Implementación de una red Wan en una escudería de F1

Trabajo Final de Carrera (TFC)

TFC 2012-2013

Luis Eduardo García Muñoz

Índice de Contenidos

Índice de Ilustraciones

1. Introducción

La escudería de Fórmula 1, Spanish F1, fue fundada recientemente y ha decidido adquirir como cabeza visible de su proyecto su sede central (headquarters) a la altura de cualquiera de los equipos que militan en la F1, decidiendo situar esta sede en Madrid.

Además de esta sede central, la escudería ha adquirido una pequeña sede en Alemania concretamente en Bobbingen, en esta sede es donde se encuentra la oficina de diseño del prototipo de coche para el año próximo y los siguientes. Se ha elegido esta ubicación porque es donde se realizó el diseño del actual coche, y se ha querido contratar almismogrupo de gente, para marcar una línea de continuidad.

Y por si no fuera poco el equipo de F1 ha llegado a un acuerdo con McLaren para poder utilizar su túnel de viento cada 15 días, las semanas que no haya carrera claro está. El túnel de viento de McLaren está situado en Inglaterra en la localidad de Woking.

Para poder conectar la sede central con la de Alemania y el túnel de viento en Inglaterra, se ha optado por plantear la implementación de una red WAN para comunicar ambas sedes con la central.

La conexión que se ha planteado para conectar la sede central con el túnel de viento es una IPLC o punto a punto Internacional de 2 Mbps con la empresa COLT, se ha optado por esta opción porque resulta más económico que desplazar cada vez que se vaya a realizar los test al equipo técnico y humano hasta allí.

Y la conexión entre Madrid y Alemania se realizará mediante MLPS de 34 Mbps con la empresa NTT Europe. Esta conexión se va a utilizar bastante y se ofrece esta opción al ser muy segura pues los datos que vamos a transportar por ella son muy importantes tanto para el desarrollo del coche del año próximo como las posibles mejores para el coche de la presente temporada.

2. Objetivos

El objetivo principal del proyecto consiste en el diseño y la implantación de una red WAN, la cual dispondrá de las siguientes características:

Una red IPLC E1 de 2 Mbps entre la sede Madrid y la sede Woking.

Una red MLPS E3 de 34 Mbps entre la sede Madrid y la sede Bobbingen.

Una red DSL E1 de backup entre la sede Madrid y la de Woking de 1 Mbps.

Una DSL de 4 Mbps de backup entre la sede Madrid y Alemania.

Este diseño permitirá tener interconectadas todas las sedes de la escudería tal y como si estuvieran en una misma red, y podrán acceder a los datos de la oficina de diseño y los reportes del túnel de viento casi en tiempo real, por todos los miembros de la escudería que se encuentren en cualquiera de las sedes.

Cuando haya test de túnel de viento, el departamento de ingeniería y el de software y simulación, podrá acceder a los datos resultantes del test en tiempo real, abaratando costes, ya que si cada 15 días que es cuando se realizan los test hay que enviar a todo el departamento de ingeniería y de software y simulación, resultaría más caro, a parte del tiempo que perderían en ir y volver hasta la localidad de Woking en Inglaterra.

Lo mismo sucede con la oficina de diseño, pues se trata de uno de los departamentos que tiene que estar en continuo contacto tanto como con el equipo de ingenieros como con el departamento de compras, incluso con los pilotos de pruebas, para buscar un camino a seguir en la construcción del coche para la próxima temporada.

2.1 Descripción de los capítulos de la memoria

En este apartado se van a describir el resto de capítulos de la memoria de una forma muy breve:

- Capítulo 2. Objetivos. Se enumeran los principales objetivos que se desarrollan en la memoria.

- Capítulo 3. Metodología. Aquí se detalla la metodología que sigue el proyecto, y se hace una estimación de las etapas y tareas que se van a llevar a cabo.

- Capítulo 4. Planificación de las fases del proyecto, consiste en ubicar en el tiempo el desarrollo de las fases del proyecto.

- Capítulo 5. Análisis general del proyecto. Se hace una análisis de los aspectos más importantes del proyecto.

- Capítulo 6. Estudio económico. Estimación económica y de financiación que permita evaluar la viabilidad del proyecto.

- Capítulo 7. Viabilidad. Se realiza una estimación sobre la viabilidad del proyecto teniendo en cuenta los datos aportados, así como el estudio económico.

- Capítulo 8. Análisis técnico del proyecto. Descripción sobre el conjunto de equipos escogidos para la implementación del proyecto.

- Capítulo 9. Seguridad. Se describen las pautas para securizar la implementación de la red.

- Capítulo 10. Sistemas de Backup y HA. Descripción de las elecciones de Backup y HA que se han tomado para el proyecto.

- Capítulo 11. Monitorización. Se detalla el sistema de monitorización elegido para la arquitectura.

- Capítulo 12.Glosario de términos.

- Capítulo 13.Referencias.

3. Metodología

Vamos a diferenciar las distintas apartados principales de las distintas fases en las que se desarrollará el proyecto.

Siendo estos apartados los siguientes:

- Planificación: es donde se expone el tema principal, el título, necesidades y distintas opciones para llevar a cabo el proyecto.
- Investigación: en este apartado es donde se revisa la información que se ha recopilado, y tras analizarla se comienza a determinar cuál es el modelo a seguir para la consecución del proyecto.
- Ejecución: en este apartado es en la que se prepara lo que contendrá la memoria que será toda la información técnica que vamos a necesitar para la consecución del proyecto.
- Finalización: en este apartado es donde se recopilan todos los datos obtenidos en los apartados anteriores, se corrigen los errores y se realizará la entrega del proyecto, también en este apartado se realiza la presentación visual del proyecto.

A continuación vemos de manera más detallada las tareas que disponen el proyecto.

4. Planificación de las fases del proyecto

Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
TFC- Implementación Red WAN en escudería F1	**121 días**	**mié 19/09/12**	**jue 17/01/13**	
Planificación	**16 días**	**mié 19/09/12**	**jue 04/10/12**	
Comienzo del Curso	1 día	mié 19/09/12	mié 19/09/12	
Presentación de la asignatura	2 días	jue 20/09/12	vie 21/09/12	3
Lectura Modulo 1	4 días	sáb 22/09/12	mar 25/09/12	4
Decisión del proyecto y comunicación con el Consultor	4 días	mié 26/09/12	sáb 29/09/12	5
Entrega PAC1	4 días	dom 30/09/12	mié 03/10/12	6
Corrección de errores detectados	1 día	jue 04/10/12	jue 04/10/12	7
Investigación	**47 días**	**vie 05/10/12**	**mar 20/11/12**	
Búsqueda de información y materiales necesarios	8 días	vie 05/10/12	vie 12/10/12	
Estudio de los equipos a utilizar	7 días	sáb 13/10/12	vie 19/10/12	10
Estudio de los distintos ISPs	7 días	sáb 20/10/12	vie 26/10/12	11
Estudio de las opciones de conexión WAN	7 días	sáb 27/10/12	vie 02/11/12	12
Conclusión sobre el estudio y análisis	7 días	sáb 03/11/12	vie 09/11/12	13
Redacción de los puntos estratégicos del proyecto	7 días	sáb 10/11/12	vie 16/11/12	14
Entrega PAC2	1 día	sáb 17/11/12	sáb 17/11/12	15
Corrección de errores detectados	3 días	dom 18/11/12	mar 20/11/12	16
Ejecución	**29 días**	**mié 21/11/12**	**mié 19/12/12**	
Elaboración de Diseño de Red	3 días	mié 21/11/12	vie 23/11/12	
Estudio de viabilidad técnica	3 días	sáb 24/11/12	lun 26/11/12	19
Estudio Planes de Backup	3 días	mar 27/11/12	jue 29/11/12	20
Elaboración Planes de Backup	3 días	sáb 01/12/12	lun 03/12/12	21
Desarrollo detallado de los recursos utilizados	3 días	mar 04/12/12	jue 06/12/12	22
Diseño y desarrollo WLAN y LAN escudería	3 días	vie 07/12/12	dom 09/12/12	23
Desarrollo WAN-MLPS	3 días	lun 10/12/12	mié 12/12/12	24
Desarrollo WAN-IPC	3 días	jue 13/12/12	sáb 15/12/12	25
Entrega PAC 3	1 día	dom 16/12/12	dom 16/12/12	26
Corrección de errores	3 días	lun 17/12/12	mié 19/12/12	27
Finalización	**29 días**	**jue 20/12/12**	**jue 17/01/13**	
Reunión de información	6 días	jue 20/12/12	mar 25/12/12	
Redacción de Memoria final	12 días	mié 26/12/12	dom 06/01/13	30
Repaso errores memoria final	3 días	lun 07/01/13	mié 09/01/13	31
Entrega de memoria	1 día	jue 10/01/13	jue 10/01/13	32
Elaboración de la Presentación	6 días	vie 11/01/13	mié 16/01/13	33
Entrega de la presentación	1 día	jue 17/01/13	jue 17/01/13	34

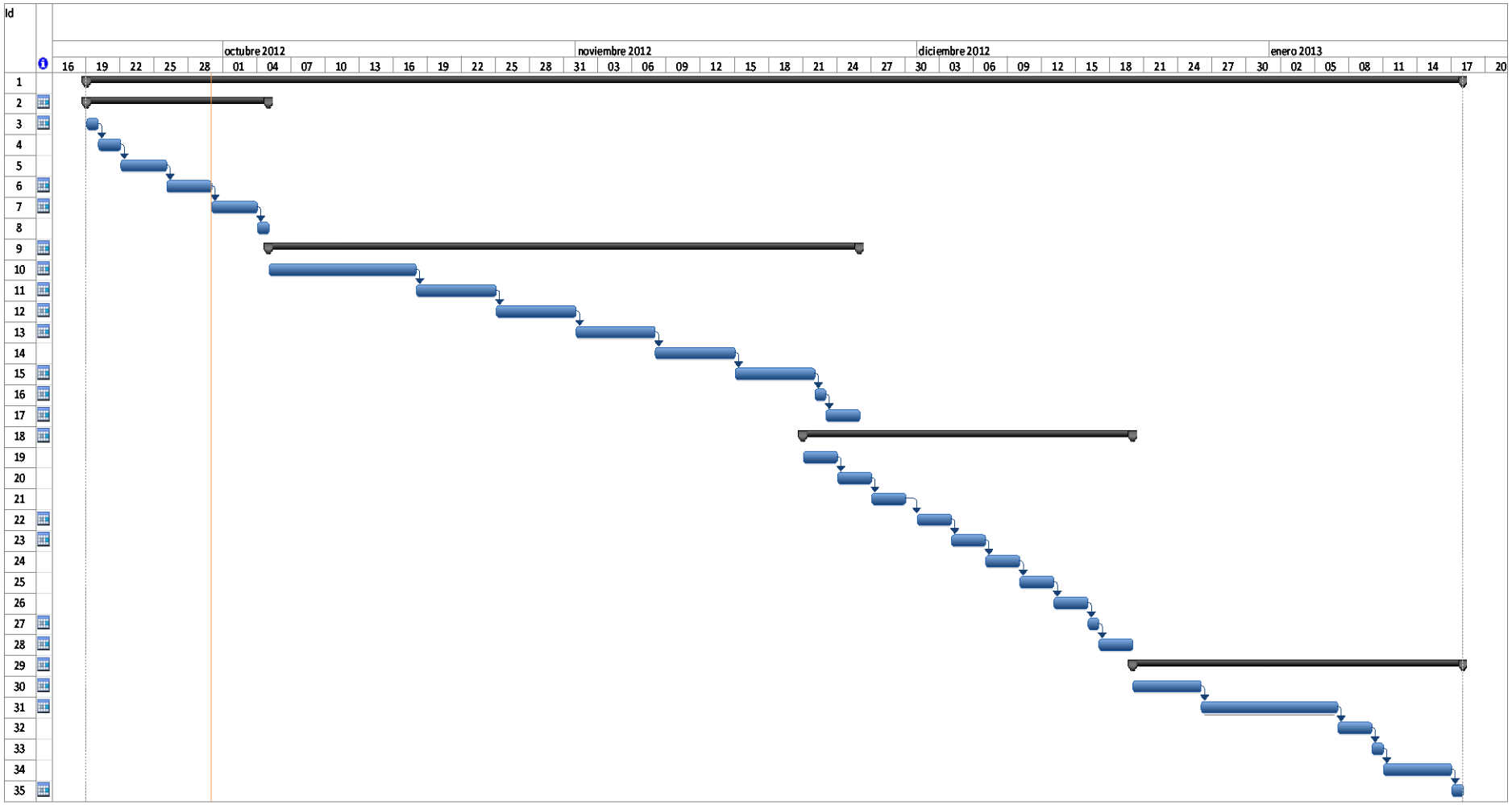

Ilustración 1. Diagrama de Gantt

5. Análisis general del proyecto

A continuación mostramos una foto de cuál es la idea general del proyecto:

