protocol de porta d'enllaç intern que utilitzen els routers per trobar el camí més ràpid utilitzant un algorisme de vector-distància.

- **SNMP** *Simple Network Management Protocol*: protocol que permet monitoritzar els equips d'una xarxa.

- **POE** *Power Over Ethernet* [7]: tecnologia que permet alimentar dispositius de xarxa mitjançant un cable Ethernet fins a 15,4 Watts.
-
- **POE+** [7]: tecnologia que permet alimentar dispositius de xarxa mitjançant un cable Ethernet fins a 25,5 Watts.

- **Ethernet**: conjunt de tecnologies basades en les xarxes de computadors LAN per al transport de veu i dades dins d'un mateix estàndard del model OSI.

- **MPLS** *Multiprotocol Layer Switching*: Xarxa privada IP que combina la flexibilitat de les comunicacions punt a punt i la fiabilitat i seguretat dels serveis Frame Relay o ATM. Ofereix alts nivells de rendiment i priorització de tràfic, així com aplicacions de veu i multimèdia.

- **VPLS** *Virtual Private Lan service* [8]: protocol que proporciona un enllaç Ethernet entre connexions multipunt basat en xarxes Ip.

- **VSS** *Virtual Switching system* [9]: Tecnologia Cisco que permet agrupar diferents dispositius Core físics en 1 de lògic permetent un increment en l'eficiència operacional.

- **Firewall**: equip utilitzat dins d'una xarxa informàtica que permet controlar les comunicacions, permetent o prohibint segons les polítiques de seguretat configurades.

- **OSI** [10]: és el model de referència d'Interconnexió de Sistemes Oberts (OSI) llançat el 1984 i va ser el model de xarxa descriptiu creat per l'ISO (Organització internacional per a l'estandardització). Va proporcionar als fabricants un conjunt d'estàndards que van assegurar una major compatibilitat i interoperabilitat entre els diferents tipus de tecnologia de xarxa produïts per les empreses a escala mundial.

- **VPN** *Virtual Private Network*: permet estendre una xarxa privada de manera segura a una xarxa pública.

- **QOS** *Quality Of Service*: protocol que permet la correcta senyalització en xarxes de comunicacions de veu.

- **SSL** *Secure sockets Layer*: protocol que permet la comunicació en una xarxa de manera segura.
- **SSH** *Secure Shell*: intèrpret d'ordres segures.
- **Malware**: Software maliciós que intenta infectar qualsevol dispositiu electrònic.
- **Appliance**: Software desenvolupat per un fabricant per tal de gestionar el dispositiu en qüestió.
- **Exploit**: fragment de dades que intenta infectar un dispositiu mitjançant errors en el software on vulnerabilitats.
- **Threat**: Amenaces cap a un sistema de comunicació de dades provinents d'una xarxa externa.
- **VTP** *Vlan Trunk Protocol* [11]: Protocol de missatge de nivell 2 utilitzat per configurar i administrar Vlans en equips cisco.
- **VLAN** *Virtual Local Area Network*: mètode per crear xarxes virtuals independents dins de la mateixa xarxa local.
- **DHCP** *Dynamic Host Configuration Protocol*: protocol de xarxa que permet a un dispositiu obtenir de manera automàtica els seus paràmetres de xarxa.
- **BPDU** *Bridge Protocol Data Unit* [12]: protocol que envia informació per la xarxa sobre l'estat STP d'aquesta.
- **RDSI** [13]: xarxa telefònica digital basada en commutació de circuits.
- **RTC** *Real Time Clock*: rellotge d'ordinador el qual està integrat dins dels dispositius.
- **SIP** *Session Initiation Protocol*: Protocl estàndard de senyalització en una xarxa de telefonia IP.

13. Webgrafia

13.1 Informació concreta

[1] Gartner, 23 març 2017, http://www.gartner.com/technology/home.jsp

[2] *Wikipedia*, 2 de juny de 2017, https://ca.wikipedia.org/wiki/Patch_panel

[3] *Viquipèdia*, 2 de juny de 2017, https://ca.viquipedia.org/wiki/Encaminador

[4] *Wikipedia*, 2 de juny de 2017, https://es.wikipedia.org/wiki/Concentrador

[5] *Wikipedia*, 2 de juny de 2017, https://es.wikipedia.org/wiki/EtherChannel

[6] *Wikipedia*, 4 de juny de 2017, https://ca.wikipedia.org/wiki/Routing_Information_Protocol

[7] *support.bb*, 4 de juny de 2017, http://support.bb-elec.com/article/14629/26756/POE-Versus-POE

[8] *Wikipedia*, 4 de juny de 2017, https://es.wikipedia.org/wiki/Virtual_Private_LAN_Service

[9] *Cisco Systems*, 5 de juny de 2017, http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-virtual-switching-system-1440/prod_qas0900aecd806ed74b.html

[10] *Viquipèdia*, 5 de juny de 2017, https://ca.viquipedia.org/wiki/OSI

[11] *Wikipedia*, 5 de juny de 2017, https://es.wikipedia.org/wiki/VLAN_Trunking_Protocol

[12] *Wikipedia*, 5 de juny de 2017, https://en.wikipedia.org/wiki/Bridge_Protocol_Data_Unit

[13] *Viquipèdia*, 5 de juny de 2017, https://ca.viquipedia.org/wiki/Xarxa_digital_de_serveis_integrats

13.2 Informació genèrica

dis.um.es, març de 2017, http://dis.um.es/~lopezquesada/documentos/IES_1213/LMSGI/curso/xhtml/xhtml6/tipos%20de%20cableado.html

es.ccm.net, març de 2017, http://es.ccm.net/contents/256-topologia-de-red

Cisco, març de 2017, www.cisco.com

Hewlett Packard, març de 2017, https://www.hpe.com/us/en/networking/switches.html

