IMPLEMENTACIÓN DE UNA RED MPLS

Pablo Ceballos Becerril
Telemática
Integración de Redes Telemáticas

José López Vicario
Pere Tuset Peiró

Fecha Entrega
09/06/2019


Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons

Copyright © 2019 PABLO CEBALLOS BECERRIL.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled "GNU Free Documentation License".

C) Copyright

© (Pablo Ceballos Becerril)
Reservados todos los derechos. Está prohibido la reproducción total o parcial de esta obra por cualquier medio o procedimiento, comprendidos la impresión, la reprografía, el microfilme, el tratamiento informático o cualquier otro sistema, así como la distribución de ejemplares mediante alquiler y préstamo, sin la autorización escrita del autor o de los límites que autorice la Ley de Propiedad Intelectual.

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Implementación de una red MPLS*
Nombre del autor:	*Pablo Ceballos Becerril*
Nombre del consultor/a:	*José López Vicario*
Nombre del PRA:	*Pere Tuset Peiró*
Fecha de entrega (mm/aaaa):	06/2019
Titulación:	*Telemática*
Área del Trabajo Final:	*Integración de Redes Telemáticas*
Idioma del trabajo:	*Castellano*
Palabras clave	*RED, SERVICIOS, MPLS*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados y conclusiones del trabajo.*

La finalidad del presente proyecto es comprender cómo funciona una red de comunicaciones en su totalidad. Hemos supuesto que, como ingenieros de telecomunicaciones, nos encargan el diseño y la implementación de toda una red corporativa. Partiendo de la información que nos reporta el pliego de prescripciones técnicas facilitado por la entidad que encomienda el proyecto, se ha diseñado la topología de red, en base a dicho diseño, se ha elegido el hardware que conforma cada una de las soluciones presentes en el proyecto. El criterio seguido para ello ha sido la excelencia del fabricante en su sector de mercado, el vanguardismo del equipo seleccionado y las características técnicas que más se adecuen al escenario planteado.

Para dejar reflejado el funcionamiento de la red de manera global, nos hemos apoyado en el modelo OSI, de esta forma, hemos ido describiendo todos las características, servicios y funcionalidades de la red apoyándonos en cada una de las capas de dicho modelo.

Gracias a la descripción de todos los elementos presentes en cada capa del modelo OSI que forman parte de la solución propuesta, hemos obtenido como resultado los flujos de trabajo, donde se muestra el funcionamiento completo de la red.

La principal conclusión que podemos extraer es que, aunque el mundo de las telecomunicaciones esté dividido en sectores como, seguridad, comunicaciones, sistemas, etc., una red funciona como un único conjunto, cuyos elementos están todos relacionados entre sí, por tanto, el ingeniero deberá tener una visión completa, detallada y profunda.

Abstract (in English, 250 words or less):

The purpose of this project is to understand how a communications network works in its entirety. As telecommunications engineers, we assume we are entrusted with the design and implementation of an entire corporate network. Based on the available information supplied by technical specifications provided by the company that commissions the project, the network topology has been designed. Based on this, the hardware which makes up each of the solutions present in the project has been chosen. The followed criteria was the manufacturer excellence in its market, the avant-garde of the equipment selected and the technical characteristics that suits better with the scenario.

In order to reflect the performance of the network in a global way, we have relied on the OSI model. In this way, we have been describing all characteristics, services and functionalities of the network, leaning on each of the layers of this model.

Thanks to the description of all the elements present in each layer of the OSI model of the proposed solution, we have obtained as a result the workflows, where the complete functioning of the network is shown.

Bearing in mind the world of telecommunications is divided into sectors such as security, communications, systems, etc., the main achievement we have reached is a network which works as a single set, being all the elements related to each other, therefore, the engineer must have a complete overview.

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

El proyecto nace como respuesta a la necesidad de una gran corporación de desarrollar una red de comunicaciones propia que permita gestionar de forma centralizada todos los servicios telemáticos de las distintas sedes que la conforman.
La red de comunicaciones es el pilar fundamental sobre el que se sustenta cualquier empresa, ya que, sea cual sea el sector al que pertenezca, en un porcentaje muy elevado, su gestión, el desarrollo del negocio o la función que lleve a cabo, se efectúa a través de sistemas informáticos.
Para acotar el planteamiento, como punto de partida, se supondrá que hemos sido contratados por la UOC con el fin de implementar una nueva red de comunicaciones para su comunidad educativa en la ciudad de Barcelona.
Se diseñará una red provista de todos los requerimientos necesarios para el desarrollo de la actividad docente por parte de la comunidad, dotándola de todas las garantías y servicios necesarios.

1.2 Objetivos del Trabajo

El objetivo del proyecto es desarrollar una red de servicios de telecomunicaciones que proporcione los siguientes elementos:

Elementos de diseño: Escalabilidad, modularidad, segmentación, tolerancia a fallos y redundancia física.

Elementos de configuración: Desarrollo de un protocolo de enrutamiento interno y externo, protocolo MPLS, protocolo de nivel 2 STP, sucurización de la red, redundancia lógica, servicios de DHCP, DNS, telefonía IP, acceso a internet, gestión de ancho de banda, balanceo de tráfico, QoS, etc.

1.3 Enfoque y método seguido

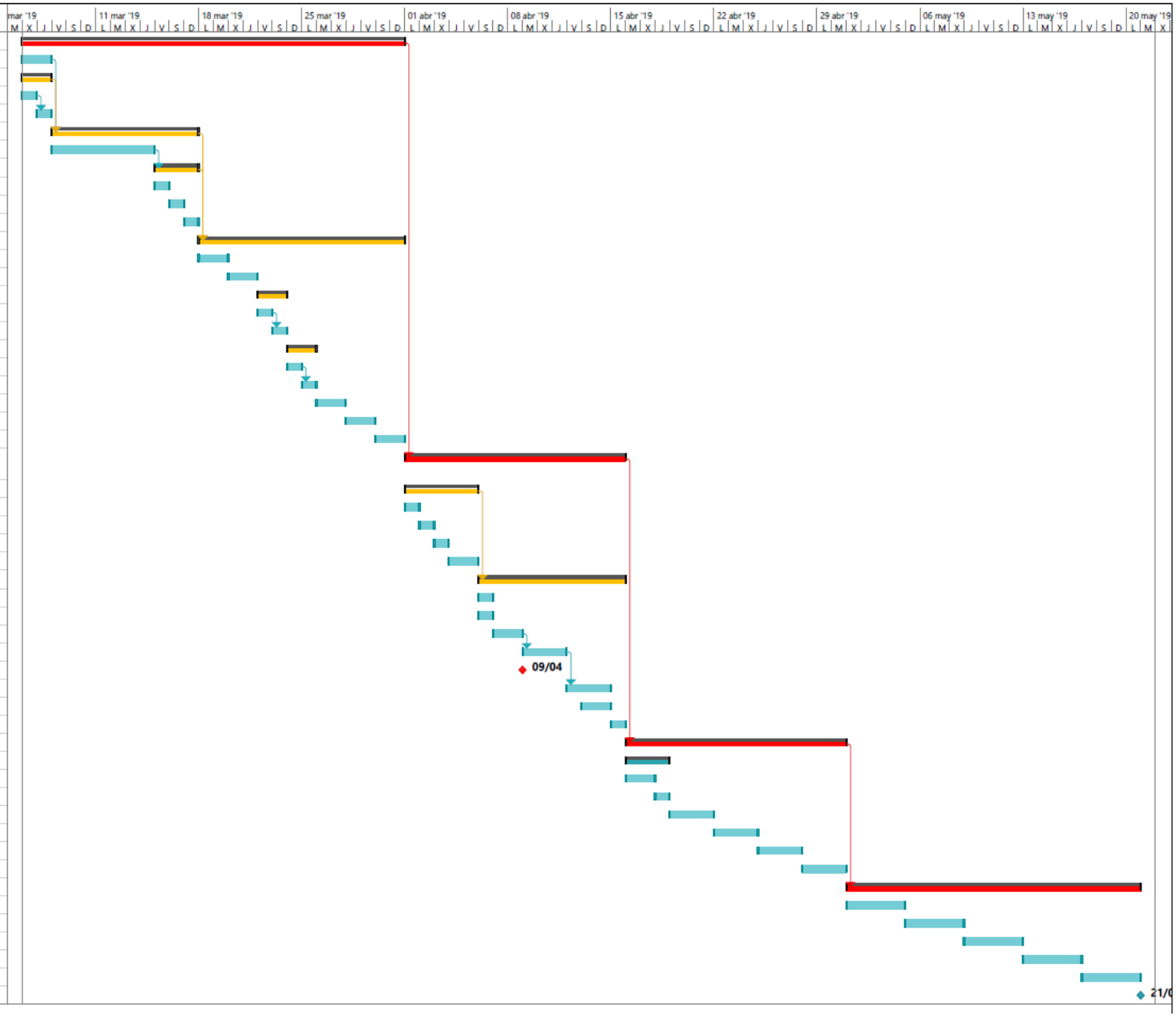
Para elaborar el proyecto se ha seguido un enfoque global de una red de comunicaciones. A lo largo de los estudios en tecnología de telecomunicaciones se han cursado asignaturas de redes, seguridad, telemática, etc. Pero ¿cómo funciona una red de telecomunicaciones en su totalidad? Es decir, ¿cómo interactúan entre si las distintas capas del modelo OSI? El método aplicado consiste en implementar una solución que sea capaz de explicar todos los procesos de comunicación desde el nivel físico hasta la capa de aplicación.

Tanto los usuarios de internet como los trabajadores del mundo de las redes informáticas, normalmente, solo tienen noción de una parte de los sucesos que intervienen en la comunicación. Por ejemplo, el usuario final solo ve que, a través de una conexión a una toma de red, la información que solicita viene y va, podemos decir que vive en la capa de aplicación. Un miembro del departamento de redes puede gestionar el switch al que se conecta dicho usuario, trabaja en la capa 2-3 del modelo OSI, sin embargo, no es consciente del segmento de comunicaciones que lleva a cabo el departamento de seguridad o no sabe cómo el departamento de sistemas distribuye la carga entre los distintos servidores.

Por todo ello, consideramos que es necesario tener una visión completa de una red de telecomunicaciones que nos ayude a entender y a interrelacionar todos los conceptos que hemos aprendido a lo largo de la carrera.

1.4 Planificación del Trabajo

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin
1		**Diseño de la topología, capa física**	**26 días**	**mié 06/03/19**	**dom 31/03/19**
2		Pliego de prescripciones técnicas	2 días	mié 06/03/19	jue 07/03/19
3		**Topología de interconexión MetroLAN**	**2 días**	**mié 06/03/19**	**jue 07/03/19**
4		Justificación	1 día	mié 06/03/19	mié 06/03/19
5		Subanillos	1 día	jue 07/03/19	jue 07/03/19
6		**Esquema general**	**10 días**	**vie 08/03/19**	**dom 17/03/19**
7		Esquema	7 días	vie 08/03/19	jue 14/03/19
8		**Redundancia y escalabilidad**	**3 días**	**vie 15/03/19**	**dom 17/03/19**
9		Core MPLS	1 día	vie 15/03/19	vie 15/03/19
10		Sedes	1 día	sáb 16/03/19	sáb 16/03/19
11		CPD	1 día	dom 17/03/19	dom 17/03/19
12		**Capa física**	**14 días**	**lun 18/03/19**	**dom 31/03/19**
13		Fibra óptica	2 días	lun 18/03/19	mar 19/03/19
14		Equipamiento de router	2 días	mié 20/03/19	jue 21/03/19
15		**Equipamiento de switching**	**2 días**	**vie 22/03/19**	**sáb 23/03/19**
16		Capa de acceso	1 día	vie 22/03/19	vie 22/03/19
17		Capa de distribución y Core	1 día	sáb 23/03/19	sáb 23/03/19
18		**Firewalls**	**2 días**	**dom 24/03/19**	**lun 25/03/19**
19		Primer nivel	1 día	dom 24/03/19	dom 24/03/19
20		Segundo nivel	1 día	lun 25/03/19	lun 25/03/19
21		Gestor de ancho de banda	2 días	mar 26/03/19	mié 27/03/19
22		Solución para DNS y DHCP	2 días	jue 28/03/19	vie 29/03/19
23		Solución para balanceador	2 días	sáb 30/03/19	dom 31/03/19
24		**Descripción de la capa de enlace de datos y red**	**15 días?**	**lun 01/04/19**	**lun 15/04/19**
25		**Capa de enlace**	**5 días**	**lun 01/04/19**	**vie 05/04/19**
26		VLAN	1 día	lun 01/04/19	lun 01/04/19
27		Agregación de enlaces	1 día	mar 02/04/19	mar 02/04/19
28		STP	1 día	mié 03/04/19	mié 03/04/19
29		VRRP	2 días	jue 04/04/19	vie 05/04/19
30		**Capa de red**	**10 días**	**sáb 06/04/19**	**lun 15/04/19**
31		VRF	1 día	sáb 06/04/19	sáb 06/04/19
32		NAT	1 día	sáb 06/04/19	sáb 06/04/19
33		MPLS	2 días	dom 07/04/19	lun 08/04/19
34		BGP	3 días	mar 09/04/19	jue 11/04/19
35		**PEC2**	0 días	mar 09/04/19	mar 09/04/19
36		OSPF	3 días	vie 12/04/19	dom 14/04/19
37		Balanceo de carga	2 días	sáb 13/04/19	dom 14/04/19
38		Rutas estáticas	1 día	lun 15/04/19	lun 15/04/19
39		**Servicios de la red corporativa**	**15 días**	**mar 16/04/19**	**mar 30/04/19**
40		**Seguridad**	**3 días**	**mar 16/04/19**	**jue 18/04/19**
41		Primer nivel	2 días	mar 16/04/19	mié 17/04/19
42		Segundo nivel	1 día	jue 18/04/19	jue 18/04/19
43		Telefonía IP	3 días	vie 19/04/19	dom 21/04/19
44		DHCP	3 días	lun 22/04/19	mié 24/04/19
45		DNS	3 días	jue 25/04/19	sáb 27/04/19
46		Gestión de ancho de banda y QoS	3 días	dom 28/04/19	mar 30/04/19
47		**Acceso a internet, flujos y conexiones VPN**	**20 días**	**mié 01/05/19**	**lun 20/05/19**
48		Internet	4 días	mié 01/05/19	sáb 04/05/19
49		Telefonía IP	4 días	dom 05/05/19	mié 08/05/19
50		DMZ	4 días	jue 09/05/19	dom 12/05/19
51		InterUOC	4 días	lun 13/05/19	jue 16/05/19
52		VPN	4 días	vie 17/05/19	lun 20/05/19
53		**PEC3**	0 días	mar 21/05/19	mar 21/05/19



1.5 Breve sumario de productos obtenidos

Topología y diseño de una red metropolitana.
Descripción del hardware para las distintas soluciones.
Implementación de protocolos de capa de enlace: STP, VRRP
Implementación de protocolos de capa de red: IBGP, EBGP, OSPF, rutas estáticas.
Implementación de servicios de red: Seguridad, telefonía IP, DHCP, DNS, gestión de ancho de banda, QoS.
Implementación de acceso a internet con redundancia de ISP y conexiones VPN.

1.6 Breve descripción de los otros capítulos de la memoria

- Diseño de la topología de red, capa física

  Este apartado se basará en la descripción del diseño de la red y de los elementos de hardware que la conforman.
  Nos introduciremos en el proyecto a través de Pliego de Prescripciones Técnicas, que nos facilitará los datos iniciales que necesitamos para llevar a cabo nuestra propuesta.
  A continuación, se detallarán las diferentes topologías, así como el esquema de red.
  Por último, definiremos el equipamiento físico que conformará nuestra propuesta. A la hora de elegir el hardware de cada una de las tecnologías que intervienen en nuestro proyecto, hemos seguido un criterio vanguardista, procurando seleccionar los elementos más actuales y punteros para cada solución.

- Descripción de la capa de enlace de datos y red

  Una vez presentada la capa física, pasaremos a la capa 2 del modelo OSI. Definiremos los protocolos de nivel 2 más destacados de nuestra solución como el concepto de VLAN, STP, HSRP o VRRP, a continuación, veremos cómo se comportan en nuestro escenario.
  Tras definir la capa de enlace de datos, nos meteremos a fondo en la capa de red. Nuestro proyecto se anuncia como una red MPLS, pues bien, definiremos en profundidad en qué consiste este protocolo, además describiremos también los otros dos protocolos de enrutamiento dinámico que intervienen en nuestra propuesta, BGP y OSPF. Para acabar con el apartado de enrutamiento, presentaremos también las rutas estáticas. Por último, veremos cómo están implementados todos estos elementos en nuestra solución.

- Servicios de la red corporativa

  Anteriormente hemos definido las máquinas o el hardware que va a prestar los servicios de la red, pero ¿Cuáles son estos servicios? En este apartado describiremos todos los servicios que daremos a nuestros usuarios y también aquellos que forman parte de nuestra red sin que ellos lo sepan.

- Acceso a internet, flujos y conexiones VPN

  Llegado a este punto, ya tenemos descritos todos los niveles de comunicación que conforman nuestra red, ha llegado el momento de ver cómo funciona una red en su totalidad. Para ello analizaremos los diferentes flujos de datos que podemos tener, por ejemplo, un usuario de cualquier sede que sale a navegar, o una consulta a la base de datos de la granja de servidores, conexiones VPN desde el exterior, etc.

2. Implementación de una red MPLS

2.1 Diseño de la topología de red, capa física

2.1.1 Pliego de prescripciones técnicas

El pliego de prescripciones técnicas, en adelante PPT, es el documento donde la entidad adjudicadora del contrato especifica los requerimientos tanto técnicos como normativos que regirán en la contratación de los servicios de comunicaciones.
A nivel técnico especifica cuales son las necesidades por cubrir y en algunos casos, el modo en el que se deberán llevar a cabo, además, en él se recogerán los datos necesarios para la ejecución del proyecto.
A nivel normativo, aunque no es objeto del alcance del proyecto, comentaremos que tanto servicios como infraestructuras deben cumplir con una serie de garantías validadas por entidades certificadoras independientes, que en muchos casos son de obligado cumplimiento por las partes contratantes. A nivel de servicios de comunicaciones, rige la certificación “UNE-ISO/IEC 27001:2005 Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI)”. En lo que se refiere a la validación una infraestructura de seguridad como la que acometeremos en el presente proyecto, se deberá cumplir con las medidas de seguridad previstas en el Anexo II del Esquema Nacional de Seguridad.
A través del PPT, la UOC facilita el emplazamiento de todas las sedes que conforman su comunidad educativa en Barcelona, así mismo, hace saber que solo la sede principal y la facultad de ingeniería cuentan con una sala de procesamiento de datos, en adelante PDP, equipadas con el

equipamiento necesario (rack de comunicaciones, sistemas de alimentación ininterrumpida, sistemas antincendios, controladores de temperatura y humedad, aislamiento acústico, etc.) para albergar los equipos de comunicaciones. El PPT también indica que, gracias a un acuerdo entre la UOC y el ayuntamiento de Barcelona, se podrá hacer uso de las canalizaciones subterráneas de la empresa Aigües de Barcelona que discurren por toda la ciudad, con el objetivo de desplegar la red de fibra que debe implementarse para la interconexión entre las distintas sedes.
A continuación, se muestra tanto el mapa con las sedes facilitado en el PPT, así como nuestra propuesta de modelo de interconexión, que posteriormente se justificará.

