Contingencia de datos con doble operador

Daniel Sarrión Mochales
Grado de Tecnologías de Telecomunicación
Integración de redes telemáticas

José López Vicario
Pere Tuset Peiró

9 de junio de 2019

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Contingencia de datos con doble operador*
Nombre del autor:	*Daniel Sarrión Mochales*
Nombre del consultor/a:	*José López Vicario*
Nombra del PRA:	*Pere Tuset Peiró*
Data de entrega (mm/aaaa):	*06/2019*
Titulación o programa:	*Grado de Tecnologías de Telecomunicación*
Área del Trabajo Final:	*Integración de redes telemáticas*
Idioma del trabajo:	*Castellano*
Palabras clave	*WAN, red informática, tecnología de la información, contingencia*

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

La finalidad de este proyecto se enmarca en demostrar, justificar y analizar la posible aplicación de una mejora que evite y/o minimice las consecuencias de las caídas críticas de servicio de los operadores de telecomunicaciones y evitar así incidencias y perdidas económicas a las organizaciones por este motivo.

Hoy en día cualquier empresa u organización con diferentes sedes necesita algún tipo de conectividad entre ellas para poder compartir datos, ya sean simples bases de datos o complejas instalaciones de VoIP. Cuando estas sedes se encuentran separadas en grandes distancias la dependencia de los operadores ISP es crucial para poder aportar este servicio.

Para encontrar una solución óptima al problema propuesto se ha analizado una empresa, con diferentes sedes repartidas por el territorio nacional, sus necesidades y criterios. El diseño y la propuesta de aportar una posible contingencia con un segundo operador viene dada por las necesidades de esta organización en concreto y se llega a aportar una posible configuración de red tanto a nivel WAN como LAN.

El resultado final es una propuesta de configuración para cada tipología de sedes con un tipo de acceso principal y secundario y un análisis de los posibles procedimientos y necesidades para una implantación idónea.

La conclusión extraída de este proyecto es que mediante la aplicación de una contingencia con doble operador se puede llegar a reducir el volumen de incidencias críticas a niveles ínfimos a cambio de un coste económico no despreciable, pero muy válido en función de las necesidades de cada entidad.

Abstract (in English, 250 words or less):

The purpose of this project is focused on demonstrating, justifying and analyzing the possible application of an improvement that avoids and/or minimizes the consequences of critical service falls of telecommunications operators and in that way avoid incidents and economic losses to organizations due to this reason.

Nowadays, any company or organization with different sites needs some type of connectivity between them in order to share data, whether they are simple databases or complex ToIP installations, for example. When these sites are separated by large distances, dependence on ISP operators is unavoidable to provide this service.

In order to find an optimal solution to the proposed problem, a company has been analyzed, with different sites located throughout the national territory, its needs and criteria. The design and the proposal to provide a possible contingency with a second operator is given by the needs of this particular organization and comes to provide a possible network configuration at both level WAN and LAN.

The final result is a proposal of configuration for each type of site with a type of main and secondary data access and an analysis of the possible procedures and needs for a suitable implementation.

The conclusion obtained from this project is that by applying a contingency with a double operator, the volume of critical failures can be reduced to negligible levels in exchange for a non-negligible economic cost, but very valid depending on the needs of each enterprise.

Índice

Lista de figuras

Lista de tablas

1. Introducción

1.1. Contexto i justificación

En el contexto actual, donde la globalización del mercado y la gran competitividad existente obliga a las empresas a maximizar tanto los servicios que aportan a sus clientes como la disponibilidad de estos, es de vital importancia la optimización de los recursos, así como la reducción de los costes asociados a cada uno de los servicios aportados por los diferentes proveedores.

En cuestión de telecomunicaciones, desde la liberalización del mercado y la apuesta de los diferentes gobiernos por la ampliación y mejora de la oferta de telecomunicaciones a nivel estatal, se han abierto una serie de posibilidades de mejora para las organizaciones que deben tener en cuenta para ser más competitivas.

La liberalización del mercado ha supuesto una mejora en la oferta de cada uno de los operadores tanto a nivel económico como tecnológico debido a la mayor competitividad que existe entre ellos. Esta mejora económica y tecnológica repercute directamente sobre las posibilidades de las empresas a la hora de contemplar nuevas opciones de configuración y comunicación entre sedes, entre sedes y servicios centrales o incluso entre sus clientes y los servicios que la empresa pone a su disposición, sobre todo a nivel web y móvil con nuevas aplicaciones o ampliación de funciones de las actuales.

Ante este escenario y con el fin del aprovechamiento de estas mejoras económicas y tecnológicas, se propone el siguiente proyecto de mejora y consolidación de una infraestructura paralela de respaldo de los servicios de telecomunicaciones, en concreto la red de datos WAN, para una organización ficticia.

Esta organización dispondría de diferentes sedes remotas o delegaciones interconectadas a través de una WAN de datos de un sólo operador (operador 1) y, a su vez, conectadas una sede central, basada en un CPD que dotaría de servicios al resto de sedes.

En cada una de las sedes (remotas y central), debido a la criticidad del servicio, se plantea disponer de una doble conexión de datos mediante un acceso principal y otro secundario con diferente operador y tecnología. Proponiendo así, no sólo una contingencia de datos a nivel de operador ISP, si no también una contingencia a nivel de tecnología gracias al uso de diferentes tipologías de acceso en cada una de las sedes y en el CPD.

En este proyecto se definirá la interconexión de todas estas sedes mediante dos redes WAN de diferentes operadores (A y B) para que, en caso de caída general de un operador 1 en una zona concreta del territorio, las sedes afectadas por ese corte puedan comunicarse con las otras sedes a través de la WAN del segundo operador, operador 2.

De esta manera, los accesos secundarios de todas las sedes y el CPD pasaran a conectarse entre ellos a través de la WAN del operador 2, disponiendo así de un segundo nivel de contingencia a nivel de operador.

1.2. Objetivos

El objetivo general del proyecto es proponer la operativa necesaria y detalles técnicos en cuanto a la integración de los dos operadores de servicios de telecomunicaciones en una misma entidad, permitiendo de esta forma un nivel extra de seguridad ante un posible fallo general de un operador o de una tecnología determinada.

Los objetivos concretos del proyecto son:

- Diseño y configuración de una red WAN del nuevo operador con accesos de datos secundarios en cada una de las sedes.
- Configuración de la interconexión de ambos operadores.
- Descripción y planificación de la infraestructura necesaria.
- Descripción y planificación del proceso de migración de los accesos secundarios de cada una de las sedes remotas.
- Valoración económica de la modificación propuesta.
- Evaluación de riesgos e impacto sobre la operativa diaria.

1.3. Planificación

Al iniciar este proyecto se planteo una planificación temporal inicial que permitiera el desarrollo de las diferentes estructuras y apartados de la que estaba compuesto el proyecto.

Esta planificación se expresó en una lista de tareas e hitos con fecha de inicio, fecha de finalización prevista y la duración aproximada según una previsión inicial.

	Name	Start	Duration	Finish	Predecessors
1	PEC1	27/02/19 09:00	6 days	05/03/19 09:00	
2	**⊟PEC2**	**05/03/19 09:00**	35 days	**09/04/19 09:00**	**1**
3	**⊟Análisis actual**	**05/03/19 09:00**	21 days	**26/03/19 09:00**	
4	Estado del arte	05/03/19 09:00	7 days	12/03/19 09:00	
5	Inventarios	12/03/19 09:00	2 days	14/03/19 09:00	4
6	Tipologias accesos/equipos	14/03/19 09:00	2 days	16/03/19 09:00	5
7	Estrutura red	16/03/19 09:00	2 days	18/03/19 09:00	6
8	Prototipos CPDs	18/03/19 09:00	4 days	22/03/19 09:00	7
9	Prototipos sede remotas	22/03/19 09:00	4 days	26/03/19 09:00	8
10	**⊟Propuesta técnica**	**26/03/19 09:00**	14 days	**09/04/19 09:00**	
11	WAN	26/03/19 09:00	3 days	29/03/19 09:00	3
12	LAN	29/03/19 09:00	3 days	01/04/19 09:00	11
13	Interconexión	01/04/19 09:00	6 days	07/04/19 09:00	12
14	Pruebas de validación	07/04/19 09:00	2 days	09/04/19 09:00	13
15	**⊟PEC3**	**09/04/19 09:00**	42 days	**21/05/19 09:00**	**2**
16	**⊟Propuesta técnica v2**	**09/04/19 09:00**	24 days	**03/05/19 09:00**	
17	Correcciones WAN	09/04/19 09:00	5 days	14/04/19 09:00	
18	Correcciones LAN	14/04/19 09:00	5 days	19/04/19 09:00	17
19	Correcciones interconexión	19/04/19 09:00	5 days	24/04/19 09:00	18
20	Correcciones PRUEBAS	24/04/19 09:00	5 days	29/04/19 09:00	19
21	Justificación criterios	29/04/19 09:00	4 days	03/05/19 09:00	20
22	**⊟Migración**	**03/05/19 09:00**	18 days	**21/05/19 09:00**	**16**
23	Procedimientos	03/05/19 09:00	6 days	09/05/19 09:00	
24	Planificación	09/05/19 09:00	6 days	15/05/19 09:00	23
25	Inventario final	15/05/19 09:00	6 days	21/05/19 09:00	24
26	Entrega memoria	21/05/19 09:00	19 days	09/06/19 09:00	15
27	Entrega presentación	09/06/19 09:00	7 days	16/06/19 09:00	26
28	Tribunal	16/06/19 09:00	9 days	25/06/19 09:00	27

Ilustración 1 - Planificación inicial.

Cada una de las tareas a realizar se concatenaron entre ellas para completar una planificación temporal expresada en un diagrama de Gannt [1] que permitiera y facilitara el seguimiento y posibles adaptaciones y modificaciones en función de los éxitos o dificultades encontrados en el proceso.

El diagrama de Gannt resultante de la concatenación de la lista de tareas anterior es el siguiente:

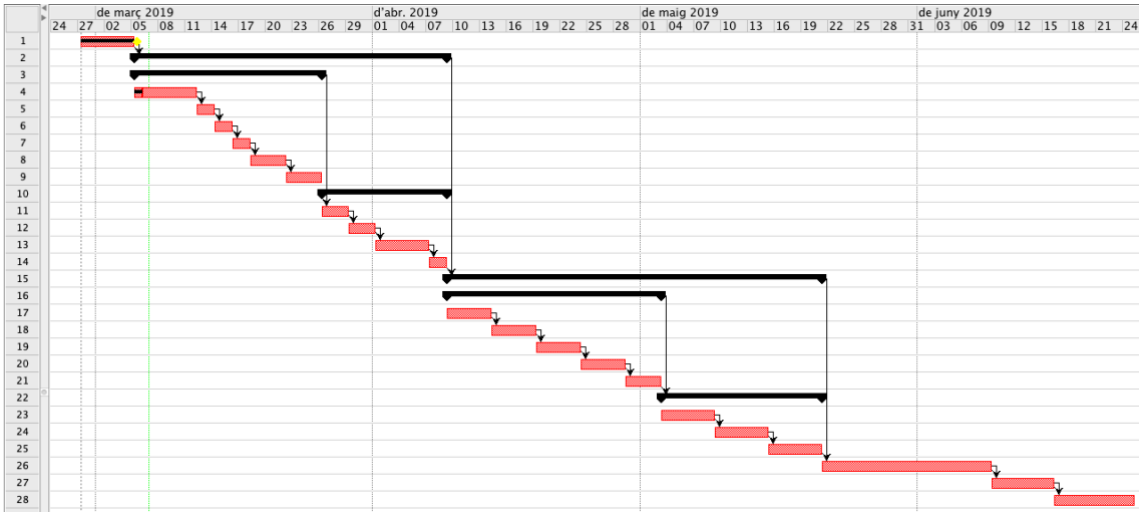

Ilustración 2 - Diagrama de Gannt.

1.4. Descripción de los otros capítulos

Los temas centrales del proyecto se han estructurado en tres grandes bloques:

- **Análisis actual**: en este apartado se analizará es mercado actual, así como posibles proyectos similares, sus ventajas e inconvenientes y similitudes con este proyecto. Además, se analizarán los diferentes protocolos de configuración de redes y los posibles accesos que los operadores ISP de telecomunicaciones pueden ofrecer.

- **Problema**: se valorará la situación actual de la empresa a nivel técnico y se entrará en detalle en prototipos técnicos actuales de las diferentes tipologías de sedes y necesidades.

- **Propuesta técnica**: se realizará una propuesta de configuración técnica a nivel WAN y LAN, así como para cada una de las tipologías de sedes definidas como prototipo y su interconexión con el CPD. Diferenciando la importancia de cada una de ellas y analizando las posibles herramientas de diseño de estas.

  Finalmente, se justificará el cumplimiento de los criterios impuestos por la organización en la fase inicial de análisis.

- **Implantación**: en el último bloque trataremos la planificación y procedimientos a llevar a cabo durante la migración de cada uno de los accesos secundarios de un operador 1, a otro operador 2.

  El resultado final de esta migración de accesos de datos deberá dar como resultado un listado de sedes actualizado con cada uno de los detalles de conexión, tanto mediante el acceso principal como con el secundario, de cada una de estas.

En los siguientes capítulos **evaluaremos el impacto económico** que tendrá sobre la organización y los **posibles riesgos** de un proyecto de esta envergadura para la operativa diaria de cada una de las sedes, servicios centrales (CPD) y cada uno de los clientes.

Finalmente, se desarrollarán las **conclusiones** extraídas durante la realización del proyecto proponiendo mejoras y posibles puntos críticos que se hayan detectado y sean susceptibles de un estudio posterior.

En los apartados "**Glosario**", "**Bibliografía**" y "**Anexos**" se adjuntará la información oportuna para cada uno de ellos y así completar el trabajo de final de grado con las referencias a cualquier otro trabajo o fuente de información, así como documentos adicionales para la correcta compresión de este.

2. Análisis actual

En los siguientes capítulos se analizan diferentes propuestas tecnológicas encontradas en la investigación previa junto a los resultados obtenidos y los posibles puntos de mejora que aportan al proyecto.

2.1. Estado del arte

Desde hace años se está considerando la idea de trabajar con más de un operador ISP, y la disponibilidad de más de una WAN, tanto para ampliar los anchos de banda y disponibilidad de servicios, como para contrarrestar posibles fallos o caídas en los servicios de alguno de los operadores.

Esta tecnología es denominada "*dual-homing*" [2] y consiste en la configuración de dos routers de acceso diferentes para que, de esta forma, siempre que haya una denegación de acceso a través de uno de los dos routers se pueda derivar el tráfico a través del otro acceso disponible y reducir los costes de protección del *core* de red.

Actualmente se encuentran disponibles diferentes tecnologías y metodologías para aplicar la disponibilidad de dos operadores ISP y el balance de cargas de la red LAN mediante firewalls o equipos específicos.

Un ejemplo de equipo específico dedicado al balance de carga entre dos operadores es la propuesta de Ernesto Pérez Estévez [3] que propone configurar una máquina con tres tarjetas de red (una para cada WAN y otra para la LAN) y el software ZeroShell que permitirá distribuir el tráfico solicitado por la LAN a través de cada uno de los ISP según nuestra preferencia.

En esta situación teórica se podría configurar cada uno de los operadores como principal o secundario según las necesidades de la organización, pero la necesidad de disponer de una máquina dedicada a la gestión del tráfico en cada una de las sedes y la dependencia de un software dedicado a ello lo convierte en una opción sumamente compleja.

Otro método para trabajar con dos operadores ISP o dos WAN, son los denominados routers Dual WAN o Multi WAN [4]. Esta tipología de routers permitirá conectar al cliente final a dos operadores directamente desde un

mismo equipo que se encargará de gestionar el uso de cada de los accesos según las necesidades de cada momento.

En la imagen del artículo de la revista Pymes y autónomos [4] se puede apreciar el esquema de funcionamiento de estos routers:

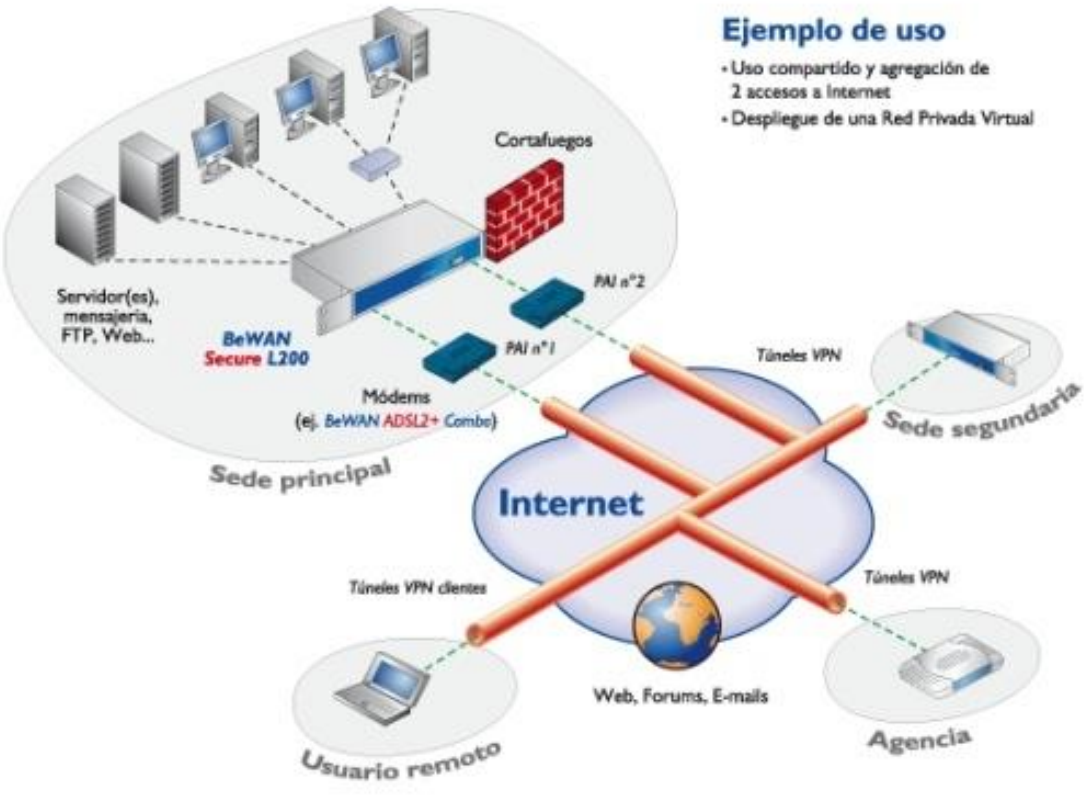

Ilustración 3 - Diagrama de red sistema Dual WAN [4].