Huawei, març de 2017, http://e.huawei.com/en/products/enterprise-networking/switches

Paloalto, abril de 2017, https://www.paloaltonetworks.com/

Paloalto, abril de 2017, https://get.info.paloaltonetworks.com/webApp/gartner-magic-quadrant-firewall-en-v2?gclid=COKnzcK-ptQCFccy0wodwWMFpQ&utm_source=google-search&utm_medium=cpc&utm_term=gartner&utm_campaign=Assets-EN-EMEA-Search&utm_content=169930599027&custom2=&CampaignId=70170000000WoZc&s_kwcid=AL!4461!3!169930599027!p!!g!!gartner&ef_id=VIbmSwAAAD55W9vD:20170605102426:s

Gartner, març i abril de 2017, http://www.gartner.com/technology/home.jsp

Wikipedia – Network topology, abril de 2017, https://en.wikipedia.org/wiki/Network_topology

Algo que decir, abril de 2017, http://algoquedecir.over-blog.es/article-que-tipos-centralitas-telefonicas-hay-86149212.html

Prezi, abril de 2017, https://prezi.com/87rpvfjuj7lz/tipos-de-telefonia-redes-telefonicas/

Wikipedia – Network Protocols, maig 2017, https://en.wikipedia.org/wiki/Lists_of_network_protocols

14. Annexos

14.1 Cisco Catalyst 2960x

Los conmutadores de la serie 2960-X ® de Cisco ® Catalyst son de configuración fija, apilables, conmutadores de Gigabit Ethernet que proporcionan acceso de clase empresarial para aplicaciones de campus y sucursales (Figura 1). Permiten operaciones de negocios escalables, seguros y energéticamente eficientes con servicios inteligentes y una amplia gama de tecnologías avanzadas de Cisco IOS ® software.

-

> Principales características del producto

Los Switches Cisco Catalyst 2960-X cuentan con:

- Puertos Ethernet 24 Gigabit o 48 con un rendimiento de reenvío de velocidad de línea
- 1 Gigabit SFP o 10G SFP + uplinks
- FlexStack Plus para el apilamiento de hasta 8 conmutadores con 80 Gbps de rendimiento de la pila (opcional)
- Power over Ethernet Plus (PoE +) con el apoyo de hasta 740W sobre PoE
- Consumo de energía reducido y características avanzadas de gestión de energía
- Las interfaces de administración de Ethernet para simplificar las operaciones y USB
- Visibilidad de aplicaciones y capacidad de planificación integrado con NetFlow-Lite
- LAN Base ® o funciones de software LAN Lite Cisco IOS
- Garantía limitada de por vida mejorada (E-LLW) ofreciendo sustitución de hardware el siguiente día hábil.

Los modelos Cisco Catalyst 2960-XR también ofrecen:

- Capacidad de recuperación de energía con fuentes de alimentación reemplazables en campo duales opcionales
- El software IP Lite Cisco IOS ® con enrutamiento dinámico y funciones de nivel 3

-

> Modelos de switch y configuraciones

Switches Catalyst 2960-X incluyen una fuente de alimentación fija y están disponibles con el Cisco IOS Base LAN o LAN Lite. Modelos de switches Catalyst 2960-XR incluyen una fuente de alimentación modular reemplazable en campo y tienen capacidad para una segunda fuente de alimentación. Catalyst 2960-XR está disponible sólo con el IOS de Cisco IP Lite.

> Catalyst 2960-X series Características del software

Todos los conmutadores de la serie Catalyst 2960-X utilizan un único universal Cisco IOS Software de imagen para todos los SKUs. Dependiendo del modelo del interruptor, la imagen de IOS de Cisco configura automáticamente tanto la LAN Lite, LAN Base o el conjunto de características Lite IP.

Modelos LAN Lite han reducido la funcionalidad y escalabilidad para implementaciones pequeñas con requisitos básicos. Catalyst Cisco 2960-X están disponibles con la LAN Base y LAN Lite.

> Cisco Catalyst 2960-X IP-Lite High-Performance Routing

La arquitectura de enrutamiento de hardware Cisco ofrece muy alto rendimiento de enrutamiento IP en el Cisco Catalyst 2960-XR Switches IP-Lite:

- **Protocolos de enrutamiento IP de unidifusión (estático, Routing Information Protocol Version 1 [RIPv1] y RIPv2, RIPng** son compatibles con las aplicaciones de enrutamiento pequeña red.
- **IP unicast protocolos de enrutamiento avanzado (OSPF de acceso enrutado)** son compatibles con el equilibrio de carga y la construcción de redes de área local escalable. Enrutamiento IPv6 (OSPFv3) es compatible con el hardware para obtener el máximo rendimiento.
- Enrutamiento **de igual costo** facilita Nivel 3 balanceo de carga y redundancia a través de la pila.
- **Enrutamiento basado en políticas (PBR)** permite un control superior al facilitar el cambio de dirección del flujo, independientemente del protocolo de enrutamiento configurado.
- **Protocolo de enrutamiento de Hot Standby (HSRP) y Virtual Router Redundancy Protocol (VRRP)** proporciona balanceo de carga dinámico y conmutación por error para los enlaces enrutados.
- **Protocolo Independent Multicast (PIM)** de multidifusión IP es compatible, incluyendo el modo de escasa PIM (PIM-SM), PIM modo denso (PIM-DM), PIM modo denso y ralo-Specific Multicast fuente (SSM).