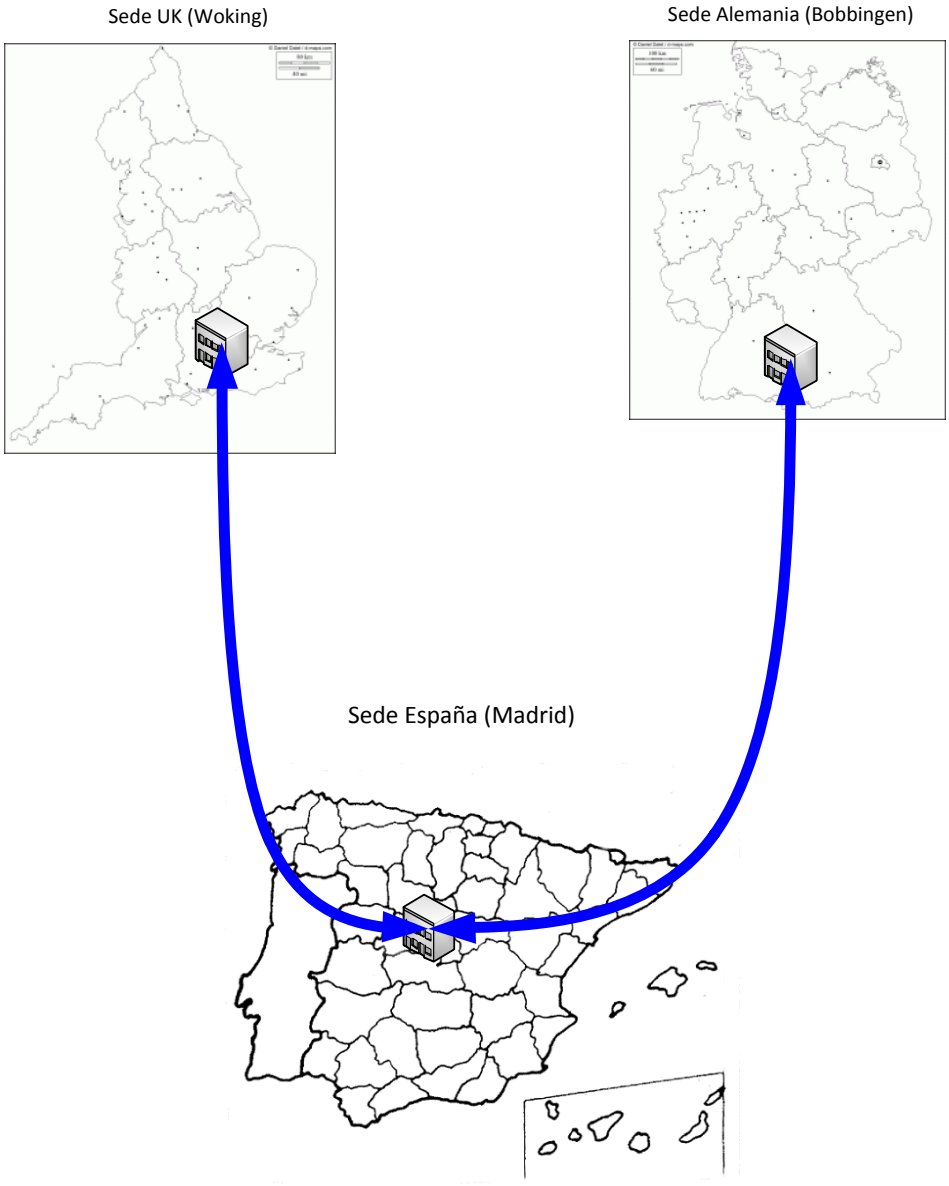

Ilustración 2. Diseño General

El equipo Spanish F1, ha optado por ubicar su cuartel general en Madrid, en esta sede es donde se ubicarán la mayoría de los departamentos que dispone la Escudería, y también es donde estarán la mayor parte del tiempo los mecánicos y los coches de la temporada actual.

Podemos ver la ubicación marcada en rojo en la siguiente foto:

Ilustración 3. Ubicación Sede Madrid

Pero de cara a la mejora del coche actual así como la evolución para el coche del año próximo, se ha decidido ubicar otra sede, en Bobbingen Alemania. Se ha elegido esta ubicación porque es donde en años anteriores se contrató al grupo humano que trabajó en la creación del coche actual. Al querer dar continuidad al proyecto se ha adquirido la planta de un edificio, en el núcleo empresarial de dicha ciudad. Las personas que fueron contratadas el año anterior para la creación del coche, han pasado a formar parte de la plantilla de la escudería. Para evitar mayores trastornos a los trabajadores, como tener que trasladarse a la ciudad donde se sitúa la sede central, hemos optado en apoyarnos en las nuevas tecnologías para conectar ambas sedes como si estuvieran físicamente en la misma red.

Esto se ha requerido de esta forma porque tanto para la creación del coche del año próximo, como las posibles mejoras para el coche actual, tendrá que haber comunicación directa entre esta sede y la sede central, que es donde se ubicarán los ingenieros de carreras, los mecánicos, así como el departamento de compras que será el encargado de una vez diseñado las distintas piezas para el coche, buscar proveedores para que fabriquen las piezas necesarias.

En la siguiente foto, marcada en rojo, podemos ver la ubicación del edifico en la que se aloja nuestra sede:

Ilustración 4. Ubicación Sede Bobbingen

Por otro lado tal y como se ha comentado anteriormente, se llegó a un acuerdo con la empresa McLaren, por el que un día cada 2 semanas, tenemos la posibilidad de utilizar el túnel de viento que esta empresa dispone en sus instalaciones.

Para hacer más cómodo el trabajo a nuestros trabajadores, y evitarles más viajes, además de los que ya hacen cada vez que se desplazan a cada carrera del campeonato de Fórmula 1, se ha decidido en cooperación con la empresa McLaren, conectar la sede central de Madrid, con el túnel de viento que la empresa dispone en sus instalaciones, por lo que tendremos acceso a los datos obtenidos en cada test en tiempo real, tal y como si estuviéramos presentes en las pruebas del túnel de viento.

Pero estas pruebas no solo son importantes para la gente de la sede central, sino que también lo son para el departamento de Diseño ubicado en Alemania, por lo que los datos serán alojados en la sede central, para que sean accesibles desde la sede de McLaren.

En la próxima foto, ubicamos la sede de Mclaren, en la que disponen de un túnel de viento:

Ilustración 5. Ubicación sede Woking

No solo vamos a proceder a la interconexión de la sede central con las dos sedes remotas, si no que también queremos incluir una red Wireless, tanto en la sede de Madrid tanto como la sede de Alemania.

La sede de Madrid al estar compuesta por una nave de dos plantas, en la que la planta baja es la zona donde se ubicarán los coches y los mecánicos, para estos últimos es más practico que accedan a la red a través de Wifi, pues están moviéndose casi de manera constante yendo y viniendo a por material, y necesitarán mandar correos electrónicos para hacer pedidos de piezas, o ver si han recibido algún correo electrónico nuevo con información de algún cambio que deban introducir en el coche. En la planta primera, es donde se ubican la zona que será denominada la zona de oficinas, es donde se ubican los departamentos de administración, secretaría, ingeniería, IT, compras, RRHH, finanzas, recepción, marketing, así como la zona de salas de reuniones y la zona de los despachos de los responsables de la escudería.

En las épocas de máxima afluencia en la sede, es decir, cuando todo el equipo se encuentra en trabajando en la sede, serán unas 200 personas, 100 son las que se mueven durante toda la temporada realizando el Mundial de F1, el resto de las 100 personas son las que están fijas en la sede y las situadas en la primera planta.

Mientras que en la sede de Alemania, el número de personas que habrá trabajando en la denominada Sede para la oficina de diseño, son unas 50 personas 20 en el departamento de Aerodinámica y 25 en el de diseño y modelado de piezas, el resto serán personal de secretaría, recepción y RRHH.

Para estas dos estaciones la red local LAN, las configuraremos a una velocidad de acceso de 100 Mbps para usuarios finales, mientras que para la comunicación entre los equipos de comunicación, será de 1000 Mbps

Debido al gran número de personas que habrá trabajando simultáneamente tanto en la sede principal como en la sede de Alemania, se ha decidido interconectar estas dos sedes mediante una conexión MPLS de 34 Mbps.

Mientras en la sede del túnel de viento de Mclaren, tendremos a 2 personas desplazada continuamente allí, que serán las que recibirán las directrices desde la sede central para las configuraciones que ha de tener el túnel de viento durante las pruebas que se realizarán, y realizar la conexión adecuadamente para que los datos sean enviados en tiempo real a la sede para que puedan ser estudiados tanto como la gente de la sede central como la gente de la sede de Alemania. Además de ver la configuración que tendrá el coche para cada prueba. Para este apartado se ha contratado una conexión IPLC, con una velocidad de 2 Mbps.

En nuestra sede de Madrid, hemos configurado una red desmitalirizada DMZ, en el que tenemos ubicado los servidores web de nuestra página web, así como el servidor de correo webmail. En esta misma sede dispondremos del centro de procesamiento de datos con los servidores centrales y un proxy común para garantizar un buen uso de los sistemas de información.

6. Estudio Económico

6.1 Estudio Económico Equipamiento

A continuación vamos a detallar el estudio económico de la sede Madrid:

Comunicaciones			
Equipo	Cantidad	Precio Unidad	Precio Total
Cisco 7204 VXR	1	5824,78	5824,78
Cisco Catalyst 3560X	2	3189,56	6379,12
Cisco Catalyst 2960 S	4	2102,78	8411,12
Cisco AIR-WLC2112-K9	1	1517,58	1517,58
Cisco AIR- LAP 1041 N- E-K9	5	215,18	1075,9
Fortigate 300 C	2	4305	8610
BlueCoat SG300-25	1	7845	7845

Equipamiento			
Equipo	Cantidad	Precio Unidad	Precio Total
Rack	2	1320	2640
Sais APC 3000	2	1694	3388
Sais APC 200	2	649,99	1299,98

Tabla 1. Estudio Económico Madrid

Siendo la suma para la sede de **Madrid**esde un total de **46991,48 €**

A continuación vamos a ver el estudio económico del equipamiento para la sede de Bobbingen Alemania.

Comunicaciones			
Equipo	Cantidad	Precio Unidad	Precio Total
Cisco Router 3845	1	5260,97	5260,97
Cisco Catalyst 4928 S	2	2634	5268
Cisco Catalyst 2960 S	2	2102,78	4205,56
Cisco AIR- AP 1041 N- E-K9	1	215,18	215,18

Equipamiento			
Equipo	Cantidad	Precio Unidad	Precio Total
Rack	1	1320	1320
Sais APC 3000	1	1694	1694
Sais APC 200	1	649,99	649,99

Tabla 2. Estudio Económico Bobbingen

Siendo la suma para la sede de**Bobbingen**esde un total de **18163,7 €**

A continuación vamos a ver el estudio económico del equipamiento para la sede de Woking UK.

Comunicaciones			
Equipo	Cantidad	Precio Unidad	Precio Total
Cisco Router 3845	1	1678,65	1678,65
APC SMART-UPS 1000VA LCD 230V	1	416,38	416,38

Tabla 3. Estudio Económico Woking

Siendo la suma para la sede de **Woking** es de un total de **2095,03 €**

Por lo que la suma en equipamiento para **todas las sedes** ascenderá a:**67250,21 €**

6.2 Estudio Económico Líneas

La contratación de las líneas la hemos establecido con dos empresas, con las que hemos llegado a un acuerdo gracias a nuestro departamento de marketing, por el que se les ofrece ser patrocinadores del equipo.

Gracias a este acuerdo se pondrá una pegatina de su empresa en el coche en un lugar preferente, a continuación paso a detallar lo acordado.

Con la Empresa NTT Communications:

20 % de descuento en la instalación.

9 % de descuento en la mensualidad durante 3 años, transcurridos los cuales se volverá a renegociar el contrato de patrocinio.

Y nos ofrecen el servicio de cliente GOLD, por el que nos aseguran un SLA del 98.5 %, y solucionar cualquier avería en menos de 4 horas.

Con la Empresa COLT:

15 % de descuento en la instalación.

15 % de descuento en la mensualidad durante 3 años, transcurridos los cuales se volverá a renegociar el contrato de patrocinio.

Y nos ofrecen el servicio de cliente GOLD, por el que nos aseguran un SLA del 96%, y solucionar cualquier avería en menos de 3 horas.