La ventaja más evidente de esta solución es la gran simplicidad técnica de la solución y las posibilidades de desarrollo que cada una de las marcas fabricantes puede llegar a facilitar.

Las desventajas más importantes, y por las cuales se ha descartado esta opción, se pueden destacar las siguientes:

- Prácticamente nula posibilidad de personalización e independencia de la solución final de conectividad.
- Elevado coste de equipo profesionales que permitan conectividad VPN o soluciones Firewall, por ejemplo.
- Dependencia de las posibles actualizaciones a nivel de firmware que pueda llevar a cabo el fabricante.

- Dependencia a nivel de mantenimiento, configuración y soporte del fabricante.

Contemplando soluciones más personalizables para el cliente final se puede optar por utilizar equipos de balance de carga mediante firewalls corporativos o equipos específicos. De esta manera podemos provocar que el tráfico se distribuya entre las líneas con diferentes posibles algoritmos en función de la configuración que se lleve a cabo:

- Activo – pasivo: donde uno de los accesos será siempre el activo y otro el pasivo, que pasará a ser el activo sólo en el momento en que el activo quede fuera de servicio.

- Distribución de carga: donde ciertos tráficos o VLANs son derivadas a conciencia por uno u otro acceso distribuyendo así el volumen de tráfico a través de cada ISP. Esta configuración es oportuna cuando un solo acceso no dispone del caudal necesario para hacerse cargo de todo el volumen de datos o cuando uno de los servicios, VLANs necesita un porcentaje de caudal priorizado para su correcto funcionamiento (VoIP, por ejemplo).

- Aleatorio: en este supuesto ambos accesos estarían configurados como activos y un algoritmo de red elegirá el mejor ISP para cada momento determinado dependiendo de diferentes parámetros (disponibilidad, saturación de la red, etc…)

2.2. Tecnologías principales

A continuación, se analizan las soluciones existentes que permitan llevar a cabo, no sólo la solución actual adoptada por la organización, si no también la futura propuesta de solución planteada en este proyecto.

A nivel de interconexión de equipos existen diferentes tipologías en función de las limitaciones físicas o la virtualización de estas redes:

- LAN (*Local Area Network*) [5]: este concepto define la conexión de diferentes equipos en un área reducida como puede ser un edificio o una sede de una empresa.

A través de ella se pueden compartir recursos como equipos, (impresoras, terminales, etc…) o información (documentos, bases de datos, etc…).

Podemos encontrar diferentes tipologías de redes LAN en función de la distribución de sus nodos (equipos):

- **Red en bus**: un mismo cable conecta a las computadoras y permite la transmisión de datos de forma sencilla siendo muy susceptible a los daños en el cableado o a la interrupción de la transmisión.
- **Red en estrella**: en la que todos los computadores se conectan a un servidor central que administra los recursos de la red y los asigna según se le solicite.
- **Red en anillo**: en la que todos los computadores están conectados con sus vecinos mediante una transmisión unidireccional, que interrumpe la red de haber un fallo en algún nivel de esta.
- **Red mixta**: combina dos o más modelos de los descritos anteriormente.

- MAN (*Metropolitan Area Network*): similares a las redes LAN, pero con alcance de metropolitano, superior pues a las redes LAN pero sin llegar a ser de ámbito nacional o internacional.
- WAN (*Wide Area Network*): con la misma filosofía que las redes LAN o MAN, pero de mayor extensión, pudiendo llegar a ser de ámbito nacional o incluso internacional.
- VLAN (*Virtual LAN*) [6]: es un concepto similar a la LAN, pero donde los equipos son agrupados de manera lógica y no física. Mediante a este concepto podemos simular una LAN sin las limitaciones geográficas. Existen diferentes tipologías de VLAN en función de los criterios de conmutación y el nivel en el que se lleva a cabo:
  - **VLAN de nivel 1**: donde se define en función de los puertos del conmutador (router o switch).

- **VLAN de nivel 2**: en la que se define basándose en la MAC de cada uno de los equipos o nodos de la red.

- **VLAN de nivel 3**: en las que se pueden utilizar las direcciones de red de los equipos o los protocolos de comunicación utilizados para definir cada red virtual.

Los protocolos de comunicación y divulgación de redes entre routers más habituales en este tipo de configuraciones son:

- RIP (*Routing Information Protocol*): es un protocolo de enrutamiento específica para la parte interna de la red [7]. Cuando un nuevo usuario se conecta avisa con un mensaje RIP al router más cercano indicando la dirección IP que dispone en ese momento.

- OSPF (*Open Shortest Path First*): al igual que el anterior, es un protocolo específico para uso en la parte interna de la red mediante el cual cada router conoce los routers más cercanos y las direcciones de estos [8]. Este protocolo envía los paquetes a través del camino más corto teniendo en cuenta el camino más corto en función de los nodos que deberá atravesar.

- BGP (*Border Gateway Protocol*): es el protocolo más complejo de los vistos hasta el momento que utiliza para la interconexión de diversas redes conectadas entre sí [9]. En la toma de decisión de la ruta idónea, este protocolo utiliza diversos parámetros (ancho de banda, saturación de la red, etc…).

- VRRP (*Virtual Router Redundancy Protocol*) / HSRP (*Hot Standby Router Protocol*): protocolo definido por la IETF [10] que permite disponer de una puerta de enlace virtual que derive el tráfico hacia la IP con mayor prioridad o carga.

En cuanto a las diversas tecnologías de accesos que ofrecen los diferentes operadores de telecomunicaciones, se pueden destacar los siguientes:

- FO (*Fiber Optic*): se caracteriza por llevar la fibra óptica desde la central del operador hasta el propio abonado. Este tipo de cableado

es exclusivo para cada abonado, por lo que no se comparte el caudal y permite así anchos de banda más amplios que pueden llegar hasta varios Gbps simétricos (de subida y bajada). La instalación de esta tecnología comporta disponer de los siguientes dispositivos:

  - ONT, convertidor de señales de luz ópticas a señales eléctricas, junto con el router del operador.
  - Router del operador con ONT incorporada, el cual transforma la señal óptica en eléctrica antes de gestionarla.

- FTTH (*Fiber To The Home*): es un tipo específico de FO que permite abaratar los costes de comercialización a las operadoras a nivel doméstico, ya que el cableado desde la central de la operadora hasta el armario de comunicaciones comunitario es compartido por todos los usuarios de la comunidad.

  El caudal de la fibra óptica es dividido en función de las necesidades de cada uno y el coste es repercutido por la operadora en función de dicho caudal.

  Al igual que la FO es necesario de disponer de una ONT o un router con ONT incorporada para la transformación de la señal.

- HFC (*Hybrid Fiber Coaxial*): la diferencia con la FTTH reside en que esta tecnología no llega con la fibra óptica hasta el abonado, sino que desde el nodo central hasta el abonado llegará con un cable coaxial. La interconexión nodal si que se llevará a cabo mediante fibra óptica.

  En esta tipología de accesos conlleva la instalación de unos divisores de señal (*splitter coaxial*) en cada uno de los puntos donde haya que dividir la señal. En casa del abonado se dispone de un cable-modem o cable-router que gestionará la señal.

  Actualmente las oferta de está tecnología la centra el operador Vodafone, mediante la red HFC que disponía ONO, y las velocidades soportadas pueden llegar a los 100 Mbps en bajada y 10 Mbps en subida.

Para mejorar está tecnología se está llevando a cabo la actualización de su estándar de transmisión, DOCSIS, a la versión 3.1 que permitirá anchos de banda de hasta 192 MHz en bajada y 96 MHz en subida.

- ADSL (*Asymmetric Digital Subscriber Line*): es la tecnología digital más extendida en la actualidad y consisten en la trasmisión de datos digitales mediante cable de par simétrico de cobre de la línea telefónica.

  Actualmente, y gracias a la tecnología ADSL 2+, pueden llegar a ofrecer hasta 30 Mbps en bajada y unos 3 Mbps en subida.

  Debido a que la señal se transmite a través del par trenzado utilizado a la línea telefónica el abonado solo deberá instalar un router que gestionará y transformará la señal en impulsos eléctricos.

- 3G / 4G: diversas compañías ya ofrecen accesos de datos basados en tecnología móvil. Con velocidades de hasta unos 100 Mbps de descarga y 8 Mbps en subida lo único necesario es un router con disponibilidad 3G/4G y cobertura móvil de la operadora seleccionada.

2.3. Contribución del proyecto

En base a los conocimientos adquiridos tanto académica como profesionalmente y a través de la información recopilada en el presente proyecto, se pretende mejorar y contribuir a una mejor concepción y comprensión de las posibilidades de configuración que nos aportan las diferentes opciones de que disponemos actualmente en el mercado de las comunicaciones de red a nivel WAN.

Con el caso simple y concreto que se ha elegido se propondrán los posibles riesgos y mejoras técnicas para poder disponer de una contingencia de doble nivel (operador y tecnología), así como procedimientos y validaciones durante el proceso de migración y configuración de una red de datos empresarial.

También se aportarán los conocimientos necesarios de alto nivel en cuanto a configuración de redes (WAN, VLAN, etc…), así como configuración a bajo nivel de equipos (router y switch) y protocolos de comunicaciones y algoritmos de asignación y calculo de prioridades.

Por último, se llevará a cabo una estimación del impacto económico que la ampliación de la red de datos con contingencia de doble nivel, operador y tecnología del acceso, pueda conllevar para la organización y los posibles métodos y/o acciones que se puedan emprender para minorarlos.

3. El problema

Hoy en día las comunicaciones entre diferentes oficinas de una organización o la conexión de estas a Internet pueden llegar a ser fundamentales para el correcto funcionamiento de la empresa, pudiendo llegar incluso a no poder dar ningún tipo de servicio a sus clientes debido a una posible caída de los accesos de datos de telecomunicaciones que conecta cada una de las sedes en cuestión con Internet o los servicios centrales de la entidad.

Para evitar estas posibles desconexiones los proveedores de servicios de internet, ISP (*Internet Service Provider*), trabajan continuamente en la mejora de la red y la redundancia de accesos y nodos para una mayor disponibilidad de sus servicios. Pero a pesar de los SLA (*Service Level Agreement*) y posibles compensaciones, económicas o no, negociadas con los operadores, el problema puede no tener fácil solución y provocar perdidas económicas, directas o indirectas, irreparables para las entidades afectadas.

En concreto, durante el 2018 la entidad tubo un total de 63 incidencias que provocaron aproximadamente 127 horas de desconexión imposibilitando el trabajo normal de alguna de las sedes. Estas incidencias se dividen en cuatro tipologías en función de la duración de la incidencia.

En la siguiente tabla se muestra un análisis resumido de este tipo de incidencias y junto a la duración total de la desconexión y los porcentajes sobre el total de horas trabajadas y el total de incidencias de este tipo:

Duración de la incidencia	Duración total	% sobre h. trabajadas (2080 h)	Total incidencias	% sobre total incidencias
t < 1 h.	35 h.	1,68%	45	71,43%
1 h. < t < 4 h.	31 h.	1,49%	14	22,22%
4 h. < t < 24 h.	25 h.	1,20%	3	4,76%
24 h. < t	36 h.	1,73%	1	1,59%
TOTAL	**127 h.**	**6,11 %**	**63 incid.**	**100 %**

Tabla 1 - Análisis incidencias críticas 2018.

En el marco de este proyecto se estudia una posible solución al problema que ayude a mitigar el porcentaje de tiempo que una organización pueda llegar a estar desconectada de Internet o de su propia red de datos por incidencias o averías de los operadores de este servicio. Para ello, se parte de una organización ficticia donde poder aplicar y teorizar sobre las medidas a tomar y posibles métodos y protocolos que habrá que tener en cuenta.

3.1. La organización

Para poder llevar a cabo el estudio teórico de la solución al problema descrito en el apartado 2 se plantea una organización ficticia y relativamente básica, aunque o suficientemente escalable para que pueda ser válida, a partir de la cual buscar la solución adecuada.

Esta organización tiene una estructura empresarial con 100 oficinas, o sedes remotas, repartidas por el territorio español y una sede central en Barcelona donde está instalado un CPD (Centro de Procesamiento de Datos) que da servicio al resto de sedes.

Este CPD, o sede central, está dotado con diferentes servidores y BDD (Bases de Datos) principales de la organización con información de clientes, proveedores, trabajadores, usuarios y demás información útil para cada uno de los trabajadores de las sedes y las funciones que desarrolla cada uno de ellos.

A nivel organizativo, la entidad cuenta con diferentes departamentos y distintos perfiles de usuarios con diferentes permisos de acceso a datos, configuración, etc… Los usuarios tienen diferentes controles de acceso a datos en función del perfil asociado a cada uno de ellos a través de aplicativos destinados exclusivamente a estos.

Dentro de todas las posibilidades de uso que la entidad podría llevar a cabo de las comunicaciones entre sedes y entre las sedes y el CPD, actualmente sólo se utilizan los accesos de datos de las sedes remotas para dos funciones principales:

- Compartición de datos: las sedes remotas consultan con bases de datos instaladas en el CPD o incluso en bases de datos puntuales

en alguna de las sedes. Los usuarios, en función del perfil de cada uno de ellos, también pueden compartir carpetas o documentos a través de las VLAN definidas para este servicio.

- Acceso a Internet: todos los usuarios disponen de acceso a Internet tanto para la operativa diaria con correo electrónico, consultas web, etc… como para ejecutar diferentes aplicativos específicos de negocio de la entidad. En la actualidad el acceso a internet es libre, aunque el tráfico es controlado a través de un firewall en cada una de las sedes.

En un futuro la organización contempla poder implementar otros múltiples servicios a través de la red de datos actual por lo que se deberán tener en cuenta a lo hora de formular los requisitos del proyecto y sobredimensionar, si fuera necesario, algún punto de la estructura de red:

- VoIP (Voz sobre IP): permitirá a la organización centralizar la salida a la red de telefonía a través de la sede central y comunicar todas sus sedes a través de la red de datos evitando así el coste en llamadas *on-net* (dentro de la misma empresa).

  También facilitará la gestión y control de las llamadas salientes tanto a fijos como móviles a través de un solo enlace central (TRUNK SIP) gestionado a través de una centralita única situada en el propio CPD.

- Tunelización IPSec: mediante el cifrado de datos se podrán tunelizar ciertas comunicaciones para mejorar la seguridad de la entidad y certificar, por ejemplo, el compromiso de confidencialidad con los clientes.

- Videoconferencias: si los caudales de los accesos de datos son adecuados se podría llegar a plantear la configuración de salas virtuales donde poder realizar videoconferencias con clientes, proveedores o reuniones no presenciales entre equipos multidisciplinares situados en sedes distantes en el territorio nacional.

Estas y otras posibles mejoras se deberán tener en cuenta a la hora de planificar y estudiar las diferentes opciones en cuanto a los accesos de datos disponibles de cada uno de los operadores ISP en cada una de las sedes remotas y la sede central.

3.2. Estructura general de la red

Actualmente, y con la función tanto de interconectar las sedes centrales con el CPD como la de conectar con Internet y otros servicios en la nube, la organización dispone de una estructura de red basada en dos tipologías de sedes según su función en la organización:

- Sede central: donde se encuentra instalado un CPD con diversos servidores que darán servicio al resto de las oficinas, sedes remotas.

- Sedes remotas: que se conectarán con el CPD y entre ellas mismas para el intercambio de información tanto a nivel de BDD o información interna como a través de Internet con las aplicaciones comunes para ello.

En la actualidad la interconexión de todos estos servicios, tanto la salida a Internet como las diferentes consultas internas a las BDD del CPD o de otras sedes, se realiza a través de una red WAN de un único operador, denominado operador 1 o principal, para diferenciarlo de otros posibles operadores que intervengan en el proyecto.

Dentro de cada una de las sedes remotas y el CPD la empresa dispone físicamente de diferentes perfiles de usuarios y terminales por lo que se separa el tráfico de cada una de las agrupaciones de grupos de terminales y servicios por perfiles de usuarios a través de diversas VLANs.

Cada una de estas VLANs aportará servicio a un grupo determinado de terminales y/o equipos de usuarios dentro de cada sede remota y se interconectarán a un servidor en particular en el CPD, sede central, y a los terminales y/o equipos de usuarios del mismo grupo de las otras sedes remotas.

3.2.1 Configuración IP

Todas estas VLANs se encuentra configuradas con una dirección IP del tipo B, con una macara /16, que permite la identificación de las diferentes VLANs a través del segundo octeto. El tercer octeto se utiliza para identificar la sede donde se encuentra ubicado el equipo. Mientras que el cuarto octeto permite identificar cada uno de los equipos.

Para la configuración teórica se identifican las 3 VLANs principales:

- VLAN1: rango 172.1.0.0 con máscara 255.255.0.0.
- VLAN2: rango 172.2.0.0 con máscara 255.255.0.0.
- VLAN3: rango 172.3.0.0 con máscara 255.255.0.0.

Por ejemplo, el terminal 2 de la sede 1 que debe utilizar la VLAN 3 para comunicarse con las otras sedes y equipos del CPD utilizará la siguiente dirección IP:

Equipo 2 de la sede 1 de la VLAN 3: ***172.3.1.2/16***

Disponer de una máscara del tipo 255.255.0.0, con dos octetos libres para identificar equipos, permite divulgar los rangos IP de cada sede realizando una fragmentación de estas redes con la mascara 255.255.255.0.

Gracias a este método de configuración IP y segregación del rango de la LAN de la organización se consigue identificar y controlar los accesos de los diferentes equipos en función de la VLAN a la que pertenece y a la sede física donde se encuentra ubicado.