2.1.2 Topología de interconexión MetroLAN

Ilustración 1 Distribución de las sedes

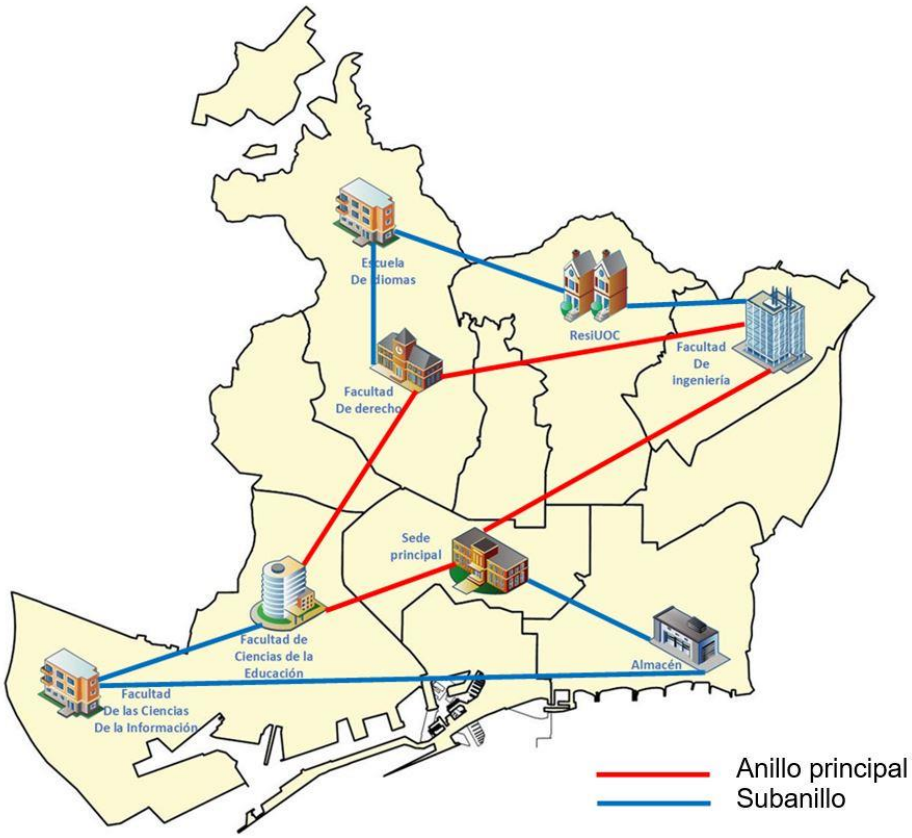
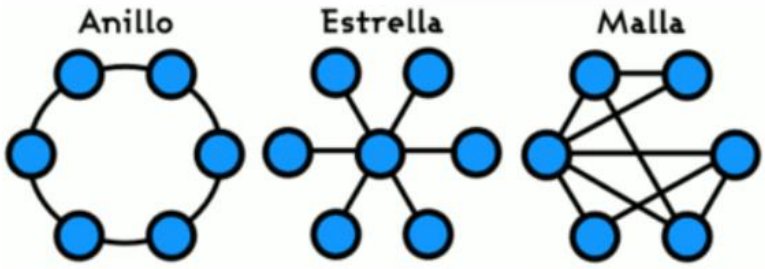


Ilustración 2 Topología en anillo

2.1.2.1 Justificación

Entre los tipos de topología que podrían considerarse a la hora de implementar una red metropolitana estarían las siguientes:



lustración 3 Topologías de red

Como se observa, la topología en estrella tiene un único punto de fallo en su nodo central, de manera que, si este cae, toda la red queda aislada, por tanto, no sería una buena solución para el proyecto.
La topología mallada interconexiona todos los nodos presentes en la red, por lo que, proporciona la máxima renundancia posible, pero recordemos que se está abordando la implantación de una red metropolitana,

conectar entre si todos los nodos existentes, supondría una excesiva inversión en infraestructuras.
Por último, la topología escogida, la topología en anillo, como se puede comprobar, no tiene un único punto de fallo, de manera que, si cae algún nodo, el resto sigue teniendo continuidad a través del otro sentido del flujo de comunicación. La inversión en infraestructuras sería mucho menor que en el caso de la estructura en malla, ya que, los kilómetros en cableado de fibra serán mucho menores.

2.1.2.2 Subanillos

La topología de interconexión propuesta muestra además un esquema de subanillos. El diseño de la solución consiste en tener un anillo principal compuesto por cuatro nodos como core MPLS, a partir de dos de ellos podrán formarse lo que hemos denominado subanillos, de tal forma que, como se observa en la ilustración 4, los nodos del subanillo estarían compuestos por los routers PE del anillo principal y una pareja de switches de distribución en cada una de las sedes que lo conformen, en apartados posteriores se definirán los elementos de red citados de manera específica, en el presente apartado solo se trataran cuestiones de diseño. Esta disposición proporciona a las sedes periféricas, aquellas que no forman parte del anillo principal, redundancia tanto a nivel local como a través de su correspondiente subanillo, se abordarán en mayor profundidad estos aspectos en el siguiente apartado mediante el desarrollo del esquema general.

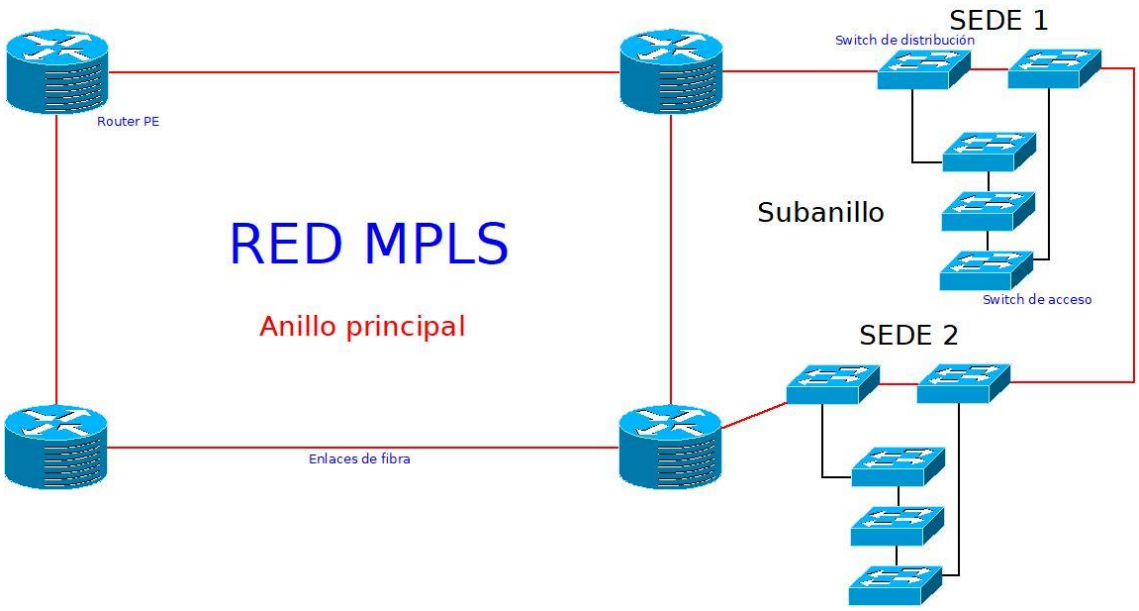


Ilustración 4 Subanillos

2.1.3 Esquema general

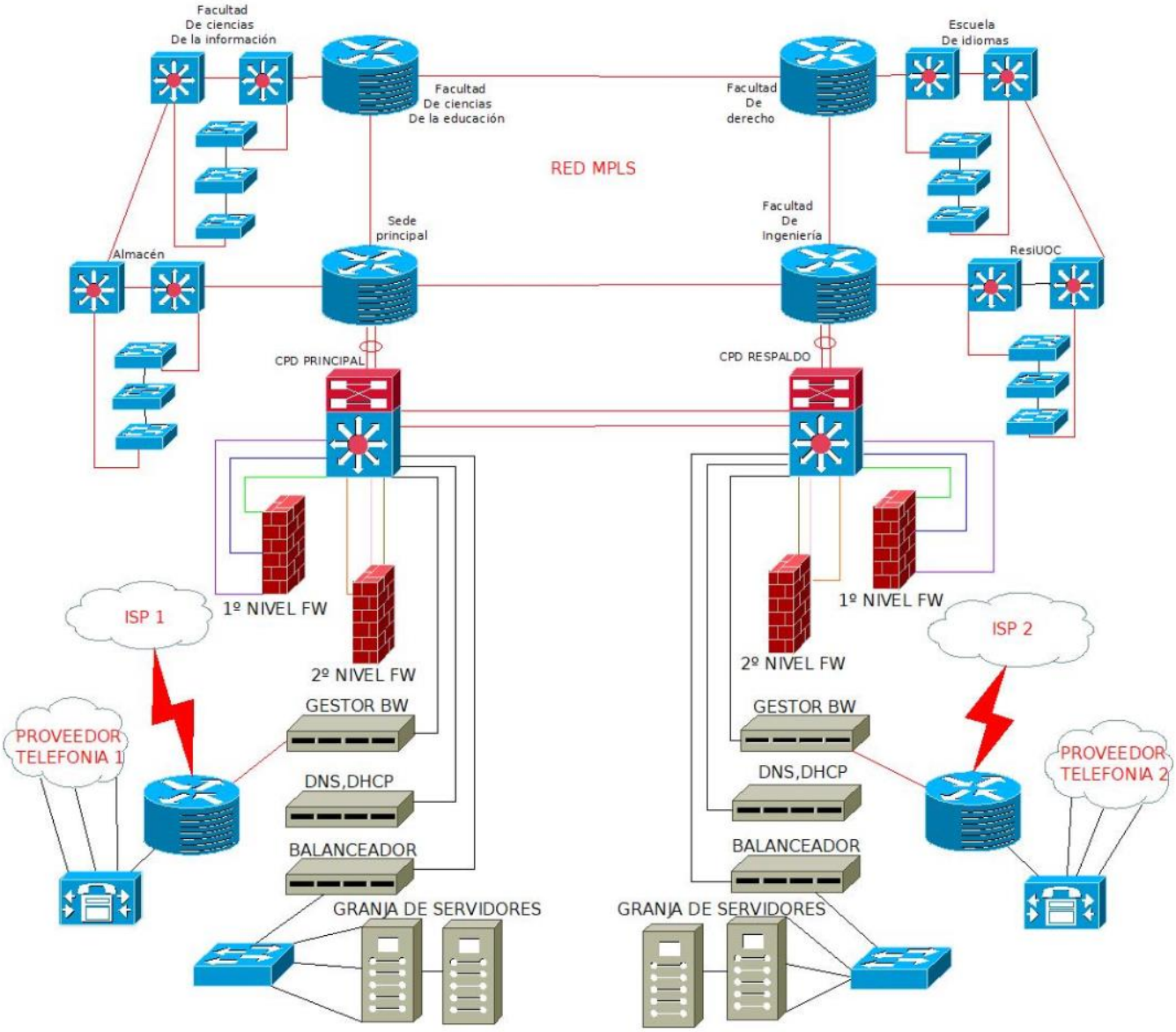


Ilustración 5 Esquema general

El esquema general de red se irá desgranando a medida que se avance en la exposición del proyecto, de momento, serán abordadas solo aquellas cuestiones relacionadas con el diseño de la topología de red y la capa física.

2.1.3.1 Redundancia y escalabilidad

2.1.3.1.1 Core MPLS

Como se ha expuesto en apartados anteriores, la disposición en anillo proporciona redundancia y tolerancia a fallos, ya que, ante la caída de uno de los nodos principales, el flujo de datos tendría continuidad a través del otro lado del anillo. Respecto a la escalabilidad, si fuese conveniente debido a los requerimientos de una nueva sede ampliar el Core del anillo MPLS con la inclusión de un nuevo router PE, únicamente habría "abrir" el anillo, recordemos que está redundado y que por tanto no habría pérdida de servicio, e incorporar el nuevo nodo a través de una nueva conexión de fibra.

2.1.3.1.2 Sedes

Para las sedes, se distinguirá aquellas que forman parte de un subanillo de las que están directamente conectadas a un nodo principal, estas últimas, por simplicidad, no aparecen en el esquema general, por ello, pasamos a ilustrar ambos tipos a continuación:

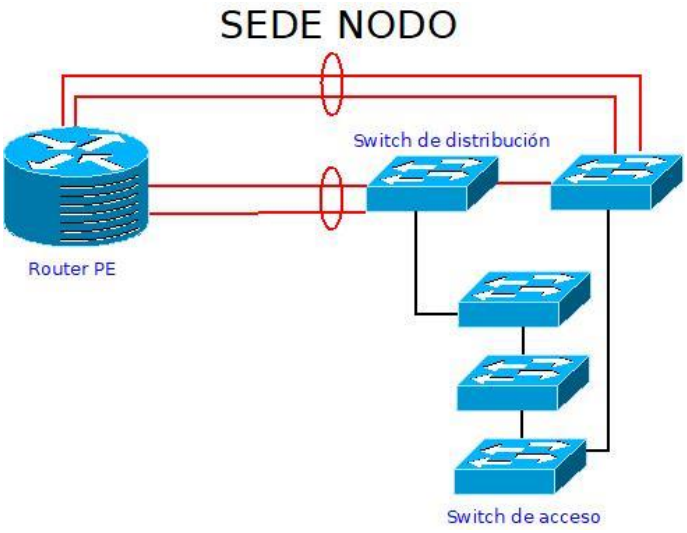


Ilustración 6 Sede conectada a nodo

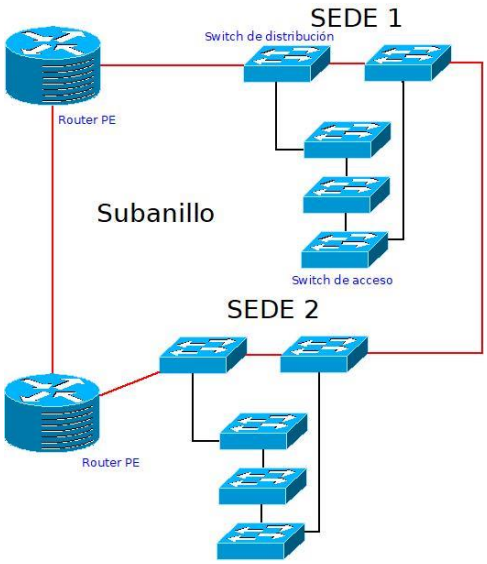


Ilustración 7 Sede subanillo

La topología de la sede es igual en ambos casos, la diferenciación viene en su conexión al anillo MPLS. En el caso de una sede que cuelga del propio nodo principal, se han dispuesto dos agregaciones de puertos, cada una de ellas conectadas a un módulo distinto del router PE, en el apartado de nivel físico, todos los equipos serán descritos en profundidad. La agregación de puertos será abordada en el capítulo que engloba la descripción de la capa de enlace de datos, a nivel físico son

dos puertos, pero a nivel lógico forman un único enlace, por tanto, además de redundancia, la solución de conexión al core de red ofrece el doble de ancho de banda.
El diseño se ha efectuado de esta forma teniendo en cuenta que las sedes que forman parte del anillo principal solo necesitan una acometida de planta interna para su conexionado al nodo, por tanto, la agregación de enlaces es una solución viable que potencia el rendimiento de la red LAN.
Para una sede perteneciente a un subanillo, la redundancia de conexión al core de la red viene a través de la topología en anillo explicada en apartados anteriores y la inclusión de dos equipos switch en la capa de distribución, la caída de cualquier equipo de comunicaciones dentro del subanillo, no supondría pérdida de servicio, la red contaría con un camino alternativo para el flujo de datos. La escalabilidad a nivel de subanillo, al igual que para el anillo principal, consistiría en “abrir” en subanillo e interconectar la nueva sede con la misma topología y disposición que las ya mostradas.
A nivel local, como ya se ha comentado, la estructura de la sede es la misma en ambos modelos de conexión al núcleo de la red. Como se puede observar, tenemos dos capas, distribución y acceso. La capa de acceso es la que conecta directamente a los usuarios finales, y la capa de distribución, la que conecta a la sede con el core MPLS. Cada switch de acceso podría corresponder por ejemplo a una planta del edificio y en el caso de que se necesitara mayor densidad de puertos, la escalabilidad consistiría en instalar un nuevo equipo respetando la interconexión presente. La redundancia se obtiene al conectar el primer y el último switch de acceso a un switch de distribución diferente, de este modo, si cae algún equipo de distribución, la sede seguirá teniendo comunicación a través del otro miembro de dicha capa.
En el capítulo de protocolos de la capa de enlace se abordará la cuestión de los bucles de red que el protocolo STP gestionará.

2.1.3.1.3 CPD

En el esquema general se puede observar como a la sede principal y a la facultad de ingeniería, están conectados el CPD principal y el de respaldo respectivamente. Ambos CDP están conectados al nodo del core a través de una agregación de enlaces a un switch de core, a su vez, cada switch de core cuenta con dos enlaces dedicados de fibra óptica entre sí. Cada CPD es un espejo del otro, por tanto, contamos con redundancia tanto a nivel de hardware como a nivel de conexionados entre los mismos y con el core MPLS.
En capítulos posteriores se abordará la cuestión de como interactúan entre sí ambos CPD y cuál sería el flujo de datos a través de cada uno.

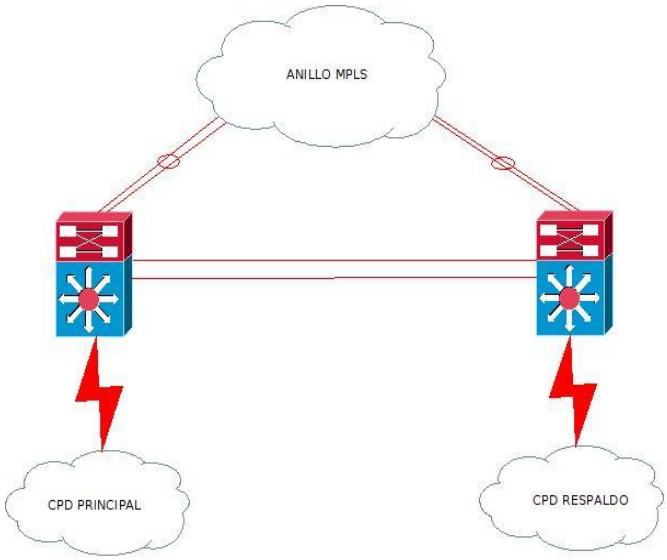


Ilustración 8 CPDs

2.1.4 Capa física

2.1.4.1 Fibra óptica

Como ya se ha referido en varias ocasiones, el conexionado tanto del anillo principal como el de los subanillos, así como el de los equipos de comunicaciones en las respectivas sedes, se efectúa a través de fibra óptica de forma directa, punto a punto entre los equipos mediante los módulos transceptores SFP. Recordemos que el circuito transcurre a través de las canalizaciones de la empresa de aguas de la ciudad.

El motivo por el que hemos elegido la fibra óptica para el diseño de la red es debido a sus muchas propiedades favorables, entre las que merecen destacar:

- gran capacidad de transmisión (por la posibilidad de emplear pulsos cortos y bandas de frecuencias elevadas),

- reducida atenuación de la señal óptica,

- inmunidad frente a interferencias electromagnéticas,

- cables ópticos de pequeño diámetro, ligeros, flexibles y de vida media superior a los cables de conductores,

- bajo coste potencial, a causa de la abundancia del material básico empleado en su fabricación (óxido de silicio). [1]

La red discurrirá por el área metropolita de Barcelona hasta el armario repartidor más cercano a cada sede, desde donde se efectuará la acometida de planta interna hasta el recito de comunicaciones donde alojaremos la conexión en un armario de parcheo óptico habilitado a tal efecto. Debido a sus características, en especial potencia y atenuación, el tipo de fibra que se utilizará hasta el citado armario de parcheo será fibra monomodo. Para el cableado vertical y horizontal dentro de la propia sede destinado a la conexión entre los equipos de comunicaciones, utilizaremos fibra óptica multimodo, ya que, las distancias son muy reducidas y las características de potencia y atenuación dejan de cobrar relevancia frente al coste de implementación mucho más reducido de este tipo de conexionado.
A continuación, se describen las características de cada tipo de fibra:

Fibra monomodo
Las fibras monomodo poseen un diámetro de núcleo muy estrecho, de manera que solo permiten un modo de transmisión. Poseen una atenuación típica de entre 0,1 dB y 0,4 dB por kilómetro. El núcleo mide entre 8 µm y 10 µm, por lo que requiere un acoplamiento de la luz muy confinado y preciso. Este diámetro tan estrecho causa, además, que el haz se propague siguiendo una trayectoria muy paralela al eje de la fibra por lo que se evita el desfase al final de la transmisión y reduce la dispersión causada. Aunque la dispersión modal no tenga sentido en la fibra monomodo, sí que la tiene por contrario, la dispersión cromática. Al disponer de un ancho de banda tan elevado, existe el problema de que no todas las longitudes de onda llegan al mismo tiempo a su destino, por lo que la dispersión cromática tiene un efecto muy considerable sobre el diseño. El elevado ancho de banda de este tipo de fibras, junto con sus bajas pérdidas y su dispersión modal inexistente, la convierten en una fibra idónea para enlaces de larga distancia como el que abordamos en actual proyecto. [2]

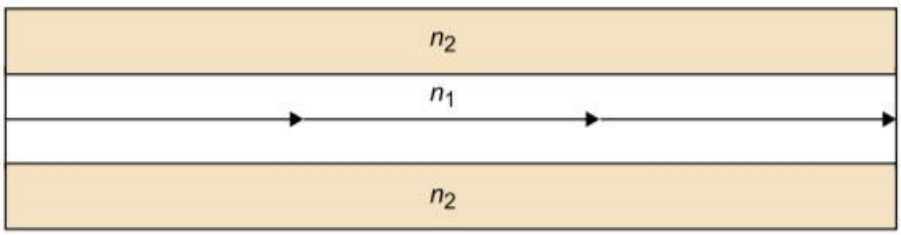


Ilustración 9 Fibra monomodo

Fibra multimodo
En las fibras multimodo se engloban todas aquellas en las cuales el diámetro del núcleo de este tipo de fibras es amplio, por lo que es capaz de propagar varios modos de transmisión simultáneamente. Poseen una atenuación típica de entre 0,3 dB y 1 dB por kilómetro. El núcleo mide en torno a 50 µm ó 62,5 µm, por lo que el acoplamiento de la luz en sus diferentes modos es más sencillo. Debido a esto, es posible utilizar un

LED como fuente emisora, así como conectores más sencillos y una instalación y mantenimiento con menos coste que la fibra monomodo. [2]

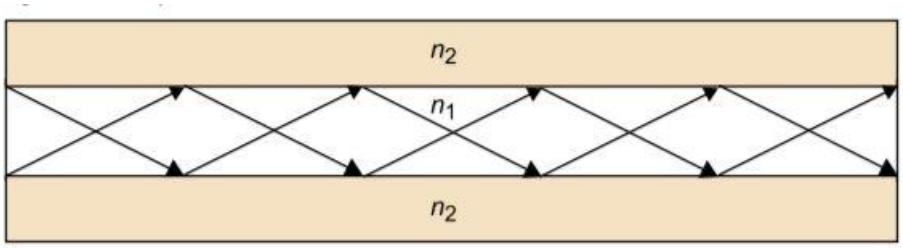


Ilustración 10 Fibra multimodo

2.1.4.2 Equipamiento de routers (anillo MPLS y conexión con el ISP)

El Juniper MX480 3D Universal Edge Router proporciona un alto rendimiento y escalabilidad para proveedores de servicios de Internet, datacenters de medianas y grandes empresas, así como servicios de agregación de acceso en redes MAN y redes de operador en Centros de Procesamientos de datos medianos y grandes.