6.2.1 Estudio Económico Línea Madrid-Bobbingen

La comunicación Madrid-Woking se ha contratado con la empresa NTT Communications, a continuación presento el presupuesto inicial que nos facilitaron:

Proveedor	Instalación	Mensualidad	Velocidad	Localización	Tipo
NTT Europe	4389€	895€	34 Mb	Madrid/Bobbingen	MPLS E1

Tabla 4. Estudio económico Línea MPLS 1

El presupuesto tras el descuentoacordadoserá:

Proveedor	Instalación	Mensualidad	Velocidad	Localización	Tipo
NTT Europe	3871,2€	814,45€	34 Mb	Madrid/Bobbingen	MPLS E1

Tabla 5. Estudio económico Línea MPLS 2

También se ha contratado una línea de Backup con la empresa COLT, la cual va a ser una DSL de 6MB, se hace con otra empresa distinta con la que tenemos contratada la línea principal por temas de redundancia y poder asegurar la alta disponibilidad (HA) en la implementación del proyecto. El presupuesto inicial será el siguiente:

Proveedor	Instalación	Mensualidad	Velocidad	Localización	Tipo
COLT	500€	230€	6144/1024 Mb	Madrid/Bobbingen	DSL

Tabla 6. Estudio económico DSL 1

Por lo que el presupuesto, tras el descuentoacordadoserá:

Proveedor	Instalación	Mensualidad	Velocidad	Localización	Tipo
COLT	425€	34,5€	6144/1024 Mb	Madrid/Bobbingen	DSL

Tabla 7. Estudio económico DSL 2

6.2.2 Estudio Económico Línea Madrid-Woking

La comunicación de la línea Madrid-Woking se ha contratado con la empresa COLT, a continuación el presupuesto inicial que nos facilitaron:

Proveedor	Instalación	Mensualidad	Velocidad	Localización	Tipo
COLT	7823€	347€	2 Mb	Madrid/woking	IPLC

Tabla 8. Estudio económico IPLC 1

Por lo que el presupuesto, tras el descuentoacordadoserá:

Proveedor	Instalación	Mensualidad	Velocidad	Localización	Tipo
COLT	6649,55€	294,95€	2 Mb	Madrid/woking	IPLC

Tabla 9. Estudio Económico IPLC 2

También se ha contratado una línea de Backup con la empresa NTT Communications, la cual va a ser una DSL de 2MB, se hace con otra empresa

distinta con la que tenemos contratada la línea principal por temas de redundancia y poder asegurar él HA en la implementación del proyecto. El presupuesto inicial sería el siguiente:

Proveedor	Instalación	Mensualidad	Velocidad	Localización	Tipo
NTT Europe	360€	160€	2048/384 Mb	Madrid/woking	DSL

Tabla 10. Estudio Económico DSL

Por lo que el presupuesto, tras el descuentoacordadoserá:

Proveedor	Instalación	Mensualidad	Velocidad	Localización	Tipo
NTT Europe	288€	145,6€	2048/384 Mb	Madrid/woking	DSL

Tabla 11. Estudio Económico DSL

7. Viabilidad

Teniendo el estudio aproximado del equipamiento, vemos que es un precio asumible teniendo en cuenta que la escudería acaba de fijar sus sedes por lo que el desembolso inicial en infraestructura es totalmente necesario y asumible, claro está.

De todos modos este desembolso se hace principalmente para evitar desplazamiento y molestias al personal que ya reside en Alemania, con el consecuente gasto que ello conlleva.

Del mismo modo se intenta evitar el gasto del desplazamiento que supondría un día cada dos semanas de unas 60 personas, 40 de la sede de Madrid y otras 20 de la sede de Alemania a la sede de Mclaren en Wokin (UK), ya no solo el gasto en el desplazamiento si no también el desembolso en dietas, transportes del aeropuerto a Woking, incluso días de alojamiento. Además de que la mayoría de las personas que se trasladarían serían los que viajan con el equipo de F1 a realizar el Mundial de F1, con el consecuente cansancio para estas personas que ya viajan por todo el mundo durante todo el año.

En cuanto a la contratación de las líneas, nuestro departamento de marketing, está reuniéndose con varias empresas que ofrecen los servicios que vamos a requerir, de cara a conseguir un acuerdo en el que consigamos una importante rebaja, a cambio de poner una pegatina de publicidad de su empresa en nuestro coche, el gasto para cualquier empresa que quiera ser nuestro patrocinador es bastante elevado, por lo que estamos barajando que empresa elegir, en función de lo que ofrezca cada una. Tal y como se muestra en el apartado anterior hemos llegado a un acuerdo con las dos empresas COLT y NTT Communications, consiguiendo los descuentos anteriormente descritas.

8. Análisis técnico del proyecto

8.1 Comunicación entre Madrid y Bobbingen.

Como se ha ido comentando con anterioridad en la memoria del proyecto, sabemos que para esta conexión vamos a utilizar una conexión MPLS de 34 Mbps, con la empresa NTT Communications.

En el siguiente esquema de red se muestran conexiones lógicas utilizadas para la conexión WAN, además de la ubicación de la red DMZ aunque este tema será desarrollado más en profundidad en el apartado de "Seguridad en la red".

El servicio MPLS es un mecanismo de transporte de datos el cual trabaja en la capa 2 y 3 del modelo OSI, y que mantiene un estado de la comunicación entre dos nodos a través circuitos virtuales.

El servicio MPLS funciona anteponiendo a los paquetes una o más etiquetas, en las cuales añade información, tal y como se puede ver a continuación:

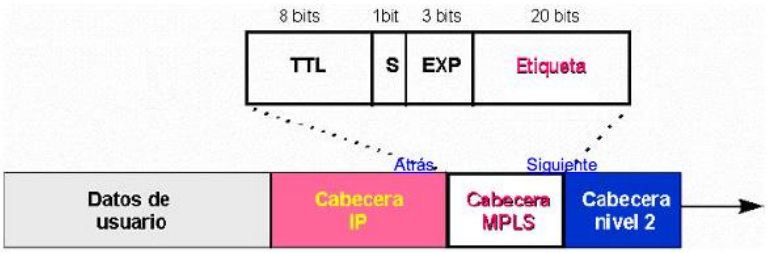

Ilustración 6. Cabecera MPLS

Por ultimo sabemos que la distribución de estas etiquetas se hace gracias al protocolo LDP (LabelDistributionProtocol) por el que sesiones TCP entre los routers MPLS que mapean las entradas con sus respectivas salidas facilitando así el envío automático de paquetes con las mismas características hacia el destino.

Para más información acerca de MPLS, consultar:

[14]http://es.wikipedia.org/wiki/Multiprotocol_Label_Switching

[15] http://www.monografias.com/trabajos29/informacion-mpls/informacion-mpls.shtml

Con la red MPLS podemos crear una VPN que nos va a proporcionar un acceso exclusivo para la empresa a través de un circuito dedicado. Este punto es de vital importancia para la escudería pues es de sobra conocido por todos, el espionaje industrial que hay en la F1 y que es vital para evitar copias o plagios de los planos de los coches.

El protocolo de comunicación utilizado para el intercambio de información con el ISP es el BGP.

Mientras que el protocolo utilizado para el intercambio de información entre los routers de la empresa, para mantener actualizadas las tablas de enrutamiento, topología y vecinos de una manera eficiente, es el protocolo EIGRP propiedad de Cisco Systems y se encuentra dentro de los del grupo denominado vector de distancias. Si se requiriera establecer comunicación mediante equipos que no fueran Cisco utilizaríamos uno de los protocolos del grupo vector distancia, como es el OSPF.

Con lo planteado hasta el momento tenemos suficientes recursos para soportar todo el volumen de tráfico generado por las sedes, así como la comunicación dentro de las mismas. Como se puede apreciar se han adquirido los equipos sobredimensionados, con vistas a una posible ampliación de personal en cualquiera de las sedes. Pues se espera que en un periodo estimado de medio plazo el equipo de Formula1 pase a estar entre los 5 primeros del campeonato. Este es el principal motivo por el que se ha sobre dimensionado los equipos adquiridos.

El esquema lógico de la red será el que se muestra a continuación.

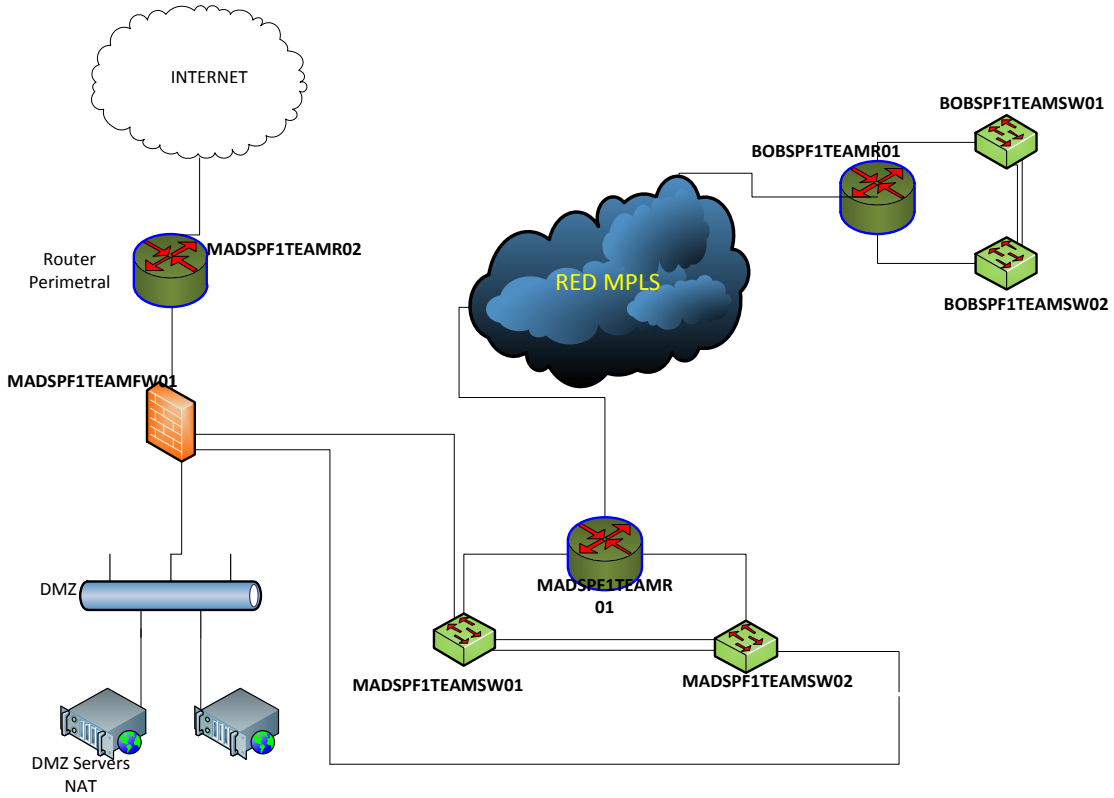

Ilustración 7. Esquema lógico de la red

8.1.1 Comunicación Sede Madrid.

Como ya se ha mencionado con anterioridad en la redacción de la memoria, Madrid es la denominada Headquarters para la empresa, por tanto en esta sede es donde encontraremos el data center, servidores de acceso externo proxy y firewall. A esta sede se conectarán tanto la sede de Alemania como la de Inglaterra, formando una

topología de red conocida como spoke-hub o topología en estrella. Se conoce como spoke-hub a la topología centralizada con un nodo central (hub) del que salen todos los ramales.

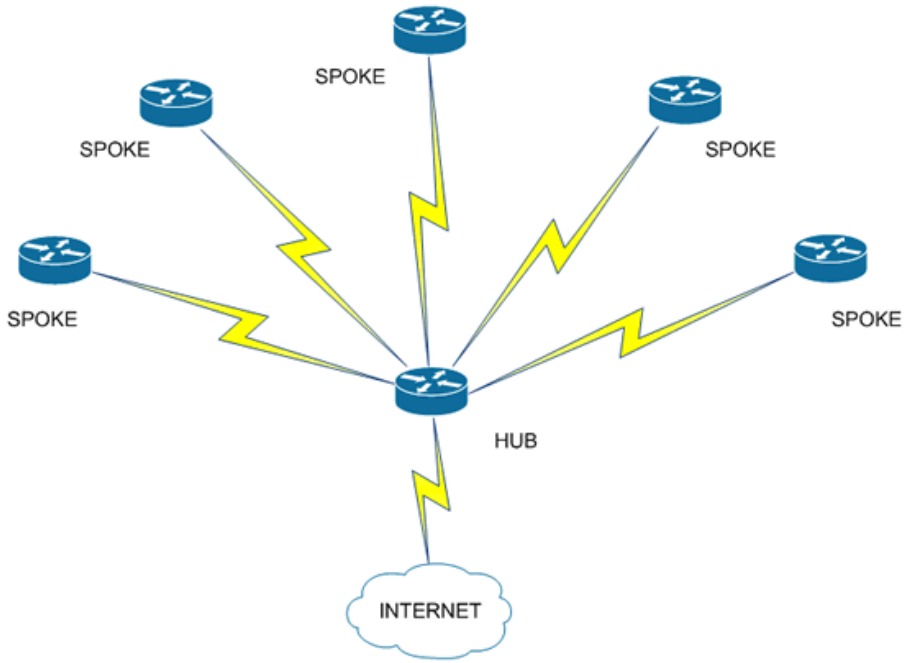

Ilustración 8. Arquitectura Spoke-Hub

En la sede principal de Madrid es donde tenemos ubicado el router*"MADSPF1TEAMR01",* este es el que unirá con la sede de Alemania y de Inglaterra, y también se podrá conectar cualquier otra sede que se quiera añadir en el futuro.

El router MADSPF1TEAMR01 es un Router Cisco, concretamente el modelo 7204 VXR, dispone de redundancia en cuanto a alimentación eléctrica, pues dispone de dos fuentes de alimentación, y se pueden cambiar sin necesidad de apagar completamente el equipo, lo cual es altamente recomendable, para poder garantizar el High Availability (HA) en toda la instalación.

Dispone de 4 slot vacíos en los que podemos añadir tarjetas para ofrecer los servicios MAN y WAN que queremos implementar, además de la velocidad a la que puede trabajar así como los servicios que ofrecen.

Gracias a esto hace que sea el ideal para poder cumplimentar los requerimientos deseados.

Ilustración 9. Router Sede Madrid Cisco7204Front

Ilustración 10. Router Sede Madrid Cisco7204 Back

Para que cumpla todas las características deseadas vamos a añadir dos tarjetas una para la conexión E3 MPLS y otra para la conexión E1 IPLC.