En la siguiente figura se identifican los elementos comentados anteriormente y las conexiones existentes entre ellos. Se pueden apreciar las dos sedes remotas y la sede central, CPD, y los diferentes terminales pertenecientes a las diferentes VLANs configuradas y comentadas anteriormente.

También se puede apreciar la conexión existente entre los terminales y los routers del operador ISP principal, operador 1, través de un switch que aporta independencia y versatilidad de configuración a la organización.

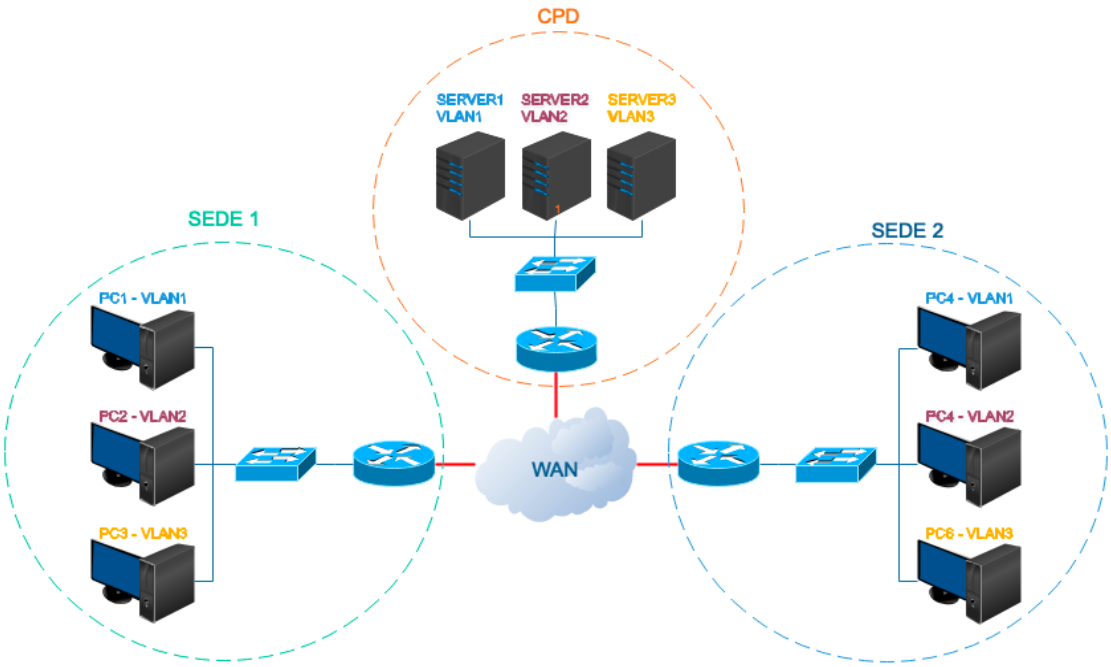

Ilustración 4 - Diagrama de red 1 ISP

3.2.2 Divulgación de redes

Para la divulgación de las diferentes VLANs a través de los equipos de la red se utiliza el protocolo eBGP utilizando la segmentación de cada una de las tres VLANs con las que trabaja la organización se comunica las redes disponibles desde cada uno de los routers hacia cada uno de los routers vecinos de las diferentes sedes.

A continuación, se concreta la configuración de los routers de cada una de las sedes remotas y el CPD a nivel de las redes que se deben divulgar hacia la red WAN del operador 1. Se debe tener en cuenta que, como se van a divulgar las VLANs de cada una las sedes, y no las VLANs globales de toda la organización, se debe divulgar las VLANs de rango /24 y no las de rango /16 comentadas en el apartado anterior.

En concreto, desde el CPD se deberán divulgar las tres VLANs que dan servicio a los tres grupos de equipos o usuarios. En el tercer octeto indicaremos el código de la sede, en este caso el 0 (código de sede para la sede central / CPD). Como siguiente salto indicaremos siempre la IP del router de la sede, que se indicará con un 1 en el cuarto octeto de la dirección IP. El resumen de las sedes a divulgar desde el router del CPD será el siguiente:

Subnet	Sede	VLAN	Rango IP	Next hop	Router interface
1.0	0	1	172.1.0.0/24	172.1.0.1	Ethernet 0/0
2.0	0	2	172.2.0.0/24	172.2.0.1	Ethernet 0/0
3.0	0	3	172.3.0.0/24	172.3.0.1	Ethernet 0/0

Tabla 2 - VLANs divulgadas a través del protocolo eBGP en el CPD.

Para la sede 1 se utilizará la misma técnica que se ha comentado anteriormente. Completando el tercer y cuarto octeto del rango IP década una de las VLANs definidas con la información de la sede y del router de esta sede, indicado con un 1. Por lo tanto, desde la sede 1 se divulgan las siguientes redes hacia las sedes remotas y el CPD:

Subnet	Sede	VLAN	Rango IP	Next hop	Router interface
1.1	1	1	172.1.1.0/24	172.1.1.1	Ethernet 0/0
2.1	1	2	172.2.1.0/24	172.2.1.1	Ethernet 0/0
3.1	1	3	172.3.1.0/24	172.3.1.1	Ethernet 0/0

Tabla 3 - VLANs divulgadas a través del protocolo eBGP en la sede 1.

Por último, seguimos la misma técnica para la composición de las VLANs a divulgar desde la sede 2. Por lo que en este caso se volverán a rellenar los octetos de la tercera posición con un 2, código de esta sede, y se volverá a identificar el router con un 1 en el cuarto octeto para la configuración del siguiente salto del protocolo eBGP.

En concreto se divulgan las siguientes redes hacia la WAN del operador principal, operador 1:

Subnet	Sede	VLAN	Rango IP	Next hop	Router interface
1.2	2	1	172.1.2.0/24	172.1.2.1	Ethernet 0/0
2.2	2	2	172.2.2.0/24	172.2.2.1	Ethernet 0/0
3.2	2	3	172.3.2.0/24	172.3.2.1	Ethernet 0/0

Tabla 4 - VLANs divulgadas a través del protocolo eBGP en la sede 2.

El protocolo dispone de la posibilidad de configurar las prioridades y pesos de cada uno de los siguientes saltos para determinar los caminos más eficientes y priorizar alguno de estos. En este caso, debido a que cada una de las VLANs divulgadas solo dispone de un único camino posibles, se dejará la configuración predeterminada.

Una vez planificada la comunicación y divulgación de VLANs a través de la WAN se deberán plantear los detalles técnicos de cada una de las sedes a nivel de configuración de router y switchs en función del prototipo de sede, sede central o CPD y sedes remotas, de la que forme parte.

3.3. Tipologías de sedes

Tal y como ya se ha comentado anteriormente la organización dispone de dos tipologías de sedes diferenciadas por el equipamiento que se encuentra en cada una de ellas y la utilidad y función de la sede dentro de la estructura de red general de la entidad.

Con estos detalles y criterios se identifican la sede central o CPD y las sedes remotas que permiten configurar diferentes prototipos de ellas en función de los cuales se llevaría a cabo la configuración de futuras sedes incorporadas a la estructura de red de la entidad.

Para cada uno de estos prototipos de debe describir y concretar de cada uno de los equipos de la sede de tal forma que permita, para futuras ampliaciones, la aplicación sistemática de la configuración lógica prevista en cada una de las VLANs y terminales definidos.

3.3.1 Sede central o CPD

Esta sede es la que da servicio al resto de sedes remotas y, por lo tanto, será preciso dotarla de un tipo de acceso y equipo de dimensiones y capacidades más altas que en el resto de las sedes remotas donde el tráfico y las capacidades son notablemente inferiores.

En esta sede central se encuentra instalado el CPD para lo que se planifica un acceso del tipo FO 1GB (100 Mbps de transmisión simétrica y dedicado) que permite la conexión con cada una de las sedes remotas y servicios varios, como la conexión con Internet.

Analizando los equipos que se encuentran en esta sede, y comenzando desde la zona más exterior y hacia el interior de la sede, se identifica un router, un switch y los diferentes servidores para cada una de las VLANs y servicio de la entidad.

A continuación, se indica el modelo del router y del switch, así como la configuración de cada uno de los puertos de estos:

- ROUTER: modelo Cisco ASR 1002 [11] con interfaces del tipo Ethernet que se utilizan para la transmisión de datos de cada una de la VLAN.

  Se configura la interfaz Ethernet 0/0 mediante 3 subinterfaces, una para cada VLAN disponible, configuradas tal y como se indica en la siguiente tabla:

Router id.	Sede	VLAN	IP / Mask	Router interface
Router 0	CPD	1	172.1.0.1/16	Ethernet 0/0.100
Router 0	CPD	2	172.2.0.1/16	Ethernet 0/0.200
Router 0	CPD	3	172.3.0.1/16	Ethernet 0/0.300

Tabla 5 - Configuración de las interfaces del router del CPD

- SWITCH: modelo Cisco Catalyst 3560-24PS [12] con 24 puertos del tipo Ethernet 10/100 para las conexiones de equipos y la conexión con el router, y 2 puertos Gigabit Ethernet, que no serán utilizados en la configuración actual.

  A diferencia del router, donde se utilizaba una sola interfaz y se dividía en tres subinterfaces, en el switch se configurará cada interfaz para una VLAN determinada excepto la Ethernet 0/0 que se configurará en modo “Trunk” para permitir la transmisión de paquetes de todas las VLANs de la entidad hacia el router. La configuración de las interfaces del switch del CPD es la siguiente:

Switch id.	Sede	VLAN	Modo	Equipo	Router interface
Switch 0	CPD	1, 2, 3	Trunk	Router 0	Ethernet 0/0
Switch 0	CPD	1	Access	Server 1	Ethernet 0/1
Switch 0	CPD	2	Access	Server 2	Ethernet 0/2
Switch 0	CPD	3	Access	Server 3	Ethernet 0/3

Tabla 6 - Configuración de los puertos del switch del CPD

Por último, en la sede central también se dispone de los servidores de datos que dan servicio a cada una de las VLANs, pudiendo ser cada una de estas tratada como un servicio diferente.

La configuración en cuanto a la dirección IP, máscara y puerta de enlace será la siguiente:

Equipo	Sede	VLAN	IP / Mask	Gateway	Switch interf.
Server 1	CPD	1	172.1.0.2/16	172.1.0.1	Ethernet 0/0
Server 2	CPD	2	172.2.0.2/16	172.2.0.1	Ethernet 0/1
Server 3	CPD	3	172.3.0.2/16	172.3.0.1	Ethernet 0/2

Tabla 7 - Configuración de los servidores / equipos del CPD

3.3.2 Sedes remotas

Para cada una de las sedes remotas se dispone de accesos de datos de diferentes tipologías, descritos en el apartado 3.4 "*Tipologías de accesos*", como por ejemplo: FTTH, HFC y ADSL que permiten, a través de la conexión de un router, el acceso a Internet o a la transmisión de información con el resto de sedes o el CPD.

Al final del acceso físico se encuentra un router de operador ISP, en este caso el operador 1, que permite la conectividad con la WAN de este operador.

A continuación del router, y en la misma disposición que en el CPD, se ubica un switch propiedad de la organización que comunica los equipos con el router y permite el acceso de estos a VLANs determinadas y la conexión con otras sedes, incluida el CPD, a través de la WAN de operador.

Los detalles, tanto en cuanto al modelo como a la configuración implementada, de los routers y switchs de las sedes remotas son los siguientes:

- ROUTER: modelo Cisco ISR 1111-4P [13] con 4 puertos Ethernet, posibilidad de configuración de hasta 32 VLANs y tecnología Wireless LAN 802.11ac.

  Del mismo modo que en la sede central, se configura la interfaz Ethernet 0/0 para la transmisión, a través de diferentes subinterfaces, de los diferentes paquetes de cada una de las VLANS o servicios.

Teniendo en cuenta que la dirección IP del router será diferente en cada una de las sedes, para la sede 1 la configuración de cada uno de las subinterfaces será la siguiente:

Router id.	Sede	VLAN	IP / Mask	Router interface
Router 1	1	1	172.1.1.1/16	Ethernet 0/0.100
Router 1	1	2	172.2.1.1/16	Ethernet 0/0.200
Router 1	1	3	172.3.1.1/16	Ethernet 0/0.300

Tabla 8 - Configuración de puertos del router de la sede 1.

Con la misma configuración lógica, y de nuevo aplicando la dirección IP adecuada, en el router de la sede 2 se dispondrá de la siguiente configuración en cada una de las subinterfaces para cada una de las VLANs:

Router id.	Sede	VLAN	IP / Mask	Router interface
Router 2	2	1	172.1.2.1/16	Ethernet 0/0.100
Router 2	2	2	172.2.2.1/16	Ethernet 0/0.200
Router 2	2	3	172.3.2.1/16	Ethernet 0/0.300

Tabla 9 - Configuración de puertos del router de la sede 2.

- SWITCH: el modelo instalado en las sedes remotas es el Cisco Catalyst 3560-24PS que cuenta con un total de 24 puertos del tipo Ethernet 10/100, útiles para conectar los equipos y terminales de las sedes y el router del operador, y 2 puertos Gigabit Ethernet, que, igual que ocurrió en la configuración del switch del CPD, no serán utilizados.

  Cada uno de los puertos Ethernet donde se conectarán los terminales finales se configurará para que pueda transmitir los datos de la VLAN a la que pertenezca el equipo conectado. Lo que implicará configurarlo en modo “Access” y con la VLAN determinada como la única validada para la transmisión de datos a través del puerto.

  En concreto, tan solo el puerto Ethernet 0/0, que será utilizado para conectar el switch con el router y este será configurado en el modo “Trunk” y con todas las VLANs de las sedes aceptadas para la transmisión de datos a través este.

Según los criterios expresados anteriormente, la configuración específica resultante para cada una de las interfaces del switch de la sede 1 será la siguiente:

Switch id.	Sede	VLAN	Modo	Equipo	Router interface
Switch 1	1	1, 2, 3	Trunk	Router 1	Ethernet 0/0
Switch 1	1	1	Access	PC1	Ethernet 0/1
Switch 1	1	2	Access	PC2	Ethernet 0/2
Switch 1	1	3	Access	PC3	Ethernet 0/3

Tabla 10 - Configuración de puertos del switch de la sede 1.

Para la sede 2, y utilizando la misma lógica, se dispondrá de la siguiente configuración de puertos en el switch:

Switch id.	Sede	VLAN	Modo	Equipo	Router interface
Switch 2	2	1, 2, 3	Trunk	Router 2	Ethernet 0/0
Switch 2	2	1	Access	PC4	Ethernet 0/1
Switch 2	2	2	Access	PC5	Ethernet 0/2
Switch 2	2	3	Access	PC6	Ethernet 0/3

Tabla 11 - Configuración de puertos del switch de la sede 2.

En cuanto a los terminales de cada una de las sedes remotas se pueden identificar un terminal para cada una de las VLANs definidas teniendo en cuenta que la dirección IP de cada uno de los equipos estará definida por la identificación de la VLAN en el segundo octeto, el código de la sede en el tercer octeto y el código del equipo en el cuarto octeto.

Además, la puerta de enlace de los equipos será siempre la dirección del router del operador 1 y dependerá siempre de la sede donde se encuentre alojado el equipo.

Con estos condicionantes la configuración de la sede 1 la siguiente:

Equipo	Sede	VLAN	IP / Mask	Gateway	Switch interf.
PC1	1	1	172.1.1.2/16	172.1.1.1	Ethernet 0/0
PC2	1	2	172.2.1.2/16	172.2.1.1	Ethernet 0/1
PC3	1	3	172.3.1.2/16	172.3.1.1	Ethernet 0/2

Tabla 12 - Configuración de los puertos de los equipos de la sede 1.

Asimismo, en la sede 2 disponen de una distribución de equipos similar con la siguiente configuración:

Equipo	Sede	VLAN	IP / Mask	Gateway	Switch interf.
PC4	2	1	172.1.2.2/16	172.1.2.1	Ethernet 0/0
PC5	2	2	172.2.2.2/16	172.2.2.1	Ethernet 0/1
PC6	2	3	172.3.2.2/16	172.3.2.1	Ethernet 0/2

Tabla 13 - Configuración de los puertos de los equipos de la sede 2.

3.4. Tipologías de accesos

Tal y como se ha comentado anteriormente, para la interconexión entre todas las sedes, sedes remotas y el CPD, es necesario conectarlos a través de la WAN del operador ISP y, para conectar esta WAN a cada una de las sedes será necesario la conexión física entre las centrales del operador y las sedes.

Esta conexión se llevará a cabo a través de un acceso físico comercializado y mantenido por el propio operador ISP y en función de la disponibilidad del operador principal, ISP 1, en cada una de las sedes se dispondrá de circuitos instalados de diferentes tipologías.

A continuación, se describen las tipologías de accesos que se encuentran en las diferentes sedes de la organización:

- FO: el acceso del CPD o sede central debería ser de más capacidad que el resto de las sedes debido a la criticidad y el caudal previsto de transmisión de datos por lo que se debería elegir está tipología con un caudal dedicado de, como mínimo, 1 Gbps simétrico de velocidad.

- FTTH: los accesos de esta tipología disponen de una velocidad simétrica de subida y bajada de 100 Mbps. A través del gran caudal que permiten estos accesos se pueden llevar a cabo conexiones multimedia e incluso configuraciones ToIP entre sedes (fuera del ámbito este proyecto).

- ADSL: es la tipología de acceso más habitual en la actualidad, aunque empieza a estar en desuso y se intentará priorizar la instalación de otras tecnologías como las FTTH o 4G.

- 3G/4G: las sedes donde no se dispone actualmente de cobertura cableada, ya sea FTTH, HFC o ADSL, son dotadas de conectividad a través de la red móvil, ya sea 3G o 4G en función de la disponibilidad del operador. Siempre que es posible se realiza a través del mismo operador que aporta los accesos de datos cableados para simplificación de configuraciones y mantenimiento.

3.5. Inventarios

Una de las tareas más importantes a la hora de comenzar un estudio que pueda llegar a comportar una modificación o ampliación de la red de datos es la consolidación de un inventario tanto a nivel de sedes implicadas en el proyecto como de los accesos de datos de cada una de las sedes.

En este caso teórico se considera que esta consolidación se ha llevado a cabo previamente y que la organización cuenta actualmente los inventarios de sedes y accesos de datos completos.