> Red de Seguridad

Los conmutadores de la serie Catalyst 2960-X Cisco proporcionan una amplia gama de características de seguridad para limitar el acceso a la red y mitigar amenazas, entre ellas:

- **Cisco TrustSec** SXP **utiliza** para simplificar la seguridad y el cumplimiento de las políticas en toda la red.
- **802.1X** Funciones **integrales** para controlar el acceso a la red, incluyendo autenticación flexible, modo de monitor 802.1x, RADIUS y el cambio de la autorización.
- **Seguridad IPv6 First-Hop** mejora de capa 2 y capa 3 acceso a la red de proliferación de dispositivos IPv6 dispositivos especialmente BYOD. Protege contra la publicidad, la falsificación de direcciones, respuestas DHCP falsas y otros riesgos introducidos por la tecnología IPv6.
- **Sensor y clasificador de dispositivos** permiten perfiles de dispositivos versátiles sin costura incluyendo dispositivos BYOD. También permiten Cisco ISE, políticas de seguridad basadas en la identidad provisión.
- **Confianza Técnica Ancla Cisco (TAT)** permite una fácil distribución de una imagen única y universal para todos los modelos Catalyst 2960-X mediante la verificación de la autenticidad de las imágenes de IOS. Esta tecnología permite el cambio a realizar comprobaciones de

integridad del IOS en el arranque mediante la verificación de la firma, verificando la confianza en Gestión de Activos (TAM) y la autenticación de la licencia.

- Características de **defensa contra amenazas de Cisco,** incluyendo Seguridad Portuaria, Dynamic ARP Inspection y IP Source Guard.
- **VLAN privadas** restringen el tráfico entre hosts en un segmento común mediante la segregación del tráfico en la capa 2, convertir un segmento de difusión en un acceso múltiple de no difusión como segmento. Esta función está disponible en función de IP-Lite establecer solamente.
  - **Private VLAN Edge** proporciona seguridad y aislamiento entre los puertos de conmutación, lo que ayuda a garantizar que los usuarios no pueden espiar el tráfico de otros usuarios.
- **Función Unicast Reverse Path Forwarding (RPF)** ayuda a mitigar los problemas causados por la introducción de las direcciones IP de origen malformados o forjado (falsificado) en una red de paquetes IP descartar que carecen de una dirección IP de origen verificable. Esta función está disponible en función de IP-Lite establecer solamente.
- La **autenticación multidominio** permite un teléfono IP y una PC para autenticar en el mismo puerto del switch mientras que colocarlas en voz apropiada y los datos VLAN.
- **Listas de control de acceso** para PV6 y IPv4 de ACE de seguridad y calidad de servicio.
  - **VLAN ACL** en todas las VLAN evitan los flujos de datos no autorizadas de ser un puente entre las VLAN.
  - **ACL Router** definir las políticas de seguridad en las interfaces enrutadas para el plano de control y tráfico de datos plano.ACL IPv6 se pueden aplicar para filtrar el tráfico IPv6.
  - **Las ACL basadas en puertos** para las interfaces de capa 2 permite políticas de seguridad que se aplicarán en los puertos de conmutación individuales.
- **Secure Shell (SSH) Protocolo, Kerberos y Simple Network Management Protocol versión 3 (SNMPv3)** proporcionan seguridad de red mediante la encriptación del tráfico del administrador durante sesiones Telnet y SNMP. Protocolo SSH, Kerberos y la versión criptográfica de SNMPv3 requieren una imagen de software de cifrado especial debido a las restricciones de exportación de Estados Unidos.
- **Switched Puerto Analyzer (SPAN),** con el apoyo de datos bidireccional, permite que el sistema de detección de intrusiones de Cisco (IDS) para tomar acción cuando se detecta un intruso.
- **TACACS + y autenticación RADIUS** facilita el control centralizado del conmutador y restringe a los usuarios no autorizados de la alteración de la configuración.
- **Notificación de direcciones MAC** permite a los administradores serán notificados de usuarios añadidos o eliminados de la red.
- **La seguridad multinivel en el acceso a la consola** evita que usuarios no autorizados puedan alterar la configuración del switch.
- **Protocolo BPDU** cierra Spanning Tree Port interfaz Fast habilitados cuando se reciben las BPDU para evitar bucles de topología accidentales.
- **Spanning Tree Root Guardia (STRG)** impide que los dispositivos de borde no en el control del administrador de la red se conviertan en nodos raíz Spanning Tree Protocol.
- **Filtrado IGMP** proporciona autenticación de multidifusión mediante la filtración de no suscriptores y limita el número de secuencias de multidifusión simultáneas disponibles por puerto.
- **Asignación de VLAN dinámica** se apoya en la aplicación de la capacidad del cliente VLAN Membresía Policy Server para proporcionar flexibilidad en la asignación de puertos a las VLAN. VLAN dinámica facilita la asignación rápida de direcciones IP.

> Redundancia y flexibilidad

Cisco Catalyst 2960-X Series Switches ofrecen una serie de características de redundancia y resistencia para evitar interrupciones y ayuda a garantizar que la red sigue estando disponible:

- **EtherChannel toda la pila** proporciona la capacidad de configurar la tecnología EtherChannel de Cisco a través de diferentes miembros de la pila para alta resistencia.
- **Flexlink** proporciona redundancia de enlaces con el tiempo de convergencia menos de 100 milisegundos.
- **IEEE 802.1s / w protocolo Rapid Spanning Tree (RSTP) y Multiple Spanning Tree Protocol (MSTP)** proporcionan una rápida convergencia spanning-tree independiente de temporizadores spanning-tree y también ofrecen la ventaja de la capa 2 balanceo de carga y el procesamiento distribuido. Unidades apiladas se comportan como un solo nodo del árbol de expansión.
- **Per-VLAN Rapid Spanning Tree (PVRST +)** permite una rápida reconvergencia spanning-tree en una base per-VLAN spanning-tree, sin que se requiera la aplicación de instancias de spanning-tree.
- **Cisco Hot Standby Router Protocol (HSRP)** el apoyo para crear redundante, falla de enrutamiento seguro topologías en 2960-XR SKUs IP-Lite.
- **Switch-puerto de auto-recuperación (Error Deshabilitar)** intenta automáticamente para reactivar un enlace que está desactivado debido a un error de red.
- **redundancia de la potencia** con una segunda fuente de alimentación opcional en los modelos XR-2960, o con un RPS externos en los modelos 2960-X.