Conectado al Port adapter slot 1 tenemos conectada una tarjeta de 4 Puertos en serie E3, que nos permite realizar hasta dos conexiones dedicadas E3. De las dos conexiones que permite realizar utilizamos una para conectar esta sede con la de Bobbingen. El otro lo tendríamos como por si fallará el primero o por si en un futuro quisiéramos hacer otra conexión con otra sede.

Utilizaremos el puerto 1/0/1 en el que definiremos encapsulación HDLC y velocidad de 34 Mbps, que es la que vamos a utilizar para conectar nuestra sede con Bobbingen.

Ilustración 11. Tarjeta 4 puertos E3

Conectado al Port adapter slot 2, tenemos conectado una tarjeta con 2 puertos E1, con esta tarjeta podemos realizar dos conexiones E1 dedicadas o podemos unir ambos interfaces mediante una interfaz virtual, por lo que podemos tener 16 HDLC (High-Level Data control) canales utilizables para E1. Para nuestro caso utilizamos la opción de virtualizar los dos puertos aunque únicamente utilizaremos una conexión E1, esto lo hacemos para asegurar la HA en nuestra implementación.

Al tratarse de una conexión punto a punto, no necesitamos más configuración.

Ilustración 12. Tarjeta 2 puertos E1

En el esquema físico de la conexión entre ambas sedes se puede ver claramente el dibujo final del enlace entre ambas sedes. Se han comprado los equipos algo sobredimensionados para una posible expansión como la adquisición de una nueva sede, en el futuro.

Ahora vamos a ver los aspectos técnicos relacionados con la conexión de ambas estaciones mediante la conexión MPLS, entre ambas sedes para que todas estén en la red común de la empresa.

Los switches de capa 3 pertenecientes a la capa Core de la arquitectura de red, los veremos más adelante.

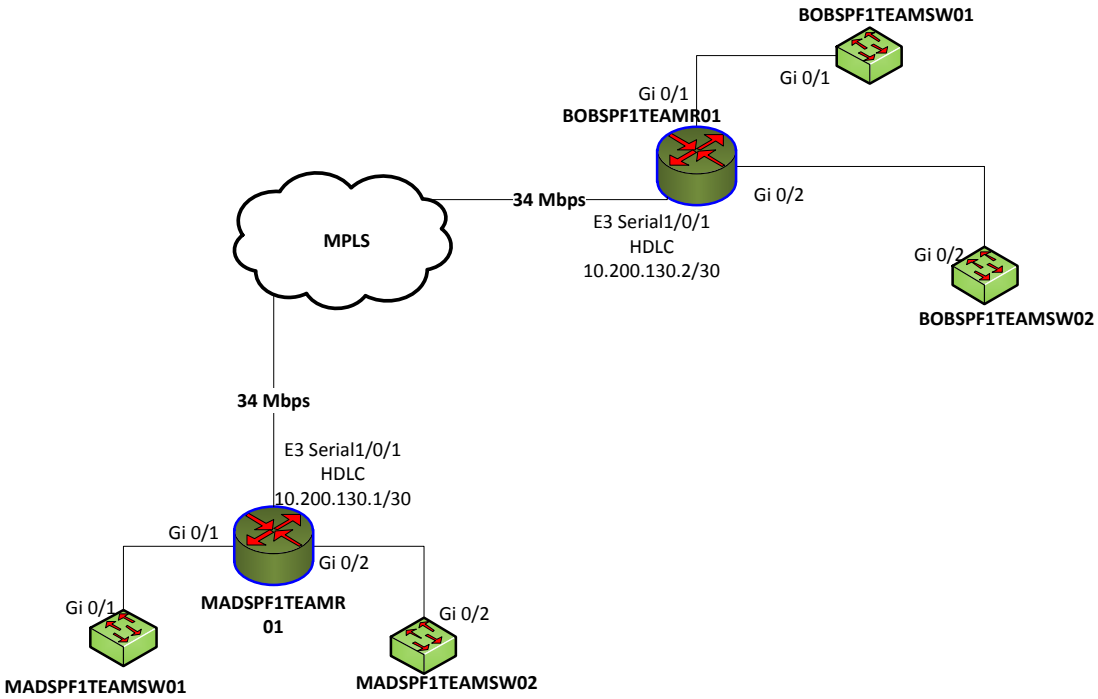

Ilustración 13. Esquema Conexión MPLS

8.1.2 Comunicación Sede Bobbingen.

Para la conexión entre la sede de Bobbingen y Madrid hemos elegido el modelo Cisco Router 3845 que es ideal para servicios avanzados en comunicaciones E3.

Este modelo de router viene integrado con dos puertos Gigabit integrados, puerto consola y un sistema eléctrico redundante. Hemos añadido además en el Slot Port adapter 0/0 una tarjeta de dos puerto FastEthernet para una WAN de alta velocidad. En el Slot Port adapter 1/0 hemos añadido una red con un puerto E3. Que tiene las características que son requeridas para nuestra conexión MPLS entre esta sede y la de Madrid, como la encapsulación HDLC.

Ilustración 14. Router Sede Bobbingen Cisco3804Front

Ilustración 15. Router Sede Bobbingen Cisco3804 Back

Este router se conectará a dos switches de capa 3, que forman la capa Core lo que nos proporcionarán redundancia ante fallos, podemos ver más datos sobre estas conexiones en los apartados próximos.

8.2 Comunicación entre Madrid y Woking.

Como ya hemos comentado con anterioridad en la memoria del proyecto, esta conexión la vamos a realizar mediante una conexión IPLC de 2 Mbps, mediante la empresa COLT.

En el siguiente esquema de la red, se pueden apreciar las conexiones utilizadas para realizar la conexión WAN, la ubicación de la red DMZ.

Hemos elegido conectar las centrales mediante líneas privadas internaciones punto a punto, por la seguridad que aporta a la información al tratarse de circuitos privados, se ha diseñado este tipo de conexión de modo que se conecte a la sede de Madrid por lo que simula una macro LAN en la que todos los servicios y aplicaciones están centralizados y adaptados a una misma política de seguridad así como disponer de servicios de telefonía IP si se requiriera en un futuro.

EL circuito IPLC permite establecer conexiones punto-a-punto permanentes y exclusivas, estos circuitos son altamente confiables, inherentemente seguros y

emplean conexiones de protocolo independiente que pueden ser usados por sus clientes para la transmisión de voz, datos o video sin restricciones.

El protocolo utilizado para el intercambio de información entre los routers del equipo y para mantener actualizadas las tablas de enrutamiento, topología de manera eficiente, será el EIGRP, que es propiedad de Cisco, y ya que disponemos de todo el material de comunicación pertenecientes a esta marca.

Para este circuito no se ha sobredimensionado pues no creemos necesario más inversión que esta, puesto que será un punto fijo como una sede más, lo que si hemos tratado de tener en cuenta es el tema de HA.

El esquema que nos quedaría sería el siguiente:

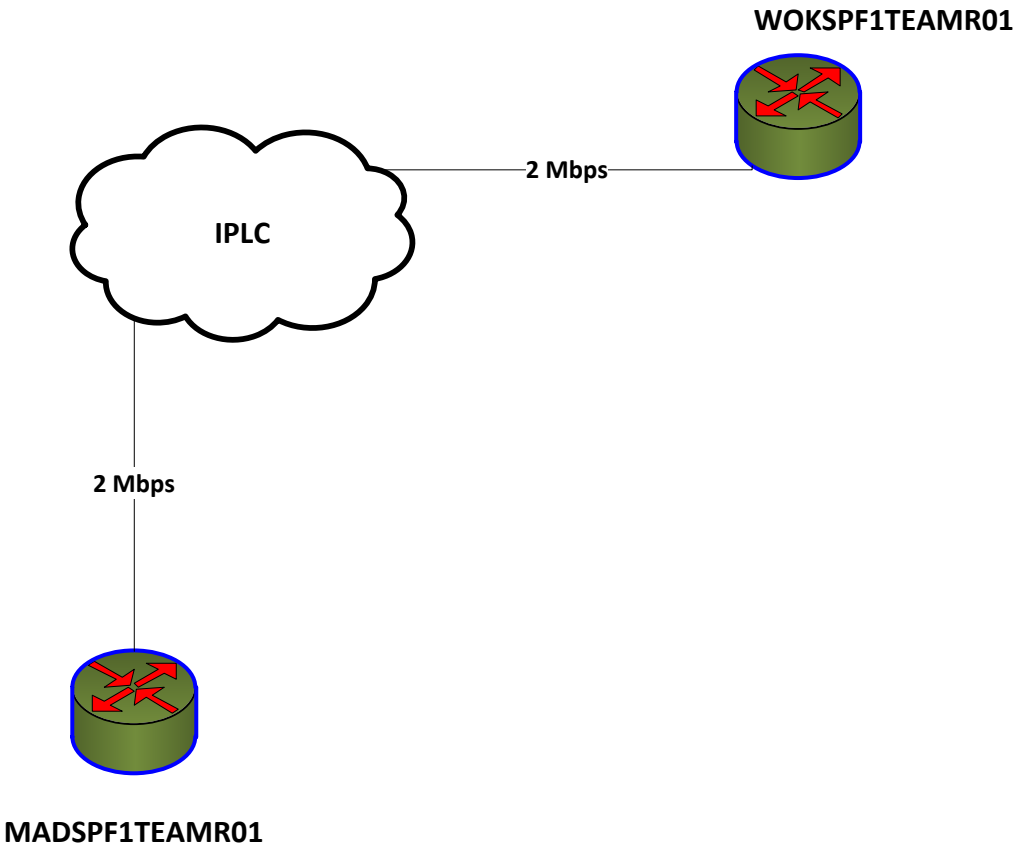

Ilustración 16. Esquema conexión IPLC

8.2.1 Comunicación Sede Woking.

Para la conexión entre la sede de Bobbingen y Madrid hemos elegido el modelo Cisco Router 2821 que permite servicios como seguridad y voz y servicios avanzados para conexión E1, que es la que vamos a utilizar para hacer este enlace.

Viene con dos puertos integrados Ethernet 10/100/1000, al tener únicamente una conexión para la red eléctrica, vamos a disponer de un pequeño SAI para evitar problemas de cortes eléctricos. En el Slot Port 0/0 añadimos una tarjeta con un puerto E1, que dispone de las características requeridas para este nuestra conexión IPLC entre Madrid y Woking.

Ilustración17. Router SedeWoking Cisco 2821 Front

Ilustración18. RouterSedeWoking Cisco 2821 Back

8.3 Implementación LAN.

Dentro del proyecto tenemos que definir dos LAN una para la sede Madrid y otra para la sede Bobbingen.

Ya que en la de Woking, está todo montado lo único que tenemos es que conectar nuestro Router a uno de sus switch y ellos se encargan de la configuración de su propio switch.

Dentro de la sede de Madrid estará ubicada la LAN más compleja, debido a su envergadura y su arquitectura, en esta sede además vamos a implementar una red WLAN sin hilos, para así permitir movilidad a todos los usuarios y que no pierdan conectividad.

Dentro de la sede de Bobbingen tenemos una LAN algo menos compleja que la de Madrid, pero únicamente por que son menos usuarios. En esta sede también vamos a crear una red WLAN sin hilos, para permitir movilidad a todos los usuarios.

8.3.1 LAN Sede Madrid.

Con motivo de los sistemas críticos que se encuentran dentro de la sede como es el centro de procesamiento de datos, los servidores de acceso externo, etc, hemos diseñado un sistema de alto rendimiento y redundante que dé continuidad a la operativa en caso de fallos.

Hemos dividido la arquitectura LAN en 2 capas que son la capa de acceso y la capa Core y de distribución, estas dos últimas pueden ir separadas pero nosotros las hemos unido en un mismo equipo.

La capa Core es la encargada de aplicar las medidas de calidad, enrutamiento, centralización de los recursos de red y donde se conectarán el resto de las sedes.

En esta sede la capa Core se compone de dos Switches Cisco Catalyst3560X, conectados entre sí mediante 2 enlaces configurados en modo PortChannel, para asegurar siempre HA en la implementación del proyecto.

Ilustración19. Switch Core Cisco 3560 (Front, Back)

Este modelo dispone de 48 puertos, por lo que está claramente sobredimensionado para futuras ampliaciones, además dispone de redundancia frente a fallos de la fuente pues dispone de dos fuentes eléctricas, que se pueden cambiar en "caliente". Además dispone de alimentación eléctrica através de la red, a esto se le denomina PowerOver Electric (POE).

En esa capa es donde conectamos por un lado un switch de la capa acceso, al que se conectarán todos los servidores internos, además del firewall que delimita la DMZ y donde se conectan los servidores externos, este apartado será explicado más en profundidad más adelante.

La configuración referente a redes virtuales de área local de los usuarios finales, servidores, red Wifi, se encuentran también en esta capa.

Para esta sede la capa de acceso vamos a utilizar Cisco Catalyst 2960S de 48 puertos, con capacidad de POE. Dispone de 2 puertos que configuraremos a gigabit los uplink para conectar a la capa core.