3.5.1 Inventario de sedes

El inventario de sedes aporta la información concreta y detallada de cada una de ellas, sea del tipo que sea la sede en cuestión, para poder planificar y ejecutar cualquier tipo de implantación posterior al estudio previo que se lleva a cabo en este proyecto.

En el caso concreto de las diferentes sedes de la organización se dispone de los siguientes datos de cada una de las sedes (incluyendo tanto el CPD como las delegaciones o territoriales):

- Código: código unívoco identificativo de cada una de las sedes mediante el cual se referenciará cualquier dato relativo a esta.

- Dirección completa: permitirá ubicar la sede a nivel geográfico y documentar los diferentes accesos datos de cara a los operadores.

- Denominación: nombre identificativo de la sede que ayudará a hacerse una imagen rápida de la ubicación geográfica, mediante la provincia o la comunidad autónoma, y tipología de la sede.

- Tipología: cada tipología de sede diferente podrá disponer de unos

servicios diferenciados o necesidades concretas en cuanto a diferentes configuraciones o prioridades.

Aunque el ámbito del proyecto no incluye las configuraciones concretas de cada una de estas sedes, es importante remarcar que se deberán tener en cuenta a la hora de realizar posibles pruebas durante la implantación.

En la actualidad la entidad diferencia entre dos tipologías de sedes remotas:

- Direcciones territoriales: que concentrarán la atención y servicio a las delegaciones u oficinas de su provincia.
- Delegaciones: oficinas que aportaran el servicio al usuario final o cliente.

Cabe destacar que estas dos tipologías no suponen ninguna diferencia a nivel de configuración de red por lo que en la estructura general de la organización han sido incluidas en la categoría de “Sedes remotas”.

- Horario: se identifica el horario de atención al público de la sede , así como cualquier detalle especial que pueda ser de interés para planificar posibles visitas de técnicos, etc…
- Persona de contacto: persona responsable de cada sede a la que contactar en caso de ser necesario.
- Teléfono de contacto: donde contactar con la persona de contacto de cada sede.
- Puestos de trabajo: número de trabajadores o puestos de trabajo de la sede.
- Configuración: datos relativos a la configuración técnica de cada una de las sedes. Se incluye toda la información útil para posibles modificaciones de configuración, altas o bajas de los servicios.

Dentro del ámbito de este estudio se tendrán en cuenta un total de 1 sede central o CPD, 15 direcciones territoriales, una en cada provincia donde la entidad tiene representación, y 85 delegaciones.

3.5.2 Inventario de accesos de datos

El inventario de accesos se puede valorar con el mismo nivel de importancia que el inventario de sedes, ya que aportará información detallada de cada uno de los accesos de datos actuales y permitirá tomar decisiones al detalle de la mejor opción para la configuración o instalación que se deba llevar a cabo en cada una de las sedes.

Al igual que el inventario de sedes, es de vital importancia disponer de él antes de comenzar la planificación o la toma de decisiones del proyecto de implantación o estudio previo ya que en base a esta información se deberán tomar decisiones trascendentes que podrán definir la correcta consecución de los objetivos finales.

Este inventario está conformado por los siguientes datos:

- Administrativo: identificador unívoco con el que el operador ISP identifica el circuito o acceso de datos. Será útil a la hora de solicitar modificaciones de caudal, bajas, etc… al operador propietario.

- Código: identificador unívoco con el que la organización identificará cada uno de los accesos. Puede ser el mismo que utiliza el operador, pero no tiene porque ser así y es preferible mantener la independencia de los datos.

- Sede: código unívoco de la sede donde da servicio. Se utilizará para vincular cada uno de los accesos a la sede de manera que diversos accesos puedan estar vinculados a una sede, pero nunca el mismo acceso puede estar vinculado a diversas sedes.

- Tecnología: tipología del acceso (ADSL, FTTH, FO, MÓVIL, etc…). Será útil para categorizar el acceso y poder clasificarlo y valorarlo económicamente.

- Tipología del acceso: detalle más concreto sobre el tipo de acceso, velocidad, simetría (en cuanto a la subida y bajada de datos), etc…

- Caudal: ancho de banda contratado y detalle de la garantía y priorización del caudal en cuanto a multimedia, por ejemplo.

- Servicios añadidos: servicios adicionales contratados como mantenimiento, buzones de voz, etc….

- Operador: operador ISP que aporta el servicio a la entidad.

- Proveedor última milla: datos del proveedor de la parte de acceso que conecta desde la sede (PTR o PTO) hasta la central de telecomunicaciones.

Para los estudios y planificaciones que se llevan a cabo en apartados posteriores de este mismo proyecto se tendrá en cuenta que en el CPD o sede central, debido a su criticidad y el ancho de banda necesario para dar servicio a todas las consultas del resto de sedes, se dispone de un acceso del tipo FO de 1 Gbps de ancho de banda.

Las 15 direcciones territoriales disponen de un acceso de FTTH simétricos de 100 Mbps de velocidad de subida y 100 Mbps de velocidad de bajada en cada una de ellas.

En las 85 delegaciones se disponen de 60 accesos del tipo ADSL, con diferentes velocidades entre los 20 Mbps y 3 Mbps de bajada y 5 Mbps y 512 Kbps de subida, 20 accesos FTTH, con velocidades simétricas de 100 Mbps de bajada y subida, y 5 accesos basados en tecnología móvil 3G/4G.

3.6. Criterios de la organización

Antes de plantear una solución óptima que recoja los diferentes conceptos tratados hasta el momento será necesario tener en cuenta las prioridades de la organización tanto a nivel de configuración, disponibilidad, tecnológica, usabilidad o económica.

El objetivo principal de este proyecto y hacia el cual se enfoca también el principal criterio de la organización es reducir al máximo los tiempos de desconexión total provocados por averías o caídas en el servicio de datos del operador 1.

Por otro lado, para la organización es de vital importancia la disponibilidad de conexión a los servidores centrales, CPD, desde cualquiera de las sedes y entre ellas mismas no sea interrumpida, por lo que se deberá tener en cuenta a la hora de configurar los diferentes accesos la no interrupción del servicio del operador principal.

Con la configuración actual, la conectividad de cualquiera de los servicios asociados a una VLAN de una sede aleatoria al CPD depende, además de los equipos locales, del correcto funcionamiento de:

- El acceso de datos de la sede.
- Red de operador ISP.
- El acceso de datos de la sede central, CPD.

Se deberá aprovechar el máximo número de equipos posible (routers, terminales, switch, etc…) y los nuevos equipos se deberán plantear en previsión de un futuro crecimiento de la organización.

Además, se deberá tener en cuenta que cualquier cambio en la configuración de la red global de la organización no podrá suponer un corte sustancial en los servicios ofrecidos promoviendo la transparencia para los usuarios finales.

Por último, a pesar de que la entidad y su dirección es consciente de las implicaciones económicas que cualquier medida que se pueda tomar en la línea de minimizar el porcentaje de duración de incidencias que provoquen cortes en las comunicaciones, será de vital importancia mitigar ese impacto económico y controlarlo lo máximo posible con propuestas de mejora y control del gasto en telecomunicaciones seleccionando la tipología, velocidad y caudal garantizado más adecuados para cada acceso en cada una de las sedes en función de las necesidades particulares de estas.

Todos estos criterios de la organización en cuanto a una posible solución propuesta se pueden resumir en la siguiente lista:

- **Reducción tiempos de desconexión**: durante el 2018 se tuvo un total de 127 horas de desconexión y el objetivo de la entidad en

este sentido es reducir este tiempo a un máximo de 20 horas anuales.

- **Reducción del tiempo de incidencias**: durante el 2018 más de un 29 % de las incidencias tuvieron una implicación en la conexión de las sedes de más de 1 hora. El objetivo de la organización es que sólo el 5 % de las incidencias tengan una duración mayor a 1 hora.

- **Aprovechamiento de los equipos actuales**: se deberán aprovechar tanto los terminales finales, como los switch y routers de operador actuales.

- **Disponibilidad de servicios durante la implantación**: se deberá asegurar que los servicios siguen estando disponibles al 100% durante la implantación de la solución propuesta.

- **Transparencia usuarios**: la implantación de la solución deberá ser transparente para los usuarios y trabajadores de la entidad por lo que la configuración de los terminales y equipos de los usuarios no deberá ser modificada.

- **Coste económico**: la solución final no puede implicar un coste de más del 60 % sobre el presupuesto actual destinado a los circuitos de telecomunicaciones que dan servicio a las sedes remotas y el CPD.

4. Propuesta técnica

Para aportar la mejor solución posible al problema propuesto dentro de las muchas posibles se han tenido en cuenta los principales criterios y necesidades de la organización.

El primero y fundamental de estos criterios es la necesidad de reducir al máximo los tiempos de desconexión total por caída del servicio del operador, por lo que se propone la redundancia de los accesos de datos en todas las sedes con un segundo operador.

De esta manera se conseguirá evitar la desconexión en caso de caída de los servicios del operador ISP, ya que en cada una de las sedes tendrán un acceso principal con el operador 1, y un acceso secundario con el operador 2.

Por otro lado, en algunos casos la caída del servicio puede verse provocada por una incidencia a nivel tecnológico y que todos los accesos de la misma tecnología se vean afectados por la incidencia sin tener en cuenta el operador que ofrezca el servicio.

Para evitar este caso de desconexión total se propone redundar la contingencia a nivel tecnológico, por lo que los accesos secundarios nunca deberían utilizar la misma tecnología que los accesos principales.

De esta forma, y teniendo en cuenta que los accesos principales siempre serán los de mayor velocidad independientemente del operador que lo pueda ofrecer, podremos tener sedes con las siguientes tipologías:

Tipologías	Acceso principal	Operador principal	Acceso secundario	Operador secundario
Tipo 1	FTTH	1	ADSL	2
Tipo 2	FTTH	1	MÓVIL	2
Tipo 3	ADSL	1	MÓVIL	2
Tipo 4	FTTH	2	ADSL	1
Tipo 5	ADSL	2	MÓVIL	1

Tabla 14 - Tipologías de sedes según accesos.

Con el simple fin de marcar un criterio, en caso de que ambos operadores puedan ofrecer el mismo tipo de acceso como mejor solución en una de las sedes se adoptará el operador 1 como principal.

Otro punto importante para la organización es la de no interrumpir la operativa diaria de las sedes remotas y el CPD, por lo que durante la fase de implementación de la nueva solución no se podrán dejar sin servicio los servicios actuales. Para ello se deberá plantear en la fase de migración una configuración intermedia en los switchs y routers actuales que permita el trabajo en paralelo con uno o dos operadores.

Además, al ser la misma entidad la propietaria actualmente de los equipos instalados en las sedes (a excepción de los routers de operador) es muy interesante poder conservar el mayor número de equipos posible. Por lo que se tendrá en cuenta la posibilidad de adoptar los actuales equipos y terminales.

Los routers de operador, a pesar de no ser de la organización en cuestión, también deberían ser tomados en cuenta a la hora del aprovechamiento del material ya que los costes de sustitución de estos puede que sean repercutidos sobre el cliente y provoque un aumento de los costes de implantación del proyecto.

Al mismo tiempo, los routers del nuevo operador deberán ser de características similares a los actuales o que mejoradas respecto a estas para permitir los mismos servicios de los que actualmente dispone la organización o incluso alguno de los previstos en ampliaciones futuras (ToIP, cifrado de datos o videoconferencia).

Otra de las ventajas de esta solución es la gran flexibilidad que aporta a la organización, ya que si en un futuro incrementa sus servicios o decide implementar alguno de los servicios descritos en apartados anteriores (ToIP, cifrado de datos, etc…) sólo dependerá de la viabilidad de los equipos actuales y las habilidades técnicas de sus ingenieros de redes para configurar los equipos adecuadamente.

4.1. Solución final

Teniendo en cuenta los parámetros anteriores y la solución descrita se propone la siguiente solución de configuración con la duplicidad de los accesos de datos en las sedes y la implementación de una segunda WAN del operador 2 que pasará a estar activa al mismo tiempo que la del operador 1 (sistema activo – activo).

En la siguiente figura se muestra la estructura general de la red según los criterios descritos anteriormente. En ella se detallan los equipos propuestos para cada una de las VLAN de las diferentes sedes, el switch que gestionará la conexión entre cada uno de los equipos anteriores y los dos routers de los operadores y la WAN de cada uno de los operadores:

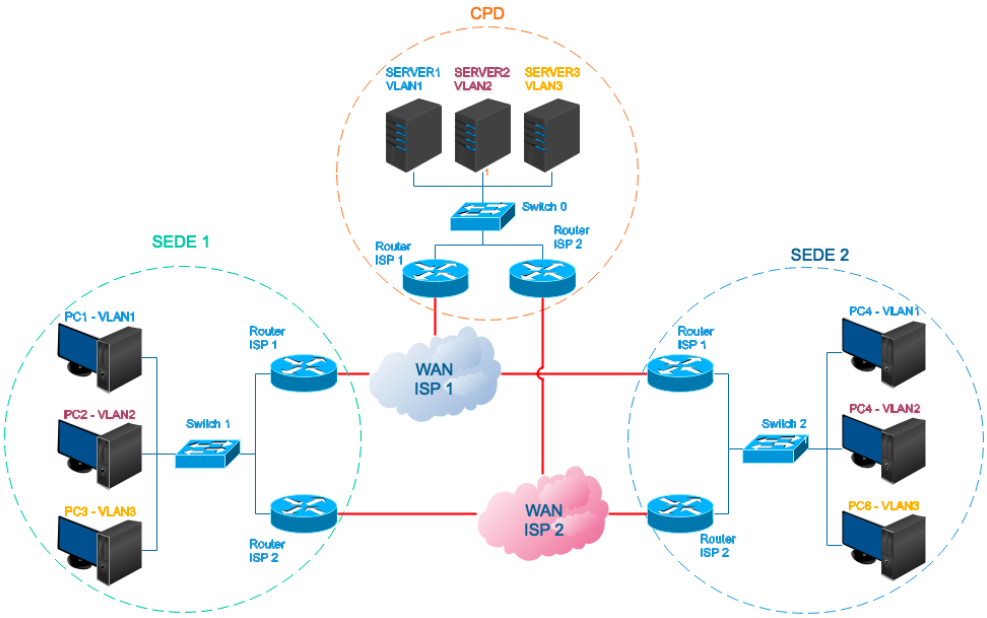

Ilustración 5 - Diagrama de red 2 ISP

4.2. Nivel WAN

A nivel WAN la comunicación entre cada uno de los routers del mismo operador ISP la gestionará cada operador mediante eBGP. Propagando cada una de VLAN de cada sede con la prioridad estándar.

Además, se compartirán las VLANs del otro operador mediante eBGP con prioridad más baja, por lo que si un operador no encuentra el enlace en su propia WAN (debido a una posible caída del acceso) dispondrá de una segunda ruta por la que acceder a través de los routers del CPD.

4.3. Nivel LAN

A nivel LAN de cada sede intentaremos preservar la configuración de los equipos para, tal y como se indicó en los criterios expuestos por la organización, favorecer la transparencia de la migración hacia el sistema de doble operador.

El punto más importante para la transparencia para los equipos y usuarios será poder mantener la configuración actual en cada uno de los equipos actuales. Por lo que no se debería modificar la configuración IP de estos y mantener, de este modo, la puerta de enlace predeterminada cada uno de ellos.

Gracias a la posibilidad de configurar grupos HSRP en los routers Cisco se podrá solventar este problema. Configurando un grupo HSRP para cada una de la VLAN en los dos routers de los operadores ISP y configurando la IP de salida de cada grupo HSRP con la actual puerta de enlace de los equipos de cada LAN en cada una de las sedes, será posible mantener la configuración previa de los equipos y que estos sigan apuntando hacia la misma dirección IP para la transmisión de los diferentes paquetes de información.

4.4. Interconexión CPD

Uno de los puntos críticos de la configuración de la red con doble operador es la interconexión de las dos WAN de ambos operadores y la transmisión de las VLANs e IPs de los equipos de una WAN a la otra.

Gracias a la gran versatilidad y compatibilidad del protocolo BGP, en su versión eBGP, se ha ello se ha elegido este para la configuración de la red y divulgar de este modo hacia el exterior de la WAN del operador las VLANs internas de la propia organización.

Esta interconexión se realizará entre los routers de los operadores ubicados en el CPD y en las sedes remotas y, a través de cada uno de ellos se divulgarán las diferentes rutas para el acceso de los datos tanto a través de la WAN del operador principal, operador 1, como a través del operador de respaldo, operador 2.

Para determinar que camino o ruta, la WAN del operador 1 o la WAN del operador 2, deberá ser el prioritario para cada una de las comunicaciones o el envío de los diferentes paquetes de información se deberá diferentes prioridades o pesos a cada una de las rutas.

De este modo, la prioridad más baja siempre será la del operador principal, dejando un valor de 100, y la prioridad más alta será la del router del operador de respaldo, con un valor de 200. La configuración final de las rutas a divulgar en cada uno de los routers del CPD, junto a su prioridad será la siguiente:

Router id.	Sede	Red	Local preference
Router 1.0	CPD	172.1.1.0/24	100
Router 1.0	CPD	172.2.1.0/24	100
Router 1.0	CPD	172.3.1.0/24	100
Router 1.0	CPD	172.1.2.0/24	100
Router 1.0	CPD	172.2.2.0/24	100
Router 1.0	CPD	172.3.2.0/24	100
Router 2.0	CPD	172.1.1.0/24	200
Router 2.0	CPD	172.2.1.0/24	200
Router 2.0	CPD	172.3.1.0/24	200
Router 2.0	CPD	172.1.2.0/24	200
Router 2.0	CPD	172.2.2.0/24	200
Router 2.0	CPD	172.3.2.0/24	200

Tabla 15 - Configuración propuesta para los routers del CPD

Dentro del CPD encontramos también los servidores que darán soporte al resto de sede y dispondrán de las posibles bases de datos de la organización. La configuración de estos, tal y como hemos explicado gracias a los grupos HSRP será la misma que en la actualidad:

Terminal	Sede	VLAN	IP / Mask	Gateway	Switch interface
Server 1	CPD	1	172.1.0.2/16	172.1.0.1	Ethernet 0/1
Server 2	CPD	2	172.2.0.2/16	172.2.0.1	Ethernet 0/2
Server 3	CPD	3	172.3.0.2/16	172.3.0.1	Ethernet 0/3

Tabla 16 - Configuración propuesta para los servidores.