Ilustración 11 Router MX480

Con sólo ocho unidades de rack (8 RUs), el Juniper MX480 ofrece 2,88Tbs full dúplex o hasta 5,76 Tbps half-dyplex de capacidad del sistema para soportar interfaces de alta densidad de 10GbE, 40GbE y 100GbE, también soporta conectividad SONET / SDH, ATM y PDH en caso de ser requerido. El equipamiento MX480 es una plataforma con una altísima densidad de puertos, un equipo altamente redundante, este router proporciona 8 slots que se pueden llenar con 6 tarjetas de línea (MPC), y una matriz de conmutación (SCB) en configuraciones de chasis no redundantes o 2 en el caso de redundantes.
La configuración ofertada en el presente proyecto incluye fuentes de alimentación, routing engine, matrices de conmutación (SCB) redundantes, y sistema de refrigeración con componentes redundados.

Estas características hacen, por tanto, de este router un equipo totalmente redundante y resiliente.
En cuanto a la escalabilidad, este chasis, a su capacidad máxima puede llegar a dar, a velocidad de línea, hasta 288 puertos Ethernet de 10 Gigabits, 24 100-Gigabit Ethernet o 72 puertos Ethernet de 40 Gigabits.
El Juniper MX480 tiene alto rendimiento y está repleto de características de enrutamiento, conmutación, seguridad y servicio altamente escalables que permite consolidación de redes, convergencia de servicios, etc. Las características clave incluyen soporte para una amplia gama de servicios VPN L2 / L3 y funciones avanzadas de pasarela de red de banda ancha, junto con servicios integrados de enrutamiento, conmutación y seguridad. [3]

2.1.4.3 Equipamiento de switching QFX5100

Los switches de la serie QFX son equipos de baja latencia y gran densidad de puertos, satisfacen las necesidades de los entornos empresariales más exigentes y de proveedores de servicios.

Ilustración 12 serie QFX5100

La familia de switches QFX de Juniper es una plataforma de switching de alto rendimiento, baja latencia y rica en funcionalidades diseñada específicamente para entornos que requieran este tipo de características, principalmente grandes datacenters, puntos neutros o de intercambio de internet donde cientos de routers mueven diariamente decenas de Tbps. Esta familia proporciona opciones de agregación desde 1GbE hasta 100GbE, pasando por 10GbE y 40GbE, y con soporte futuro de 400GbE. En este tipo de entornos no solo es importante la necesidad de capacidad sino de funcionalidades. Todo ello también gestionado a través del sistema operativo carrier-class JunOS, que corre en todas las familias de producto de Juniper, y que facilitará la gestión de una solución completamente basada en equipamiento Juniper.
La familia de switches QFX5100 son conmutadores de capa 2/3 altamente escalables que están optimizados para los entornos más exigentes, especialmente contiene un poderoso conjunto de características no sólo para los entornos de Data Center y Data Center virtualizado, sino para cualquier entorno en los cuales características

como el rendimiento, latencia, funcionalidad y la flexibilidad sean importantes. La línea de producto QFX5100 incluye switches con configuraciones de puertos fijos de 10GbE, uplinks de 40GbE y solo puertos de 40GbE. A esta gama, dentro de la familia QFX5100, se ha incorporado recientemente los QFX5110 que incluyen configuraciones de puertos fijos de 10GbE y uplinks de 40GbE/100GbE o solo puertos de 40GbE con opción de 100GbE de los cuales se puede hacer breakout a 10GbE.
Esta familia de producto corre el mismo sistema operativo JunOS que la familia QFX10K, switches EX, o routers de la familia MX, asegurando una implantación consistente, y un plano de control común entre toda la estructura de producto de Juniper.
Entre las características destacables de estos switches se encuentran:

- Alta densidad de puertos – Hasta 72 puertos 10GbE en los modelos QFX5100-48S; 96 puertos 10GbE en QFX5100-96S en 2(RU) unidades de rack; hasta 32 puertos 40GbE, o 20 puertos 40GbE y 4 100GbE, en 1(RU)unidad de rack.

- Equipo con soporte completo de nivel 2 y nivel 3 – BGP Add-path, MPLS, L3 VPN y IPv6 6PE. Con un rendimiento de hasta 2.56 Tbps y una latencia tan baja como 550 ns.

- Hardware – CPU de 1.5 GHz dual-Core Intel con 8 GB de memoria y almacenamiento de 32 GB SSD en el caso de la gama QFX5100 y 1.8 GHz quad-core Intel CPU con 16 GB de memoria y almacenamiento de 64 GB SSD para la gama QFX5110.

- Alta disponibilidad – La familia QFX dispone de las mejores prestaciones de alta disponibilidad del mercado a través de sus soluciones de Chassis Virtual. [4]

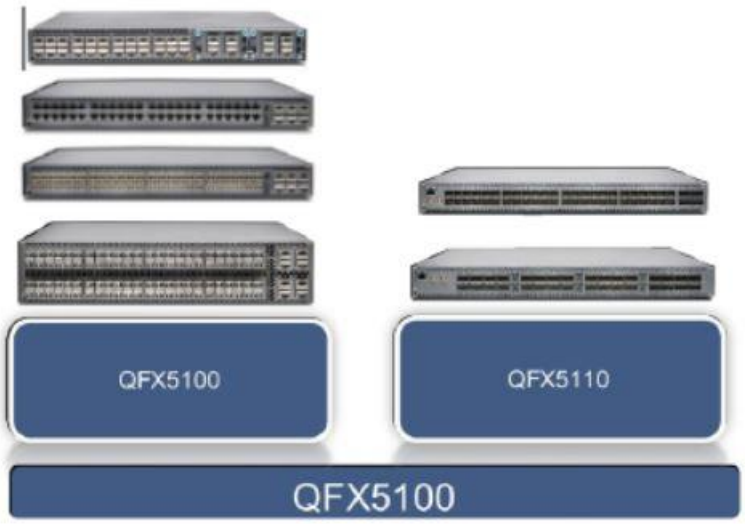


Ilustración 13 Modelos QFX5100

Tras la presentación de la familia de switches que formarán parte de la solución del proyecto, se indica el modelo concreto para cada capa dentro de la red:

2.1.4.3.1 Capa de acceso

QFX5100-48T

El switch QFX5100-48T es un equipo compacto de 1(RU) unidad de rack, wire-speed, de muy baja latencia que incorpora un rico conjunto de funcionalidades embebidas en el sistema operativo JunOs. El plano de control incorpora un procesador Intel Quad-Core de 1.5GHz con 8GB de memoria y un disco duro de 32GB SSD. Este equipo incorpora 48 puertos tri-rate para 100Mbps, 1GbE y 10GbE en cobre. Adicionalmente incorpora 6 puertos QSFP+ de 40GbE con un ancho de banda agregado de 1.44Tbps o 1.08 Bpps por switch.

Este equipo se encuentra disponible tanto en AC como en DC y se encuentra disponible con ventilación “front-to-back”, o AFO, y “back-to-front”, o AFI. El equipo incluye 2 fuentes de alimentación con redundancia 1+1 y 5 ventiladores, todo ellos son “hot-insertable” y “hot-removable” en redundancia n+1. [4]

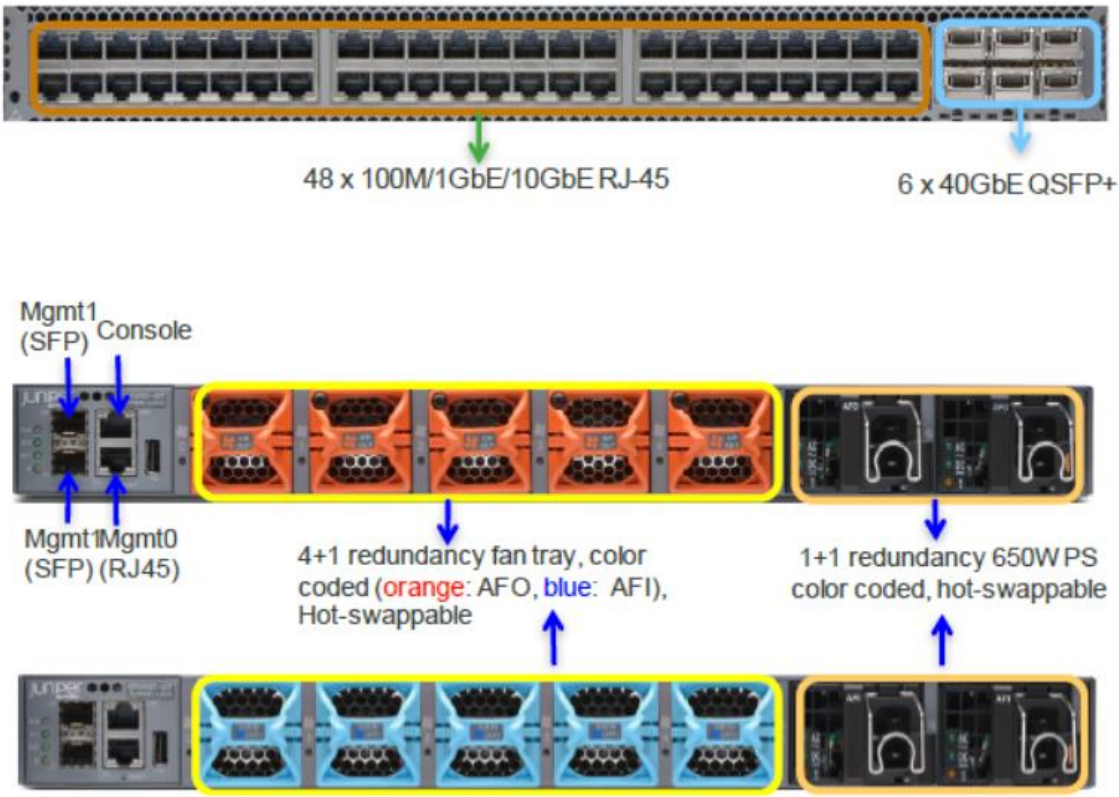


Ilustración 14 QFX5100-48T

2.1.4.3.2 Capa de distribución y Core

QFX5110-48S

Se trata de un equipo compacto de 1(RU) unidad de rack, wire-speed, de muy baja latencia que incorpora un rico conjunto de funcionalidades embebidas en el sistema operativo JunOs. El plano de control ha sido mejorado también con un potente procesador Intel quad-core de 1.8GHz con 16GB de memoria y un disco duro de 64GB SSD.

Este equipo incorpora 48 puertos que pueden alojar tanto SFP como SFP+ para 1GbE y 10GbE. Adicionalmente, incorpora 4 puertos QSFP28 40GbE/100GbE con un ancho de banda agregado de 1.76 Tbps o 1.32Bpps.

Este equipo se encuentra disponible tanto en AC como en DC y se encuentra disponible con ventilación “front-to-back”, o AFO, y “back-to-front”, o AFI. El equipo incluye 2 fuentes de alimentación con redundancia 1+1 y 5 ventiladores, todo ellos son “hot-insertable” y “hot-removable” en redundancia n+1. [4]

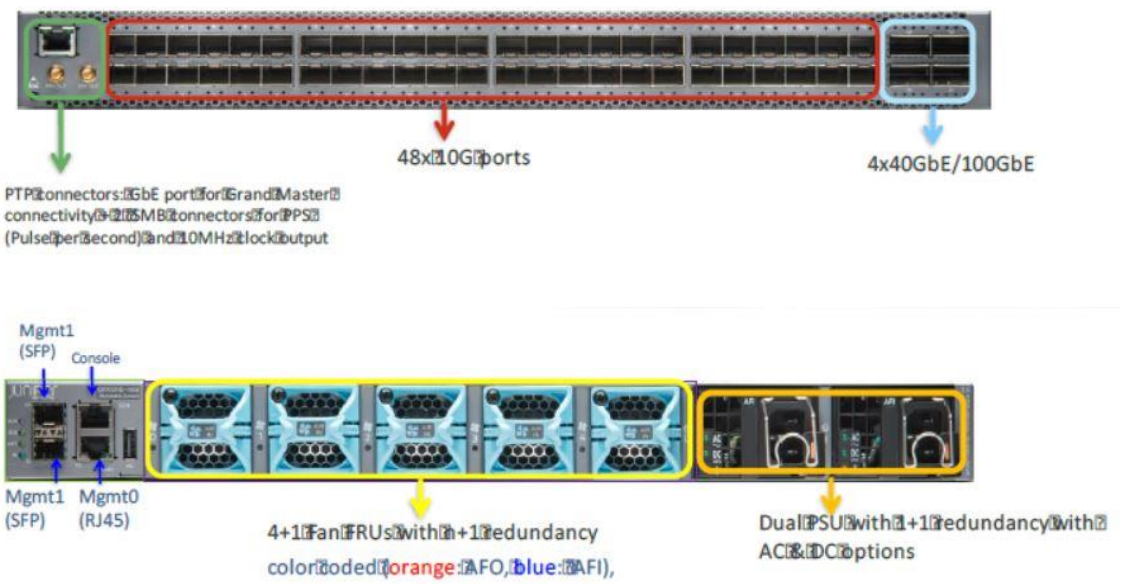


Ilustración 15 QFX5110-48S

El hecho de que el QFX5110-48S posea mayor potencia de procesador, RAM y disco duro, lo convierten en un candidato óptimo para las capas de distribución y core, ya que, estos segmentos de red tendrán que afrontar labores de procesamiento más complejas que sus homólogos de la capa de acceso, como enrutamiento y protocolos de redundancia. Además, su densidad de puertos es más que suficiente para satisfacer la demanda planteada en cada CPD y a nivel de capa de distribución.

2.1.4.4 Firewalls

2.1.4.4.1 Primer nivel

Check Point 15600

Funcionalidades:

- Cortafuegos
- Detección y prevención de intrusiones en la red
- Detección y bloqueo de malware
- Detección y mitigación de ataques de DDoS
- NAT bidireccional
- NAT transversal
- Control de acceso para sedes remotas
- Accesos Externos

Ilustración 16 Check Point 15600

La principal justificación de incluir a Check Point en la capa externa o primer nivel, es precisamente que no solo contribuirá a la mejor seguridad a nivel de perímetro, sino que con la funcionalidad de SandBoxing para la mitigación y prevención de amenazas avanzadas, estaría actuando lo más cerca posible de internet y lo más alejada de la red interna.
Las funcionalidades de seguridad pura, como pueden ser IPS, AV, ABOT, ThreatEmulation y ThreatExtraction deben colocarse en el perímetro externo, ya que cuanto antes se pare un ataque procedente de internet más eficiente es el rendimiento en la red.
La tecnología de Check Point a través de su licencia y funcionalidad Next Generation Threat Prevention dispone de firmas necesarias para la prevención de malware conocido y tiene la capacidad de actualización diaria de sus firmas para la detección de malware día cero.

Las capacidades más relevantes son las siguientes:

Capacidades de rendimiento	**Check Point 15600**
Firewall throughput	30 Gbps
Threat prevention throughput	3 Gbps
IPS throughput	8 Gbps
Max sessions per second	185.000
Capacidades HW	
I/O	(4)100/1000/10G Cu, (4) Gig/10Gig SFP/SFP+, (2) 40G QSFP+
Power Supply (Avg/Max Power Consumption)	600 Watts
Rack Mount (Dimensions)	2U, 19” standard rack

[5]

2.1.4.4.2 Segundo nivel

Palo Alto-3260

Funcionalidades:

- Cortafuegos
- Detección y bloqueo de malware

Ilustración 17 PA-3260

El Cortafuegos de Segundo Nivel es recomendable que sea de diferente tecnología que el primer nivel, ya que, si se diera algún tipo de vulnerabilidad o ataque que afectara a un solo fabricante, toda nuestra red no se vería comprometida, por ello, se propone Palo Alto Networks, el cual figura como líder de tecnología NGFW (Firewall de próxima generación) del cuadrante Gartner en los últimos 6 años, destacando en proporcionar seguridad ante prevención de intrusos y amenazas

emergentes así como el manejo de mayor caudal con un mínimo de pérdida de rendimiento.

Las capacidades más relevantes son las siguientes:

Capacidades de rendimiento	**PA-3260**
Firewall throughput	8,8 Gbps
Threat prevention throughput	4,7 Gbps
IPS throughput	4,8 Gbps
Max sessions per second	135.000
Capacidades HW	
I/O	(12)100/1000/10G Cu, (8) Gig/10Gig SFP/SFP+, (4) 40G QSFP+
Power Supply (Avg/Max Power Consumption)	180/240 Watts
Rack Mount (Dimensions)	2U, 19” standard rack

[6]

2.1.4.5 Gestor de ancho de banda

ALLOT SSG-600

La tecnología planteada como solución de inteligencia de red es la de Allot en formato appliance. En concreto, se hará uso de un equipo SSG-600 con bypass óptico externo en cada uno de los 2 CPD. Este equipo se utilizará para la inteligencia de red tanto de los segmentos de las redes externas no confiables como para los segmentos de red interna de la topología propuesta.
Se podrá tener conocimiento y control exhaustivo y detallado de las aplicaciones, los usuarios, las conexiones y los servicios que circulan por las redes monitorizadas. Se hará uso de la consola NetXplorer de Allot para la gestión centralizada: autodescubrimiento de aplicaciones, monitorización en tiempo real y pasado, planificación de informes, eventos y alarmas, gestión de políticas centralizada.
El SSG-600 proporciona el servicio de garantía de ancho de banda que permite limitar y priorizar los distintos tráficos de la red. El servicio permitirá la configuración de una limitación de ancho de banda por organismo o sede de la UOC con la granularidad suficiente para realizar la gestión de caudales por clases de servicio, URLs destino, protocolos de capa de aplicación y por direccionamiento IP. El servicio proporciona las herramientas necesarias para la elaboración de informes y estadísticas de gestión de QoS a nivel de sede, así como un portal de

gestión remota que permita la consulta en tiempo real del consumo de cada centro educativo.[7]

Ilustración 18 ALLOT SSG-600

2.1.4.6 Solución para DNS y DHCP

Infoblox Trinzic 2215

El servicio de DNS para cada uno de sus roles, DNS caché recursivo, DNSs Externos Autoritativos, DNSs internos secundarios y DNS exclusivos para la funcionalidad de Accesos externos se basará en solución tecnología proporcionada por Infoblox.
Así mismo, esta tecnología también será la encargada de proporcionar el servicio de DHCP para disponer de IPs dinámicas que faciliten el mantenimiento del direccionamiento.

Además, dispondremos de la funcionalidad IPAM, fundamental para una gestión eficiente del direccionamiento IP, ya que permite controlar, monitorizar y generar reportes en base a la actividad y utilización del espacio de direcciones.