> Mejora de la calidad de servicio

El Cisco Catalyst 2960-X Series Switches ofrece una gestión inteligente del tráfico que mantiene que todo fluya sin problemas. Mecanismos flexibles para el marcado, la clasificación y programación ofrecen un rendimiento superior para datos, voz y tráfico de vídeo, todo ello a velocidad de cable. Las características principales de QoS incluyen:

- Hasta **ocho colas de salida** por puerto (cuatro en el 2960-X o al apilar el 2960-XR) y la estricta gestión de colas de prioridad para que los paquetes de mayor prioridad son accesibles por delante de el resto del tráfico.
- **Round Robin** programación **en forma de** (SRR) **y** soltar **la cola ponderada** (DMP) para evitar la congestión.
- **Velocidad de flujo basado en** la **limitación** y hasta 256 agregados o policers individuales por puerto.
- **Clase de servicio 802.1p** (CoS) y **servicios diferenciados punto de código** (DSCP) la clasificación, con el marcado y reclasificación en función de cada paquete de origen y destino IP, la dirección MAC o la Capa 4 número de puerto TCP / UDP.
- **Toda la pila** para permitir **QoS** QoS se configura a través de una pila de 2960 X switches de la serie.
- La función de **la tasa de información comprometida Cisco (CIR)** proporciona ancho de banda en incrementos tan bajos como 8 kbps.
- **Tasa** se proporciona **limitación** basada en la Capa 4 TCP / UDP información de origen y la dirección IP de destino, el origen y la dirección MAC de destino, o cualquier combinación de estos campos, el uso de QoS ACL (ACL IP o ACL MAC), mapas de clase, y los mapas de la política.

> Cisco FlexStack-Plus

•

Cisco FlexStack-Plus ofrece apilar hasta ocho switches 2960-X con el módulo opcional FlexStack-Plus.

El módulo FlexStack-Plus es intercambiable en caliente y se puede agregar a cualquier Cisco Catalyst 2960-X o Catalyst 2960-X con una ranura FlexStack-Plus. Switches conectados a una pila pasará

automáticamente a ser de Cisco IOS Software versión de la pila y transparente unirse a la pila sin intervención adicional.

Cisco FlexStack-Plus y Cisco IOS Software ofrecen cierto apilamiento, con todos los conmutadores en una pila que actúa como un detector individual. FlexStack-Plus proporciona un plano unificado de datos, configuración unificada y única dirección IP para la gestión de cambio. Las ventajas del verdadero apilamiento incluyen un menor costo total de propiedad y una mayor disponibilidad a través de una gestión simplificada, así como a través del stack, incluyendo EtherChannel, SPAN y FlexLink.

14.2 Catalyst 3850-12S

El Cisco®Catalyst® 3850 Series es la próxima generación de clase empresarial Ethernet apilable y de acceso y agregación de switches de capa multigigabit Ethernet que proporcionan una convergencia total entre cableada e inalámbrica en una sola plataforma. nuevos Unified Access Data Plane (Uadp) circuito integrado (ASIC) poderes específicos de la aplicación de Cisco el interruptor y permite la aplicación uniforme por cable, inalámbrica política, visibilidad de las aplicaciones, la flexibilidad y optimización de aplicaciones. Esta convergencia se basa en la capacidad de adaptación de la nueva y mejorada tecnología de Cisco StackWise-480. Los conmutadores de la serie Cisco Catalyst 3850 soportan completa IEEE 802.3 en Power over Ethernet Plus (PoE +), de alimentación universales de Cisco a través de Ethernet (Cisco UPOE), módulos de red modulares y reemplazables en el campo, interfaces de enlace descendente RJ45 y basados en fibra, y ventiladores redundantes y poder suministros. Con velocidades que alcanzan los 10 Gbps, el Cisco Catalyst 3850 multigigabit pueden soportar velocidades inalámbricas actuales y de próxima generación y estándares (incluyendo 802.11ac Wave 2) en la infraestructura de cableado existente.

> Descripción del producto

-
- Capacidad de controlador inalámbrico integrado con:
  - Hasta 40 G de capacidad inalámbrica por switch (modelos de 48 puertos).
  - Admite hasta 100 puntos de acceso y 2000 clientes inalámbricos en cada entidad de switching (switch o pila).
- Modelos:
  - Modelos de 24 y 48 puertos 10/100/1000 de datos y PoE+ y Cisco UPOE con Ethernet de óptimo rendimiento energético (EEE, energy-efficient Ethernet).
  - Modelos 24 y 48 de 100 Mbps / 1 / 2.5 / 5/10 Gbps de Cisco UPOE con Ethernet de óptimo rendimiento energético (EEE, energy-efficient Ethernet).
  - Modelos de 12 y 24 puertos modelos basados en SFP Gigabit Ethernet
  - Modelos de 12 y 24 puertos 1/10 Gigabit Ethernet SFP +
  - Modelos de 48 puertos 1/10 Gigabit Ethernet SFP + con 4 enlaces ascendentes fijos a 40 Gigabit Ethernet QSFP +

- La tecnología Cisco StackWise-480 proporciona escalabilidad y recuperabilidad con capacidad de apilamiento de 480 Gbps.
- La tecnología Cisco StackPower™ proporciona apilamiento de energía entre los miembros de la pila para obtener redundancia de alimentación.
- Tres módulos ascendentes opcionales con 4 puertos Gigabit Ethernet, 2 o 4 puertos 10 Gigabit Ethernet.
- Fuentes de alimentación modulares, redundantes y duales y tres ventiladores modulares que proporcionan redundancia.
- Totalmente compatible con IEE 802.3at (PoE+), con 30 W de potencia en todos los puertos en un factor de forma de 1 unidad de bastidor (RU, rack unit).