Tal y como se ha comentado anteriormente será necesaria la configuración de un grupo HSRP para cada una de las VLANs definidas, de tal forma que cada equipo tenga una puerta de enlace que interrelacione los dos routers de los operadores y, por lo tanto, la solución elegida sea totalmente transparente para el usuario final.

Por lo tanto, en el CPD se aplicarán los siguientes grupos HSRP:

HSRP grupo id.	Sede	VLAN	IP
100	CPD	1	172.1.0.1
200	CPD	2	172.2.0.1
300	CPD	3	172.3.0.1

Tabla 17 - Configuración grupos HSRP del CPD.

Así mismo, será necesario implementar la prioridad de cada uno de los routers dentro del grupo HSRP aplicando valores superiores para el router principal, dejando el predeterminado de 200 ya puede ser válido, y valores inferiores para el router del operador de respaldo, operador 2:

Router id.	Sede	HRSP id.	Subinterface	Priority
Router 1.0	CPD	100	Ethernet 0/0.100	200
Router 1.0	CPD	200	Ethernet 0/0.200	200
Router 1.0	CPD	300	Ethernet 0/0.300	200
Router 2.0	CPD	100	Ethernet 0/0.100	100
Router 2.0	CPD	200	Ethernet 0/0.200	100
Router 2.0	CPD	300	Ethernet 0/0.300	100

Tabla 18 - Configuración HSRP en los routers del CPD.

4.5. Sedes remotas

De la misma manera que en el CPD, en cada una de las sedes remotas será necesario aplicar las configuraciones del protocolo eBGP, versión específica del protocolo BPG, a nivel WAN para la divulgación de las diferentes VLANs de cada sede.

Asimismo, se deberá llevar a cabo la aplicación y configuración de los grupos HSRP para la elección del prioritaria de router del operador principal y la transparencia total en la configuración de los equipos de los usuarios finales y trabajadores.

En cuanto a la configuración del protocolo eBGP se definirán las siguientes VLANs en cada una de las sedes con el peso determinado en la variable "*Local preference*":

Router id.	Sede	Red	Local preference
Router 1.1	1	172.1.1.0/24	100
Router 1.1	1	172.2.1.0/24	100
Router 1.1	1	172.3.1.0/24	100
Router 2.1	1	172.1.1.0/24	200
Router 2.1	1	172.2.1.0/24	200
Router 2.1	1	172.3.1.0/24	200
Router 1.2	2	172.1.2.0/24	100
Router 1.2	2	172.2.2.0/24	100
Router 1.2	2	172.3.2.0/24	100
Router 2.2	2	172.1.2.0/24	200
Router 2.2	2	172.2.2.0/24	200
Router 2.2	2	172.3.2.0/24	200

Tabla 19 - Configuración del protocolo eBGP a nivel WAN.

Utilizando la misma lógica que en el CPD y gracias a los grupos HSRP, la configuración de los routers de las sedes remotas será la siguiente:

Router id.	Sede	VLAN	IP / Mask	Router interface
Router 1.1	1	1	172.1.1.201/16	Ethernet 0/0.100
Router 1.1	1	2	172.2.1.201/16	Ethernet 0/0.200
Router 1.1	1	3	172.3.1.201/16	Ethernet 0/0.300
Router 2.1	1	1	172.1.1.202/16	Ethernet 0/0.100
Router 2.1	1	2	172.2.1.202/16	Ethernet 0/0.200
Router 2.1	1	3	172.3.1.202/16	Ethernet 0/0.300
Router 1.2	2	1	172.1.1.201/16	Ethernet 0/0.100
Router 1.2	2	2	172.2.1.201/16	Ethernet 0/0.200
Router 1.2	2	3	172.3.1.201/16	Ethernet 0/0.300
Router 2.2	2	1	172.1.1.202/16	Ethernet 0/0.100
Router 2.2	2	2	172.2.1.202/16	Ethernet 0/0.200
Router 2.2	2	3	172.3.1.202/16	Ethernet 0/0.300

Tabla 20 - Configuración propuesta para los routers de las sedes remotas.

Debido a que los grupos HSRP permitirán mantener la configuración actual en los equipos de cada una de las sedes se dispondrá de la misma configuración IP, incluida la puerta de enlace, la para cada uno de ellos:

Terminal	Sede	VLAN	IP / Mask	Gateway	Switch interface
PC1	1	1	172.1.1.2/16	172.1.1.1	Ethernet 0/1
PC2	1	2	172.2.1.2/16	172.2.1.1	Ethernet 0/2
PC3	1	3	172.3.1.2/16	172.3.1.1	Ethernet 0/3
PC4	2	1	172.1.2.2/16	172.1.2.1	Ethernet 0/1
PC5	2	2	172.2.2.2/16	172.2.2.1	Ethernet 0/2
PC6	2	3	172.2.2.2/16	172.3.2.1	Ethernet 0/3

Tabla 21 - Configuración propuesta para los equipos de las sedes remotas.

En cada una de las sedes deberemos configurar un grupo HSRP para cada una de las VLANs definidas, de tal forma, que cada equipo tenga la misma configuración actual según los criterios expresados por la organización.

Para ello configuraremos los grupos HSRP con la dirección IP actualmente configurada en los equipos y en la configuración de cada uno de los grupos HSRP daremos prioridad más elevada al router que ejerza de principal, por ejemplo 200, y una prioridad inferior al router que trabaje como secundario, por ejemplo 100 (la predeterminada).

Por lo que se deben configurar los siguientes grupos HSRP en cada una de las sedes indicadas en la siguiente tabla:

HSRP grupo id.	Sede	VLAN	IP
101	1	1	172.1.1.1
102	1	2	172.2.1.1
103	1	3	172.3.1.1
104	2	1	172.1.2.1
105	2	2	172.2.2.1
106	2	3	172.3.2.1

Tabla 22 - Configuración de grupos HSRP en las sedes remotas.

Por último, cada uno de los routers deberá tener configurados los grupos pertenecientes a su sede e incluir las prioridades en función de si ejerce como principal o secundario:

Router id.	Sede	HRSP id.	Subinterface	Priority
Router 1.1	1	100	Ethernet 0/0.100	200
Router 1.1	1	200	Ethernet 0/0.200	200
Router 1.1	1	300	Ethernet 0/0.300	200
Router 2.1	1	100	Ethernet 0/0.100	100
Router 2.1	1	200	Ethernet 0/0.200	100
Router 2.1	1	300	Ethernet 0/0.300	100
Router 1.2	2	100	Ethernet 0/0.100	200
Router 1.2	2	200	Ethernet 0/0.200	200
Router 1.2	2	300	Ethernet 0/0.300	200
Router 2.2	2	100	Ethernet 0/0.100	100
Router 2.2	2	200	Ethernet 0/0.200	100
Router 2.2	2	300	Ethernet 0/0.300	100

Tabla 23 - Configuración de los grupos HSRP en routers de sedes remotas.

4.6. Pruebas de validación teóricas

Una vez definida la configuración teórica de cada uno de los elementos de la red es de vital importancia corroborar el correcto funcionamiento de las propuestas teóricas descritas en el apartado anterior antes de llevar a cabo de la posible instalación y configuración de los equipos.

Con estas pruebas de validación teóricas se corroborará que la caída del acceso principal, circuito del operador 1, no va a implicar un corte en el servicio, y, por lo tanto, se evitarán todas las incidencias críticas sufridas por la caída del servicio de uno de los operadores y de esa forma se cumplirán dos de los principales criterios de la organización: reducción tiempos de desconexión y de incidencias, aprovechamiento de equipos y transparencia para los usuarios finales.

Otros criterios, como la disponibilidad de servicios durante la implantación y el coste económico de la nueva estructura, serán justificados mediante la correcta planificación del proyecto y el coste económico de este en apartados posteriores.

Para estas pruebas de validación teóricas se configurará la red se utilizará una de las herramientas de simulación y visualización de redes más versátiles y utilizadas del mercado: Cisco Packet Tracer [11]. Dentro de las diferentes versiones del programa se elige la versión 7 ya que, además de ser la última actualización, es la primera versión que contempla la compatibilidad con BGP y HSRP.

Con la solución diseñada y configurados los equipos en Cisco Packet Tracer se simulará la caída de alguno de los circuitos principales y, simulando en envío de paquetes ICMP entre diferentes dispositivos, se validará el correcto funcionamiento de la red con la recepción correcta de la respuesta de los equipos.

En concreto se contemplan las siguientes pruebas:

- Todo el sistema activo: se validará la correcta selección de la red principal, la del operador ISP 1, mediante la transmisión de paquetes ICMP y el correcto retorno por la misma red.

- Caída del router principal del CPD: en este caso la red elegida por el transmisor deberá ser la de respaldo, la del operador ISP 2. Al igual que en la prueba anterior de validará mediante la transmisión de diferentes paquetes ICMP desde equipos tanto pertenecientes al CPD como a alguna de las sedes remotas. La comunicación entre ambas sedes remotas deberá llevarse a cabo a través del circuito principal, operador ISP 1, por lo que se deberá realizar la prueba de comunicación entre las sedes 1 y 2 y corroborar que tanto la ida como el retorno del paquete ICMP se realiza por este circuito.

- Caída del router principal de una sede remota: en esta última prueba se validará que ante una caída del router principal de una de las dos sedes remotas del diseño la transmisión entre esta sede y cualquier equipo del CPD o de la otra sede se lleva a cabo a través de la red del segundo operador, red de respaldo o red del operador ISP 2. También se validará que la comunicación entre el CPD y la sede con el router principal activo se realiza correctamente entre los equipos de estas sedes a través de la red principal, operador ISP 1. Para ello serán enviamos paquetes ICMP

desde ambas sedes hacia uno de los equipos del CPD. En la sede con el router principal caído deberá realizarse la comunicación a través de la red secundaria y en la sede con el router principal activo deberá realizarse la comunicación a través de la red secundaria, operador ISP 2.

Una vez configurada toda la red en Cisco Packet Tracer 7, según las configuraciones determinadas en apartados anteriores se procede al registro de estas en las diferentes plantillas de configuración anexadas al final del presente documento.

Es importante guardar estas configuraciones en *.txt independientes y, asimismo, guardarlas como la configuración inicial de cada router para que al apagar y encender cada equipo retome de nuevo la configuración correcta.

Si no se llevara a cabo este paso, al reiniciar los equipos tomarían la configuración predeterminada sin ninguna de las especificaciones detalladas antes de su reinicio y se deberán cagar de nuevo las plantillas, con los retrasos que ello conlleva.

El código que permite el guardado de la configuración actual a la configuración inicial al arrancar el dispositivo es:

```
copy running-config startup-config
```

Una vez realizadas todas las copias de seguridad (plantillas de configuración *.txt) y la copia de la configuración actual a la configuración inicial de todos los equipos, se procederá a realizar las pruebas determinadas anteriormente en cada uno de los escenarios supuestos.

4.6.1 Todo el sistema activo

Este escenario será en el que más habitualmente trabajen los equipos de la organización ya que las probabilidades de caída de alguno de los circuitos, redes o equipos debería ser potencialmente bajas en comparación con el tiempo de trabajo de la red en estado activo total.

Se planteará como el escenario inicial y base a partir del cual se podrán contemplar las diferentes opciones propuestas en cuanto a caídas de

circuitos principal o secundario de los accesos de alguna de las sedes remotas o centrales (CPDs).

En base a las características descritas se puede proceder a la realización de un primer ping (envío de paquetes ICMP) desde el equipo servidor de la VLAN1 del servidor, "*S0-Server1-V1*" hacia el PC1 de la Sede 1, "*S1-PC1-V1*".

El resultado de la prueba se muestra en la siguiente figura:

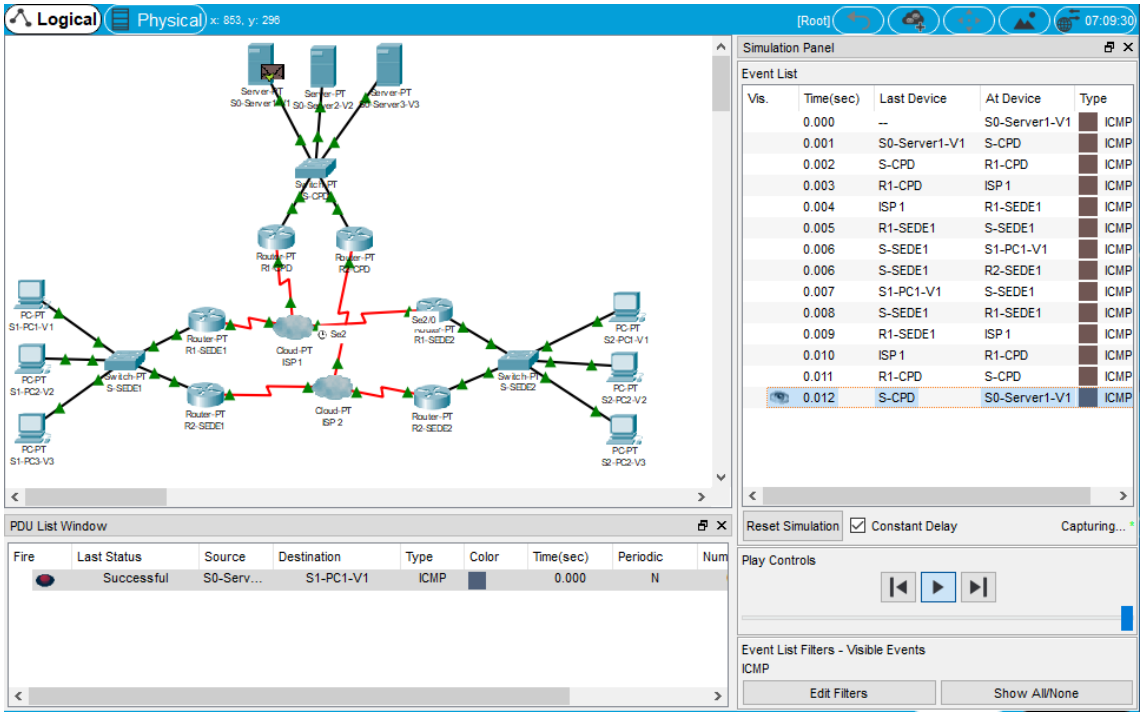

Ilustración 6 - Escenario 1. Prueba ping CDP - Sede 1

En una primera comprobación se puede dar por completada la transmisión según nos indica el campo "*Last Status*" de la ventana de lista protocolos de unidad de datos, "*PDU List Window*", con la confirmación de validez, "*Successful*".

Además, tal y como se aprecia en la captura de pantalla del proceso completo de envío y retorno del paquete ICMP, están incluidos en la lista de eventos las transmisiones los equipos configurados en la simulación, como la WAN y los routers, del operador ISP 1, "*ISP 1*".

En las líneas 4 y 5 se encuentran los referentes a la fase de envío del paquete ICMP y en las líneas 11 y 12 los referentes a la fase de retorno del paquete ICMP.

Por lo tanto, se puede confirmar que el ping se realiza (“*Successful*”) y, tal y como se había previsto, a través de la red principal

Para la validación de la configuración de la segunda sede se procede a la realización de un segundo ping desde el equipo servidor de la VLAN1 del servidor, “*S0-Server1-V1*” hacia el PC1 de la Sede 2, “*S2-PC1-V1*”.

El resultado de la prueba se muestra en la siguiente figura:

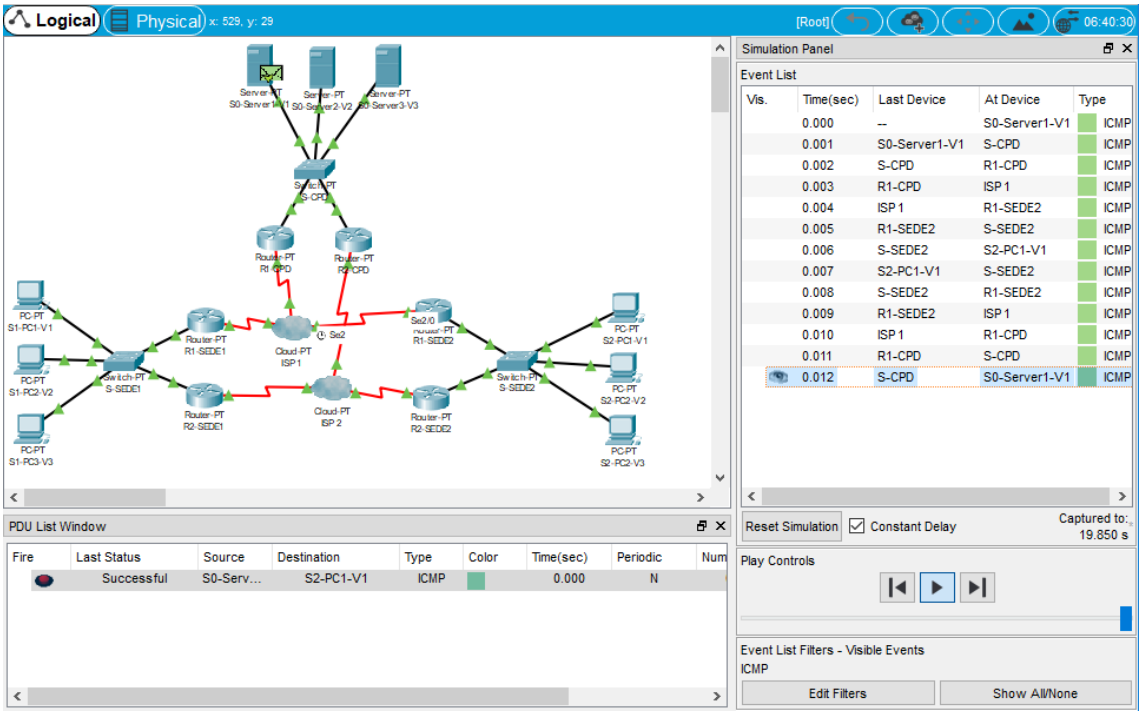

Ilustración 7 - Escenario 1. Prueba ping CPD - Sede 2

De nuevo se puede comprobar con el paquete ICMP ha llegado a destino correctamente y se ha recibido la repuesta por el “*Successful*” obtenido en la “*PDU List Window*” de la captura de pantalla realizada.