Ilustración 19 Infoblox Trinzic 2215

Dispondremos de dos dispositivos Infoblox Trinzic 2215, uno por cada CPD con configuración en GRID, una funcionará como Master del GRID (CDP principal) y el otro como miembro del GRID (CPD respaldo), de esta forma facilitarán el mantenimiento de la infraestructura global, ejerciendo un control centralizado sobre la misma.

La arquitectura GRID permite desplegar y mantener servicios de red “non-stop” en entornos distribuidos. De esta forma, los appliances funcionan y se gestionan como si se tratase de un único sistema, proporcionando así:

- Gestión centralizada de los servicios de red
- Capacidades de backup y restore
- Monitorización y reportes
- Disaster recovery

En la arquitectura GRID, los appliances denominados “Member” son coordinados por el appliance “Grid Master”. De esta manera, todos los appliances comparten una base de datos distribuida y se comunican entre sí a través de túneles SSL - VPN.[8]

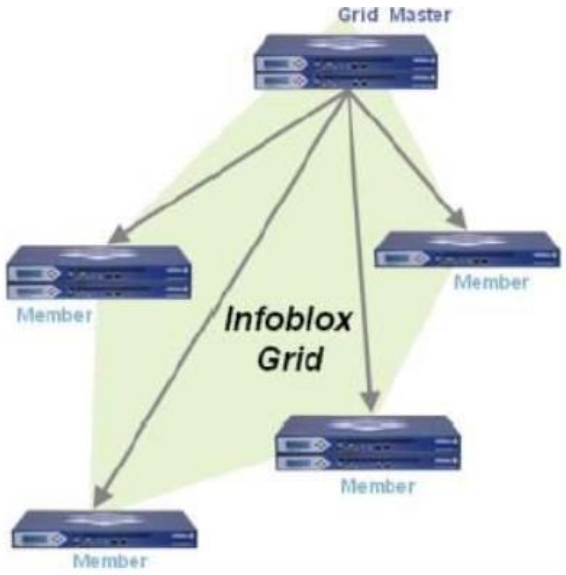


Ilustración 20 Grid Infoblox

2.1.4.7 Solución para balanceador

F5 BIG-IP i5600

Para cubrir las funcionalidades de balanceo local de servicios (LTM) se propone una solución basada en la tecnología del fabricante F5, formada por dos equipos modelo BIG-IP i5600.

BIG-IP Local Traffic Manager (LTM): Ofrece un profundo conocimiento del tráfico de la aplicación de la red, así como un control sobre cómo se maneja. Transforma el caótico volumen de tráfico de red en flujos de datos ensamblados y, a continuación, toma decisiones inteligentes sobre la gestión del tráfico mediante la selección del destino correcto según el rendimiento del servidor, la seguridad y la disponibilidad.[9]

Ilustración 21 F5 BIG-IP i5600

La gestión y administración de todos los equipos de F5 se realiza de forma distribuida a través de la interfaz web de cada uno de los equipos incluidos en la infraestructura.

2.2 Descripción de la capa de enlace de datos y red

2.2.1 Capa de enlace

A continuación, pasamos a describir los principales protocolos, entidades y conceptos perteneciente a la capa de enlace que conforman principalmente nuestro proyecto.

2.2.1.1 VLAN

Una VLAN es un grupo lógico de dispositivos finales, comparten el mismo domino de broadcast, en el diseño de redes modernas, cada VLAN corresponde con una subred. A través de enlaces troncales podemos interconectar switches transportando varias VLAN. Para su enrutamiento necesitaremos dispositivos de capa 3, tal y como veremos en el apartado de flujos.

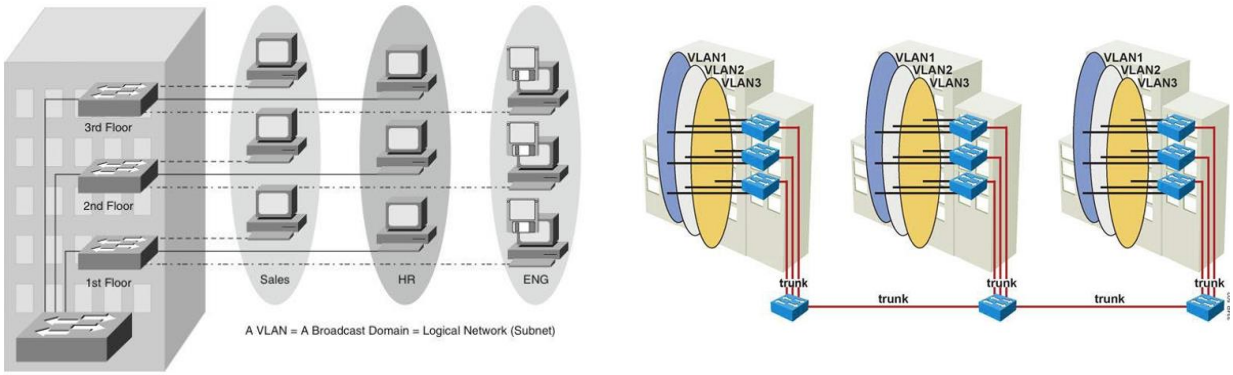


Ilustración 22 VLAN / TRUNK

En el presente proyecto, para cada sede hemos separado a través de sus respectivas VLAN, el tráfico de datos del tráfico de voz, así mismo, se ha disgregado el tráfico cuyo origen o destino es alguno de los miembros de la granja de servidores de la empresa a través de una VLAN DMZ, cuyo concepto, también expondremos más adelante, por último, continuando con las recomendaciones del código de buenas prácticas para el diseño de una red de comunicaciones, hemos generado también una VLAN para la red de administración o gestión, de esta forma, dicho tráfico queda aislado de las redes de usuario,

asegurándonos que solo los administradores de la red, podrán tener acceso a la gestión del equipamiento.

2.2.1.2 Agregación de enlaces

La agregación de enlaces consiste en agrupar varios enlaces físicos, hasta ocho dependiendo del fabricante, en un solo enlace lógico. De esta forma, además de redundancia, tendríamos disponible el ancho de banda correspondiente a la suma de los miembros de nuestra interfaz virtual. El protocolo estándar de la industria para esta tecnología es el LACP. En nuestro proyecto hemos incluido varias agregaciones de enlaces que describiremos con posterioridad, la representación gráfica de una agregación es la siguiente.

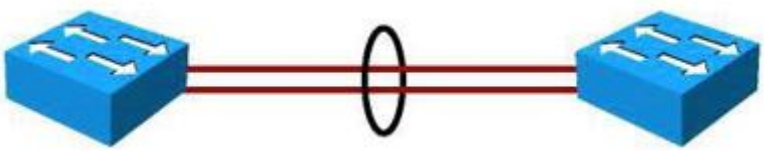


Ilustración 23 Agregación de enlaces

2.2.1.3 STP

Spanning Tree Protocol (STP) es un protocolo de capa 2 que se ejecuta en bridges y switches. La especificación para STP es IEEE 802.1d. El propósito principal de STP es garantizar que no creemos loops o bucles cuando se tengan caminos redundantes en la red. Un bucle pondría en riesgo la estabilidad de nuestra red, podríamos generar la saturación de los enlaces e incluso propiciar una denegación de servicio.

Tal y como dejamos de relieve en el apartado “Redundancia y escalabilidad”, todos los equipos de nuestras sedes cuentan con redundancia física o más de un camino para el flujo de datos, por tanto, la configuración de STP es uno de los hitos más indispensables para el correcto funcionamiento de las comunicaciones en nuestro proyecto.

En la siguiente imagen podemos observar un ejemplo del funcionamiento de STP. Ante la misma prioridad configurada y el mismo ancho de banda de cada uno de los enlaces, el protocolo otorga funciones de Root al equipo cuya MAC es menor. De esta forma, bloquea los caminos alternativos con menor prioridad con el objeto de no generar bucles de red tal y como ya hemos comentado. En el supuesto de que alguno de los enlaces principales cayera, STP gracias a los cálculos de su algoritmo (STA), convergería y el flujo de datos pasaría a los enlaces anteriormente en estado de bloqueo.

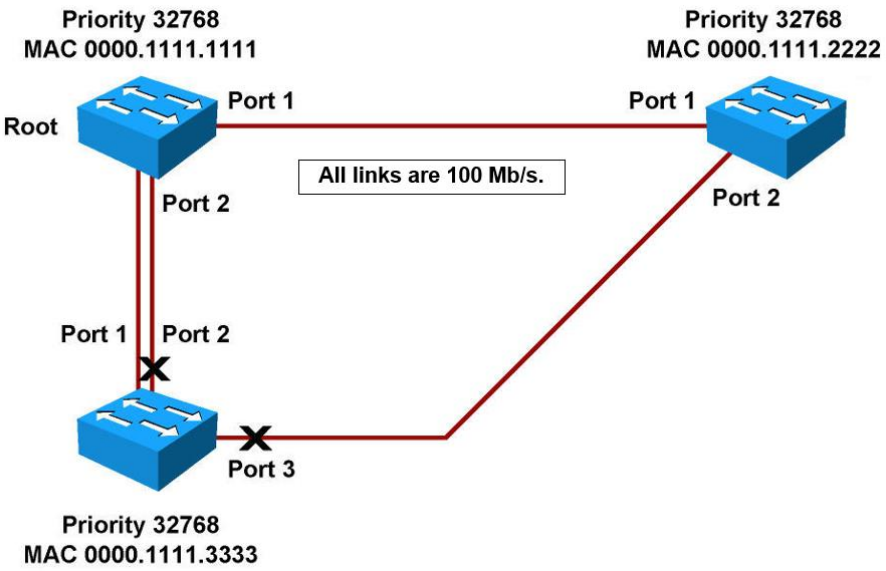


Ilustración 24 STP

Existen muchas modalidades de STP, no tenemos por qué bloquear un puerto por completo, podemos simplemente permitir ciertas VLAN por algunos enlaces y otras por otro camino alternativo, de esta forma además de redundancia estaríamos aislado el tráfico que más nos interese, así como balanceando la carga. Para nuestro proyecto, hemos elegido el STP en su modalidad RSTP (Rapid Spanning Tree Protocol) el cual se puede considerar una evolución del estándar 802.1d, veamos sus principales características de forma resumida.
El 802.1d se define en estos cinco estados de puerto diferentes: inhabilitado, escucha, aprendizaje, bloqueo, reenvío. Mientras que en RSTP (802.1w) podemos definir los siguientes:

Estado del puerto	Descripción
Descarte	Este estado se ve tanto en una topología activa estable como durante la sincronización y los cambios de la topología. El estado de descarte evita el reenvío de data frames, lo que "rompe" la continuidad de un bucle de Capa 2.
Aprendizaje	Este estado se ve tanto en una topología activa estable como durante la sincronización y los cambios de la topología. El estado de aprendizaje acepta marcos de datos para completar la tabla MAC para limitar la inundación de unicast frames desconocidos.
Reenvío	Este estado se ve solo en topologías activas estables. Los puertos del conmutador de reenvío determinan la topología. Después de un cambio de topología, o durante la sincronización, el reenvío de data frames ocurre solo después de una propuesta y proceso de acuerdo.

Principales diferencias con STP:

Estado de Puerto de STP (802.1D)	Estado de Puerto RSTP (802.1w)	¿El puerto está incluido en la topología activa?	¿El puerto detecta direcciones MAC?
Inhabilitado	Descarte	No	No
Bloqueo	Descarte	No	No
Escucha	Descarte	Yes	No
Aprendizaje	Aprendizaje	Yes	Yes
Reenvío	Reenvío	Yes	Yes

Funciones de los puertos:

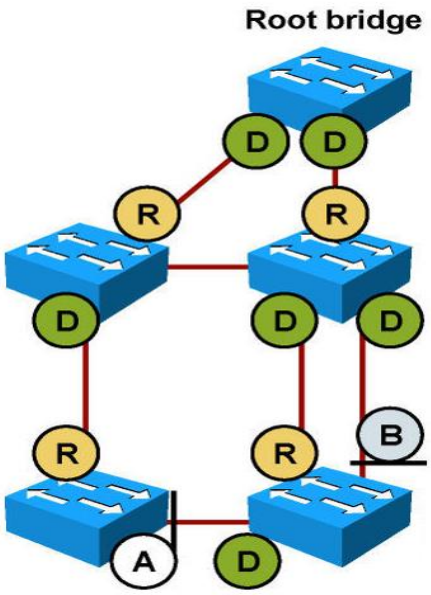


Ilustración 25 puertos RSTP

Las funciones de los puertos root y designado permanecen con la misma funcionalidad que en STP, mientras que la función del puerto de bloqueo se divide en las funciones de puerto alternativo y de respaldo. El algoritmo de spanning tree (STA) determina la función de un puerto según las unidades de datos de protocolo de bridge (BPDU). Para simplificar las cosas, el punto que se debe recordar sobre una BPDU es que hay siempre un método para comparar dos de ellas y decidir si una es más útil que la otra. Esto se basa en el valor almacenado en la BPDU y, en ocasiones, en el puerto en que se recibe.

Puerto Root

El puerto que recibe la mejor BPDU en un bridge es el puerto root. Este es el puerto más cercano al bridge root en términos de costo de trayectoria. STA selecciona un solo bridge root de toda la red puenteada (por VLAN). El bridge root envía las BPDU que son más útiles que las que envía cualquier otro bridge. El bridge root es el único bridge en la red que no tiene un puerto root. Todos los demás bridges reciben BPDU en al menos un puerto.

Puerto Designado:

Un puerto es designado si puede enviar la mejor BPDU en el segmento al que está conectado. Los bridges 802.1D conectan diversos segmentos entre sí, como segmentos de Ethernet, para crear un dominio puenteado. En un segmento dado, solo puede haber una trayectoria hacia el bridge root. Si hay dos, hay un loop de bridging en la red. Todos los bridges conectados a un segmento dado escuchan las BPDU de cada uno y se ponen de acuerdo en qué bridge envía la mejor BPDU y lo convierten en el bridge designado para el segmento. El puerto en ese bridge que corresponda es el puerto designado para ese segmento.

Puerto Alternativo y de Respaldo:

Estas dos funciones de puerto corresponden al estado de bloqueo de 802.1d. El puerto bloqueado se define como el que no es designado o puerto raíz. Un puerto bloqueado recibe una BPDU más útil que la que envía de su segmento. Recordemos que un puerto requiere necesariamente recibir las BPDU para permanecer bloqueado. RSTP introduce estas dos funciones para ese propósito.
Un puerto alternativo recibe BPDU más útiles de otro bridge y es un puerto bloqueado.
De igual forma, un puerto de respaldo recibe BPDU más útiles del mismo bridge en el que se encuentra y es un puerto bloqueado.
La lógica es que un puerto alternativo proporciona una trayectoria alternativa hacia el bridge root y, por lo tanto, puede reemplazar al puerto root si este falla. Por supuesto, un puerto de respaldo proporciona conectividad redundante al mismo segmento y no puede garantizar una conectividad alternativa al bridge root.

Para dar por finalizada nuestra exposición sobre RSTP, mencionaremos la función más importante que introduce, la transición rápida, El STA heredado esperaba pasivamente la convergencia de la red antes de pasar un puerto al estado de reenvío. El logro de una convergencia más rápida era una cuestión de ajuste de los parámetros predeterminados conservadores (los temporizadores de demora de reenvío y vencimiento máximo) y, a menudo, ponía en juego la estabilidad de la red. El nuevo STP rápido puede confirmar activamente que un puerto puede realizar una transición segura al estado de reenvío sin tener que depender de ninguna configuración de temporizador. Ahora existe un verdadero mecanismo de retroalimentación entre los bridges en conformidad con RSTP. [10]

2.2.1.4 VRRP

VRRP se basa en el protocolo IP de capa 3, ¿por qué lo hemos incluido entonces en el apartado de la capa de red? Aunque su funcionamiento se basa en la conectividad a nivel IP, VRRP no funciona si no existe visibilidad a nivel 2, es decir, en el nivel de la capa de enlace, es un aspecto muy importante que debemos tener en cuenta a la hora de

diseñar la topología de nuestra red. Por ello, hemos preferido incluir VRRP en el presente apartado y centrar el apartado de red en los protocolos de enrutamiento. Pasemos a explicar los aspectos más destacados de VRRP.

Virtual Router Redundancy Protocol (VRRP), tal y como nos indica su nombre, proporciona redundancia virtual de nivel 3 a través de una conectividad de capa 2. Nos apoyaremos en la ilustración 26 para ofrecer una descripción más gráfica de su funcionalidad.

El router PE de la Sede principal y el de la facultad de ingeniería son los nodos principales de nuestra red, poseen las rutas por defecto hacía los CPDs que nos enrutan hacia los servicios corporativos, ¿Cuál es el papel de VRRP? Gracias a que implementamos VRRP entre ambos PE, la ruta por defecto a la que acuden los equipos de nuestra red en su camino hacia los distintos servicios corporativos, telefonía, internet, servidores, etc., apuntan hacia una IP virtual que comparten sendos PE. Aquel equipo cuya prioridad de VRRP configuremos con mayor valor, será el router activo de nuestra red, quedando el otro como router standby. En nuestro caso particular, en el supuesto de que caiga el router principal, para el enrutamiento de la red sería un acontecimiento transparente, la sede principal quedaría sin conexión, pero la ruta por defecto de nuestra red seguiría siendo la misma, es decir, la IP virtual que comparten los PE. Gracias a la sincronización de VRRP, el router principal ahora sería el PE de la facultad de ingeniería y todo el tráfico de red saldría a través del CPD de respaldo. De esta forma, conseguimos que la caída de la sede principal no deje aisladas las comunicaciones del resto de sedes que conforman el anillo de fibra.

Cuando el PE de la sede principal, vuelva a tener conectividad, VRRP detectará que existe un nodo con prioridad más alta que el actual y la red convergerá de nuevo hacia el CPD principal.

VRRP es un protocolo abierto dentro del estándar de las telecomunicaciones, es decir, puede ser implementado por cualquier fabricante, un protocolo similar, pero de propiedad del fabricante es por ejemplo el protocolo HSRP de CISCO.

Como comentábamos al comienzo del apartado, es necesario que ambos PE tengan conectividad de capa 2 para el funcionamiento de VRRP. En nuestro diseño esta función está garantizada por los switches de core, que tal y como se refleja en la ilustración 26, cuentan con un doble enlace de fibra dedicado.

Por último, comentaremos que gracias a la implementación de VRRP, unido a al diseño de la topología física ya descrito, nuestra red cuenta con dos CPDs en configuración activo-pasivo o Cold Standby que la dotan de redundancia y robustez, el cual era uno de los hitos planteados al comienzo del proyecto.

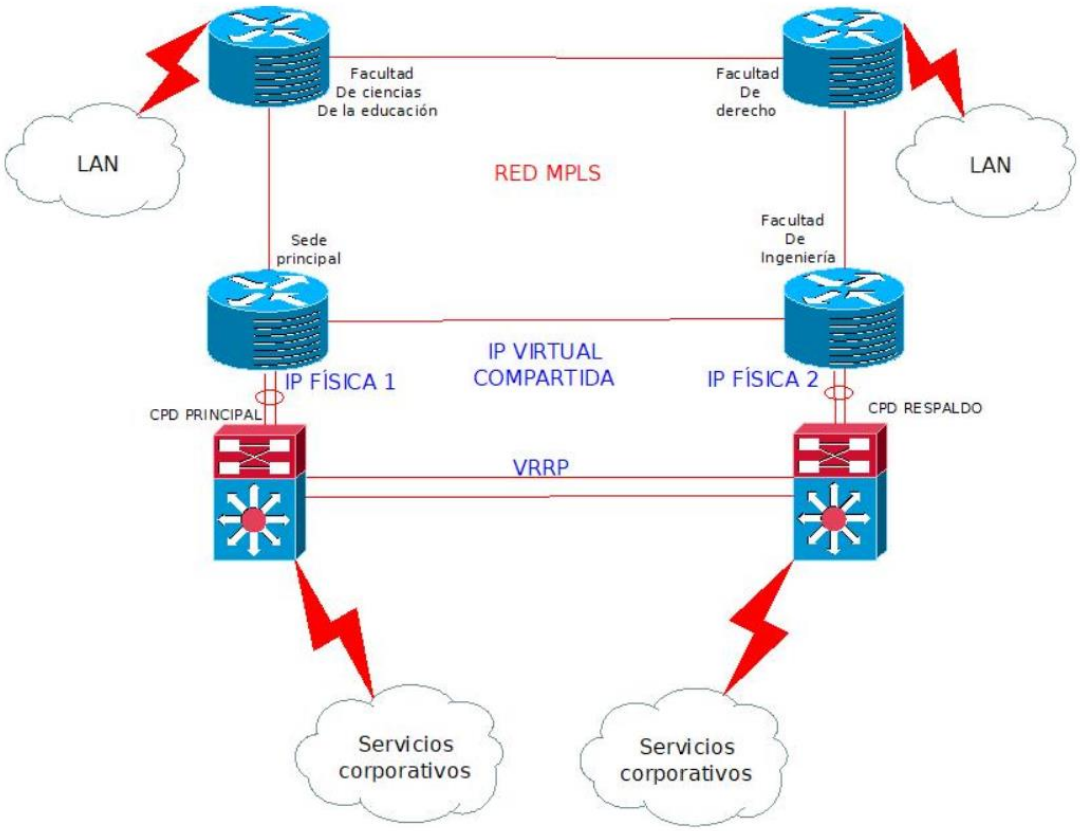


Ilustración 26 VRRP

2.2.2 Capa de red

2.2.2.1 VRF

Comenzaremos el apartado de la capa de red antes de dar paso a los protocolos de enrutamiento, definiendo qué es una VRF. (Virtual Routing and Forwarding) son instancias de enrutamiento, a nivel práctico es como si dividiésemos el router en cada una de estas instancias. Cada VRF posee su propia tabla de enrutamiento dentro del dispositivo de capa 3. Es una manera más de segmentar nuestra red y aislar aquellas redes que en ningún caso queremos que tengan visibilidad entre sí, a menos que un dispositivo de seguridad como un firewall se la proporcione. En nuestro proyecto, agruparemos las VLANs de datos dentro de las VRF de datos, de tal forma que tendremos una VRF de datos por cada una de las sedes de nuestro esquema. Así mismo, generaremos una VRF de voz, otra para las conexiones a los servidores denominada DMZ y otra para la administración de los equipos llamada GESTIÓN.