14.3 Cisco Catalyst 6840-X

Network traffic has grown exponentially over the last several years, and this trend is expected to continue into the foreseeable future. By 2018, there will be 20+ billion networked devices, up from 10 billion in 2011. Business IP traffic is expected to reach 13.1 exabytes per month in 2016[1]. Networks must be capable of scaling well beyond the needs of today to deal with the traffic of tomorrow while at the same time providing investment protection.

The Cisco® Catalyst® 6840-X Series Switch (Figure 1) is a 2RU fixed backbone switch in the Cisco Catalyst 6800 family. The 6840-X is based on the Cisco Catalyst 6800, with more than 3000 features and maturity of software code. The Cisco Catalyst 6840-X is the smallest Multiprotocol Label Switching (MPLS) aggregator or Instant Access controller in the Cisco 6800 Catalyst Family. The 6840-X offers the following four SKUs:

- 16 and 32 ports of 10G SFP/SFP+
- 24 and 40 ports of 10G SFP/SFP+ with 2 Native uplink ports of 40G QSFP

This 10G/40G-ready platform is ideal for those who want to introduce premium 10G services in small or midsize campus backbones. This unique platform offers 10G port density, full IPv4/IPv6 and MPLS/VPLS functionality with large table sizes (up to 256,000 FIB entries), and more than 15 years of best-in-class features. With a full suite of L2/L3, virtualization, security, multicast, IPv6, application visibility, smart operations, and rich media services, the Cisco Catalyst 6840-X delivers unprecedented capabilities on day one. This platform also runs on the same architecture as the Cisco Catalyst 6500 Supervisor Engine 2T and therefore offers stability with proven operating system software.

The Cisco Catalyst 6840-X Series chassis offers integrated resiliency by providing 1+1 power supply redundancy, single removable fan-tray with four redundant fans, and support for Virtual Switching System (VSS), thereby limiting network downtime, and makes sure of workforce productivity, customer satisfaction, and profitability.

Cisco Catalyst 6840-X Product Details

The Cisco Catalyst 6840-X provides flexibility to build desired port density through four chassis versions. The four models come with a minimum of fixed 16x10G ports and up to 40x10G ports using SFP/SFP+. Two of the models come with 2x40G uplink ports with native QSFP. Table 1 outlines the 6840-X models and their capabilities.

Table 1. 6840-X Models and Capabilities

6840-X Models	C6816-X-LE	C6832-X-LE	C6824-X-LE-40G	C6840-X-LE-40G
Native Optics	SFP/SFP+	SFP/SFP+	SFP/SFP+ and QSFP	SFP/SFP+ and QSFP
Number of 10G Ports	16	32	24 + 8 using breakout cable	40 + 8 using breakout cable
Number of 40G Ports	0	0	2	2
Features	Full-feature L2/L3 with MPLS, VPLS, IPv4/IPv6 capabilities, 512K Netflow	Full-feature L2/L3 with MPLS, VPLS, IPv4/IPv6 capabilities, 1M Netflow	Full-feature L2/L3 with MPLS, VPLS, IPv4/IPv6 capabilities, 1M Netflow	Full-feature L2/L3 with MPLS, VPLS, IPv4/IPv6 capabilities, 1.5M Netflow
Additional Hardware Features	Large buffers, SGT, MACSec, LISP, dual priority queues, two-level shaping, Instant Access	Large buffers, SGT, MACSec, LISP, dual priority queues, two level shaping, Instant Access	Large buffers, SGT, MACSec, LISP, dual priority queues, two-level shaping, Instant Access	Large buffers, SGT, MACSec, LISP, dual priority queues, two-level shaping, Instant Access

Figure 1. Cisco Catalyst 6840-X Series Chassis with All Four SKUs

The Cisco Catalyst 6840-X Series offers premium Campus Backbone features and benefits, including:

- **Platform scalability:** The platform supports up to 960Gbps of switching capacity, which doubles up to 1.92Tbps with VSS technology.
- **Security:** Support for Cisco TrustSec® to provide IEEE 802.1AE MACsec encryption and role-based ACL, CoPP to prevent DoS attacks, and Cisco ISE to safeguard and manage end-to-end security for the enterprise.
- **Virtualization:** Comprehensive suite of virtualization features, including L2/L3 VPN, full MPLS, EVN, VRF-aware applications for NAT Netflow, GRE for v4/v6, L2 extensions with VPLS, and so on to segment different user groups and serve unique security/QoS policy requirements of each of these diverse user groups.
- **Application visibility and control (AVC):** Supports enhanced application monitoring such as Flexible and Sampled NetFlow and advanced priority queuing capabilities such as Hierarchical QoS.
- **Smart operations:** The Cisco Catalyst 6840-X supports Cisco Catalyst Instant Access*, which allows an Instant Access client to act as a remote line card of the Cisco Catalyst 6840-X, as well as Smart Install Director, which provides zero-touch deployment of access switches.
- **High availability:** Two Cisco Catalyst 6840-X Series Switches can be combined into a VSS. In addition to high availability VSS, provides ease of operation by providing a single point of management, eliminating the need for First Hop Routing Protocol (FHRP) and removing the reliance on Spanning Tree Protocol (STP) for link failure restoration.

14.4 HP 3com 5130

The HPE 5130 EI Switch Series comprises Gigabit Ethernet switches that support static and RIP Layer 3 routing, diversified services, and IPv6 forwarding, as well as provides four 10-Gigabit Ethernet (10GbE) interfaces. Unique Intelligent Resilient Fabric (IRF) technology creates a virtual fabric by managing several switches as one logical device, which increases network resilience, performance, and availability, while reducing operational complexity. These switches provide Gigabit Ethernet access and can be used at the edge of a network or to connect server clusters in small data centers. High availability, simplified management, and comprehensive security control policies are among the key features that distinguish this series.