Además, igual en prueba realizada con la Sede 1, la captura de pantalla permite apreciar que en la lista de eventos aparecen tan solo la WAN y los equipos implicados en el envío y retorno de la información del operador principal: “*R1-CPD*”, “*ISP 1*” y “*R1-SEDE2*”.

Debido a que en ningún momento entra en funcionamiento la red secundaria del operador de respaldo, ISP 2, se puede considerar como valida la configuración planteada en una primera instancia y a expensas de los resultados del resto de pruebas.

4.6.2 Caída del router principal del CPD

En la primera de las pruebas de conmutación del sistema se validará que las comunicaciones del CDP no se ven interrumpidas por la caída del servicio del operador principal, ISP 1.

Para ello se llevará a cabo la desconexión del router principal y se enviará un paquete ICMP desde uno de los equipos el CPD hasta uno de los terminales de una de las dos sedes.

El resultado final de la prueba realizada se muestra en la siguiente figura:

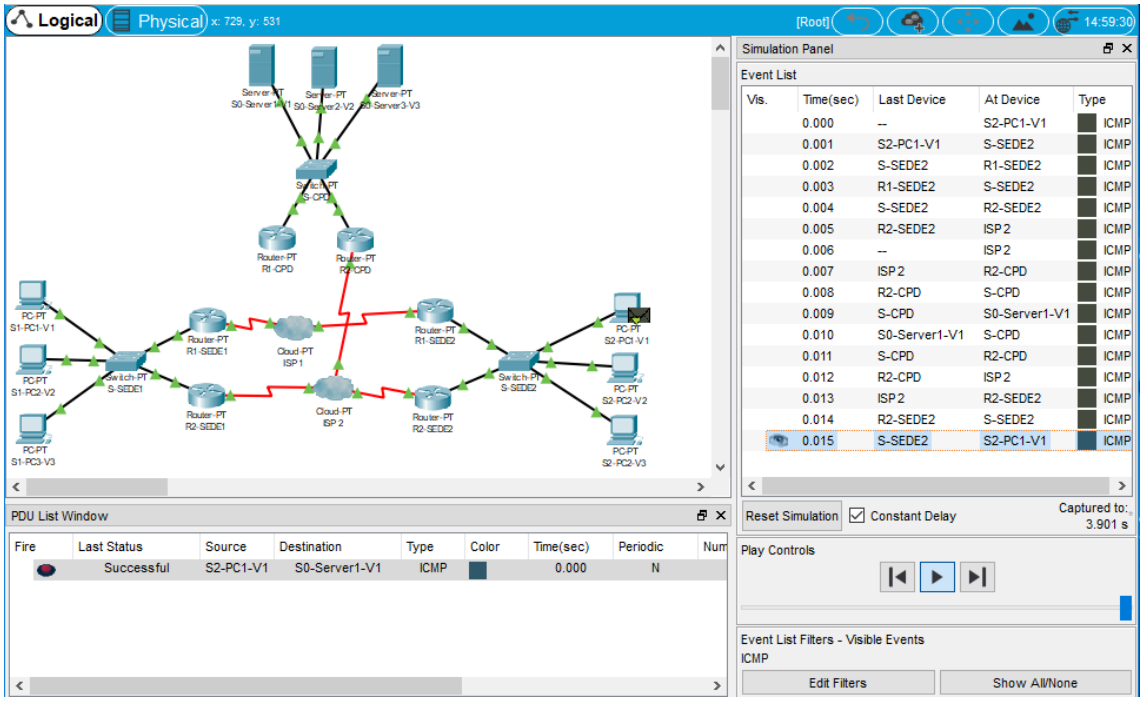

Ilustración 8 - Escenario 1. Prueba ping CPD - Sede 2.

Al desconectar el router principal del CDP y realizar una prueba básica de conectividad entre uno de los equipos de la Sede 2 y otro del CPD se observa como el paquete ICMP primero intenta acceder al router del ISP 1, "*R1-SEDE2*", que está configurado como principal en el grupo HSRP.

Las tablas de enrutamiento adquiridas gracias a la configuración BGP permite que el router "*R1-SEDE2*" conozca la ruta más eficiente en cada uno de los escenarios y, por lo tanto, envía de vuelta el paquete ICMP contra el "*R2-SEDE2*" para que sea enviado por la red secundaria, la del ISP 2.

Se puede apreciar también que el retorno se lleva a cabo de nuevo por la red WAN del operador secundario, ISP 2. Por lo tanto, esta prueba verificará el correcto funcionamiento de la solución técnica propuesta también en este segundo escenario.

En este mismo escenario se podrá corroborar a su vez que las comunicaciones entre ambas sedes remotas, sedes 1 y 2, se lleva a cabo correctamente y a través del operador principal, ya que ninguna de ellas se está viendo afectada por la caída del servicio del operador principal.

Para corroborar este caso enviaremos un paquete ICMP desde uno de los terminales de la sede 1 hacia uno de los terminales de la sede 2 y corroboraremos que tanto el envío como el retorno de estos se realiza por la WAN del ISP 1.

El resultado de la prueba se muestra en la siguiente figura:

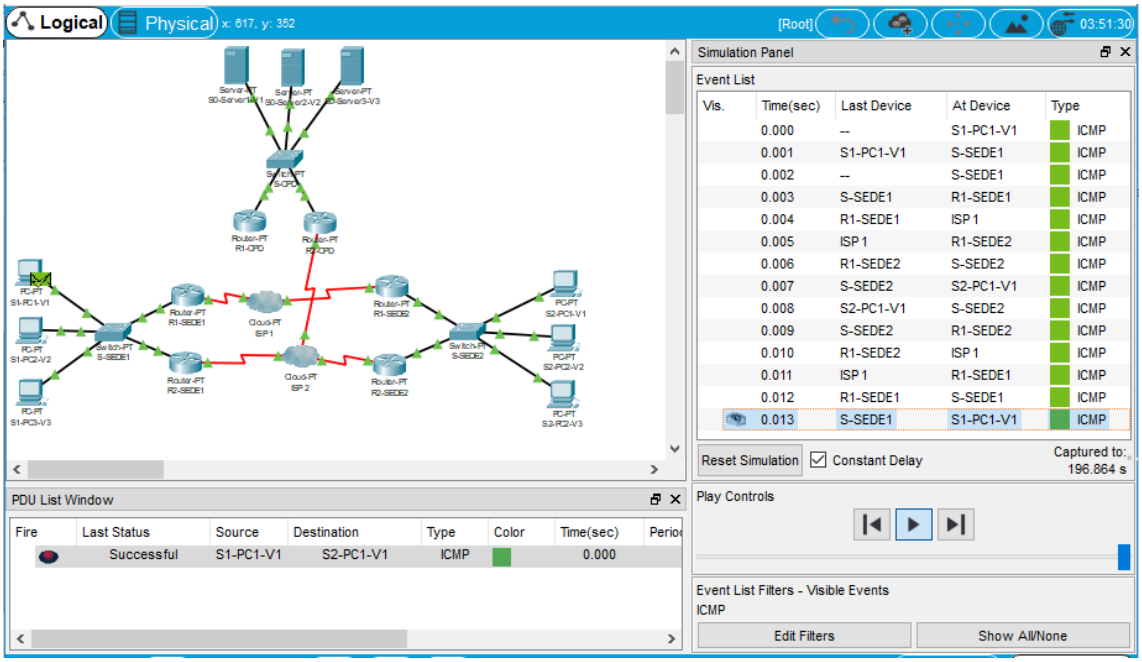

Ilustración 9 - Escenario 1. Prueba ping Sede 1 - Sede 2

Tal y como se preveía la transmisión del paquete ICMP se lleva a cabo a través de la red del operador principal, por lo que el comportamiento de la red es el esperado y se puede validar la solución propuesta en este escenario concreto.

4.6.3 Caída del router principal de una sede remota

En este segundo escenario de conmutación se plantea la posibilidad de la caída del servicio del operador principal en alguna de las sedes remotas y, como en el escenario anterior, se corroborará que la comunicación a entre esa sede remota y alguna de las otras dos, CPD o la otra sede remota, se realiza a través del circuito del operador secundario.

Para simular la caída del servicio se desconectará el cableado entre el router del operador principal de la sede 2 y la WAN del operador principal, ISP 1, simulando así un corte en la línea.

De nuevo se ejecutará un "*ping*", entre los equipos "*S0-Server1-V1*" y "*S1-PC1-V1*" y se validará que los paquetes ICMP toman el camino correcto a través de la WAN del operador secundario.

El resultado de la prueba se muestra en la siguiente figura:

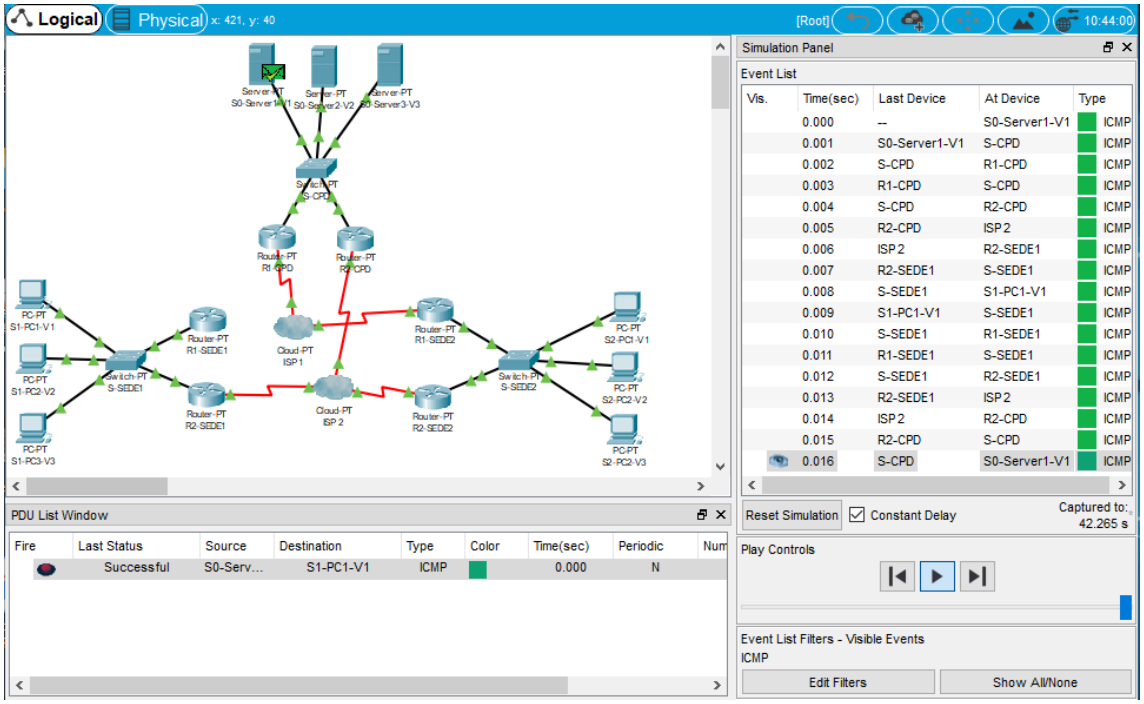

Ilustración 10 - Escenario 2. Prueba ping CPD – Sede 1

Como se puede apreciar en la captura de pantalla, el paquete ICMP llega al router principal del CPD, "*R1-CPD*", que lo reenvía al secundario, "*R2-CPD*", gracias a las tablas de enrutamiento adquiridas mediante el protocolo BGP aplicado en la configuración de todos los equipos.

El retorno se realiza también por la red secundaria sin que se detecte ningún problema. Se verifica entonces que en este escenario la solución planteada también cumple con las expectativas en cuanto a la conmutación entre las redes principal y secundaria.

Para finalizar las pruebas teóricas deberá validarse que ante este segundo escenario de caída del acceso principal en una de las sedes remota la comunicación entre la otra sede remota y el CPD se lleva a cabo a través de la red WAN del operador principal y que, por lo tanto, esa comunicación no se ve afectada por la caída del servicio en la sede 2.

Para ello se repetirá la prueba con el router principal de la sede 1 desconectado y enviando ahora un paquete ICMP desde uno de los terminales de la sede 2, sede con ambos accesos activos, hasta un servidor del CPD, sede central también con ambos accesos activos.

El resultado obtenido se muestra en la siguiente captura de pantalla:

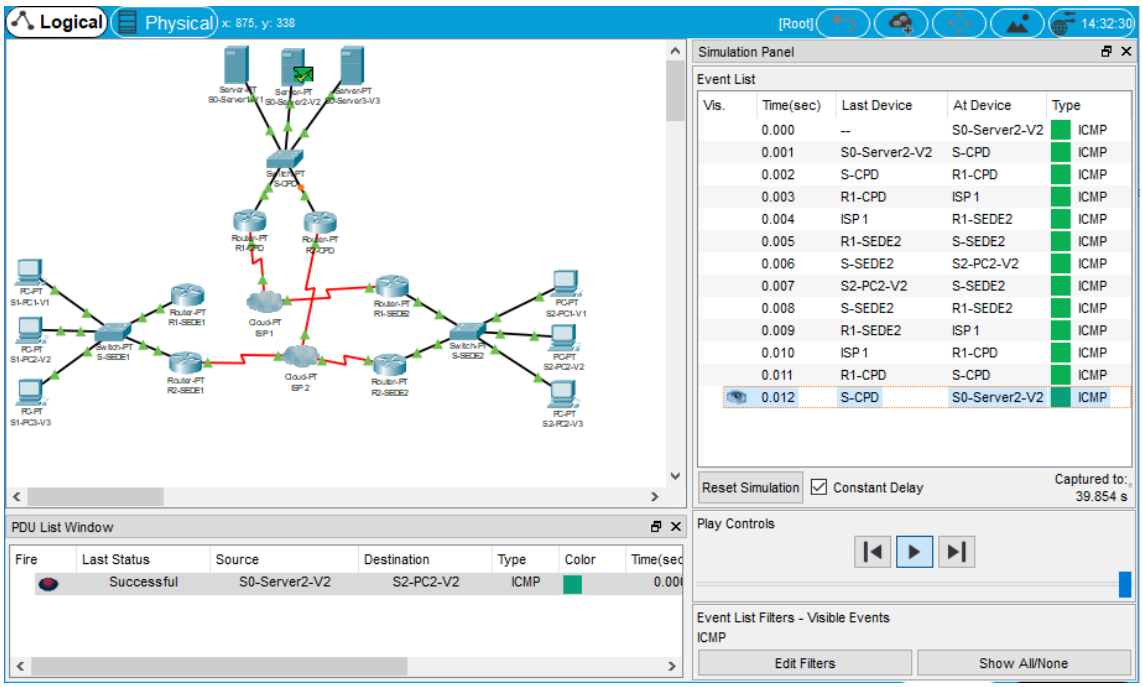

Ilustración 11 - Escenario 2. Prueba ping CPD – Sede 2.

Efectivamente, el envío y el retorno se realizan a través de la red del operador principal y, por lo tanto, se valida la correcta conmutación y entre los dos operadores en todos los casos propuestos.

4.7. Pruebas de validación prácticas

Una vez finalizada la fase de validación teórica, con la propuesta teórica probada sobre un simulador como Cisco Packet Tracer 7 y confirmada por la organización, el siguiente paso, antes de llevar a cabo la configuración de los accesos de datos en cada una de las sedes, debe ser la validación práctica de esta misma propuesta teórica.

Estas pruebas de validación práctica deberán ser las determinantes y fundamentales para que la organización de el visto final a la implantación de la solución propuesta y que, por lo tanto, se puedan empezar a planificar y ejecutar las siguientes fases del proyecto global. En este caso, la implantación de circuitos de accesos de datos de respaldo para cada una de las sedes de la entidad.

Para una correcta y completa validación se deberán tener en cuenta que en estas pruebas prácticas no sólo deberá testearse la correcta conmutación de los servicios de datos de ambos operadores en una sede tras el fallo del operador principal, si no que también se deberán validar cada una de las tipologías de accesos con las diferentes aplicaciones utilizadas por la entidad.

En este sentido será de obligatorio cumplimiento que sea la entidad la que aporte la información concreta de que aplicaciones utiliza en cada una de las sedes, pero como norma general podemos disponer de casuísticas generalizadas:

- Navegación internet: navegación habitual por diferentes páginas web con y sin certificados de seguridad.
- Navegación cifrada: navegación a través de páginas web con uso habitual de certificados de seguridad.
- Correo electrónico: consultas del correo electrónico tanto corporativo como no corporativo a través de herramientas habituales (*Microsoft Outlook*, *Mozilla Thunderbird*, etc..).

- Aplicativos específicos: se deberán probar las aplicaciones típicas documentadas por la organización en base a la funcionalidad de cada una de las sedes.

Una vez documentadas todas las pruebas prácticas que se deberán llevar a cabo para validar la solución se llevarán a cabo la fase de configuración de pilotos de pruebas. Esta fase consta de dos etapas en las que se configurarán en primer lugar una sede ficticia de laboratorio y, en un segundo paso, la ejecutará una primera instalación y configuración de un circuito de respaldo del operador 2 en una sede real.

Para la consecución y el éxito de esta fase de validación práctica es imprescindible y fundamental la participación y el compromiso de los equipos técnicos de ambos operadores y del posible mantenedor de switchs y equipos de la organización. En función de posibles errores o problemas técnicos que producidos durante el proceso puede ser necesaria la modificación de ciertos parámetros de la configuración de alguno de los equipos implicados.

En fase de pruebas prácticas en las sedes piloto, laboratorio y sede real, deberán validarse tanto la funcionalidad (que cada el conjunto de la configuración realiza lo esperado según los criterios del cliente) como la usabilidad (que cada uno de los accesos de datos probados permite un uso fluido y correcto de cada una de las aplicaciones) de cada una de las aplicaciones o usos que la entidad haya descrito en los pasos previos a estas pruebas.