Dentro de una misma VRF las redes o equipos pueden verse entre sí, para alcanzar un host o red fuera de nuestra VRF y por tanto de nuestra tabla de enrutamiento, tendremos que acudir a un dispositivo de capa 3

que enrute entre VLAs siguiendo una política de permisos, esta función como ya puede intuirse, la desempeñarán los firewalls.

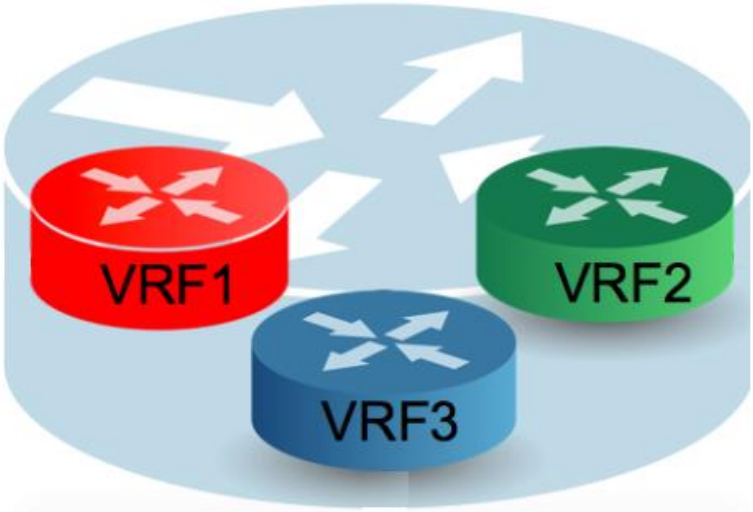


Ilustración 27 VRF

2.2.2.2 NAT

Natear consiste en traducir o trasladar una dirección IP a otra, también lo podemos definir como un mecanismo utilizado para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Por ejemplo, si un usuario de la red desea salir a navegar a internet, no podría hacerlo con su dirección de área local, ya que, es una dirección privada y por internet solo discurren direcciones públicas:

Rangos de IP(s) Privadas

CLASE A:	10.0.0.0 a 10.255.255.255 (8 bits red, 24 bits hosts).
CLASE B:	172.16.0.0 a 172.31.255.255 (12 bits red, 20 bits hosts). 16 redes clase B contiguas, uso en universidades y grandes compañías.
CLASE C:	192.168.0.0 a 192.168.255.255 (16 bits red, 16 bits hosts). 256 redes clase C continuas, uso de compañías medias y pequeñas además de pequeños proveedores de internet (ISP).

✓Se llaman privadas o reservadas, ya que estos rangos se utilizan para conectar a varios computadores y/o dispositivos dentro de una LAN.

Ilustración 28 IPs privadas

Rango de IP(s) Públicas	
Clase A	1.0.0.0 - 126.255.255.255
Clase B	128.0.0.0 - 191.255.255.255
Clase C	192.0.0.0 - 223.255.255.255

Ilustración 29 IPs públicas

Podemos distinguir los siguientes tipos de NAT:

Estática
Una dirección IP privada se traduce siempre en una misma dirección IP pública.

Dinámica
El dispositivo que natea el tráfico, en nuestro caso el firewall de salida a internet CheckPoint, tiene asignadas varias direcciones IP públicas, de modo que cada dirección IP privada se mapea usando una de las direcciones IP públicas que el firewall tiene asignadas, de esta forma a cada dirección IP privada le corresponde al menos una dirección IP pública.

Cada vez que un host requiera una conexión a Internet, el firewall le asignará una dirección IP pública que no esté siendo utilizada. Con este sistema se aumenta la seguridad ya que dificulta que un host externo ingrese a la red, debido a que las direcciones IP públicas van cambiando.

Sobrecarga
La NAT con sobrecarga o PAT (Port Address Translation) es el más común de todos los tipos. Se pueden mapear múltiples direcciones IP privadas a través de una dirección IP pública, por lo que optimizamos el uso del direccionamiento público. También se ahorran direcciones IPv4, ya que aunque la subred tenga muchas máquinas, todas salen a Internet a través de una misma dirección IP pública.

Para poder hacer esto el firewall hace uso de los puertos. En los protocolos TCP y UDP se disponen de 65.536 puertos para establecer conexiones. De modo que cuando una máquina quiere establecer una conexión, el firewall guarda su IP privada y el puerto de origen y los asocia a la IP pública y un puerto aleatorio. Cuando llega información a este puerto elegido de manera aleatoria, el firewall comprueba la tabla y lo reenvía a la IP privada y puerto de origen que correspondan.

Por último, comentaremos que la traducción NAT puede tener dos sentidos, de entrada y de salida. Hemos descrito solo el de salida, pero un alumno que desde su casa consulte la página de la UOC, también será traducido desde la IP pública a la que solicita su petición, a la IP privada del servidor que aloja la información.

2.2.2.3 MPLS

MPLS Multi Protocol Label Switching es un estándar de arquitectura multinivel basado en la conmutación de etiquetas, capaz de soportar cualquier tipo de tráfico.
MPLS es un mecanismo de envío de paquetes mediante el cual el envío se realiza basado en etiquetas, se mandan tramas a través de una red usando la información contenida en las etiquetas añadidas por el protocolo asociado.
La arquitectura MPLS describe los mecanismos para realizar la conmutación de etiquetas que combina los beneficios del envío de paquetes basados en la conmutación de Nivel 2 con los beneficios de Nivel 3, ya que, además MPLS fue diseñado para permitir el envío de otros protocolos.
La diferencia más significativa entre MPLS y otros protocolos es la manera en que se asignan las etiquetas y la capacidad para transportar una PILA de etiquetas adjuntas a un paquete.
La arquitectura se divide en 2 modelos separados, el envío (o plano de datos) y el componente de control (plano de control). En un nodo MPLS (LSR) la tabla de enrutamiento IP se emplea para determinar el intercambio de enlace de etiquetas.
Las etiquetas pueden corresponder a redes IP destino (igual que un envío IP tradicional) o también a otros parámetros, como calidad de servicio (QoS) o dirección origen.
Otra gran ventaja es que evitamos analizar cada trama en cada nodo, únicamente se analiza el paquete en el primer nodo y en el último, los nodos intermedios conmutan etiquetas.

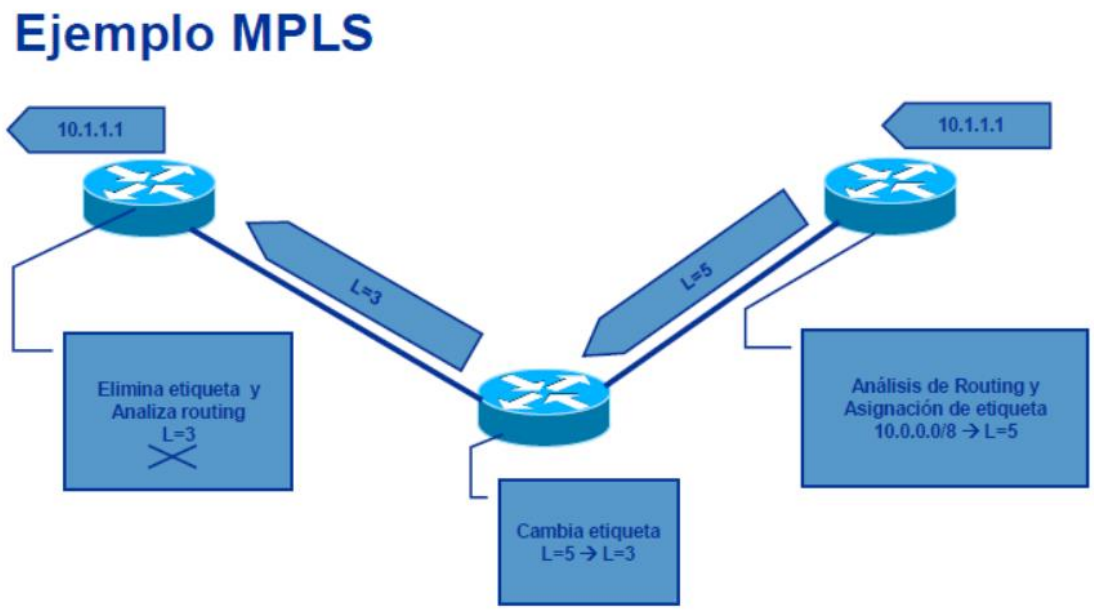


Ilustración 30 Ejemplo MPLS

Sólo los routers frontera realizan análisis de routing, los routers Core conmutan paquetes basados en un simple análisis y cambio de etiquetas.

Como hemos comentado anteriormente, la arquitectura MPLS tiene dos principales componentes:

- Control plane:
  - Intercambio de información de Nivel 3 y etiquetas
  - Usa protocolos para el intercambio de información de routing, como OSPF, EIGRP, ISIS y BGP.
  - Para el intercambio de etiquetas usa otros protocolos como TDP, LDP, BGP y RSVP.
  - Se encarga del mantenimiento de los contenidos de la tabla de conmutación de etiquetas, también llamada LFIB.

- Data plane:
  - Envío de paquetes basado en etiquetas.
  - Consta de un simple motor de etiquetas.

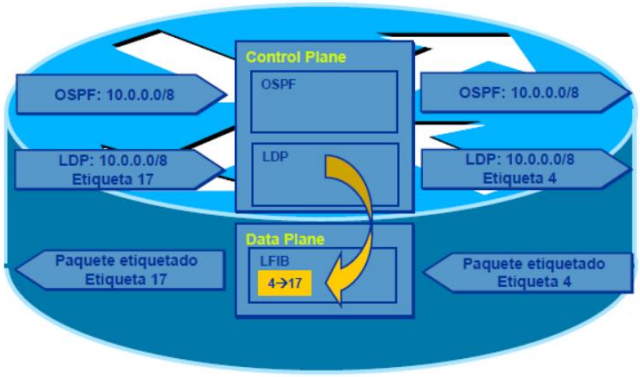


Ilustración 31 Control & Data plane

La imagen ilustra la funcionalidad del router dividida en los dos planos anteriormente descritos, Control y Data.

Una vez analizado el protocolo MPLS y descrito sus ventajas, la solución que presentamos en el diseño de capa 3 de la red, consiste en implementar MPLS con OSPF para el anillo principal, y BGP como protocolo de enrutamiento de los subanillos, las rutas estáticas, que presentaremos en siguientes apartados, apuntarán hacia los servicios corporativos.

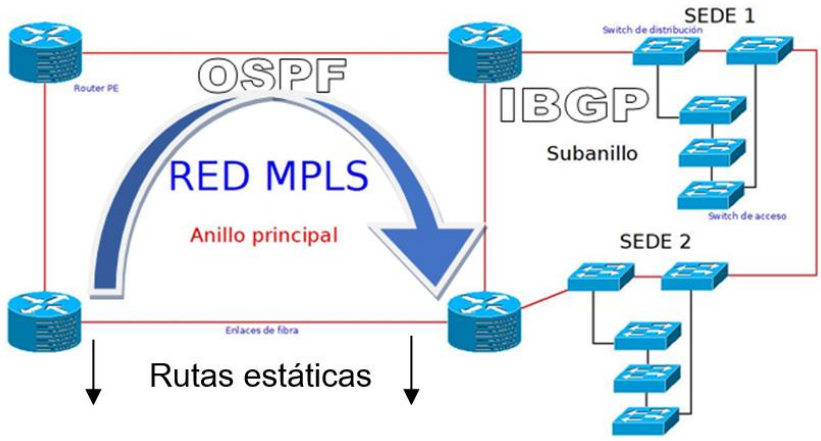


Ilustración 32 Enrutamiento

Cuando se analicen los flujos en el último apartado veremos la manera de trabajar de los diferentes protocolos de enrutamiento, no obstante, no entraremos a ver la forma de configurarlo, ya que, no existe un estándar, sino que cada fabricante tiene un lenguaje de programación propio corriendo en el sistema operativo del router o switch y la forma de efectuar una misma configuración varía incluso entre distintas versiones de OS del mismo fabricante. Por ello, nos limitaremos a describirlos y más tarde, ver cómo actúan.

2.2.2.4 BGP

Para entrar a definir BGP, primero se hará una pequeña introducción de los tipos de protocolos que existen.

Existen dos tipos principales de protocolos de enrutamiento:

- Interior Gateway Protocols (IGP): Protocolo de enrutamiento diseñados para intercambiar información de routing dentro de un sistema autónomo. RIP, EIGRP, OSPF
- Exterior Gateway Protocols (EGP): Utilizados para intercambiar información entre rotures de sistemas autónomos distintos. BGP.

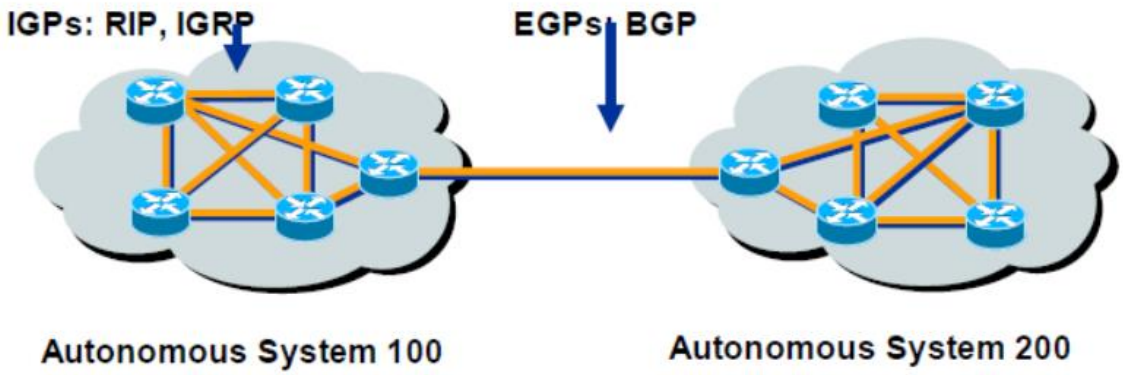


Ilustración 33 Protocolos IGP, EGP

BGP se diseñó originalmente para el intercambio de rutas entre proveedores de servicio (ISP), por tanto, se considera un protocolo de routing exterior (EGP). Se basa en el concepto de que Internet se divide en SAs (Sistemas Autónomos).

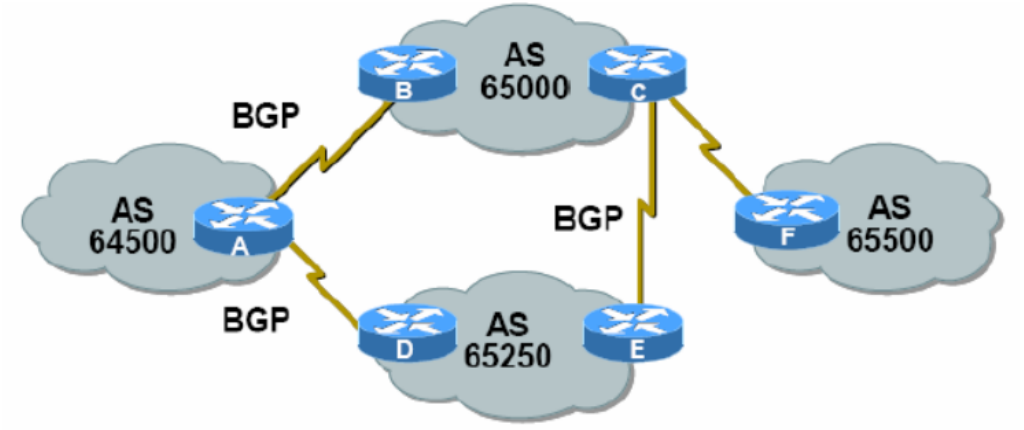


Ilustración 34 AS BGP

Un sistema autónomo es una red que depende de un solo administrador que se identifica con un número (1– 65536) que es único dentro del SA. Dentro del SA se pueden utilizar números privados (64.512 hasta el 65.535), pero para conectarse con Internet existe una organización que se encarga de asignarlos (IANA).
BGP funciona mediante el establecimiento de sesiones de vecindad, no existe descubrimiento automático de vecinos, se configuran manualmente, se denominan “peers”.
BGP se basa en conexiones TCP puerto 179 entre dos routers no necesariamente conectados físicamente. Los update de BGP son incrementales, excepto en el proceso de establecimiento, cuando el volumen de routing puede ser elevado. Para comprobar que el proceso BGP / TCP sigue activo se envían keepalives (cada 60 seg por defecto).
Hay dos tipos de “peer” BGPs, External BGP (EBGP), entre As e Internal BGP (IBGP), dentro de un As.
Un router BGP nunca envía una ruta aprendida de un vecino IBGP a otro vecino IBGP.
EBGP peers s iempre envían las rutas aprendidas de un EBGP tanto a EBGP como a IBGP.

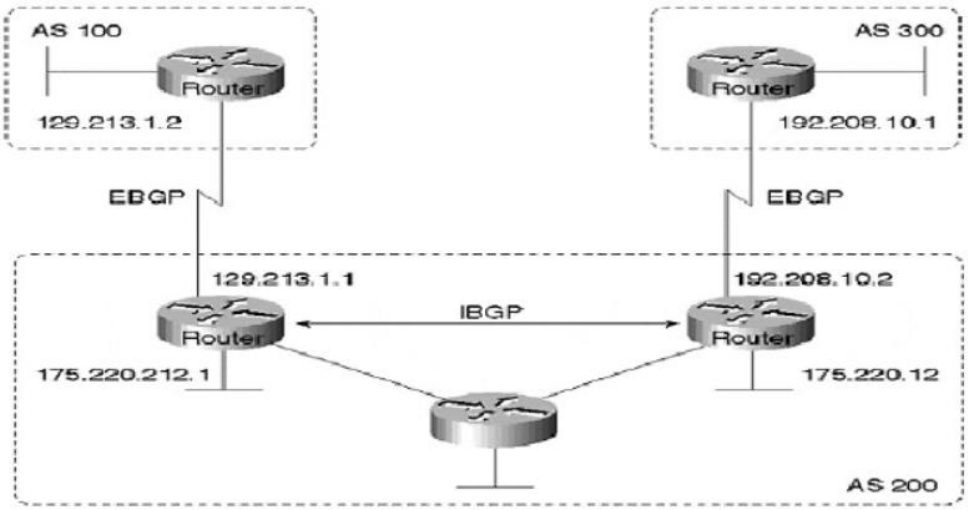


Ilustración 35 IBGP EBGP

En BGP un router mantiene varios caminos a un destino, pero sólo elige uno para enviar los paquetes. El mejor camino se elige teniendo en cuenta los atributos asociados con las rutas que se intercambian los “peers”.
BGP es básicamente un protocolo de vector distancia que maneja una lista de ASs por los que atraviesa la ruta para evitar bucles. Si ve una ruta en la que aparece su AS la tira.
Un EBGP añade su propio AS a la lista antes de enviar la ruta a otro EBGP peer.