14.5 HPE 5700

La serie de conmutadores HPE FlexFabric 5700 proporciona una puerta abierta para la expansión de la red empresarial mediante la adición de capacidad con conmutación local y soporte L2/Light L3. Aproveche las ventajas de las mejoras de IRF para las configuraciones spine/leaf, para simplificar la gestión de la red y ampliar la conectividad de servidor.

Capacidad de recuperación y facilidad de gestión vienen de la mano con el FlexFabric 5700. Al mismo tiempo que IRF reduce las complejidades de gestión hasta en un 88 %, también ofrece < 50 ms de tiempo de convergencia.

Puede confiar en FlexFabric 5700 para reducir el coste total de propiedad con un coste hasta un 25 % menor que con los dispositivos de la competencia.

› Características

Amplíe su red de centro de datos con seguridad

La serie de conmutadores HPE FlexFabric 5700 amplía su red empresarial mediante la adición de la capacidad de conmutación local para una mejor capacidad de ampliación, por lo que usted puede admitir más clientes.
Hasta treinta (30) conmutadores HPE FlexFabric pueden añadirse a la red y gestionarse a través de un conmutador de control de puente (CB), mejorando la conectividad de servidor.
La serie de conmutadores FlexFabric 5700 le ofrece opciones que se adaptan a su presupuesto y al medio ambiente ofreciendo puertos 1/10 GbE, compatibles con SFP y la BASE-T con vínculos superiores 10/40 GbE.

Conmutación de centro de datos de alto rendimiento

La serie de conmutadores HPE FlexFabric 5700 ofrece hasta 960 Gbps de capacidad de conmutación para las aplicaciones más exigentes.
Proporciona conmutación local y participa en la red, a diferencia de los puertos multiplexores de la competencia.
Baja latencia, menos de 1,5 µs de latencia de 10 GbE, proporciona un rendimiento mejorado y menos pérdida de paquetes.

Agilidad del negocio y resiliencia con Comware 7

La serie de conmutadores HPE FlexFabric 5700 ofrece un tiempo de convergencia IRF <50 ms lo que permite un menor tiempo de respuesta de la aplicación.
La serie de conmutadores 5700 es compatible con spine/leaf ORF para mejorar la agilidad de la red con ECMP y una convergencia más rápida.
La actualización de Software en servicio (ISSU) permite la alta disponibilidad con las actualizaciones que se llevan a cabo sin un ciclo de alimentación o reiniciar el sistema, en el fondo.

Simplicidad y TCO inferior

La serie de conmutadores HPE FlexFabric 5700 simplifica la administración del conmutador hasta el 88% con IRF.
Sin costes ocultos de licencias de software, todas las características de SO incluidas con la compra del conmutador.
Automatice las tareas pesadas con la red definida por software (SDN) y recupere los recursos desperdiciados.

14.6 HPE Flexfabric 5930

La serie de conmutadores HPE FlexFabric 5930 proporciona funciones avanzadas y alto rendimiento en una arquitectura de conmutador de centro de datos para la parte superior del bastidor. El 5930, que consta de un conmutador 1U de 32 puertos 40 GbE QSFP+, una versión modular de 2 ranuras con 2 puertos 40 GbE y una versión modular de 4 ranuras, ofrece alta densidad en un espacio reducido.

El IRF de 9 unidades reduce las complejidades de la gestión en hasta un 88 %, a la vez que ofrece < 50 ms de tiempo de convergencia. Puede confiar en la serie de conmutadores FlexFabric 5930 para mejorar la utilización de conmutador y reducir el coste total de propiedad, al tiempo que ofrece alta disponibilidad y resistencia del negocio.

> Características

Conmutadores de centro de datos avanzados de alta densidad

La serie de conmutadores HPE FlexFabric 5930 está disponible con factores de forma 1RU de 32 puertos de 40 GbE QSFP+, 2RU de 2 ranuras con 2 40 GbE QSFP+ y 2RU de 4 ranuras.
Los puertos de 40 GbE pueden dividirse en cuatro puertos de 10 GbE cada uno para un total de 96 puertos de 10 GbE con 8 enlaces ascendentes de 40 GbE por conmutador.
Las opciones de puerto modular incluyen 10 GbE SFP+, 10GBASE-T, puertos convergentes que admiten 1/10 GbE y canal de fibra 4/8 Gbps y QSFP+ 40 GbE.

Conmutación de centro de datos de alto rendimiento

La serie de conmutadores HPE FlexFabric 5930 ofrece hasta 2,56 Tbps de capacidad de conmutación para las aplicaciones más exigentes.
Admite hasta 1.492 MPPS para entornos con gran cantidad de datos.
La baja latencia, menos de 1,5 µs de latencia de 10 GbE, proporciona agilidad al negocio.
Soporte VXLAN para la virtualización de red y las soluciones de recubrimiento.
OVSDB para la gestión de túnel VXLAN dinámica

Agilidad del negocio y resiliencia con Comware 7

La serie de conmutadores HPE FlexFabric 5930 ofrece un tiempo de convergencia IRF <50 ms, para un menor tiempo de respuesta de la aplicación.
La actualización de Software en servicio (ISSU) permite la alta disponibilidad con las actualizaciones que se llevan a cabo sin un ciclo de alimentación o reiniciar el sistema, en el fondo.

Simplicidad y TCO inferior

La serie de conmutadores HPE FlexFabric 5930 simplifica la gestión del conmutador hasta un 88 % con Intelligent Resilient Fabric (IRF) de 9 unidades.
No hay costes adicionales ocultos, con una sencilla licencia por conmutador para todas las funciones del sistema operativo.
Todos los puertos de conmutador están activos y listos para usar sin necesidad de licencias de activación.
Automatice las tareas pesadas con una red definida por software (SDN) y recupere los recursos desperdiciados.