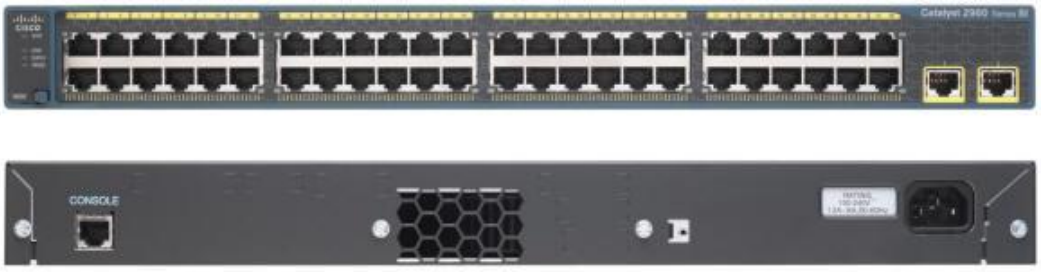

Ilustración20. Switch acceso Cisco 2960S (Front, Back)

El diagrama físico de la red de área local LAN, quedará tal y como se muestra a continuación:

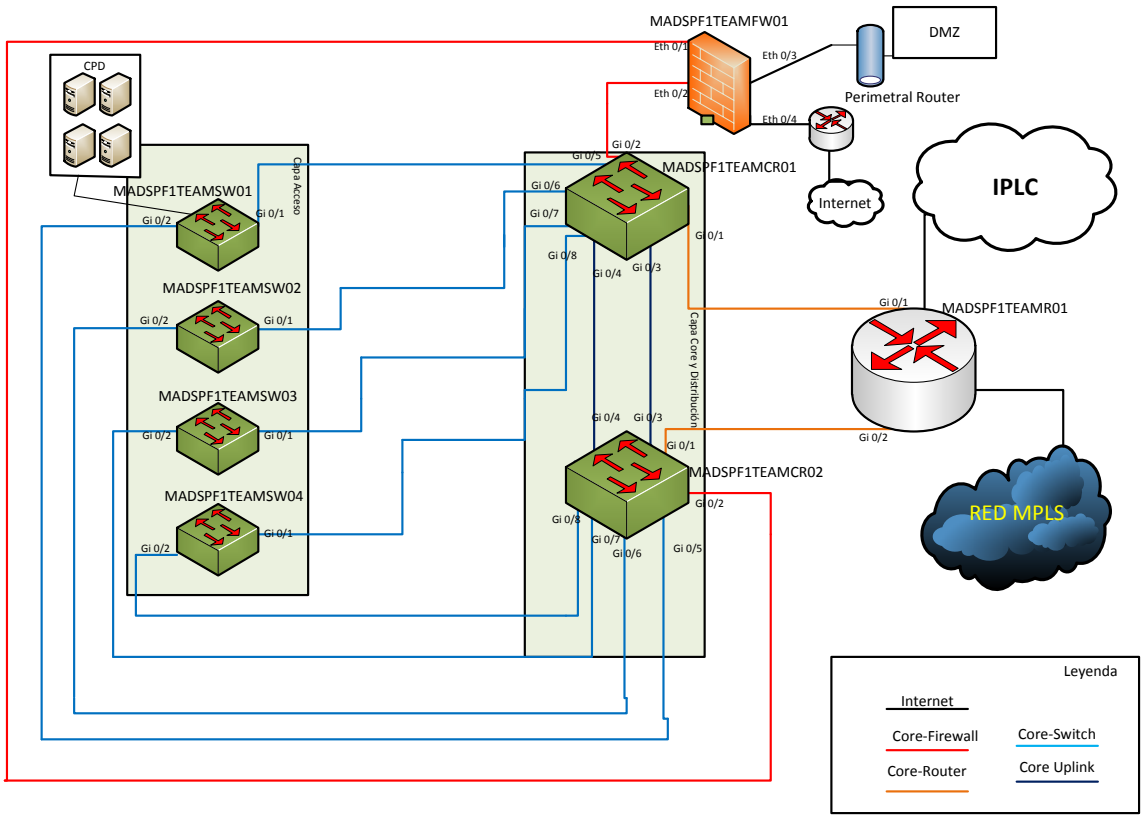

Ilustración 21. Esquema LAN Madrid

8.3.2 LAN Sede Bobbingen.

En la sede de Woking la arquitectura de la red es muy similar a la de Madrid, de hecho también se pueden diferenciar las 3 capas acceso, Core y distribución. La

única diferencia reseñable está en que los equipos son modelos inferiores a los anteriores, pues el número de usuarios, así como la carga que han de soportar es muchísimo menor.

Los equipos utilizados en la capa de acceso son los modelos Catalyst 2960 de 48 puertos POE.

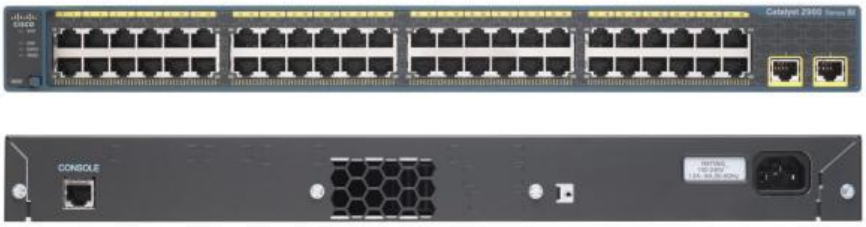

Ilustración22. Switch acceso Cisco 2960S (Front, Back)

Para la capa de distribución y Core hemos seleccionado dos switches4928S

Ilustración23. Switch Core Cisco 4928S Front

Ilustración24. Switch Core Cisco 4928S Back

El diagrama físico de la red de área local LAN, quedará tal y como se muestra a continuación:

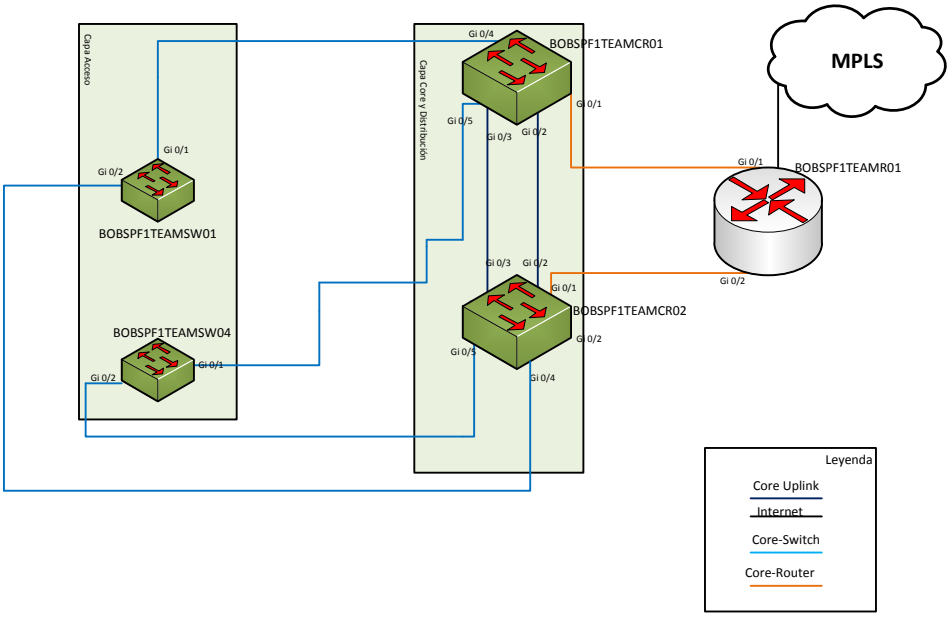

Ilustración 25. Esquema LAN Bobbingen

8.3.3 LAN Sede Woking.

Ya hemos mencionado anteriormente que para esta sede no vamos a implementar ninguna LAN, puesto que ya está creada y nosotros no somos los administradores o implementadores de ella. Nuestra única función es configurar el Router 2821conectado a nuestra sede de Madrid mediante la conexión IPLC, y de una de los puertos a Gigabit conectarlo a un puerto del Switch perteneciente a la red MClaren, y pasarle la configuración a la persona encargada de la administración de la red y ellos se encargarán de mandarnos por esa conexión los datos de la pruebas del túnel de viento.

8.4Proxy.

El modelo de proxy elegido sería el Bluecoat SG300-25 que nos proporciona licencias para un número ilimitado de usuarios y tiene dos fuentes de alimentación redundantes además de un disco de 250 GB y 4 GB de RAM, este proxy nos permite redirigir las peticiones de todos los usuarios de la red a través del proxy en lugar de tener que instalar uno para cada sede, lo que nos ahorra costes.

Ilustración 26. Proxy BlueCoat SG300-25

A continuación podemos apreciar un esquema general de su filosofía de trabajo:

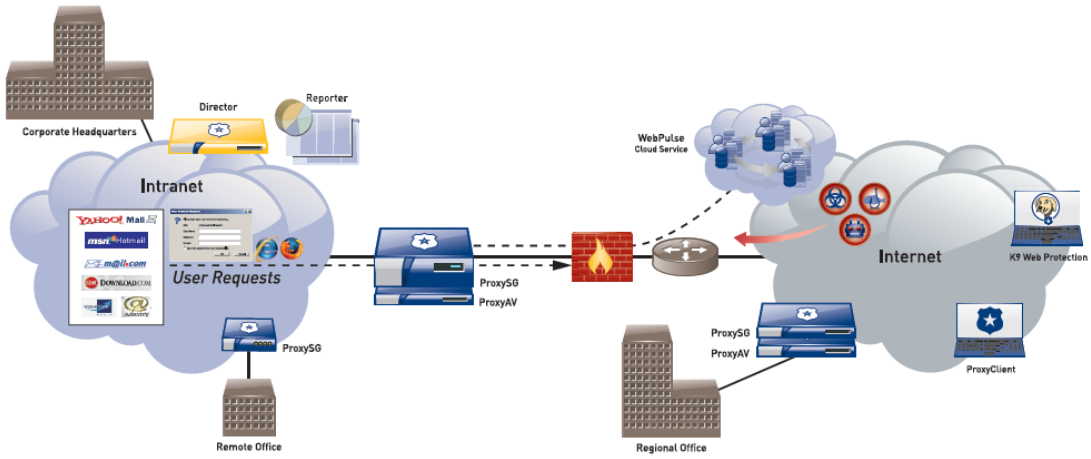

Ilustración 27. Filosofía de trabajo

El proxy proporciona una defensa en capas contra amenazas Web 2.0 aprovechando la tecnología de la nube WebPulse para unos 75 M usuarios, protegidos contra Gateway web y usuarios remotos. Ofrece una política flexible incomparable, con un alto rendimiento y fiabilidad para asegurar las redes, así como para acelerar el contenido.

8.5Firewall.

Se ha elegido como firewall el modelo Fortigate 300C que soporta hasta 10000 sesiones y tiene 8 GB de throughput.

Ilustración 28. Firewall Front

Ilustración 29. Firewall Back

A continuación muestro la ubicación física que tendría el firewall.

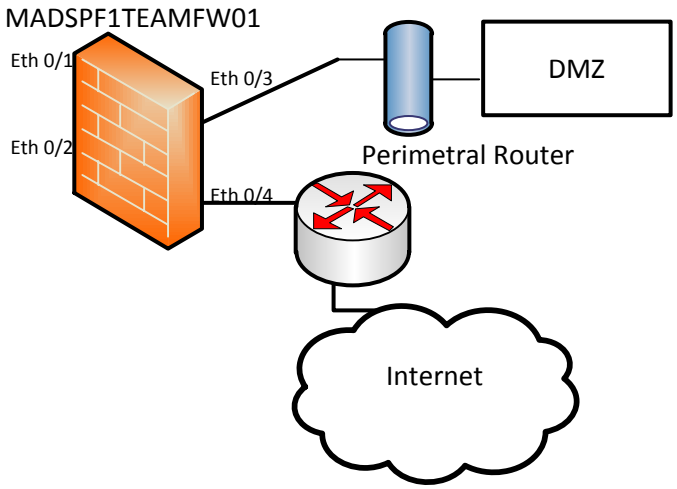

Ilustración 30. FW Sede Madrid

8.6 Implementación WLAN.

Tal y como se ha indicado en los puntos previos de la elaboración de la memoria, queremos implementar una red sin hilos WLAN. Para facilitar la movilidad sobre todo en el área de trabajo denominada taller, así como en el resto de las sedes.

La configuración de esta red varía considerablemente respecto de una sede y otra, ya no solo por el número de AP que vamos a instalar si no también la manera que estos puntos serán gestionados y configurados. Por lo tanto vamos a describir la implementación por separado

8.6.1 WLAN Sede Madrid

Esta sede estará compuesta por 5 puntos de acceso que darán cobertura a toda la sede, aunque en el presupuesto se puede apreciar que hemos comprado 5 lo hemos hecho para disponer de uno de backup. A continuación podemos ver el desarrollo del cálculo que se ha hecho para determinar el número de puntos de acceso que se han de instalar en la sede. Recordar que esta sede consta de dos plantas de 1200 metros cuadrados cada una de las plantas.

A continuación podemos ver el plano de dimensiones de ambas salas.