2.2.2.5 OSPF

OSPF es un protocolo de enrutamiento IP de estado de enlace basado en estándares descrito en RFC 2328.
Fue desarrollado para satisfacer la incapacidad de RIP para escalar más de 15 routers.
Propuesto por IETF en 1988 y formalizado en 1991, hay 2 versiones; OSPFv2 es para IPv4 y OSPFv3 es para IPv6.
Las características más destacadas de OSPF son:

- Convergencia rápida
- Soporta VLSM
- Uso eficiente del ancho de banda: los cambios de enrutamiento activan las actualizaciones de enrutamiento (sin actualizaciones periódicas)
- Soporta gran tamaño de red
- Enrutamiento basado en la mejor selección de ruta
- Agrupación de miembros en Áreas

Con los protocolos de enrutamiento de estado de enlace, cada enrutador tiene una imagen completa de la topología de la red y puede tomar una decisión de forma independiente basada en una imagen precisa de la topología de la red.
Para hacerlo, cada enrutador de estado de enlace mantiene un registro de:

- Sus vecinos inmediatos enrutadores.
- Todos los demás enrutadores en la red, o en su área de red, y sus redes conectadas.
- Los mejores caminos a cada destino.

OSPF responde rápidamente a los cambios de red, enviar actualizaciones activadas cuando se produce un cambio de red. Así mismo, envía actualizaciones periódicas (actualización del estado del enlace), a intervalos largos, cada 30 minutos.
Utiliza los LSA para confirmar la información de la topología antes de que la información salga de la base de datos de estado de enlace.

Entre sus principales componentes destacamos:

Bases de datos / tablas OSPF:
- Base de datos de adyacencia OSPF = Tabla de vecinos
- Base de datos de estado de enlace OSPF = tabla de topología
- Base de datos de reenvío OSPF = tabla de enrutamiento

Anuncios de estado de enlace (LSA)
Base de datos de estado de enlace (LSDB)

Algoritmo de enrutamiento de ruta más corta primero (SPF)
- Algoritmo Dijkstra

Árbol SPF
Áreas OSPF
- Backbone (tránsito) y áreas estándar.

Tipos de enrutadores OSPF:
- Enrutador interno, enrutador de red troncal, enrutador de borde de área (ABR), enrutador de límite de sistema autónomo (ASBR)
- Enrutador designado (DR) y Enrutador designado de respaldo (BDR)

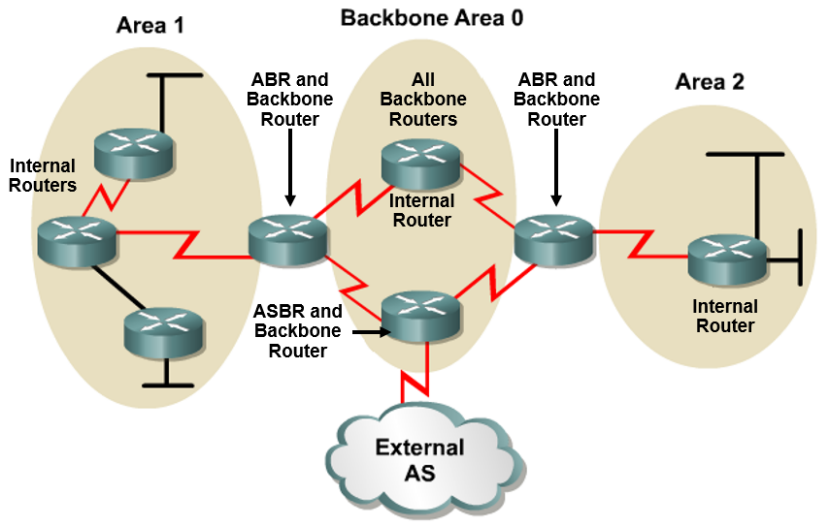


Ilustración 36 OSPF

Base de datos	Tabla	Descripción
Base de datos de adyacencia	Tabla de vecinos	- Lista de todos los enrutadores vecinos a los que un enrutador ha establecido comunicación bidireccional. - Esta tabla es única para cada enrutador.
Base de datos de estado de enlace	Tabla de topología	- Lista de información sobre todos los demás routers en la red. - La base de datos muestra la topología de la red. - Todos los enrutadores dentro de un área tienen bases de datos de estado de enlace idénticas.
Base de datos de reenvío	Tabla de enrutamiento	- Lista de rutas generadas cuando se ejecuta un algoritmo en la base de datos de estado de enlace. - La tabla de enrutamiento de cada enrutador es única y contiene información sobre cómo y dónde enviar los paquetes a otros enrutadores.

2.2.2.6 Balanceo de carga

El balanceo de carga dentro de nuestro esquema de red es una funcionalidad llevada a cabo por los dispositivos F5 descritos en el apartado “Solución para balanceador” a través de su módulo LTM.
Esta implementación surge como necesidad de distribuir la carga entre los distintos integrantes que forman la granja de servidores de cada uno de los CPDs.
Como hemos comentado, la comunidad educativa de la UOC posee sendas granjas de servidores en cada CPD, en dichos servidores se alojan la base de datos de todos sus alumnos, el servidor web de la UOC, así como la imagen de todos los recursos de software que son necesarios para la comunidad: programas de gestión ofimática, laboratorios para sus alumnos, repositorios de apuntes, etc.
Debido a la criticidad de los datos descritos, los servidores están redundados, tanto por seguridad como por el volumen de peticiones que reciben, que no hacen viable que todas sean asumidas por un mismo host.

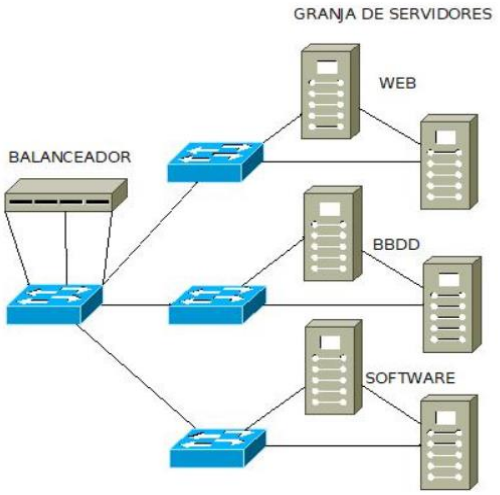
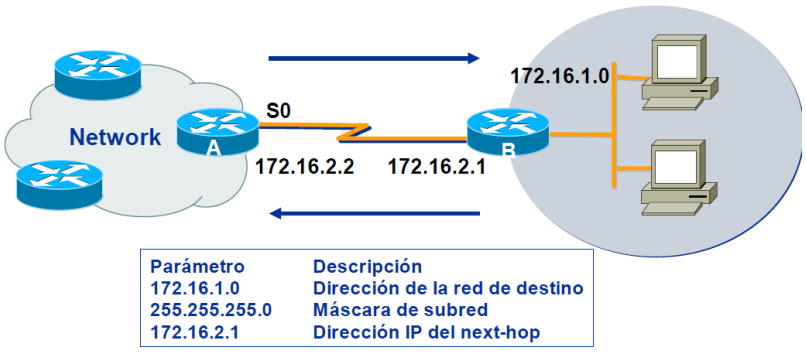


Ilustración 37 Balanceo

Nuestro balanceador tiene configurada una interfaz por cada uno de los servicios alojados en la granja de servidores: web, BBDD, software. La IP de cada interfaz es la puerta de enlace a la que apunta la red para acudir a dicho recurso. De esta manera, la ip de los servidores es desconocida para los usuarios, es nuestro dispositivo balanceador el que redirecciona el tráfico a los miembros de la granja, con ello estaríamos añadiendo además de un elemento de distribución de carga, un elemento más de seguridad, ya que también los dispositivos F5 son capaces de detectar comportamientos anómalos en las peticiones de los usuarios, como inyección de código ilícito o peticiones masivas de denegación de servio.
El criterio que utilicemos para balancear la carga entre los distintos miembros de la granja puede atender a diversos criterios. Podemos implementar un método meramente estadístico, tener nodos principales y otros de backup, dirigir el tráfico a aquellos con menor número de peticiones o aquel cuya CPU tenga mayor rendimiento y esté más liberada.

2.2.2.7 Rutas estáticas

Las rutas estáticas son aquellas rutas que el administrador de red introduce en el router de forma manual. Cuando se producen cambios en la topología de la red, estas rutas deben se actualizadas manualmente.




```
ip route 172.16.1.0 255.255.255.0 172.16.2.1
```

Ilustración 38 Rutas estáticas

La ruta estática es unidireccional, se debe configurar en ambos sentidos.
Definimos el camino a la red de destino a un next-hop o a una interfaz.
Para medios de acceso múltiple (LAN), se recomienda especificar la IP del next-hop en lugar de interfaces.
Un tipo especial de ruta estática es la ruta por defecto:

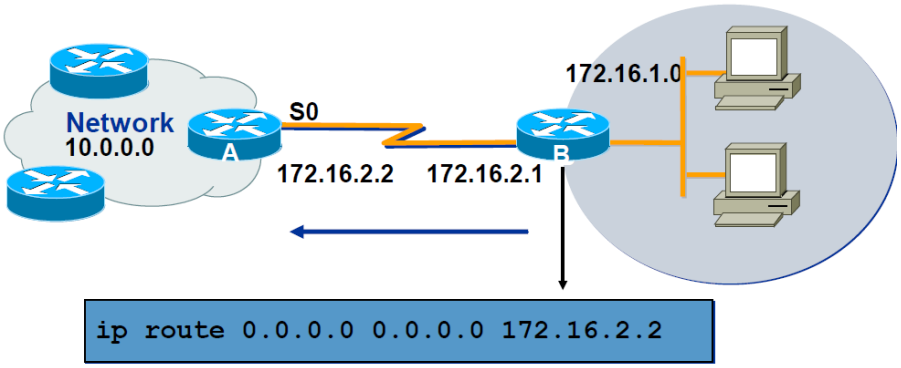


Ilustración 39 Ruta por defecto

Esta ruta permite que cualquier paquete cuyo destino no conozca el router B sea enviado al router A.
En nuestro proyecto, haremos uso de las rutas estáticas y por defecto en los PE se la sede principal y de la escuela de ingenieros, así como en los firewalls. La manera en la que funcionan la explicaremos en el apartado de flujos.

2.3 Servicios de la red corporativa

2.3.1 Seguridad

Nos encontramos ante uno de los puntos más críticos del núcleo de cualquier red de comunicaciones, la seguridad. El diseño de los niveles de seguridad no es una cuestión trivial, en materia certificaciones debemos considerar:

- Esquema Nacional de Seguridad (ENS), definido por el Gobierno de España. Tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Dicho esquema se regula en Real Decreto 3/2010, de 8 de enero, y es establecido en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos

- ISO 27001, por la que se garantiza una gestión eficaz de la seguridad de la información, garantizando su confidencialidad, integridad y disponibilidad.

- ISO 20000, por la que se garantiza una gestión de servicio alineado con las necesidades y objetivos del negocio, con calidad, fiabilidad y valor añadido para los clientes.

El motivo por el cual nuestra topología de red implementa dos niveles de firewall y de distintos proveedores, es siguiendo precisamente las recomendaciones del ENS que describe la necesidad de implementar un sistema de firewalls en uno o dos niveles, definiendo dos tipos de arquitecturas, tipo-5 (APP-5) o tipo-6 (APP-6), en la cual se pueden desplegar dos tecnologías de firewall del mismo o diferente fabricante.
La decisión de incluir distintos fabricantes viene motivada por la consideración de si un fabricante sufre un ataque o se descubre una vulnerabilidad que pueda afectar a nuestra red, ésta no se vea comprometida en su totalidad, sino solo en aquel segmento en el que se encuentre dicho fabricante.
Las funcionalidades de cada uno de los firewalls que elegimos para nuestra solución ya fueron descritas en apartados anteriores. Podemos observarlo de manare resumida en la ilustración 37

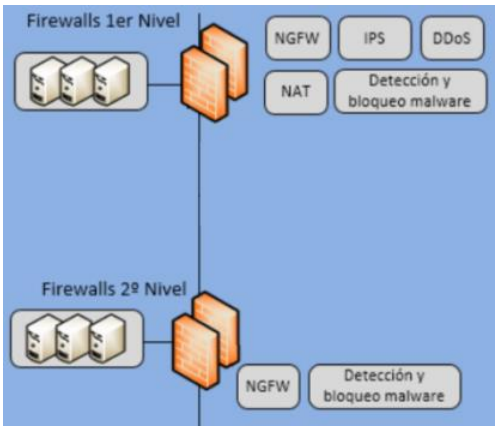


Ilustración 40 Perímetros de seguridad

2.3.1.1 Primer nivel

En el apartado Firewalls, definimos como firewall de primer nivel a un dispositivo del fabricante Check Point. Dicho equipo será la primera barrera de entrada a nuestra red y la puerta de salida para los usuarios internos hacia el exterior, además será el responsable de efectuar los NAT tanto de entrada como de salida, los servicios de VPN y DMZ están conectados en este primer elemento. Los conceptos de NAT, VPN y DMZ serán tratados en próximos apartados.
Esta primera barrera nos protegerá de atacantes externos en primer lugar de forma pasiva gracias a la configuración de la red en dos niveles, la red de usuarios no está conectada a este elemento, por lo que, no es posible atacarla, lo mismo ocurre con los servidores internos. En segundo lugar, contamos con los elementos activos de protección con los que cuenta el motor del dispositivo, como IPS, DDoS, detección y bloqueo de malware, etc. Además de los sistemas de detección de intrusos o vulnerabilidades, denegación de servicio y sandboxing, los administradores de seguridad deben implementar en los firewalls las políticas de seguridad.

Las políticas de seguridad definen los permisos que decidimos darle a determinados usuarios o redes para que alcancen algún recurso de nuestra red. Nuestros firewalls pueden implementar políticas a nivel de la capa de aplicación o de la capa de transporte y red.

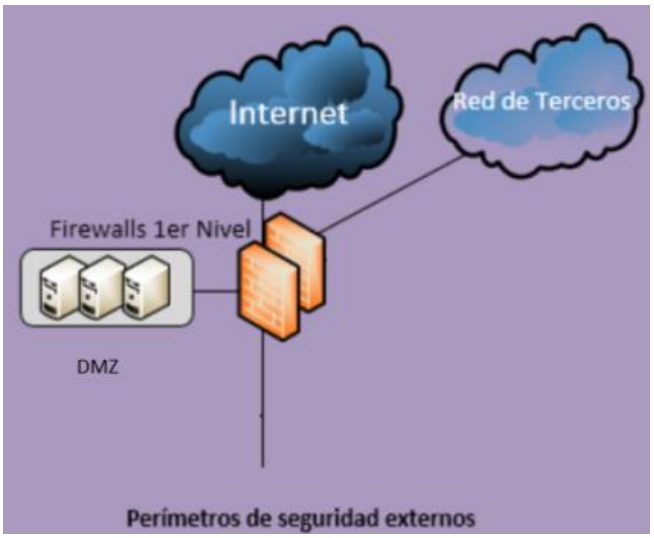


Ilustración 41 Perímetro externo

Por ejemplo, imaginemos que estamos en una de las sedes que conforman la comunidad educativa de la UOC, queremos conectarnos a uno de los servidores alojados en la DMZ para cargar la imagen de un sistema operativo, pero ¿Tenemos permiso para llegar desde nuestra IP hasta el servidor? Para que la conexión se efectúe, tiene que existir una política de seguridad específica que la permita, si no, por defecto existe una denegación implícita que nos impedirá llegar. Podemos permitir todo tipo de conexiones o solo algunos puertos determinados como los de FTP o TFTP para la transferencia de archivos.

Imaginemos ahora que detectamos un atacante externo que pretende inundar de peticiones alguno de nuestros servidores, primero nuestro sistema de denegación de servicio detectaría la IP de origen y tras ello, como buenos administradores de seguridad, implementaríamos una política de seguridad en la que con origen la IP del atacante, deneguemos todas las conexiones.

2.3.1.2 Segundo nivel

La segunda barrera de firewalls de nuestra red será un cluster formado por dos equipos de PaloAlto tal y como describimos en apartados anteriores. Esta segunda barrera será sin embargo el primer salto para los usuarios internos, ya que tanto la red de usuarios como los servidores internos, cuelgan de este dispositivo. En el apartado de flujos veremos en profundidad las rutas que seguirán los datos desde los diferentes orígenes.

Ya hemos comentado las ventajas de disgregar el tráfico de nuestra red en dos niveles distintos de seguridad, además de seguir las recomendaciones de los estándares de las diferentes normativas, aislamos las redes más críticas de los accesos externos y securizamos con un segundo nodo de protección. Como hemos comentado para el firewall de primer nivel, debemos implementar las políticas de seguridad que permitan o no a los usuarios acceder a determinados recursos. Aprovechando las funcionalidades de capa 7, podemos permitir por ejemplo a los usuarios acceder a redes sociales, pero capar vídeos, descargas o limitar la subida de archivos para evitar una hipotética fuga de información sensible de nuestras bases de datos. Si contamos con un

servidor RADIUS, nuestro dispositivo podrá sincronizarse con él e identificar las conexiones a nivel de usuario, esto nos permitiría tener mayor control y granularidad a la hora de conceder permisos de conexión o no.

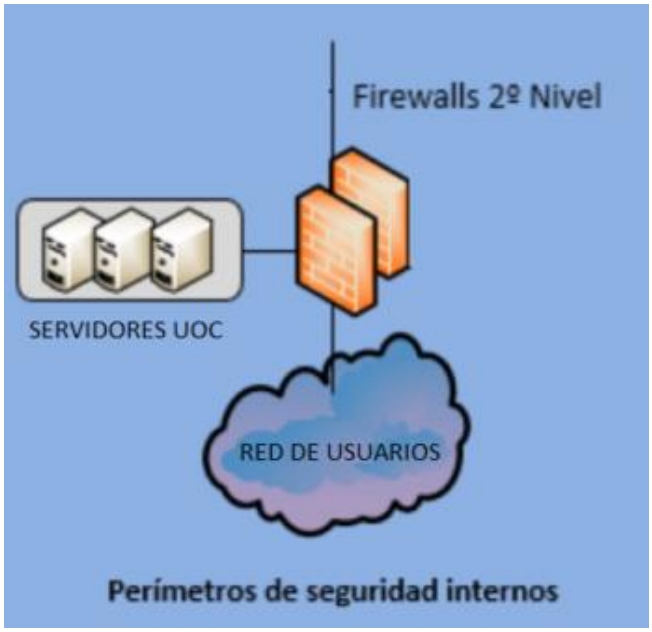


Ilustración 42 Perímetro interno

Para finalizar con el apartado de seguridad, comentaremos que los equipos de firewall cuentan con muchas más funcionalidades de las descritas en el presente punto, por ejemplo, serían capaces de aplicar QoS, servicios de DHCP y DNS, etc., nuestra solución incluye un dispositivo específico para cada función, ya que, así no concentramos en un único equipo varios servicios, lo cual supondría un punto de fallo mayor, además, también conllevaría un considerable aumento del rendimiento de la CPU del equipo. Así mismo, otros elementos de la red que no forman parte específica de la solución de seguridad implementan muchas medidas que contribuyen a salvaguardar la integridad de los de las comunicaciones. Por ejemplo, los equipos de switching, incluyen políticas que añaden seguridad a los puertos de acceso, como pueden ser el control de los flujos unicast o permitir solo un determinado número de MACs en un único puerto a la vez, otros elementos como los balanceadores cuentan también con detectores de vulnerabilidades para aplicaciones.

2.3.2 Telefonía IP

La telefonía es uno de los servicios más críticos e importantes dentro de una corporación, gran parte del modelo de negocio suele estar basado en este medio. Nuestra solución de basa en un sistema de telefonía IP con un plan de numeración interno para las llamadas corporativas y conexión a un proveedor de telefonía que a través de líneas E1 nos de salida hacia la red nacional pública de telefonía.

La telefonía fija E1es un servicio dedicado de telefonía digital que cuenta con una capacidad de 30 canales de voz, que permiten un máximo de 30 llamadas simultáneas (salientes y/o entrantes). Está diseñado para cubrir la necesidad de tener contratadas varias líneas telefónicas y manejar un alto volumen de llamadas.

El Gateway de voz que hemos incluido en nuestra solución dispone además de un sistema de gestión de llamadas, de esta forma, podemos controlar el plan de numeración interno de la comunidad, así como establecer los permisos que queremos conceder a los diferentes usuarios a la hora de efectuar una llamada saliente. Por ejemplo, si le permitimos efectuar llamadas únicamente nacionales, a móviles,

internacionales, etc., incluso restringir las llamadas externas a partir de que la cuantía de la tarificación de dicha línea supere unos márgenes previstos.
El Gateway enrutará la llamada hacia el proveedor de telefonía a través de las líneas E1 que hayamos contratado en el caso de que el número de destino se encuentre fuera del plan de numeración interno, o encaminará la llanada hacia la sede correspondiente en el caso de que se trate de un número corporativo.
En el apartado de flujos explicaremos con precisión como se efectúa la comunicación de voz a través de la red que hemos planteado.