14.7 Huawei S1720-52GWR-4X

Innovative energy-saving design

The S1700/S1720/1720-E supports Energy Efficient Ethernet (EEE), which enables the switch to enter a power-saving mode when traffic is light.

The S1700 can adjust the power output for transmissions based on the cable length. It can also set any ports that are not transmitting traffic to sleep mode.

The models that use a fan-free design reduce power consumption and noise.

Non-blocking and high-speed forwarding

All S1700 ports provide Layer 2 wire-speed forwarding capabilities to ensure non-blocking packet forwarding. S1700 models provide optical and electrical GE uplink ports, which facilitate user access and are cost-effective.

The S1700/S1720/S1720-E MAC address table supports up to 8K/16K/16K of MAC addresses, making it easy to expand networks and deploy new services. The S1700 support layer 3 static routing-forwarding which include IPv4 and IPv6 protocols. The S1720-E support RIP, RIPng, OSPF.

Convenient management and maintenance

The S1700 is easy to manage and maintain, being equipped with a one-key operation button on the front panel.

Web-managed S1700 models come with a web network management system, making it easy to configure switches.

Web/SNMP-based S1700 models allow for the use of an SNMP-based NMS for centralized configuration and management.

Web/SNMP-based S1720/S1720-E models can support CLI and console port configuration.

Powerful security performance

The S1700 provides a range of security features, including 802.1x, RADIUS, Portal and NAC. The S1700 also supports packet filtering based on MAC addresses or ports in order to defend against hackers and virus attacks.

Great networking and bandwidth extensibility

The S1700 provides LACP, STP, RSTP and MSTP functions to implement link aggregation and backup. S1720 switches support up to 64 MSTP instances for flexible networking.

The S1700 series enterprise switches (S1700s) are next-generation energy-saving Ethernet access switches. The S1700 uses high-performance hardware, which offers a wide array of features to help customers build secure, reliable, high-performance networks. The S1700 is easy to install and maintain, and is ideal for small-size and medium-size enterprises, Internet cafes, hotels, and schools.

The S1700 consists of unmanaged switches, a web-managed switch and Web/SNMP-based switches:

・Unmanaged switches include the S1700-24-AC, S1700-52R-2T2P-AC, S1724G, S1700-24GR and S1700-16G

・The web-managed switches include the S1728GWR-4P, S1720-10GW-2P, S1720-10GW-PWR-2P, S1720-28GWR-4P, S1720-28GWR-4X, S1720-28GWR-PWR-4P, S1720-28GWR-PWR-4X, S1720-52GWR-4P, S1720-52GWR-4X, S1720-52GWR-PWR-4P, S1720-52GWR-PWR-4X, S1720-28GWR-PWR-4TP

・Web/SNMP-based switches include the S1700-28FR-2T2P-AC, S1700-28GFR-4P-AC, S1700-52FR-2T2P-AC, S1700-52GFR-4P-AC, S1720-20GFR-4TP and S1720-28GFR-4TP, S1720-10GW-2P-E, S1720-10GW-PWR-2P-E, S1720-28GWR-4P-E, S1720-28GWR-4X-E, S1720-28GWR-PWR-4P-E, S1720-28GWR-PWR-4TP-E, S1720-28GWR-PWR-4X-E, S1720-52GWR-4P-E, S1720-52GWR-4X-E, S1720-52GWR-PWR-4P-E, S1720-52GWR-PWR-4X-E

14.8 Huawei S5720-32x

Item		S5700(S)-LI/S5710-LI*	S5700-SI*	S5700-EI/S5710-EI/S5720-EI*	S5700-HI/S5710-HI/S5720-HI*
Fixed Port	EI	S5720-32X-EI-24S-AC: 24×100/1000Base-X SFP, 4×10/100/1000Base-T, 4×10GE SFP+			
MAC address table		IEEE 802.1d compliance			
		MAC address learning and aging			
		Static, dynamic, and blackhole MAC address entries			
		Packet filtering based on source MAC addresses			
		MAC address entries: S5700S-LI series: 8K, S5700-LI/S5700-SI series: 16K, S5700-EI series: 32K, S5720-EI series: 64K, S5700-HI series: S5700-HI: 32K, S5710-HI: 456K, S5720-HI: 128K			
VLAN		4K VLANs			
		Guest VLAN and voice VLAN			
		GVRP			
		MUX VLAN			
		VLAN assignment based on MAC addresses, protocols, IP subnets, policies, and ports			
		1:1 and N:1 VLAN Mapping			
		SuperVLAN(supported by the S5700-SI/S5700-EI/S5700-HI series)			
Ring protection		RRPP ring topology and RRPP multi-instance			
		Smart Link tree topology and Smart Link multi-instance, providing the millisecond-level protection switchover			
		SEP			
		ERPS(G.8032） (supported by the S5700-LI/S5700-SI/S5700-EI/S5700-HI series)			
		STP, RSTP, and MSTP			
		BPDU protection, root protection, and loop protection			
		BPDU Tunnel			
Reliability		Ethernet OAM (IEEE 802.3ah and 802.1ag)			
		ITU-Y.1731			
		DLDP			
		LACP			
		E-Trunk(supported by the S5700-SI/S5700-EI/S5700-HI series)			
		BFD for OSPF, BFD for IS-IS, BFD for VRRP, and BFD for PIM (supported by the S5700-EI/S5700-HI series)			