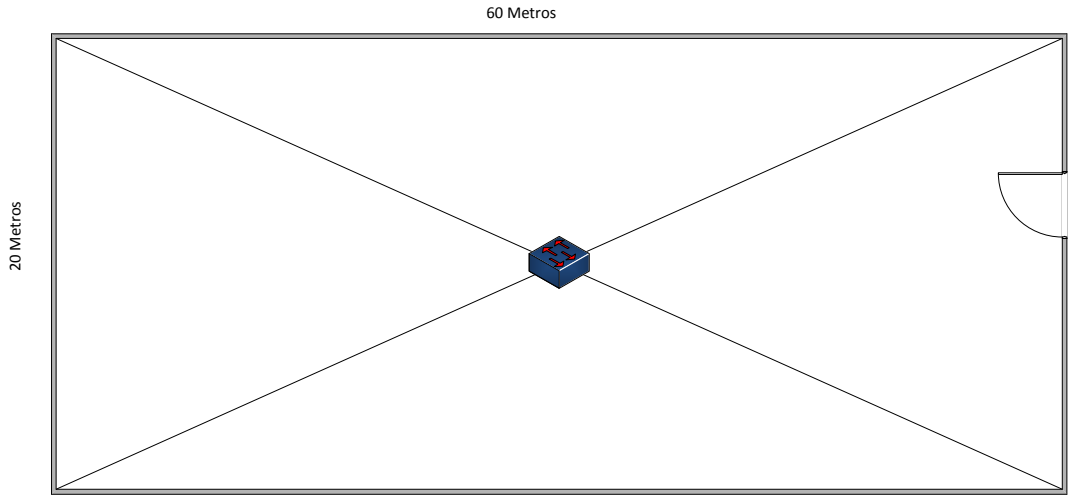

Ilustración 31. Plano Ubicación AP

$$c^2 = a^2 + b^2 = 60^2 + 20^2 \rightarrow \sqrt{4000} = 63.245 \text{ m}$$

Si consideramos ubicar un único punto de acceso en el centro de la sala tendremos que el punto más lejano se encontrará a 31.622 metros de distancia.

Para calcular el número de puntos de acceso necesario, vamos a utilizar el método de COST 231 para interiores, que considera las perdidas de penetración individuales de cada muro y de cada piso dependiendo del material que los constituye. Este método se utiliza principalmente para calcular de manera teórica y aproximada, tanto el número de Puntos de Acceso que son requeridos dependiendo del máximo numero de usuarios que podríamos disponer, y al mismo tiempo averiguar cuál sería la posición idónea en la que habría que ubicar los puntos de acceso, teniendo en cuenta el tipo de obstáculos que hay en la trayectoria.

Para más información sobre el método COST-231 de interiores, adjunto las siguientes referencias:

[17]http://bibing.us.es/proyectos/abreproy/11761/fichero/Volúmen2%252F11-Cap%C3%ADtulo6+-+Modelos+de+propagación+en+interiores.pdf

[18]http://www.escet.urjc.es/~fisica/personal/alexandre/docencia/mpe_tema3.pdf

Para calcular la sensibilidad que tendría que tener la señal para propagarse en el medio tendremos que tener en cuenta, que el espectro de radio a utilizar es 2.4 Ghz para el estándar 802.11b/g.

Por lo que poniendo los datos a la formula nos quedará:

$$20 * \log\left(\frac{4\pi * d}{\gamma}\right) = 20 * \log\left(\frac{397{,}364}{0{,}125}\right) = 70.0455 \text{ dB}$$

Para la planta baja, en la que se encuentran los mecánicos podemos tener como máximo 4 tabiques cuya atenuación es de 8 db por cada uno de ellos.Este dato lo podemos obtener de las tablas que han sido publicadas en las páginas de referencia, anteriormente enunciadas, calculamos 8 db por tabique que es la atenuación estándar para un tabique de grosor medio, por lo que tendremos:

$$70.0455 + 8 * 4 = 102.045 \text{ dB}$$

Según las características de transmisión que nos facilita el proveedor de Acces Point es de 20 dbm y 5dbpor antena, por lo que tendremos:

$$-102.045 \ + 20 + 5 = -77.045 \ dBm$$

Otro dato que nos facilita el proveedor es que para una sensibilidad de señal recibida de -77dbm la señal transmitida es de 36 Mbps, por lo que tendremos:

$$\frac{36 \ Mbps}{100 \ usuarios} = 0.36 \ Mbps \ para \ cada \ usuario$$

Como podemos ver esta velocidad es insuficiente, no está dentro del mínimo requerido por lo que se ha optado por disponer de 2 puntos de acceso en vez de uno solo.

Por lo que la ubicación final sería la siguiente:

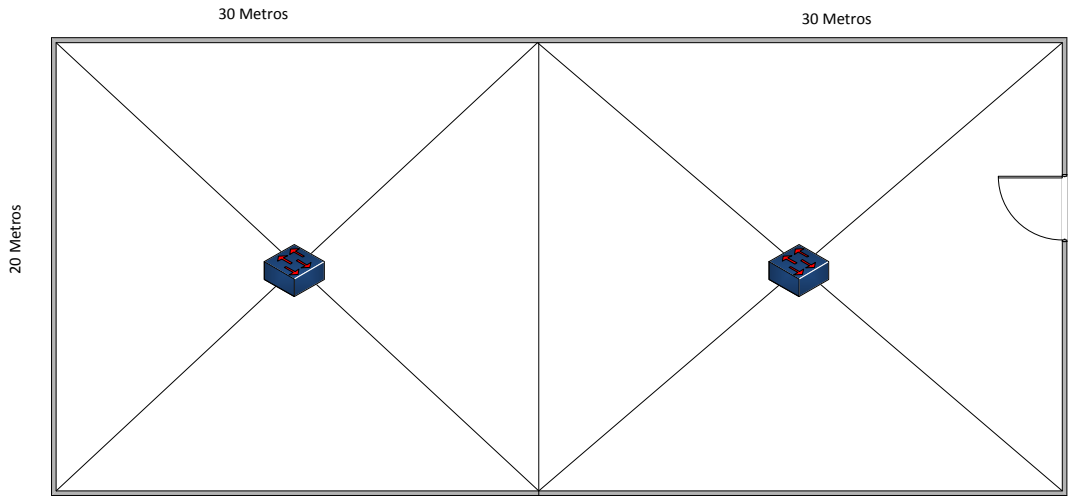

Ilustración 32. Plano Ubicación 2 APs

Vamos a recalcular los datos para dos puntos de acceso:

$$c^2 = a^2 + b^2 = 30^2 + 20^2 \rightarrow \sqrt{1300} = 36{,}055$$

Por lo que la distancia al punto más lejano desde la ubicación de cualquier punto de acceso será de 15,811 metros.

Aplicamos de nuevo el método COST 231 para interiores. Con esto calculamos la velocidad que puede ofrecer el punto de acceso a un usuario situado en el punto más lejano de la planta.

Para calcular la sensibilidad que tendría que tener la señal para propagarse en el medio tendremos que tener en cuenta, que el espectro de radio a utilizar es 2.4 Ghz para el estándar 802.11b/g.

Por lo que poniendo los datos a la formula nos quedará:

$$20 * \log\left(\frac{4\pi * d}{\gamma}\right) = 20 * \log\left(\frac{198{,}628}{0{,}125}\right) = 64.022 \text{ dB}$$

Para la planta baja, en la que se encuentran los mecánicos podemos tener como máximo 3 tabiques, teniendo en cuenta la posición actual de los puntos de acceso,sabiendo que la atenuación es de 8 db por cada uno de los tabique. Este dato lo podemos obtener de las tablas que han sido publicadas en las páginas de referencia, anteriormente enunciadas, calculamos 8 db por tabique que es la atenuación estándar para un tabique de grosor medio, tendremos:

$$64.022 + 8 * 3 = 88.022 \text{ dB}$$

Según las características de transmisión que nos facilita el proveedor es de 20 dbm y 5dB por antena, por lo que tendremos:

$$-88.022 \ + 20 + 5 = -63.022 \ dBm$$

Otro dato que nos facilita el proveedor es que para una sensibilidad de señal recibida de -63dbm la señal transmitida es de 54 Mbps, por lo que tendremos:

$$\frac{54 \ Mbps}{100 \ usuarios} = 0.54 \ Mbps \ para \ cada \ usuario$$

Esta será la velocidad mínima que recibirá un usuario situado en el punto más alejado de un punto de acceso, siempre y cuando estén los 100 usuarios conectados por wifi y al mismo AP, algo poco probable, por lo que entra dentro de los mínimos requeridos.

Para la planta primera tendremos el mismo escenario, por lo que habrá que poner otros 2 puntos de acceso, los de la planta baja no nos llegan por que la zona de la primera planta en la que está ubicada no está exactamente encima de la planta baja. Debajo de la zona de la primera planta en la que se ubican las oficinas están el gimnasio y la piscina, y la zona de los talleres está separada de ellas por un tabique de medio metro de hormigón, por lo que la perdida de señal es muy alta.

Los puntos de acceso que hemos elegido son el modelo Cisco AIR LAP 1041 N.

Ilustración 33. Cisco LAP 1041

Estos dispositivos disponen de compatibilidad con el estándar 802.11n, tienen capacidad para ser alimentados eléctricamente através de los switches que tenemos en la capa de acceso. Por lo general no todos los equipos que disponemos admiten el estándar 802.11n, por lo que si alguno lo puede utilizar está permitido.

Ya que disponemos de 4 puntos de acceso, y configurarlos, administrarlos y revisarlos uno por uno supondría mucho trabajo, se ha añadido a la instalación el modelo Cisco Wirellescontroller 2112.

Ilustración34. Wireless Controller Cisco 2112 (Front, Back)

El Wirellescontroller 2112, cuenta con 8 puertos dos de ellos admiten POE directamente a los dispositivos directamente conectados a estos dos puertos.

Mediante este dispositivo vamos a configurar los 4 puntos de acceso necesarios para nuestras instalaciones. Este dispositivo estará conectado a uno de nuestros switches de la capa de acceso, y los puntos de accesos se conectarán cada uno a uno de los switches, ya que Cisco no recomienda conectar los puntos de acceso directamente al WirellesController. Lo único que necesita el Wirellescontroller para poder gestionar un punto de acceso es conectividad mediante la red con el mismo, una vez que lo encuentra le asigna una IP, y desde el propio Wirellescontroller se le pone la configuración, se le indica la id de la WLAN a la que pertenece cada punto de acceso así como la seguridad que van a tener en la clave. Gracias a este sistema, cualquier cambio o nueva configuración que queramos establecer, únicamente debemos aplicarla en el WirellesController y se puede establecer que puntos de acceso queremos que reciban dicha actualización de configuración.

Para ello se creará en el Wirellescontroller el siguiente Id WLAN SPF1-TEAM, la clave de acceso se le define una encriptación mediante el protocolo WPA2-TKIP. Se le define varios canales en los que pueden operar cambiándose entre ellos automáticamente si llegan a algún conflicto.

A continuación podemos ver el esquema de conexión de la red WLAN para esta sede:

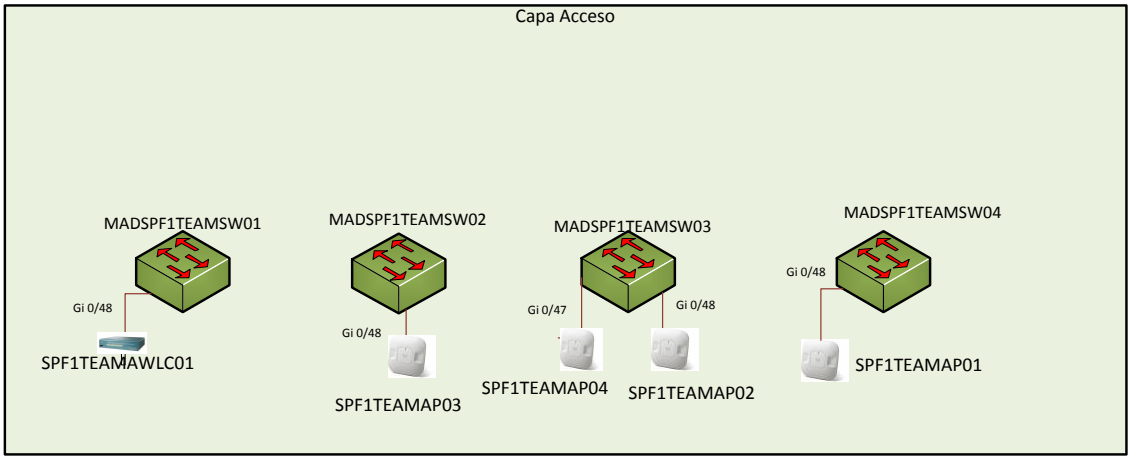

Ilustración 35. Esquema WLAN Madrid

8.6.2 WLAN Sede Bobbingen

Esta sede estará compuesta por un punto de acceso que dará cobertura a toda la sede. A continuación podemos ver el desarrollo del cálculo que se ha hecho para determinar el número de puntos de acceso que se han de instalar en la sede. Recordar que esta sede consta de una plantade 200 metros cuadrados.

A continuación podemos ver el plano de dimensiones la sede.

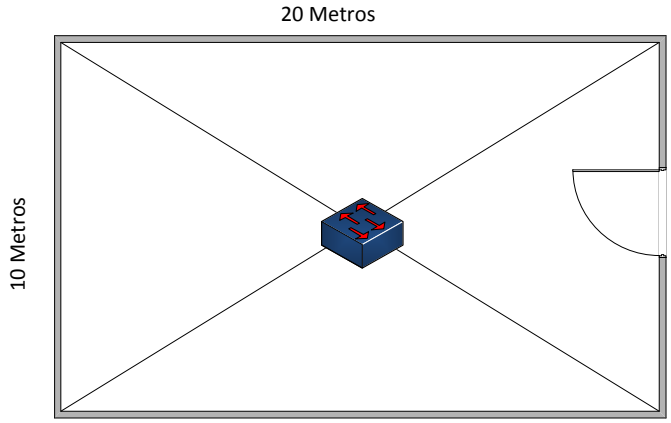

Ilustración 36. Plano ubicación AP Bobbingen

Vamos a recalcular los datos para dos puntos de acceso:

$$c^2 = a^2 + b^2 = 20^2 + 10^2 \rightarrow \sqrt{500} = 22.36$$

Por lo que la distancia al punto más lejano desde la ubicación de cualquier punto de acceso será de 11,18 metros.