Al finalizar estas pruebas se deberá valorar cualitativamente cada uno de los accesos de datos del nuevo operador y la solución global mediante valoraciones subjetivas de las personas testadoras y valoraciones objetivas de los circuitos. Algunos de estos valores objetivos que se pueden tomar en cuenta son:

- Tiempo de respuesta: desde un simple ping hasta el tiempo de respuesta de una consulta completa a una BDD (es importante valorar siempre en las mismas condiciones)

- Número de paquetes perdidos: paquetes que se pierden en la red en el proceso de conmutación del operador 1 al operador 3 o

viceversa, o los paquetes perdidos sin conmutación trabajando con un operador u otro.

- Número de saltos: cantidad de saltos de nodos para llegar a un mismo destino a través de un operador y otro.

- Velocidad de conexión a Internet: tasa de Mbps que aporta cada uno de los diferentes accesos de los dos operadores.

Todas las pruebas realizadas deberán recogerse, junto con los resultados obtenidos, en un registro de pruebas que será documentado junto el proyecto final como un entregable más a los responsables de la entidad para la aprobación final de la propuesta de solución. Sin la aprobación oportuna de la dirección del proyecto se deberán llevar a cabo las modificaciones oportunas en la propuesta realizada.

Una vez validada la configuración por la organización en las sedes piloto, sede laboratorio y sede real, se podrá proceder a la ejecución de la implantación de la solución a nivel global teniendo que definir antes de empezar los diferentes equipos designados por cada una de las partes interesadas, procedimientos a seguir, planificación, etc…

5. Implantación

Una vez la propuesta de solución técnica ya ha sido validada por todos los actores del proyecto, organización y operadores, se deberá plasmar la configuración de red propuesta en cada una de las sedes remotas y la sede central, el CPD.

Para ello se deberá llevar a cabo la redacción de procedimientos y de la planificación de cada una de las fases y etapas en la que consistirá el proceso completo de implantación de los nuevos accesos y equipos del operador 2 así como la configuración de los actuales equipos propiedad de la organización y del operador 1.

Este es un trabajo que debe ser concretado y validado por cada uno de los equipos participantes en el proyecto a través de la figura del “Jefe de Proyecto” de cada uno de ellos, que será el interlocutor válido en cada una de las reuniones planificadas para ello.

5.1. Procedimientos

La primera etapa de la implantación de servicios, una vez se dispone de inventarios y la solución técnica aprobada, será la redacción y validación de los procedimientos a seguir para validar cada una de las instalaciones que se deben llevar a cabo.

En la definición de estos procedimientos se debe que tener en cuenta los criterios formulados por la organización, así como la disponibilidad de cada uno de los equipos de trabajo implicados. Por ello, cada uno de estos procedimientos deberá ser aprobado por los jefes de proyecto de ambos operadores y de la organización.

El primer procedimiento que definir será el de la estructura global de implantación, el cual dependerá de diferentes fases o subprocesos y de los posibles grupos de trabajo multidisciplinares que se puedan organizar. Las fases de las que está formado el procedimiento global de implantación del proyecto son:

Ilustración 12 - Fases de la implantación del proyecto.

- Configuración de equipos de cliente: esta fase de configuración del switch y/u otros equipos de la organización implicados en el cambio de estructura de la red deberá llevarse a cabo antes de la instalación de los nuevos equipos y el acceso de datos del nuevo operador, ISP 2.

  Para que en el momento de la instalación del nuevo acceso se pueda conectar el nuevo router al switch con una configuración básica sin provocar caídas en el servicio se deberá asegurar en esta etapa de configuración del switch se deja uno de los puertos caído administrativamente, *shutdown*. Un responsable de la organización deberá comunicar que puerto ha sido preparado en cada sede para que el instalador de nuevo router deje conectado el equipo al puerto correcto.

  Lo aconsejable es disponer siempre del mismo puerto de conexión para cada uno de los equipos, o por lo menos mantener una distribución lógica de las conexiones.

  En principio el resto de equipo no necesitarían ningún cambio en la configuración, ya que, tal y como solicitaron los responsables de la entidad en su momento, el cambio se ha planteado para que sea lo más transparente posible y no se deba modificar la configuración de todos los equipos y terminales.

- Instalación de los nuevos accesos de datos: una vez preparado el switch las sedes implicadas se procederá a la instalación de los accesos del nuevo operador, ISO 2. El responsable de este procedimiento será el equipo de trabajo de este operador y, debido a los procesos internos podrá iniciar la tramitación de estos antes incluso que la configuración del switch, pero nunca podrá finalizar la instalación en la sede hasta recibir la notificación oportuna del responsable o jefe de proyecto de la organización. Una vez finalizada cada una de las instalaciones comunicará la finalización de esta al responsable o jefe del proyecto para el inicio de la siguiente fase.

- Configuración del router 1: debido a que la configuración propuesta es totalmente transparente para los equipos y terminales de cada

una de las sedes, el operador actual de los accesos de datos de la organización podrá ejecutar los cambios en la configuración de sus routers en paralelo a la configuración de los switch, instalación del acceso de datos nuevo.

Este punto supondrá inexorablemente un corte en las comunicaciones de la sede donde se lleva a cabo la instalación por lo que se deberá planificar fuera del horario laboral de cada una de las sedes y deberá ser comunicada con antelación al responsable del proyecto de la organización y, a posteriori, transmitir un informe con los resultados de las configuraciones aplicadas.

- Configuración del router 2: una vez aplicada la configuración en el router del acceso principal se podrá configurar el router que hará de respaldo. Debido a que quedará en "*standby*" en todos los grupos HSRP configurados y que los puertos de los switch estarán en deshabilitados administrativamente, este proceso se podrá llevar a cabo con la sede abierta y en cualquier horario.

  Al finalizar cada una de las configuraciones de las sedes, el responsable del operador 1 transmitirá un informe diario con las configuraciones aplicadas en cada una de las sedes para que puedan ser validadas por el cliente.

- Validación de la instalación: llegados a este punto, con todos los equipos configuración, un técnico de la organización levantará de nuevo el puerto del switch donde está conectado el router de respaldo, router 2, y validará que la conectividad es correcta mediante simples "*ping*" (envío de paquetes ICMP), a través de las diferentes VLANs, a los terminales de la sede.

  Si transcurridas 48 horas los usuarios de la sede no han transmitido errores en su trabajo y procesos diarios se dará como finalizada y validada la instalación.

Se redactarán procedimientos para cada uno de estas fases y trabajos a realizar y deberán ser aprobados por los equipos implicados y los jefes de proyectos de estos, sean de un operador o de la organización.

Además, cualquier modificación de estos procedimientos, sea con la implantación iniciada o no, deberá ser nuevamente validada por cada uno de los jefes de proyecto de todos los equipos, suponga o no una modificación en sus condiciones de trabajo.

En el siguiente diagrama se muestra la temporización de la ejecución de cada una de las fases en las que se ha segregado la implantación y desarrollo del proyecto:

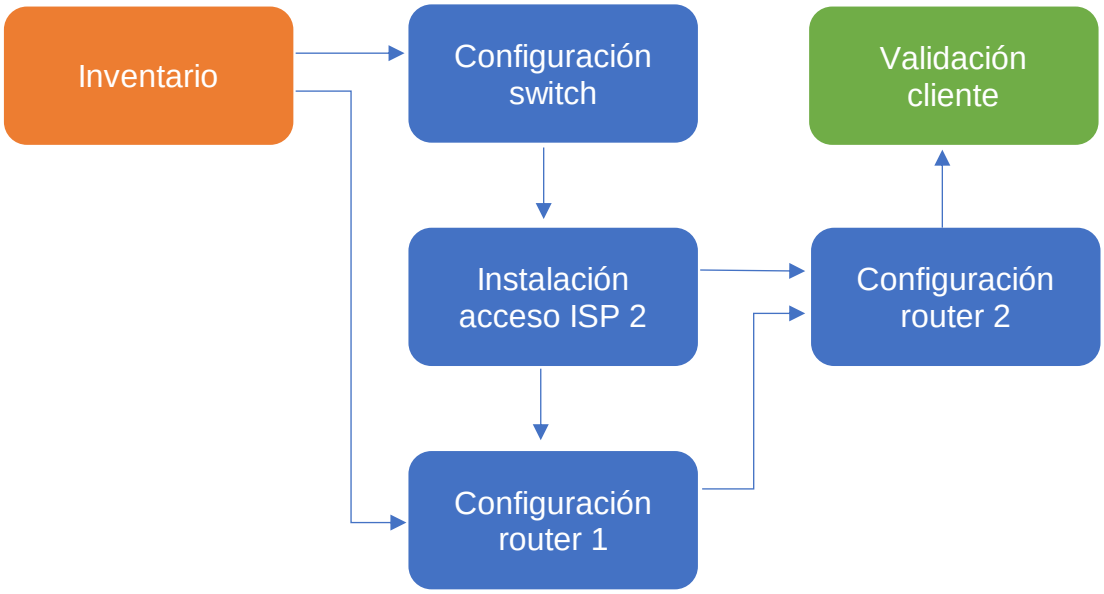

Ilustración 13 - Diagrama de fases de implantación.

5.2. Planificación

Con las fases de la implementación descritas, definidas al detalle y validadas por los diferentes equipos es el momento de planificar la ejecución de cada una de ellas para lo que se deberá tener en cuenta la disponibilidad de cada uno de los equipos y detalles de cada una de las fases.

Además, en este nivel de planificación cabe destacar que la ejecución de la instalación y configuración del CPD debe realizarse al inicio de la implantación ya que ninguna de las sedes tendría disponible el acceso a los servidores a través de la WAN del operador 2 hasta que este estuviera operativo.

Por lo tanto, además de las fases descritas anteriormente, se deberá tener en cuenta la priorización de cada una de las sedes y la posible segregación de la implantación en dos etapas en función de esa priorización:

- Sede central: donde se llevará a cabo la instalación y configuración de los servicios centrales, CPD.
- Implantación masiva: en la que se llevarán a cabo las instalaciones y configuraciones de las sedes remotas (85 delegaciones y 15 direcciones territoriales).

Es importante que cada uno de los equipos reporten periódicamente la información de sus avances en cada una de las fases y que se lleve un control adecuado del proyecto por parte de los responsables designados.

5.3. Inventario final

Tal y como se comentó anteriormente, el primer proceso a realizar y uno de los más importantes para la correcta consecución del proyecto es la consolidación de un inventario de sedes y accesos de datos.

Del mismo modo, una vez finalizada la implantación y antes de dar por finalizado el proyecto se deberá aportar un inventario final que recoja cada un de los accesos de datos, principales y de respaldo, junto con los detalles de cada uno de ellos.

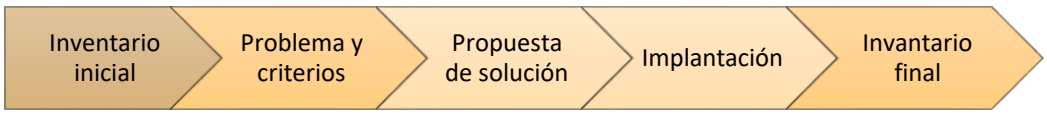

Ilustración 14 - Fases globales del proyecto.

La base de este inventario será el utilizado en el inicio del proyecto y tan sólo se deberán añadir un campo que designe la utilidad o función (principal o respaldo) del mismo:

- Administrativo: identificador unívoco con el que el operador ISP identifica el circuito o acceso de datos.
- Código: identificador unívoco con el que la organización identificará cada uno de los accesos.

- Sede: código unívoco de la sede donde da servicio. Se utilizará para vincular cada uno de los accesos a la sede de manera que diversos accesos puedan estar vinculados a una sede, pero nunca el mismo acceso puede estar vinculado a diversas sedes.

- Tecnología: tipología del acceso (ADSL, FTTH, FO, MÓVIL, etc…). Categoriza el acceso para valorarlo económicamente.

- Tipología del acceso: detalle más concreto sobre el tipo de acceso, velocidad, simetría (en cuanto a la subida y bajada de datos), etc…

- Caudal: ancho de banda contratado y detalle de la garantía y priorización del caudal en cuanto a multimedia, por ejemplo.

- Servicios añadidos: servicios adicionales contratados como mantenimiento, buzones de voz, etc….

- Operador: operador ISP que aporta el servicio a la entidad.

- Proveedor última milla: datos del proveedor de la parte de acceso que conecta desde la sede (PTR o PTO) hasta la central de telecomunicaciones.

- Función: desplegable que permita elegir entres las funciones que puede realizar un acceso de datos, PRINCIPAL o RESPALDO.

Se podrá dar por finalizada la implantación de la contingencia de datos con doble operador una vez que este inventario, junto con el resto de entregables del proyecto, sea presentado a los responsables de la organización y validados por estos tal y como se describe en el siguiente diagrama del PBBook [12]:

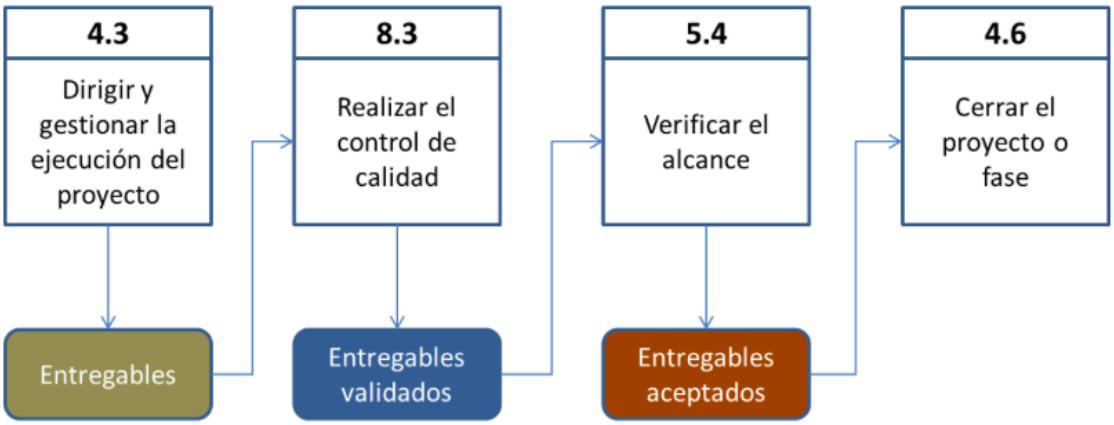

Ilustración 15 - Entregables de un proyecto según PMBook [12].

6. Impacto económico

Uno de los elementos clave para la apreciación positiva de cualquier proyecto o innovación tecnológica es el impacto económico directo que esta conlleva. De todas formas, la mejora del servicio y seguridad de la red de comunicaciones de una entidad es lógico que venga acompañado de un aumento de los costes de comunicaciones.

Es evidente que este impacto económico derivado del proyecto, en este caso debido a la duplicidad de los accesos de datos, es inevitable y se debe asumir como un coste derivado de la criticidad del servicio. Más allá de este impacto directo se deberán valorar posibles opciones para mitigarlo y controles del gasto para controlar la correcta evolución de este.

Para realizar un estudio detallado del impacto económico que supondrá la implantación del proyecto se ha valorado inicialmente el coste de la red de datos de toda la estructura previa de la organización. Para ello se han aplicado los costes mensuales individuales en el operador inicial, operador 1, por cada una de las tipologías de accesos que dispone la organización y la cantidad de accesos de cada una de esas tipologías:

Tipo de acceso	Cantidad	Coste unitario	Coste total
FO 1 Gbps	1	500,00 €	500,00 €
FTTH 100Mb/100Mb	15	95,00 €	1.425,00 €
ADSL (varios caudales)	85	40,00 €	3.400,00 €
TOTAL			**5.325,00 €**

Tabla 24 - Coste mensual red de datos principal.

Para calcular el coste de la red de datos tras la implantación del doble operador se tendrá en cuenta la asignación de accesos secundarios en cada una de las sedes de categoría inferior, a excepción del CPD donde la necesidad de un caudal dedicado y prioritario hace necesaria la instalación de otra FO de 1 Gbps.

De este modo en las 15 territoriales se configurará una ADSL como acceso secundario y en las 85 delegaciones se configurará un acceso 3G/4G como circuito secundario.

El coste de la red de datos secundaria, la utilizada como respaldo del operador 2, lo podremos calcular en base a las mismas tarifas aplicadas en el calculo previo:

Tipo de acceso	Cantidad	Coste unitario	Coste total
FO 1 Gbps	1	500,00 €	500,00 €
ADSL (varios caudales)	15	40,00 €	600,00 €
MÓVIL 3G/4G	85	20,00 €	1.700,00 €
TOTAL			**2.755,00 €**

Tabla 25 - Coste mensual red de datos secundaria.

Con los datos de los costes mensuales de cada una las redes podemos valorar el coste total de la red de datos tras la implantación completa del proyecto en un total de 8.080,00 € mensuales. Este coste implica un aumento final sobre el coste inicial, previo a la implantación del 51 %, lo que supone la consecución de los criterios económicos de la organización:

- ***Coste económico**: la solución final no puede implicar un coste de más del 60 % sobre el presupuesto actual destinado a los circuitos de telecomunicaciones que dan servicio a las sedes remotas y el CPD.*

Además, para gestionar y controlar mejor el gasto que supone la red de datos se propone a la organización mantener actualizado el inventario de accesos de datos y utilizar este como planta a partir de la cual revisar la facturación de los operadores implicados, ya que la ineficiencia de los métodos de facturación de estos puede suponer un desvío considerable frente a la planta real.

Otras medidas de control y revisión pueden ser la negociación de ejecutar una facturación concertada con una revisión anual o semestral. De esta forma no será necesario revisar la facturación mensual de cada uno de los operadores y se simplificarán los procesos que esto implica.

Por último y con el fin de reducir el coste de estos accesos de datos es interesante valorar la opción de realizar un *benchmark* y una posterior licitación a través de una RFP (*Request For Proposal*).

7. Justificación criterios de cliente

Con la propuesta técnica completada y validada por los responsables de la organización y ambos operadores corroboran que los criterios iniciales de la entidad han sido cumplidos y que los objetivos, principales y secundarios, del proyecto han sido consecuentemente cumplidos.

Para poder validar que el primordial objetivo del proyecto, reducir los tiempos de desconexión, haya sido conseguido será necesario realizar un estudio a posteriori que englobe una comparativa de tiempos de desconexión antes y después de la implantación de la nueva solución.