2.3.3 DHCP

DHCP (Dynamic Host Configuration Protocol) es un conjunto de reglas para dar direcciones IP y opciones de configuración a ordenadores y estaciones de trabajo en una red.
Veamos cómo se efectúa la asignación de IP con la solución que hemos diseñado en nuestra red, para ello nos apoyaremos en el esquema de la ilustración 40.
Nuestra propuesta para la solución de DHCP está basada en el dispositivo infoblox presentado en apartados anteriores.
Cuando la estación de un usuario efectúa una petición de DHCP, ésta a través del switch de acceso al que está conectado llega hasta el gateway de dicho switch, en nuestro caso, el switch de distribución que por simplicidad hemos ilustrado como un único dispositivo. Una vez que la petición ha llegado al switch de distribución de nuestra sede, éste identifica la etiqueta de la VLAN de datos y comprueba si en la interfaz VLAN correspondiente hay configurado un DHCP relay. El DHCP relay no es más que una redirección de nuestra petición hacia otro dispositivo, por tanto, en la interfaz de la VLAN de datos del usuario, debemos configurar un DHCP relay hacia la IP de nuestro servidor DHCP, el infoblox. A través de la MPLS y con los permisos pertinentes en los nodos de seguridad, nuestra petición llegará al servidor DHCP. En dicho servidor tendremos configurado un pool de direcciones para cada VLAN de usuarios, y el equipo se encargará de asignar una IP de forma dinámica o establecerá siempre la misma (asignación estática) si asociamos la IP que estimemos conveniente a la MAC del PC que efectúa la petición inicial.
¿Cómo sabe infoblox de qué pool debe elegir la IP para la solicitud que le ha llegado? El pool está asociado a un filtro y el ítem que identifica el filtro es la IP de la interfaz VLAN del switch de distribución que efectuó el DHCP relay. De esta forma, el servidor DHCP asigna IP al equipo y guarda en su caché la dirección asignada hasta que dicha asignación caduque, momento en el cual consultará si la dirección está siendo aún utilizada o no para liberarla si ningún host está haciendo uso de ella, en el caso contrario, renovará el “alquiler” si aún está en uso.

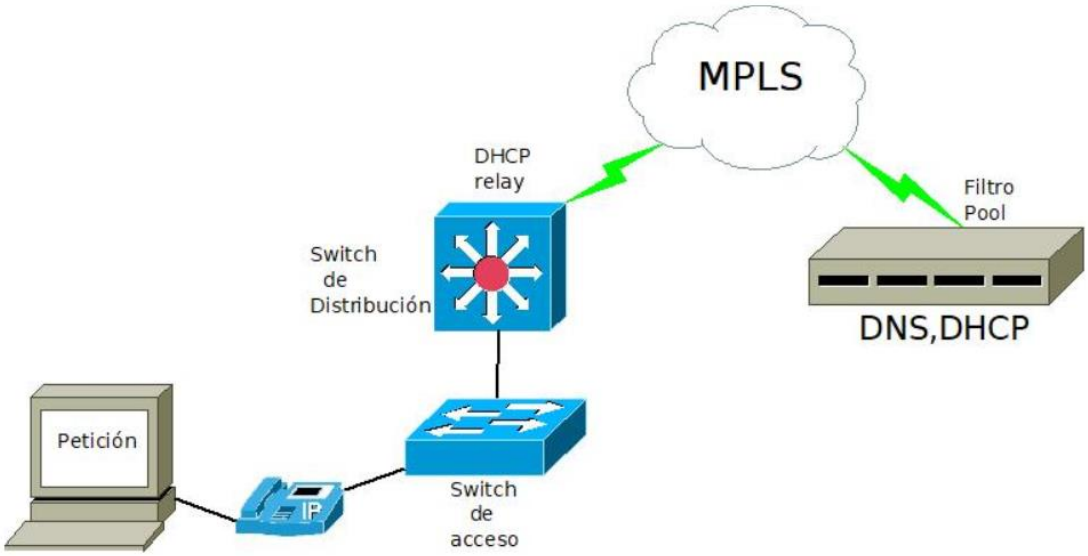


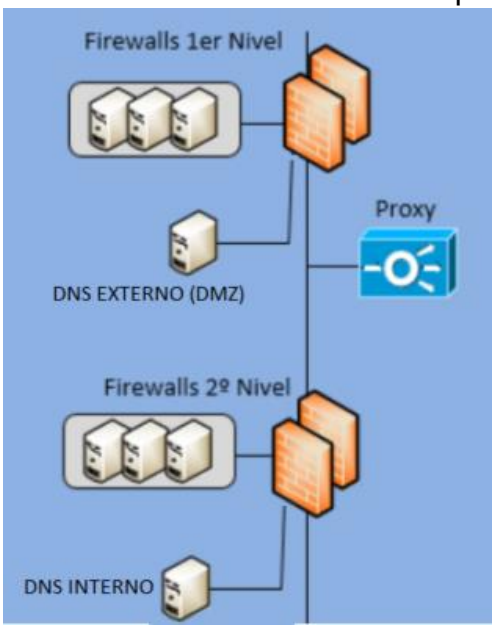
Ilustración 43 DHCP

Para las conexiones que se efectúen mediante VPN, aunque más adelante describiremos cómo se llevan a cabo dichas conexiones, el procesor para adquirir IP es prácticamente el mismo que ya hemos descrito, con la salbedad de que el filtro del pool que configuramos en el servidor no es la IP de una interfaz VLAN, sino el nombre del usuario VPN que establece la conexión a través del finalizador de túneles Ipsec, en el caso de la solución que hemos diseñado, el firewall de primer nivel CheckPoint que será el que efectúe el relay hacia los infobloxs.

2.3.4 DNS

Domain name server (DNS) es el sistema por el cual se traducen los nombres de dominio a las correspondientes direcciones IP del servidor que aloja el servicio solicitado. En nuestra propuesta, este servicio es llevado a cabo también por los servidores infoblox.
Podemos discernir entre dos tipos de servicios DNS dentro de nuestra propuesta, los internos y los externos.
El motivo por el cual nos decantamos por la tecnología infoblox como solución de DNS es, entre otras, que su módulo DNS efectúa labores también de servidor proxy, sirviendo de intermediario entre la conexión a internet y el usuario, si bien no efectúa tareas de inspección de contenidos ni gestiona los datos, (sería un proxy transparente), sí es capaz de cachear la páginas web más recurrentes de nuestra red y servirlas al usuario de manera local, de esta forma ahorramos ancho de banda y bajamos considerablemente la latencia de nuestra conexión.
Los DNS internos proporcionarán a los usuarios además de las traducciones de nombres de dominio, el servicio proxy-caché indicado anteriormente. Además, traducirá también aquellos dominios internos

que se encuentren alojados en los servidores de nuestra comunidad con IP privada. Para tal fin crearemos dominios privados del tipo @uoc.edu.
La función de los DNS externos será la publicación de servicios hacia internet. Esta funcionalidad se mueve en otro plano de conexión ya que, al provenir las peticiones de origen desde redes desconocidas, el servicio de DNS externo debe alojarse en una zona restringida de nuestra red denominada zona desmilitarizada (DMZ). Las consultas se encuentran en una red aislada para prevenir posibles ataques.



En el esquema de la ilustración 41, reflejamos las tres funcionalidades de nos proporciona el servidor de DNS descritas anteriormente.
Por un lado, tenemos la función de intermediario entre los dos niveles de seguridad con la función proxy. Por otro, los DNS internos y externos, cada uno en su segmento de red.
Aunque a nivel lógico observemos varios dispositivos, a nivel físico se trata del mismo GRID de dispositivos, configurando cada servicio en interfaces de red distintas.

Ilustración 44 DNS

2.3.5 Gestión de ancho de banda y QoS

Nuestra propuesta como gestor de ancho de manda e inteligencia de red, está basada en la tecnología de ALLOT.
El gestor de ancho de banda nos permite asignar un determinado caudal a las IPs públicas que se conectan a internet, de esta forma, estamos garantizando que ninguna conexión colapse toda nuestra salida a internet, dejando sin servicio al resto de usuarios o servicios.
Otro aspecto muy interesante es la aplicación de niveles de calidad de servicio (QoS), podemos crear políticas que garanticen por ejemplo el caudal de voz, de esta forma, las comunicaciones telefónicas nunca verán mermadas su calidad, de igual forma ocurre con otros servicios considerados críticos como las videoconferencias. La granularidad de un gestor de ancho de banda permite también limitar el caudal de las conexiones distinguiendo a nivel de capa de transporte y aplicación. Por ejemplo, imaginemos que tenemos permitido dentro de nuestra política de seguridad corporativa las conexiones P2P tipo Torrent, puede que nivel de seguridad estén controladas, pero ¿Cómo impedimos que no se adueñen de todo el ancho de banda de nuestra conexión? Simplemente

crearíamos un perfil en nuestro gestor para este tipo de conexiones. De igual forma ocurriría con FTP, descarga de contenidos multimedia, etc.

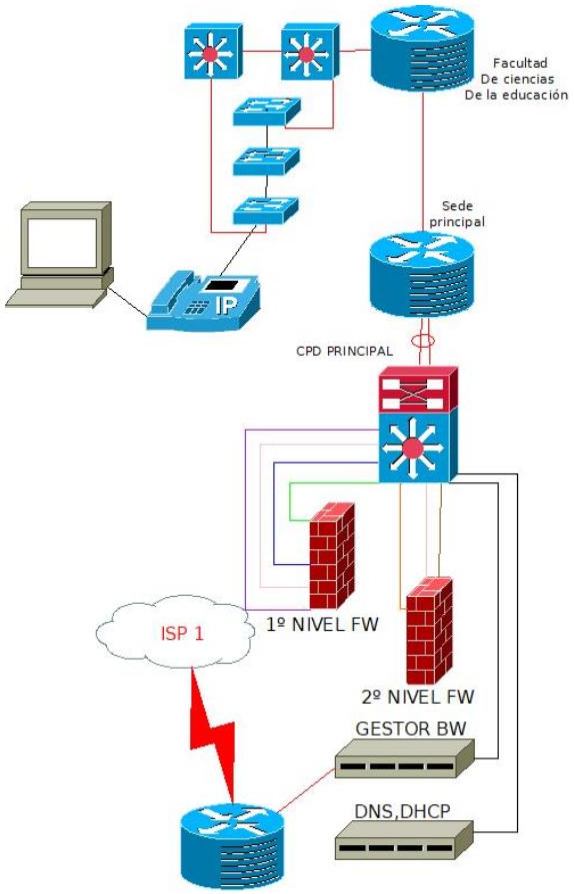


Ilustración 45 Gestor de ancho de banda

¿por qué hablamos también de inteligencia de red? La posición que ocupa en la topología el gestor de ancho de banda y las funciones que lleva a cabo, le permiten sacar estadísticas de la red como el ancho de banda consumido por usuario, IP pública, sede, etc. El caudal total que estamos utilizando, las IPs de destino más recurrentes, previsiones de saturación, etc. Toda esta información es de suma importancia para la gestión de una red.

No es casualidad que el gestor de ancho de banda sea el último salto antes de llegar a internet, el tráfico entra y sale de manera transparente y debe llegar ya nateado con las IPs públicas de navegación, para ello debe haber atravesado todos los niveles de seguridad.

En la ilustración 42 mostramos el esquema topológico en el que se ubica el gestor de ancho de banda a través de su salida por el CPD principal. A simple vista parece un único punto de fallo en nuestra red, ya que, si este cae y como hemos comentado, el tráfico discurre a través de él de forma transparente, nos quedaríamos sin acceso a internet. Para que no pueda darse esta circunstancia, el dispositivo cuenta con un sistema denominado bypass, que simplemente consiste en que si el gestor deja de dar servicio, incluso perdiendo la alimentación eléctrica, se comporta como un cable de red, o fibra en este caso, dejando atravesar todo el tráfico hacia el router PE de salida a internet, aunque lógicamente perdiendo todas sus funcionalidades.

Como administradores de red, si detectamos la caída de uno de los nodos de gestión de ancho de banda, podríamos redirigir el tráfico hacia el CPD de respaldo.

2.4 Acceso a internet, flujos y conexiones VPN

Una vez definida la topología, las tecnologías, los distintos protocolos de nivel 2 y 3 que intervienen, así como los servicios que dispensa la red

que hemos diseñado, llega el momento de agrupar toda la información y ver cómo funciona una red de comunicaciones en su conjunto.

2.4.1 Internet

El primer supuesto que analizaremos será el de un usuario que, desde una de las sedes de cualquier subanillo, desee conectarse a internet.
En primer lugar, a nivel de la capa de aplicación, dicho usuario abriría su navegador web y se dirigiría a cualquier página de internet.
La petición saldrá por la tarjeta de red del usuario atravesando la conexión con su teléfono IP como tráfico no etiquetado, hasta llegar al switch de acceso al que se encuentra conectado.
El switch de acceso es un dispositivo de capa 2, su puerto está etiquetado en la VLAN del usuario para datos, pero él no es capaz de enrutar el tráfico, por lo que, se lo entregará a su puerta de enlace predeterminada o Gateway, el switch de distribución.
Una vez que el paquete llega al equipo de distribución, él si sabe dirigir el tráfico, ya que es un dispositivo de capa 3 que forma una sesión IBGP, en nuestro ejemplo con el PE de la facultad de ciencias de la información. Su tabla de rutas le dirá que no encuentra el destino ya que es una IP pública que no se encuentra en su red y la desconoce. Por tanto, hará uso de su ruta por defecto, que es donde va a parar todo el tráfico para el que no existe una ruta más específica, en este caso el PE de la facultad de ciencias de la información.
Cuando el tráfico llega el citado PE, éste tampoco conoce el destino, no es posible tener en nuestra tabla de rutas todo el direccionamiento público de internet, por lo que, también se lo entregará a su ruta por defecto. Gracias a OSPF conoce a todos sus compañeros del anillo de fibra principal, y a través del parámetro de configuración de “local preference” de BGP, sabe que el mejor camino para las rutas por defecto es el PE de la sede principal, aunque si este cayera, sería el de la facultad de ingeniería.
Ahora nuestro paquete se encuentra en el router PE de la sede principal, el destino sigue siendo desconocido, en esta ocasión entra en juego una ruta estática que el PE tiene configurada como ruta por defecto para cada una de las VRF de nuestra red. Todo el tráfico que no conoce se lo entrega a través de esta ruta al firewall de segundo nivel por la interfaz de la VRF de datos que lo conecta a dicho dispositivo mediante el switch de core.
La petición se encuentra en el firewall de segundo nivel, nuestro PaloAlto, él si conoce el destino, tiene creado un objeto llamado IANA PUBLIC que es un rango en el que está incluido todo el direccionamiento público de internet. Nos toca aplicar todos nuestros motores de inspección de paquetes para comprobar si la petición del usuario puede suponer un riesgo para la red, si no es así, buscaremos en nuestra política de seguridad alguna regla en la que esté especificada que la IP del usuario que solicita ir hacia internet, tiene permiso para ello, como ya se ha comentado, también es posible si estamos sincronizados con un servidor RADIUS, aplicar reglas por usuario. Si encuentra una regla que permite el tráfico hacia IANA por el puerto 80 o 443, dejará salir el tráfico

y se lo entregará al destino que tenga configurado en su tabla de rutas para internet, en este caso, el firewall de primer nivel, el CheckPoint.
La petición del usuario se encuentra en el firewall de segundo nivel que inspecciona el paquete en búsqueda de posibles riesgos, a continuación, al igual que en el firewall de primer nivel, busca un macheo en su política de seguridad que compruebe que el usuario tiene permisos de seguridad para salir a internet, si machea en alguna regla que permita dicha conexión, ahora el firewall deberá natear la IP de origen a una de las IPs públicas de la entidad tenga asignada por organismos como RIPE.
Una vez nateado el tráfico, ya estamos listos para dar el último salto para salir en búsqueda del servidor web de destino, las comunicaciones salen por la interfaz configurada como salida a internet de nuestro CheckPoint hacia el PE de salida a internet.
Recordemos que, de manera transparente, antes de llegar al PE, el tráfico ha atravesado el gestor de ancho de banda que ha reconocido la IP pública gracias a las QoS que tiene configuradas, y ha aplicado las restricciones de caudal necesarias.
Cuando el tráfico llega al PE, es enrutado hacia nuestro proveedor de servicios de internet gracias a la sesión EBGP full routing que tenemos implementada mediante un sistema autónomo público también gestionado por RIPE.
Cuando el servidor web externo responde a la petición, nuestro ISP nos devuelve el paquete con la repuesta, encontramos el camino de vuelta gracias a la funcionalidad “proxy arp” de la interfaz de salida a internet del CheckPoint. Ahora debemos devolver el tráfico a una dirección de red privada que se encuentra dentro de nuestra red. Dicha dirección es conocida por todos los elementos de routing de nuestra red ya que es propia. Por tanto, a través de los protocolos de enrutamiento descritos anteriormente, la respuesta llegará de nuevo al equipo de distribución de la sede, el cual encontrará el host de destino buscando en su tabla ARP de la VLAN de datos la MAC que viene en la cabecera del paquete IP.

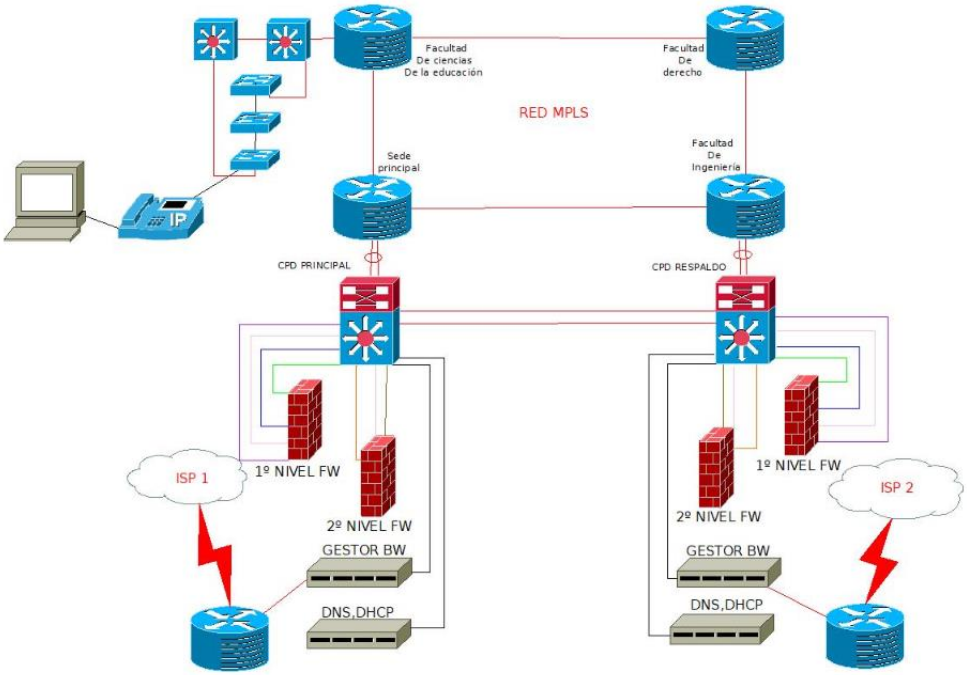


Ilustración 46 Flujo internet

2.4.2 Telefonía IP

Veamos el flujo de una llamada telefónica. El usuario descuelga el teléfono y marca una numeración, el paquete de datos sale de su teléfono IP como tráfico etiquetado, por ello, debemos configurar en el puerto de acceso del switch una VLAN de voz.
El tráfico etiquetado llega al switch de distribución, el cual cuenta con un comando donde se indica cual es el Gateway de voz principal y de respaldo de nuestra red.
La IP del Gateway es interna y como se encuentra en la misma VRF de voz, no es necesario enrutarla hacia otra VRF y no pasa a través del firewall.
La tabla de rutas de IBGP conoce la IP del Gateway a través de su vecino PE, y este a su vez, también a través de la tabla de rutas de IBGP, sabe que el dispositivo al que está conectado dicha red es el PE de la sede principal, el cual conoce gracias a la sesión OSPF que comparten.
El PE entrega la petición de llamada al Gateway de voz. Si la llamada es interna, éste encontrará el teléfono IP de destino gracias a su dirección de capa 3 a través de los dispositivos enrutadores de nuestra red, ya que, habrá necesariamente algún equipo de distribución anunciando una red de la que el dispositivo de destino mencionado forme parte.
En el caso de que fuera una llamada externa, el Gateway revisará en su política si la numeración de origen tiene permitida el tipo de llamada que desea ejecutar, si no es así podría devolver una locución informando de dicha falta de autorización, y si el usuario tuviera concedidos los permisos, entonces la llamada sería entregada al proveedor de telefonía quien la enrutaría hacía la red nacional de telefonía.