Aplicamos de nuevo el método COST 231. Con esto calculamos la velocidad que puede ofrecer el punto de acceso a un usuario situado en el punto más lejano de la planta.

Para calcular la sensibilidad que tendría que tener la señal para propagarse en el medio tendremos que tener en cuenta, que el espectro de radio a utilizar es 2.4 Ghz para el estándar 802.11b/g.

Por lo que poniendo los datos a la formula nos quedará:

$$20 * \log\left(\frac{4\pi * d}{\gamma}\right) = 20 * \log\left(\frac{140{,}492}{0{,}125}\right) = 61{,}014\ \text{dB}$$

Para la planta podemos tener como máximo 3 tabiques, teniendo en cuenta la posición actual de los puntos de acceso, sabiendo que la atenuación es de 8 db por cada uno de los tabiques, tendremos:

$$64.022 + 8 * 3 = 85{,}014\ \text{dB}$$

Según las características de transmisión que nos facilita el proveedor es de 20 dbm y 5por antena, por lo que tendremos:

$$-85{,}014\ \text{dB} + 20 + 5 = -60.022\ dBm$$

Otro dato que nos facilita el proveedor es que para una sensibilidad de señal recibida de -60dbm la señal transmitida es de 54 Mbps, por lo que tendremos:

$$\frac{54\ Mbps}{50\ usuarios} = 1.08\ Mbps\ para\ cada\ usuario$$

Esta será la velocidad mínima que recibirá un usuario situado en el punto más alejado de un punto de acceso, por lo que entra dentro de los mínimos requeridos.

Por lo que para esta sede únicamente necesitaremos un punto de acceso, y tampoco necesitaremos WirellesController.

Para esta sede se ha elegido el modelo Cisco AIR- AP 1041N, destacar que la única diferencia respecto al de la sede de Madrid es que el otro es compatible con WirellesController mientras que este no lo es.

Ilustración 37. Cisco AP 1041N

Se ha configurado este dispositivo en el canal 11, además permite tecnología 802.11b/g/n, pueden ser alimentados a través de los siwtches por POE. Se ha elegido el mismo método de encriptación para el ID de wifi que en la sede de Madrid WPA2-TKIP.

9. Seguridad de la Red

En una red la seguridad siempre es un tema que ha de tener mucha importancia, pero para nuestro caso, si cabe esta ha de tener un plus de importancia, ya que el espionaje industrial es algo muy dado en el mundo de la F1, por lo que haremos especial hincapié en este tema. Lo que se busca es tanto evitar el acceso a los sistemas a personas externas, además de asegurar la integridad y la continuidad de las aplicaciones.

Una de las principales medidas que ha de tomar la escudería, para garantizar la seguridad es la de formar e informar de manera constante a los usuarios finales, tanto en temas de seguridad como en prevención haciendo especial hincapié en aplicaciones como el correo electrónico, discos duros externos de almacenaje, acceso a internet, etc, además de esto se han adoptado 3 medidas indispensables para reforzar las medidas de seguridad. Estas medidas son:

- Firewall, para prevenir acceso de terceras personas a los sistemas internos de la empresa.
- Proxy, para controlar el acceso a Internet.
- Radius, para controlar el acceso a la red.

9.1Firewall

Se ha instalado un sistema de cortafuegos o Firewall en nuestra red que evita el acceso a usuarios ajenos a nuestra red, desde fuera de la misma, únicamente se deja una pasarela abierta para acceder a los servidores web y de webmail, que quedarán protegidos dentro de la red Desmilitarizada (DMZ).

El sistema de Firewall que hemos implementado se trata de dos dispositivos situados en la parte externa de la red, denominado FW1 y que constituye el primer filtro que tienen que atravesar los equipos que quieran acceder a los servidores web y Webmail. La configuración básica de este equipo consistirá en permitir el acceso a los servicios permitidos, como el protocolo tcp puerto 80, protocolo tcp 443, protocolo tcp 143 IMAP, y protocolo tcp 25 SMTP. El resto de acceso estará bloqueado.

En la parte interna de la DMZ, se encuentra un segundo dispositivo, denominado FW2, que asegurará que si alguien logra acceder a la zona desmilitarizada con malas intenciones, no pueda acceder a la zona de la red interna, en este FW las reglas que tendremos principalmente serán la de denegar el acceso a cualquier dispositivo cuya dirección provenga de una red externa de la escudería.

Para configurar esto hemos cread una red local virtual (VLAN) específica para los equipos servidores que se deben encontrar en la zona DMZ, para además de securizaraúnmás la zona, especificando rango de Ips que podrán acceder, nos facilitará la tarea de aplicar las reglas de seguridad en los FW.

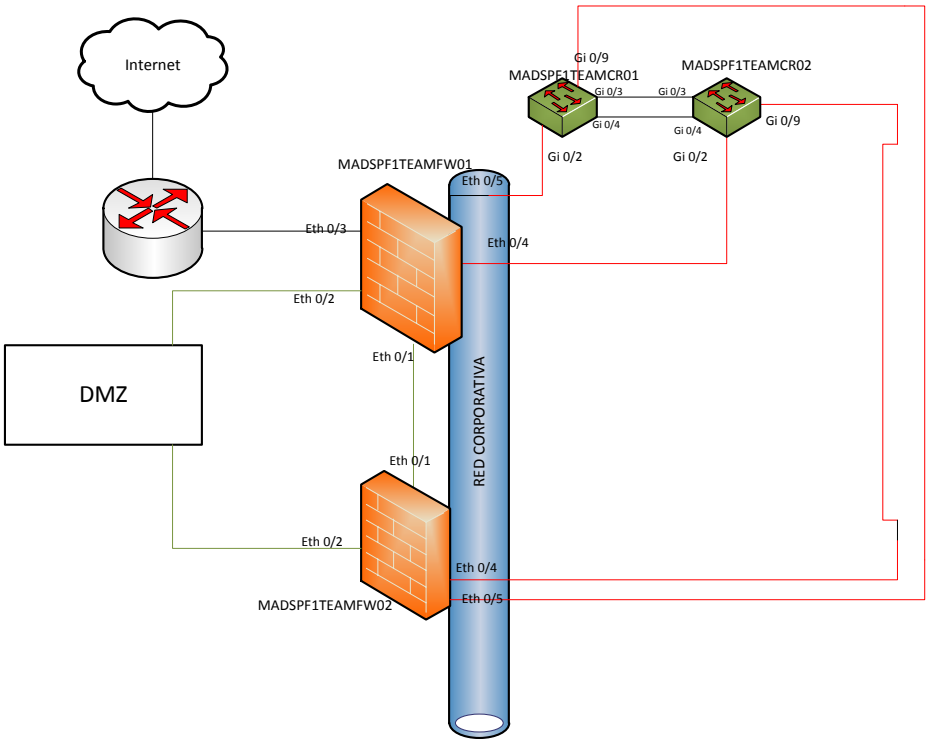

Ilustración 38. Esquema LAN DMZ

Los servidores situados en la DMZ se han conectado a dos Firewall distintos. Los FW están conectados a su vez, cada uno a un switch, siempre buscando que se cumpla la premisa de HA en nuestra implementación.

9.2Proxy

Para poder acceder a internet desde la red de la escudería todos los equipos tendrán que tener configurado en su navegador de internet el proxy.

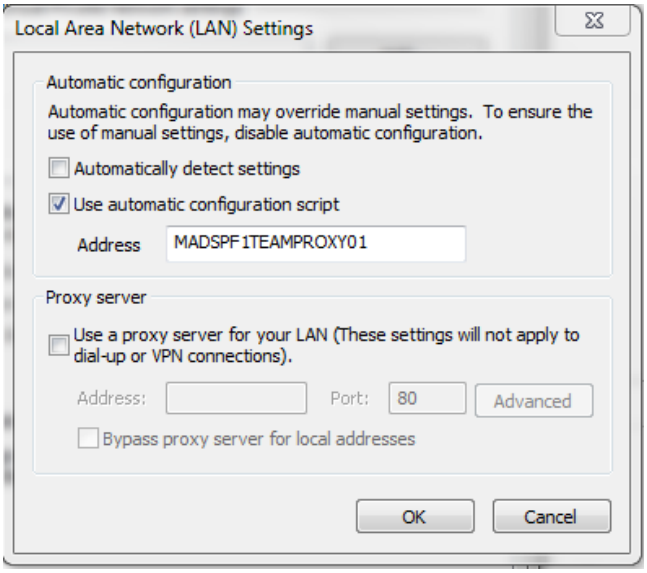

Ilustración 39. Configuración Proxy Navegador

La función principal del proxy es garantizar que las páginas catalogadas como maliciosas o sospechosas de ser maliciosas, o que no cumplan con lo estipulado en el régimen interno de la empresa no puedan ser accedidas.

El modelo de proxy escogido es el mencionado anteriormenteBluecoat SG300-25.

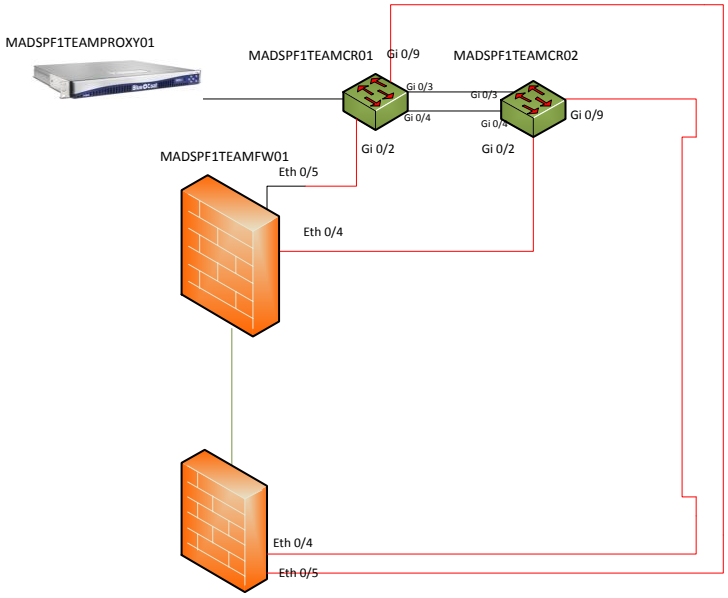

Ilustración 40. Ubicación Proxy SG

Otro de los aspectos importantes del proxy, es que es el único punto por el que se sale a internet desde dentro, por lo que si alguien quiere realizar un ataque contra un equipo de la red interna, deberá de pasar por el proxy, lo que anulará el ataque.

9.3 Radius

Para obtener un control de los usuarios que están haciendo uso de los recursos de la compañía, se van a integrar en la misma servidores de control de acceso en HA. La tecnología a implementar es la que ofrece el fabricante Cisco más específicamente la familia ACS, el modelo concreto será: "Cisco SecureAcces Control System 5.3"

Este sistema ofrece una serie de ventajas y capacidades para otorgar a la plataforma un control avanzado sobre los recursos de la misma.

- Soporte para protocolos Radius para control de acceso aalared y TACACS+ para control de acceso a los dispositivos de red.
- Utilización de multiples bases de datos para proporcionar flexibilidad a la hora de aplicar políticas de acceso.
- Capacidad para la implementación de políticas avanzadas de acceso, basadas en autenticación bajo varios requerimientos previos.
- Integración en la solución de reportes, monitorización y herramientas de resolución de incidencias.

10. Sistema de Backup y HA (Alta Disponibilidad)

- Un aspecto a tener muy en cuenta a la hora de diseñar la implementación en cualquier empresa es la de ofrecer continuidad de servicio en todo momento a los usuarios, para esto es necesario diseñar una arquitectura que sea capaz de sobreponerse ante situaciones de contingencia. Por lo que para nuestro diseño se ha implementado una arquitectura de HA en todos los dispositivos.
- Para poder cumplir con estos requisitos hemos diseñado las siguientes funcionalidades:
    - Sistemas redundados
    - Sistemas de Backup para líneas de comunicación
    - SAIs

10.1 Sistemas redundados:

Cada dispositivo dispondrá de un gemelo o esclavo, el cual asumirá la responsabilidad del servicio en caso de que el que está actuando como maestro deje de funcionar, esta filosofía de maestro y esclavo es principalmente para que puedan sincronizar configuraciones y sesiones de manera automática. Para ello el traspaso de rol de maestro a esclavo ha de realizarse sin que implique un corte de servicio para los usuarios, los dispositivos deberán poder estar continuamente monitorizando su estado para poder sincronizar sesiones o configuraciones.

Esta tecnología maestro esclavo estará presente sobre todo en los puntos más críticos de nuestro sistema, como son la capa Core de las sedes de Madrid y Bobbingen.

Otro punto en el que hemos tenido especial cuidado es en que todos los equipos adquiridos dispongan de doble fuente de alimentación, para evitar cortes por algún problema eléctrico en la fuente de alimentación.