MPLS features	MPLS L3VPN
	MPLS L2VPN(VPWS/VPLS)
	MPLS-TE
	MPLS QoS
	Notes: supported by S5710-EI, S5700-HI and S5710-HI
IP routing	Static routing
	RIPv1, RIPv2 and RIPng,ECMP(supported by the S5700-SI/S5700-EI/S5700-HI series)
	OSPF, OSPFv3, IS-IS, IS-ISv6, BGP and BGP4+ (supported by the S5700-EI/S5700-HI series)
IPv6 features	Neighbor Discovery (ND)
	Path MTU (PMTU)
	IPv6 ping, IPv6 tracert, and IPv6 Telnet
	ACLs based on the source IPv6 address, destination IPv6 address, Layer 4 ports, or protocol type
	MLD v1/v2 snooping
	6to4 tunnel, ISATAP tunnel, and manually configured tunnel(supported by the S5700-SI/S5700-EI/S5700-HI series)
Multicast	IGMP v1/v2/v3 snooping and IGMP fast leave
	Multicast forwarding in a VLAN and multicast replication between VLANs
	Multicast load balancing among member ports of a trunk
	Controllable multicast
	Port-based multicast traffic statistics
	IGMP v1/v2/v3, PIM-SM, PIM-DM, PIM-SSM, MSDP (supported by the S5700-EI/S5700-HI series)
QoS/ACL	Rate limiting on packets sent and received by an interface
	Packet redirection
	Port-based traffic policing and two-rate three-color CAR
	Eight queues on each port
	WRR, DRR, SP, WRR+SP, and DRR+SP queue scheduling algorithms
	WRED (supported by the S5710-EI and S5700-HI)
	Re-marking of the 802.1p priority and DSCP priority
	Packet filtering at Layers 2 through 4, filtering out invalid frames based on the source MAC address, destination MAC address, source IP address, destination IP address, TCP/UDP port number, protocol type, and VLAN ID
	Rate limiting in each queue and traffic shaping on ports
Security	User privilege management and password protection
	DoS attack defense, ARP attack defense, and ICMP attack defense
	Binding of the IP address, MAC address, interface, and VLAN
	Port isolation, port security, and sticky MAC
	MFF
	Blackhole MAC address entries
	Limit on the number of learned MAC addresses
	802.1x authentication and limit on the number of users on an interface
	AAA authentication, RADIUS authentication, HWTACACS authentication, and NAC
	SSH v2.0
	Hypertext Transfer Protocol Secure (HTTPS)
	CPU defense
	Blacklist and whitelist
Access Security	DHCP Relay, DHCP Server, DHCP Snooping, DHCP Security
Management and maintenance	Virtual cable test
	Port mirroring and RSPAN (remote port mirroring)
	Remote configuration and maintenance using Telnet
	SNMP v1/v2c/v3
	RMON
	Web NMS
	HGMP
	System logs and alarms of different levels
	802.3az EEE (supported by the S5700(S)-LI, S5710-EI, S5700-HI and S5710-HI)
	Dying gasp (supported by the S5700-HI, S5710-HI and S5700(S)-LI(except battery LAN switches)
	NetStream (supported by the S5710-EI, S5700-HI and S5710-HI)

14.9 S7703 16p

Item	S7703	S7706	S7712
Switching capacity	1.92 Tbps	3.84 Tbps/5.12 Tbps	3.84Tbps/5.12 Tbps
Forwarding performance	576 Mpps/1440 Mpps	1152 Mpps/2880 Mpps	1344 Mpps/3360 Mpps
Service Slot	3	6	12
VLAN	Three types of interfaces: access, trunk, and hybrid		
	Default VLAN		
	VLAN switching		
	QinQ and selective QinQ		
	MAC address-based VLAN assignment		
MAC address	MAC address learning and aging		
	Static, dynamic, and blackhole MAC address entries		
	Packet filtering based on source MAC addresses		
	Limit on the number of MAC addresses learned on ports and VLANs		
Ring Protection	STP(IEEE 802.1d), RSTP(IEEE 802.1w), and MSTP(IEEE 802.1s)		
	SEP		
	BPDU protection, root protection, and loop protection		
	BPDU tunnel		
	ERPS(G.8032)		
IP routing	IPv4 routing protocols, such as RIP, OSPF, BGP, and IS-IS		
	IPv6 dynamic routing protocols, such as RIPng, OSPFv3, ISISv6, and BGP4+		
Multicast	IGMPv1/v2/v3 and IGMP v1/v2/v3 snooping		
	PIM-DM, PIM-SM, and PIM-SSM		
	MSDP and MBGP		
	Fast leave		
	Multicast traffic control		
	Multicast querier		
	Multicast packet suppression		
	Multicast CAC		
	Multicast ACL		
MPLS	Basic MPLS functions		
	MPLS OAM		
	MPLS-TE		
	MPLS VPN/VLL/VPLS		
CSS switch fabric clustering	CSS Switch Fabric Clustering (S7706 and S7712)		
Service port clustering	Service Port Clustering (S7706 and S7712)		
Reliability	LACP and E-Trunk between devices		
	VRRP and BFD for VRRP		
	BFD for BGP/IS-IS/OSPF/static route		
	NSF and GR for BGP/IS-IS/OSPF/LDP		
	TE FRR and IP FRR		
	Ethernet OAM (IEEE 802.3ah and 802.1ag)		
	ITU-Y.1731		
	DLDP		
	ISSU		
QoS	Traffic classification based on Layer 2 protocol packet header, Layer 3 protocol information, Layer 4 protocol information, and 802.1p priority		
	ACL, CAR, re-mark, and scheduling		
	Queue scheduling algorithms including SP, WRR, DRR, SP+WRR, and SP+DRR		
	Congestion avoidance mechanisms, such as WRED and tail drop		
	Traffic shaping		
Configuration and maintenance	Easy Operation		
	Console and SSH terminals		
	Network management protocols, such as SNMPv1/v2/v3		
	File uploading and downloading using FTP and TFTP		
	BootROM upgrade and remote upgrade		
	Hot patches		
	User operation logs		
Security and management	802.1x authentication and portal authentication		
	NAC		
	RADIUS and HWTACACS authentication		
	Different user levels for commands, preventing unauthorized users from using certain commands		
	Defense against DoS attacks, TCP SYN Flood attacks, UDP Flood attacks, broadcast storms, and heavy traffic attacks		
	1K CPU queues		