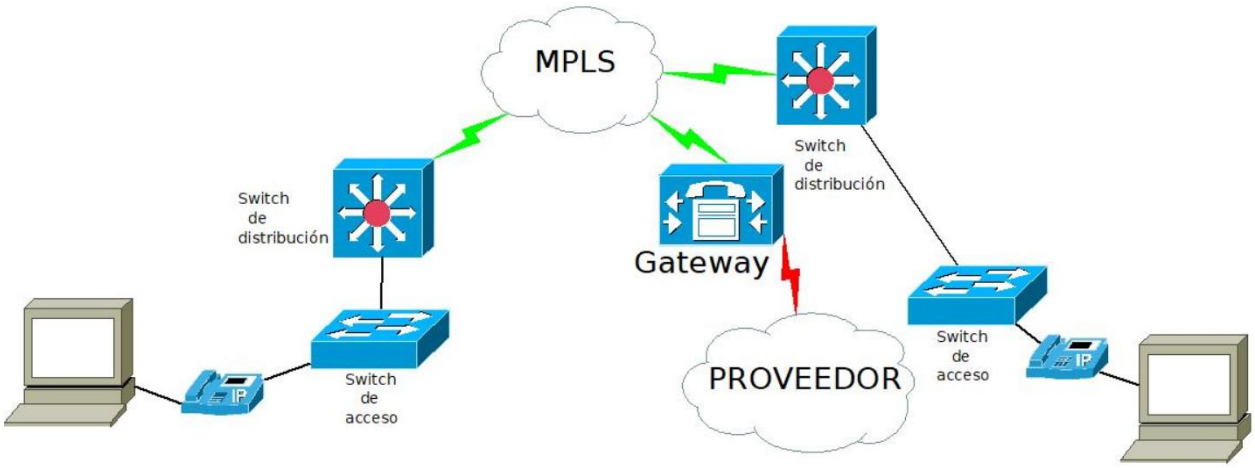


Ilustración 47 Telefonía

2.4.3 DMZ

La DMZ o zona desmilitarizada, es un segmento de red que aislamos del resto de redes de nuestra corporación debido a que a dicho segmento accederán redes no confiables que podrían suponer un gran riesgo para la integridad de la red.

En la DMZ quedarán alojados los servidores que web de nuestra corporación, por ejemplo, la del domino UOC.eu, veamos el flujo de las comunicaciones.

Un alumno desde su casa solicita a su navegador abrir la página de la UOC, los servidores DNS de Google por ejemplo, resuelven el nombre de nuestro dominio, y la petición llega hasta nuestro ISP, ya que él le anuncia al mundo que conoce nuestra red de direccionamiento público. Nuestro proveedor nos entrega el tráfico en el PE de conexión a internet y éste sabe enrutar el tráfico gracias al proxy arp de la interfaz de salida del nuestro firewall de primer nivel, que anuncia el direccionamiento público de nuestra comunidad.

La petición llega a nuestro CheckPoint y los motores de inspección de paquetes analizan si ésta supone una amenaza, si no es así, analizará las reglas de seguridad para comprobar si desde el exterior (IANA PUBLIC) está permitido acceder a la IP de destino solicitada. Si existe una regla que permite la conexión, entonces pasará a comprobar la reglas de NAT donde la IP pública del servidor de destino es trasladada a la IP privada de la granja del balanceador de carga donde se encuentra dicho servidor ya en el segmento de red DMZ.

Ahora el balanceador, nuestro F5, que también cuenta con un módulo WAF, analiza posibles comportamientos anómalos en la petición recibida, si no detecta ninguna anomalía, dirigirá la petición hacia alguno da los nodos configurados en la granja teniendo en cuenta el criterio de balanceo que tengamos implementado.

El servidor responderá a la petición, este sentido del tráfico para nuestra red es tráfico upload, de subida, antes de llegar al PE de salida a internet de nuevo y entregar nuestra página web al usuario, el gestor de ancho de banda aplicará el filtro pertinente que garantice que no vamos a saturar nuestra red.

De nuevo el paquete sería entregado al ISP quien lo enrutaría hacia su destino.

Anteriormente ya hemos citado que las tareas de enrutamiento entre nuestro PE y el proveedor de servicios de internet, se efectúa a través de EBGP y su establecimiento de vecindades mediante un sistema autónomo público que en el caso de EUROPA nos asigna la agencia RIPE NCC.

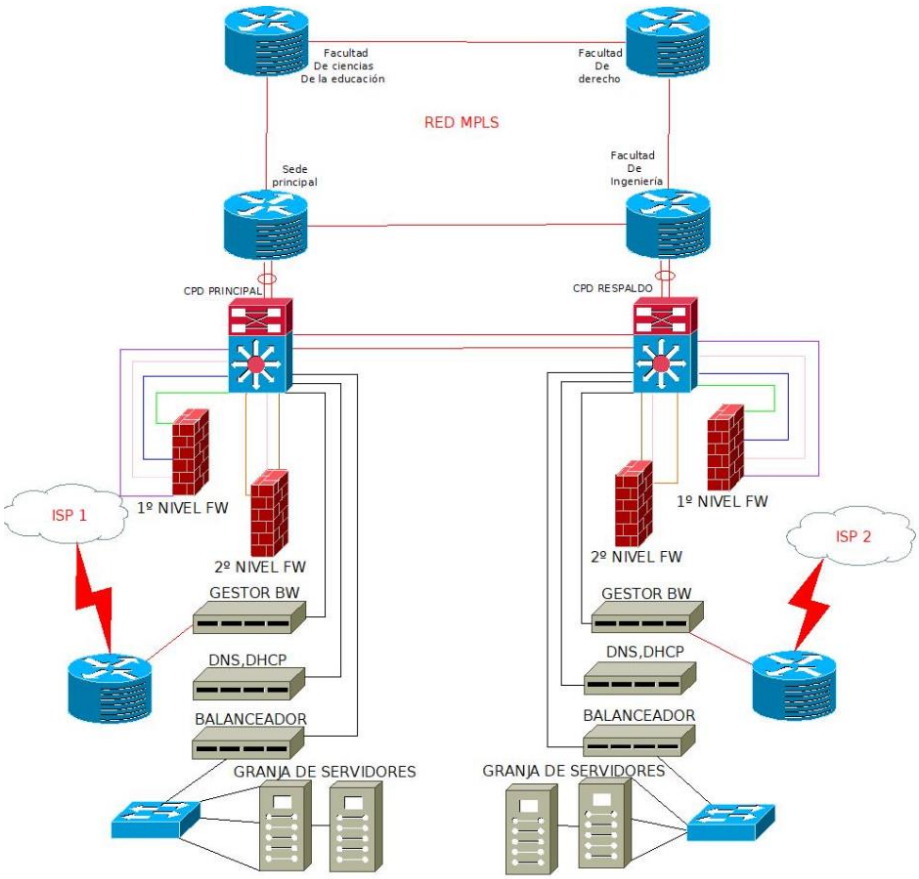


Ilustración 48 DMZ

2.4.4 InterUOC

Situemos a dos alumnos A y B, uno en la facultad de ciencias de la información y otro en la escuela de idiomas. Cada uno se encuentra en su VLAN de datos correspondiente y deciden abrir una conexión de escritorio remoto.

El alumno A intenta establecer la conexión con una IP que, aunque es privada y se encuentra dentro de la red corporativa, no se encuentra en la VLAN de datos de su sede ni pertenece a su VRF, por tanto, de nuevo el flujo de datos gracias a BGP pasa del equipo de distribución al PE de su propia sede y de éste al PE de la sede principal.

El PE de la sede principal para cada VRF de datos tiene una ruta estática hacia el firewall de nivel 2, PaloAlto.

El firewall conoce todas las redes y es el encargado de efectuar el enrutamiento entre VRFs dentro de la red corporativa. Esta característica está diseñada así para aprovechar los sistemas de detección de amenazas que tienen los dispositivos corta fuegos, además en ellos implementamos las políticas de seguridad que conceden los permisos para alcanzar destinos fuera de nuestra VRF.

Después de inspeccionar las posibles amenazas, el firewall comprueba en sus políticas de seguridad si la conexión tcp por el puerto 3389 (escritorio remoto) está permitida entre ambas IPs, si fuera así, devolvería el tráfico al PE de la sede principal pero ya con el cambio de VRF efectuado, ahora el PE preguntará a sus vecinos si alguien conoce

una red que contenga la IP de destino, el PE de la facultad de derecho le informará que tiene en su tabla de rutas una red que la escuela de idiomas le está anunciando por IBGP y que efectivamente, contempla la IP de destino. El paquete llegará al switch de distribución y este consultará su tabla arp de la VLAN de datos para encontrar la MAC del dispositivo de destino que ha desencapsulado de la cabecera de la trama ethernet. La conexión queda establecida.

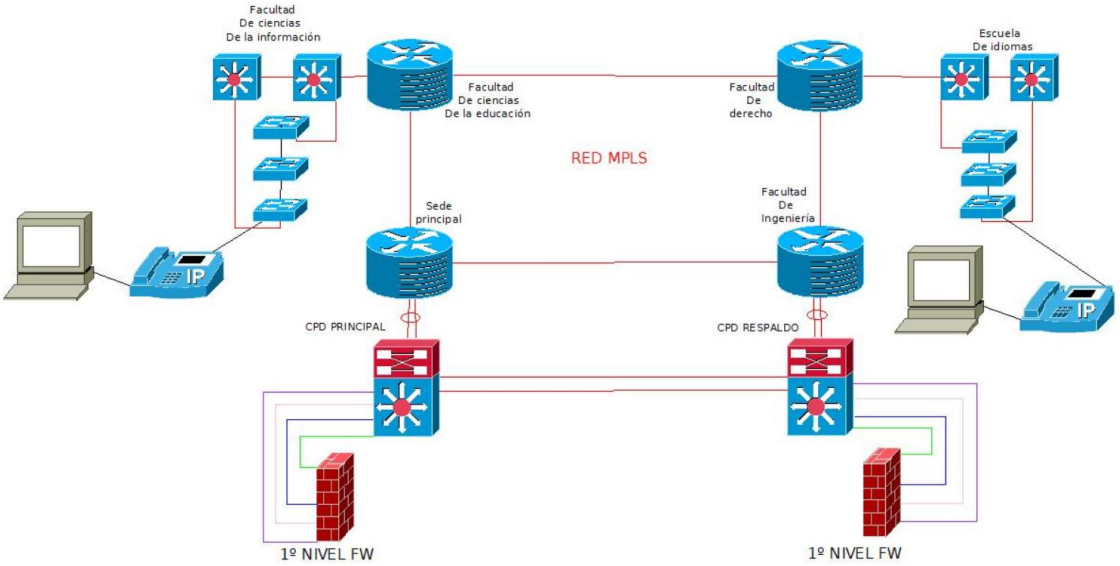
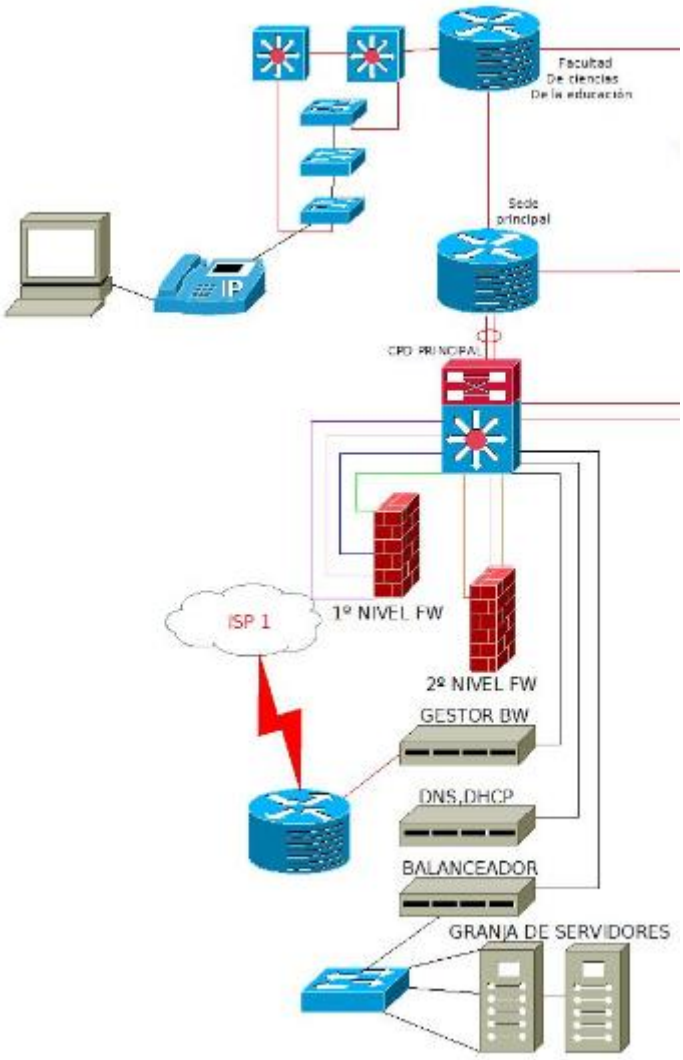


Ilustración 49 InterUOC

2.4.5 VPN

Virtual Private Network (VPN) es una conexión remota que establecemos a través de una red ajena, normalmente pública, para acceder a los recursos privados de nuestra red tal y como si estuviéramos dentro de ella.
Fundamentalmente se trabajan con dos tipos de conexiones, SSL e IPsec. La solución propuesta para nuestro entorno es un túnel IPsec mediante el firewall de primer nivel CheckPoint.
Imaginemos que un profesor que colabora con la UOC tiene que acceder a los servidores internos de la universidad para rellenar algún acta de notas.
La UOC le facilita a tal efecto una conexión VPN, para lo cual le suministra un software de conexión, un usuario y una contraseña, ¿cómo sería el flujo de datos en esta ocasión?



En primer lugar, el profesor instalaría el software de conexión en su equipo personal, tras ello, tendría que configurar la VPN introduciendo la Gateway pública de nuestro finalizador de túneles. Al conectar le solicitará usuario y contraseña. El ISP nos hará llegar la petición IPsec, y de nuevo el PE de conexión a internet enrutará los datos hacia el firewall de primer nivel, esta vez a través de la interfaz de accesos externos. Lo primero que hará el firewall nada más recibir la petición será comprobar en su base de datos de usuario o en el servidor RADIUS si lo tuviera, si las credenciales son correctas, incluso podemos sucurizar más la conexión implementando certificados digitales como los que emite la fábrica de moneda y timbre. Si las

Ilustración 50 VPN

credenciales del usuario son correctas, se establece el túnel ipsec. El tráfico que discurra a través de este irá encriptado.
A continuación, tal y como se explica en el apartado concerniente al DHCP, el firewall hará una petición DHCP al servidor en este caso infoblox y éste le responderá con una de las IPs del pool que tenga configurado para el grupo de usuarios al que pertenezca el profesor.
Una vez asignada la IP, en el sofware del ordenador personal del profesor la conexión aparecerá establecida, y podrá acceder a todos los recursos de la red corporativa que los nodos de seguridad le permitan por políticas y por análisis de riesgos, tal y como ya hemos explicado en apartados anteriores.

3. Conclusiones

El producto principal de nuestro proyecto ha sido la obtención de los flujos de trabajo.
Gracias a las diferentes asignaturas que hemos ido cursando durante nuestros estudios en ingeniería de telecomunicaciones, aprendimos los diferentes conceptos que hemos aplicado a la hora de diseñar la red. Conceptos sobre sistemas distribuidos, redes, seguridad, telemática, comunicaciones, etc.
El logro principal ha sido interrelacionar todos estos conocimientos a través de su integración con la capa OSI y de esta forma ser capaces de ofrecer una solución integral sobre la implementación de una red metropolitana completa. Desde la capa física con la descripción de los enlaces de fibra, pasando por la investigación sobre las tecnologías más actuales de los diferentes fabricantes para los distintos servicios que ofrece la red, hasta su implementación en los distintos segmentos de la solución propuesta.
Si bien hemos obtenido el objetivo principal que nos planteábamos y la metodología seguida ha sido correcta, sin tener que buscar otro enfoque, debemos comentar que la solución propuesta podría haber sido más completa y granular si la extensión del proyecto pudiera ser más amplia. Por ejemplo, para la solución VPN podríamos haber implementado otro elemento más de red como los servidores PULSE SECURE, disgregando la propuesta del firewall de primer nivel. Podríamos también haber potenciado el rendimiento de nuestra red con unos servidores proxy dedicados, directos y reverse para las publicaciones de servicios, por ejemplo, de la familia BLUECOAT. No obstante, con el diseño de la solución que hemos presentado, aunque no abarque al cien por cien todos los elementos que estarían presentes en una solución real, si nos ha servido para, como ya hemos comentado, ver el funcionamiento global de una red de telecomunicaciones.
Como líneas de trabajo futuro que no han podido ser abordadas en el presente proyecto, tenemos la integración de los servicios corporativos con el CLOUD COMPUTING. El presente y el horizonte de las telecomunicaciones parece apuntar en este sentido, el hardware propio dentro de las corporaciones tiende a ser sustituido por la contratación de los llamados servicios en la nube.
Otra tecnología incipiente son las redes gestionadas por software, donde la inteligencia de red permitirá la gestión de estas de forma sencilla y centralizada.

4. Glosario

Appliance
Dispositivo o equipo diseñado para realizar una tarea específica

Arp
(Address Resolution Protocol) es un protocolo de comunicaciones de la capa de red,1 responsable de encontrar la dirección de hardware (Ethernet MAC) que corresponde a una determinada dirección IP.

ATM
Modo de transferencia asíncrona (Asynchronous Transfer Mode, ATM)

BGP
Protocolo de puerta de enlace de frontera o BGP (del inglés Border Gateway Protocol)

BOOT
arranque o secuencia de arranque (bootstrapping, boot o booting)

Bypass

Circuito que actúa como válvula modificando el flujo normal de datos hacia una ruta alternativa si se produce una caída

CPD
Centro de procesamiento de datos

DDoS
Denegación de servicio

DHCP
Protocolo de configuración dinámica de host

DNS
Servidor de nombre de dominio

EBGP
External Border Gateway Protocol

EIGRP
Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado

HSRP
Hot Standby Router Protocol

IBGP
Internal Border Gateway Protocol

IPS
sistema de prevención de intrusos
IS-IS
Intermediate System to intermediate System

ISP
Proveedor de servicios de internet

LDAP
Lightweight Directory Access Protocol

MPLS
Multiprotocol Label Switching

NAT
Traducción de direcciones de red

OSPF
Open Shortest Path First

PDH
Jerarquía digital plesiócrona

PE
Provider Edge

PPT
Pliego de prescripciones técnicas

QoS
Calidad de servicio

RSVP
Resource Reservation Protocol

SDH
jerarquía digital síncrona

SONET
Red óptica sincronizada

SSL
Secure Sockets Layer

STP
Spanning Tree Protocol

VLSM
Máscaras de subred de tamaño variable

VPN
Red privada virtual
VRRP
Virtual Router Redundancy Protocol

5. Bibliografía

[1] Mª Carmen España Boquera, Comunicaciones Ópticas. Ediciones Díaz de Santos, S. A. Madrid, 2005.
[2]https://docplayer.es/26412550-Comunicaciones-opticas-1-introduccion-a-las-comunicaciones-opticas-area-fotonica-de-comunicaciones-profesor-alejandro-carballar.html
01/04/2019
[3]https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000597-en.pdf
01/04/2019
[4]https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000480-en.pdf
01/04/2019
[5] https://www.checkpoint.com/products/large-enterprise-security/
01/04/2019
[6] https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall/pa-3200-series
01/04/2019
[7] https://www.allot.com/resources/DS_SSG.pdf
01/04/2019
[8] https://www.infoblox.com/wp-content/uploads/infoblox-datasheet-ddi-appliances.pdf
01/04/2019
[9] https://www.f5.com/pdf/products/big-ip-platforms-datasheet.pdf
01/04/2019
[10]https://www.cisco.com/c/es_mx/support/docs/lan-switching/spanning-tree-protocol/24062-146.html
07/05/2019