Para conseguir esto además, se han tenido en cuenta los siguientes Aspectos:

- Sede Madrid:
  Una de las fuentes irá conectada al SAI principal y la otra fuente irá conectada al SAI secundario.
- Sede Bobbingen:
  Una de las fuentes irá conectada al SAI principal y la otra fuente irá conectada al SAI secundario
- Sede Woking:
  Aunque aquí ya está instalado el CPD nos hemos asegurado que permiten estas condiciones.

Además los servidores disponen de dos tarjetas de red, por lo que cada una se conectará a dos switches distintos. Para habilitar la redundancia en los switches de Core y el balanceo de carga, utilizaremos el protocolo HSRP (Hot

StandbyRouterProtocol) que establece uno de los equipos como maestro y el otro como esclavo dependiendo de las prioridades de cada uno.

Por lo que el equipo con prioridad más alta será el encargado del enrutamiento de las VLANs, y el otro por tanto el backup, este pasará a ser maestro de manera automática en el momento en el que el principal deje de funcionar correctamente, este volverá de nuevo a ser el principal cuando haya recuperado conectividad.

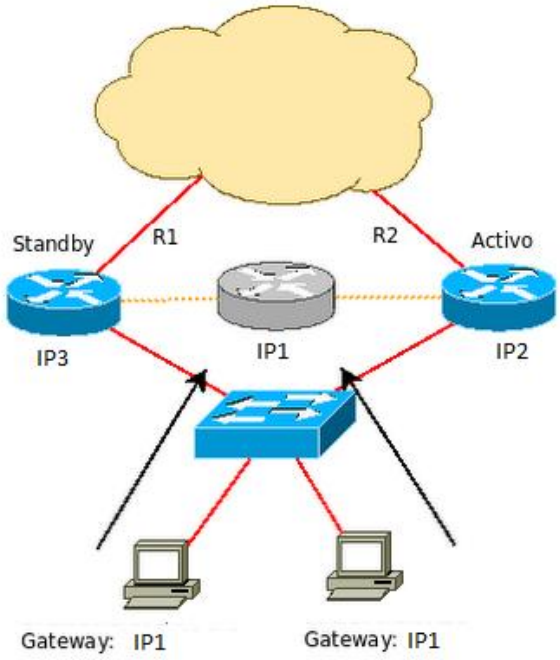

Ilustración 41. Protocolo HSRP

A la hora de habilitar el balanceo de carga de los switches, se ha configurado uno como principal de la mitad de las VLANS, y el segundo switch como principal del resto de VLANs.

10.2 Sistemas de Backup para líneas de comunicación:

Vamos a comentar los sistemas de Backup para cada una de las líneas.

10.2.1 Línea Backup Madrid-Bobbingen.

Para esta línea de Backup, se ha contratado una línea DSL de velocidad 6 Mbps de bajada y 1Mbps de subida, con la empresa Colt.

La configuración de la línea quedaría tal y como se muestra a continuación:

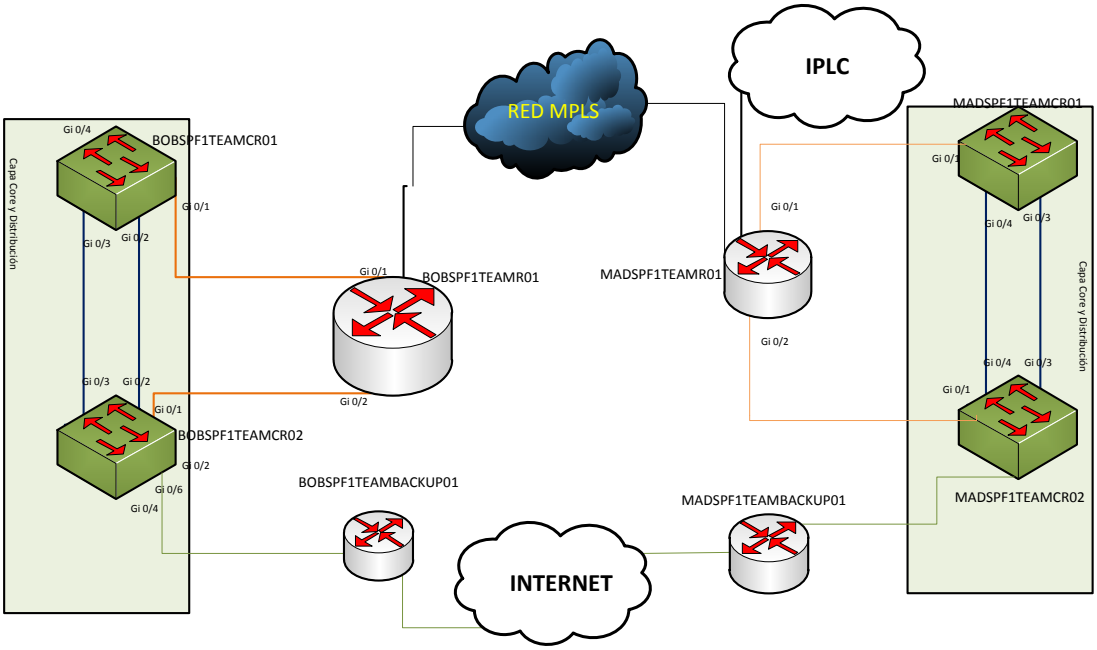

Ilustración 42. Conexión BackupDSL Madrid-Bobbingen

10.2.2Línea Backup Madrid-Woking.

Para esta línea de Backup, se ha contratado una línea DSL de velocidad 2 Mbps de bajada y 384 bps de subida, con la empresa Colt.

La configuración de la línea quedaría tal y como se muestra a continuación:

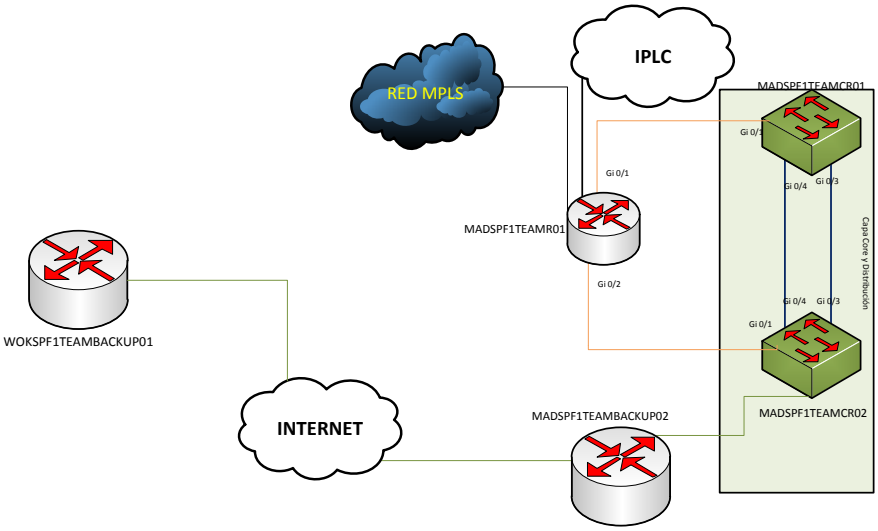

Ilustración 43. Conexión Backup DSL Madrid-Woking

11. Monitorización

Al disponer de tal cantidad de equipos se hace indispensable disponer de una herramienta de monitorización, para ser capaces de determinar el estado de todos y cada uno de los equipos, y gracias a ello poder actuar anticiparse a los posibles problemas que puedan surgir.

Para hacer posible la implementación de la infraestructura de monitorización vamos a necesitar los siguientes elementos:

- Activar la configuración SNMP en todos los dispositivos de la escudería, (FW, Switches, Servidores …)
- Envio de todos los eventos registrados por los dispositivos hasta la consola de monitorización

El funcionamiento de la monitorización se hará gracias a que el servidor de monitorización recopilará toda la información enviada por los dispositivos a través de SNMP inerpretándola y mostrándola en gráficos, informes, alertas, etc …

Por lo tanto a través de esta plataforma podremos recopilar información sobre el consumo de ancho de banda, CPU, memoria, lo que nos permitirá conocer en todo momento el estado en el que se encuentra nuestra arquitectura.

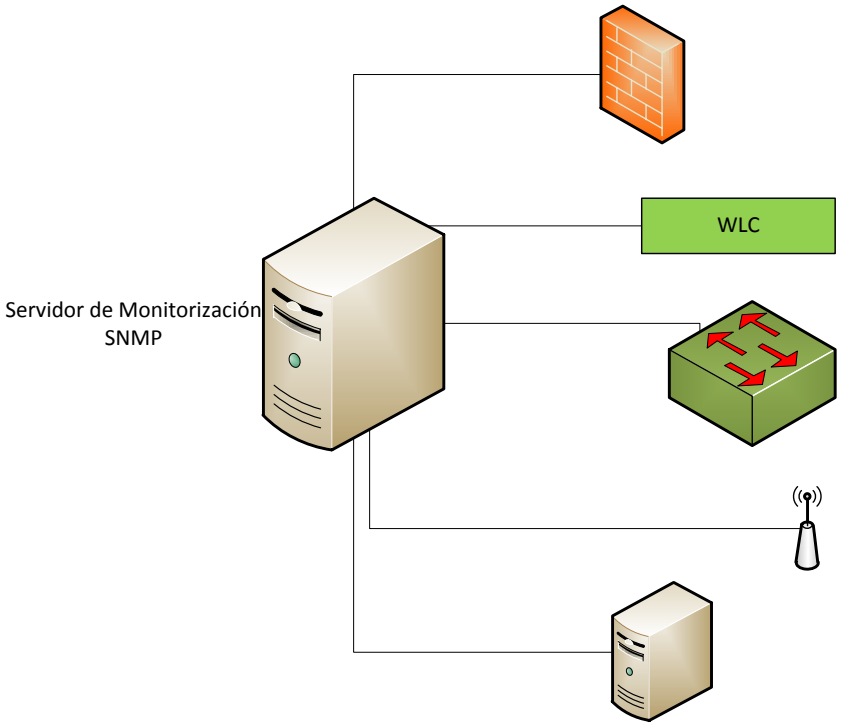

Ilustración 44. Servidor de Monitorización

12. Glosario de términos

AP: Acces Point

CORE: Es el concepto que define el núcleo de la red de datos

CPU: Center ProccesUnit. Dispositivo que realiza el núcleo de operaciones de cualquier dispositivo.

CPD: Centro de Proceso de datos

DMZ: zona desmilitarizada (DemilitarizedZone).

DNS: DomainNameSystem. Es un sistema de nombres jerárquicos para máquinas o servicios conectados a una red privada o internet.

EIGRP: Protocolo de enrutamiento de pasarela interior mejorado (Enhaced Interior Gateway RoutingProtocol)

FW: Cortafuegos (Firewall)

HA: High Availability (Alta Disponibilidad).

HDLC: Control de datos de enlace de alto nivel (High-Level Data control).

HSRP: Hot Standby Router Protocol. Protocolo de enrutamiento Host Standby

HTTP: Hypertext Transfer Protocol. Protocolo de transferencia de hipertexto, es el protocolo utilizado en cada transacción WWW.

IPLC: Línea de transmisión de datos privada internacional (International PrivateLeaseCircuit).

ISP: Proveedor de servicios de internet (Internet ServiceProvider)

LAN: Red de área local (Local Area Network).

LDP: Protocolo de distribución de intercambio de etiquetas. LabeldistributionProtocol.

LSR: Router de Intercambio de etiquetas. Label Switchin Router

MPLS: Multiprotocol Label Switching.

OSPF: Abre la ruta más corta primero (Open ShortestPathFirst).

POE: Alimentación eléctrica a través de la red (PowerOver Ethernet).

PROXY: Dispositivo de red que realiza acciones en representación de otro, como gestionar peticiones a internet en nombre de los usuarios internos de la red.

RADIUS: Remote Authentication Dial-in User Server. Protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP.

SAI: Sistema de alimentación ininterrumpida.

SLA: Acuerdos de calidad de servicio (ServiceLevelAgreement).

SNMP: Simple Network Management Protocol. Protocolo simple de Administración de Red, es un protocol de aplicación que facilita el intercambio de información de administración entre dispositivos de la red.

VLAN: Virtual Area Network. Redes lógicamente independientes pero dentro de una misma red física.

WAN: Red de area amplia (Wide areanetwork).

WLAN: Red de área local sin hilos (Wireless local área network).

WLC: Wirelles LAN Controller

13. Referencias.

[1] http://www.cisco.com/en/US/products/hw/routers/ps341/index.html

[2] http://www.cisco.com/en/US/products/hw/switches/ps5528/index.html

[3]http://www.cisco.com/cisco/web/solutions/small_business/products/routers_switches/catalyst_2960_series_switches/index.html#2960

[4] http://www.cisco.com/en/US/products/ps5855/index.html

[5] http://www.cisco.com/en/US/products/ps6021/index.html

[6] http://www.cisco.com/en/US/products/ps5855/index.html

[7] http://www.cisco.com/en/US/products/ps11203/index.html

[8]http://www.cisco.com/en/US/products/ps7206/tsd_products_support_configure.html

[9] http://www.colt.net/es/es/index.htm

[10] http://www.eu.ntt.com/es/productos-y-servicios.html

[11] http://www.ramonmillan.com/tutoriales/mpls.php

[12]http://www.escet.urjc.es/~fisica/personal/alexandre/docencia/mpe_tema3.pdf

[13] http://www.fortinet.com/products/fortigate/300C.html

[14]http://www.bluecoat.com/sites/default/files/products/datasheets/bcs_ds_fullproxy_300-600_v2g.pdf