A priori se puede avanzar que la solución aporta las medidas oportunas para que este objetivo sea consolidado sin demasiados problemas ya que se ha validado, mediante las pruebas teóricas y practicas, que la conmutación entre ambos operadores es correcta y que la funcionalidad y usabilidad de ambos operadores es correcta.

Con el fin de cuantificar la posible mejora y para validar la solución según los criterios definidos por la entidad se deberá valorar el porcentaje de tiempo en la que el operador principal estuvo sin poder dar servicio a alguna de las sedes. Para ello se divide el tiempo total donde el operador no ha podido dar servicio y las horas totales de trabajo de las 100 sedes:

$$P_{incidencia}(\%) = \frac{127\ horas}{208.000\ horas/año} * 100 = \ 0{,}0610\ \%$$

Aplicando esta probabilidad actual con un solo operador al nuevo escenario de dos operadores, y bajo la suposición de que ambos operadores tienen la misma probabilidad de tener una incidencia, podremos calcular la probabilidad de que en algún momento ambos operadores tengan incidencia en sus accesos (P_{total}) y alguna de las sedes quede incomunicada:

$$P_{total} = P_{incidencia}^{2} \ = \ 0{,}0037\ \%$$

Por lo tanto, y teniendo en cuenta el total de horas trabajadas por las sedes de la entidad, 208.000 horas al año, podemos calcular el tiempo con incidencia total que tendrán con la nueva solución:

$$t_{incidencia} = 0{,}0037\ \% * 208.000 \frac{horas}{\text{año}} = 7{,}7\ horas/\text{año}$$

Tal y como podemos ver se cumple el criterio de la entidad de reducir el tiempo de desconexión por incidencias del operador a menos de 20 horas al año.

Otro de los criterios cuantitativos de la entidad indicaba la necesidad de recudir el porcentaje de incidencias con duración superior a 1 hora a menos del 5 % de incidencias. Aplicando las estadísticas de 2018 para ambos operadores y teniendo en cuenta las probabilidades de que ambos operadores tengan una incidencia crítica al mismo tiempo, calculada en el punto anterior (P_{total} = 0,0037 %), se puede valorar el porcentaje de las incidencias sufridas por el operador principal, operador 1, donde casualmente el operador 2 también tendrá incidencia crítica en su acceso:

$$P_{incidenciaTotal} = P_{total} * P_{incidencia\ >1\ h.} = 0{,}0037\ \% * 29{,}57\ \% = 0{,}10\ \%$$

El porcentaje de incidencias con tiempo de duración mayor a 1 hora se reducirá al 0,10 % debido a que cualquier incidencia del operador 1 será cubierta por el operador 2. Por lo tanto, el segundo criterio cuantitativo de la entidad también debería ser consolidado con la solución propuesta.

Además, los responsables de la organización indican una serie de criterios que provocan que la implantación se lleve a cabo con una planificación y unos procedimientos determinados y muy concretos. Gracias a la temporización, el trabajo asincrónico entre los diferentes equipos y la configuración técnica propuesta se consigue que el servicio no sea interrumpido para cualquiera de las sedes.

Esta configuración técnica propuesta habilita también el aprovechamiento máximo de los equipos actuales instalados en las sedes remotas y la sede central, CPD, cumpliendo así otro de los criterios primordiales de la entidad.

En concreto, la utilización y configuración de grupos HSRP en los routers de los operadores permite que los equipos y terminales de los trabajadores y usuarios puedan seguir funcionando correctamente con la puerta de enlace que ya tenían configurada.

Por último, tras los cálculos económicos realizados el gasto en telecomunicaciones previsto para la implantación del proyecto se sitúa dentro del margen aceptado por la organización. En un principio se había situado el límite en el aumento del coste de un 60 % y se ha consolidado con un aumento del 51 %.

Además, este coste económico está sujeto a posibles medidas para reducirlo, como podrían ser un estudio de mercado y posterior licitación publica para mejorar las ofertas de los operadores.

Con todas estas justificaciones podemos concluir que se cumplen todos y cada uno de los criterios expresados por la organización:

- **Reducción tiempos de desconexión**: se reducen de 127 horas anuales a tan solo 8 horas anuales cumpliendo así el objetivo de no superar las 20 horas anuales.

- **Reducción del tiempo de incidencias**: se reducen del 29 % a 0,10 % el volumen total de incidencias con duración mayor de 1 hora.

- **Aprovechamiento de los equipos actuales**: gracias a la configuración aplicada se aprovechan todos y cada uno de los equipos actuales tanto de operador como de la organización.

- **Disponibilidad de servicios durante la implantación**: gracias a la planificación de la implantación se consigue que todos los servicios estén disponibles durante la implantación.

- **Transparencia usuarios**: la configuración aplicada permite que los terminales de los trabajadores y usuarios no deban ser modificados en su configuración.

- **Coste económico**: la solución final supone un aumento del coste del 51 %, inferior al 60 % marcado como límite por la entidad.

Por todos estos detalles y conclusiones se puede concluir que el proyecto en su globalidad cumple con los criterios generales del cliente y será, en buena medida, satisfactorio para este.

8. Evaluación de riesgos

Con la propuesta de configuración y la solución aprobada bajo la aceptación y validación de los criterios teóricos presentados en este proyecto habrá que tener en cuenta diferentes casuísticas que hacer fracasar la ejecución de este.

En cuanto al diseño de la nueva red de datos secundaria que dará servicio de respaldo a todas las sedes, remotas y central, habrá que valorar y confirmar con el operador, operador 2, la disponibilidad de cada una de las tipologías de accesos previstas en cada una de las sedes.

Si alguna de estas no estuviera disponible en alguna de las sedes del listado dependería de la dirección del proyecto la posible aprobación de otra tipología puntualmente teniendo en cuenta las posibles modificaciones económicas que esto supondría.

En el caso concreto de los accesos de ADSL habrá que tener en cuenta que debido al Proyecto FARO [13] llevado a cabo por Telefónica de España, S.A. esta tecnología va a ser sustituida gradualmente por FTTH o HFC, dependiendo del operador. Esto provocará la sustitución de todos los accesos del tipo ADSL por algún tipo de fibra óptica y el consiguiente aumento del coste de la planta total, así como la mejora de las capacidades de la red de datos actual.

A la hora de la gestión de la instalación o posibles incidencias con el servicio de algunas tipologías de acceso habrá que tener en cuenta que es posibles que algunos de estos sean entregados hasta el abonado por un operador diferente al que oferta el servicio.

En estos casos las gestiones de estos circuitos pueden conllevar una complejidad añadida a la hora de la instalación, reparación y/o reclamación de incidencias. Por ejemplo, en la actualidad todos los accesos basados en ADSL pertenecen a Telefónica de España, S.A. a pesar de que el servicio lo ofrezca otro operador.

Otro de los problemas que debe tenerse en cuenta es la dificultad de concreción de la configuración por parte de los responsables de la organización que, con la ayuda de los técnicos especialistas de ambos

operadores, deberán validar una solución óptima y segura para cada una de las problemáticas y diferentes casuísticas de la entidad tanto a nivel de funcionalidad como seguridad y conectividad.

Para la correcta configuración y posibles modificaciones durante el ciclo de vida habrá que tener en cuenta el desconocimiento de la estructura y particularidades de la organización por parte de los técnicos de la nueva operadora que aportará el servicio de respaldo. Será muy útil realizar sesiones informativas con estos y ponerles al día de cualquier detalle que les pueda ser útil para no provocar problemas en el servicio.

La planificación de la implantación del nuevo servicio puede verse alterada por cualquiera de los motivos anteriores y deberá tenerse en cuenta ante cualquier compromiso que se adquiera con posibles clientes, proveedores u otros departamentos de la misma organización. Es útil en estos casos determinar posibles indemnizaciones en función del retraso obtenido si fuera responsabilidad de alguno de los actores de la implantación; operadores, instaladores, etc…

Una vez completada la implantación de la solución propuesta y validada por la organización y debido a que el circuito de respaldo sólo entrará en servicio cuando caiga el acceso principal, será imprescindible planificar una serie de pruebas sistemáticas y periódicas en cada una de las sedes para confirmar que la conmutación entre los circuitos principal, del operador 1, y respaldo, del operador 2, se lleva a cabo correctamente.

Por último y a nivel general del proyecto deberá realizarse una evaluación periódica, semestral o anualmente, de la propuesta de configuración de contingencia con doble operador para validar que continúa siendo válida según los criterios expuestos por la organización. Ya que debido a posibles modificaciones, ampliaciones o recortes en los inventarios pueden verse modificados los costes o las necesidades y criterios de la organización.

9. Conclusiones

En el proyecto se ha elaborado un análisis y estudio de la problemática de una entidad en cuanto al volumen y criticidad de las incidencias sufridas con un operador de telecomunicaciones en concreto y una posible solución aplicando contingencia a través de un segundo operador.

En una primera instancia se ha llevado a cabo un estudio previo de la estructura y peculiaridades generales de la organización tanto a nivel de la red de telecomunicaciones de la que dispone en la actualidad como en su estructura de oficinas y sedes para poder planificar y cuantificar posibles propuestas posteriores.

Dentro del conocimiento de la organización y su estructura de red de datos es importante conocer los criterios y motivaciones que provoca la realización de este estudio y la aplicación de posibles mejoras al actual servicio. Para ello se ha descrito y cuantificado cada uno de los criterios de la organización, lo que ha permitido tenerlos continuamente en cuenta a la hora de diseñar la propuesta de solución.

Esta propuesta de solución has sido presentada a nivel técnico de una forma básica y general que permitiera ser aplicada de forma personalizada en otras estructuras similares. El nivel de detalle a que cada organización pueda llevar a cabo esta configuración de contingencia con doble operador dependerá de las peculiaridades de esta.

Se ha concretado mediante pruebas teóricas a través de Packet Tracer 7.0 que la solución aporta las correcciones necesarias. La selección de esta herramienta fue dada por la gran compatibilidad de esta con los equipos actuales de cada una de las sedes, así como la facilidad de uso y aprendizaje de uso que demuestra la misma.

Para las pruebas prácticas se detallan las más recomendables para esta tipología de proyecto y se planifican posibles procedimientos a llevar a cabo tanto en una sede piloto como en las sedes definitivas donde la configuración deberá funcionar sin ningún tipo de interrupción del servicio actual.

Una vez descrita la solución propuesta, se ha definido los criterios más importantes que se deben tener en cuenta en la implantación de la solución. Incluyendo una posible planificación y temporización y posibles problemas que pudieran surgir basándonos en los conocimientos adquiridos durante el proyecto.

Por último, se ha cuantificado económica a través de una aproximación teórica del coste que tendrá la implantación de la propuesta definitiva sobre la estructura de red de datos de la organización y se han evaluado los posibles riesgos que un proyecto de esta envergadura puede conllevar tanto a nivel de pequeñas incidencias como a nivel global para toda la entidad.

Una vez finalizado el proyecto se puede valorar muy positivamente la posibilidad de configurar una contingencia de datos mediante la implantación de un segundo operador y añadir, de este modo un doble nivel de contingencia, un segundo operador y tipologías diferentes de circuitos.

Sin embargo, el coste que esta duplicidad de la red conlleva hará que esta solución solo sea factible para organizaciones que precisen un nivel de efectividad en su servicio muy cercana al 100 % ya que puede conllevar aumentos en el coste de la red de datos de más del 50 % en función de los accesos elegidos en cada una de las oficinas.

10. Glosario

A

ADSL: Asymmetric Digital Subscriber Line.

B

BDD: Base de Datos.

BGP: Border Gateway Protocol.

C

CPD: Centro de Procesamiento de Datos.

D

DOCSIS: Data Over Cable Service Interface Specification.

E

eBGP: External Border Gateway Protocol.

F

FO: Fiber Optic.

FTTH: Fiber To The Home.

FTP: File Transfer Protocol.

H

HFC: Hybrid Fiber Coaxial.

HSRP: Hot Standby Router Protocol.

I

ICMP: Internet Control Message Protocol.

IP: Internet Protocol.

IPSec: Internet Protocol Security.

ISO: International Organization for Standardization

ISP: Internet Service Provider.

L

LAN: Local Area Network.

M

MAN: Metropolitan A rea Network.

O

ONT: Optical Network Terminal.

OSPF: Open Shortest Path Fitst.

P

PC: Personal Computer.

PEC: Prueba de Evaluación Continua.

PMBook: Project Manager Book.

PTO: Punto de Terminación Óptico.

PTR: Punto de Terminación de Red.

R

RDSI: Red Digital de Servicios Integrados.

RIP: Routing Information Protocol.

RFP: Request For Proposal.

S

SIP: Session Initiation Protocol.

SLA: Service Level Agreement.

V

VLAN: Virtual Local Area Network.

VoIP: Voice over Internt Protocol.

VPN: Virtual Private Network.

VRRP: Virtual Router Redundancy Protocol.

W

WAN: Wide Area Network.

11. Bibliografía

[1] OBS Business School, «¿Qué es un diagrama de Gantt y para qué sirve?,» [En línea]. Available: https://www.obs-edu.com/es/blog-project-management/diagramas-de-gantt/que-es-un-diagrama-de-gantt-y-para-que-sirve. [Último acceso: Abril 2019].

[2] J. &. V. V. &. J. R. &. Q. X. &. R. B. &. J. J. Wang, «Dual-homing protection in IP-over-WDM networks,» *Lightwave Technology,* nº 23, pp. 3111-3124, 2005.

[3] E. P. Estévez, «HC6PE - Ernesto "Epe" Pérez Estévez,» 2013. [En línea]. Available: https://www.pymesyautonomos.com/tecnologia/routers-multi-wan-gestionando-mas-de-un-acceso-a-internet. [Último acceso: 2019].

[4] Pymes y Autonomos, «Pymes y Autonomos,» 22 Abril 2019. [En línea]. Available: https://www.pymesyautonomos.com/tecnologia/routers-multi-wan-gestionando-mas-de-un-acceso-a-internet. [Último acceso: 2019].

[5] Concepto.de, «Concepto.de,» 10 diciembre 2018. [En línea]. Available: https://concepto.de/red-lan/#ixzz5not22NaO. [Último acceso: mayo 2019].

[6] J.-F. Pillou, «CCM.net,» 13 septiembre 2017. [En línea]. Available: https://es.ccm.net/contents/286-vlan-redes-virtuales. [Último acceso: mayo 2019].

[7] Cisco, «IP Routing: RIP Configuration Guide, Cisco IOS Release 15M&T,» 26 01 2018. [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_rip/configuration/15-mt/irr-15-mt-book/irr-cfg-info-prot.html. [Último acceso: 2019].

[8] Cisco, «OSPF Design Guide,» 10 8 2005. [En línea]. Available: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html. [Último acceso: 2019].

[9] Cisco, «IP Routing: BGP Configuration Guide,» 20 1 2018. [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-16/irg-xe-16-book/configuring-a-basic-bgp-network.html. [Último acceso: 2019].

[10] Network Working Group, «Virtual Router Rdundancy Protocol (VRRP),» IETF, 5 2004. [En línea]. Available: https://tools.ietf.org/html/rfc3768. [Último acceso: 2019].

[11] Router-Switch, «Data Sheet Cisco ASR 1002,» [En línea]. Available: https://www.router-switch.com/pdf/asr1002-datasheet.pdf. [Último acceso: 2019].

[12] Router-Switch, «Data Sheet Cisco Catalyst C3560-24PS,» [En línea]. Available: https://www.router-switch.com/pdf/ws-c3560-24ps-s-datasheet.pdf. [Último acceso: 2019].

[13] Router-Switch, «Data Sheet Cisco C1111-4P,» [En línea]. Available: https://www.router-switch.com/pdf/c1111-4p-datasheet.pdf. [Último acceso: 2019].

[14] Cisco, «Networking Academy,» [En línea]. Available: https://www.netacad.com/es/courses/packet-tracer.

[15] Á. N. Pérez, «¿Cómo se traspasan los entregables a los clientes? Según PMBOK,» Wolf Project, 2018. [En línea]. Available: https://wolfproject.es/como-se-traspasan-los-entregables-a-los-clientes-segun-pmbok/. [Último acceso: mayo 2019].

[16] Telefónica, «TELEFÓNICA APAGARÁ UNA CENTRAL DE COBRE AL DÍA HASTA 2020,» 7 junio 2018. [En línea]. Available: https://www.telefonica.com/documents/23283/142691915/ndp-trasformacion-red-telefonica.pdf/8680b0c3-b50f-3068-9478-7137f2d99a35?version=1.0. [Último acceso: enero 2019].

[17] B. C. Pavón, «Diseño de una red WAN para una compañía nacional,» UOC, Integración de redes telemáticas E.T.T. Telemática, Junio 2012.

[18] M. G. Medina, «Estudio de las Aplicaciones de Gestión de la red WAN de un Operador de Telecomunicaciones,» UOC, Integración de redes telemáticas E.T.T. Telemática, Junio 2012.

[19] Movistar, «Tarifas y Precios PVP,» mayo 2019. [En línea]. Available: http://www.movistar.es/particulares/atencion-cliente/ficha-ayuda/tarifas-servicio-telefonico-basico. [Último acceso: mayo 2019].

12. Anexos

ANEXO 1: Configuración del CPD

Switch del CPD:

```
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 100
 switchport mode trunk
!
interface FastEthernet1/1
 switchport access vlan 100
!
interface FastEthernet2/1
 switchport access vlan 200
!
interface FastEthernet3/1
 switchport access vlan 300
!
interface FastEthernet4/1
 switchport mode trunk
!
interface FastEthernet5/1
!
interface Vlan1
 no ip address
 shutdown
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
end
```

Router operador 1 del CPD:

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname CPD-R100
!
ip cef
no ipv6 cef
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.100
 encapsulation dot1Q 100
 ip address 172.1.0.2 255.255.255.0
 standby 1 ip 172.1.0.1
 standby 1 priority 200
 standby 1 preempt
!
interface FastEthernet0/0.200
 encapsulation dot1Q 200
 ip address 172.2.0.2 255.255.255.0
 standby 2 ip 172.2.0.1
 standby 2 priority 200
 standby 2 preempt
!
interface FastEthernet0/0.300
 encapsulation dot1Q 300
 ip address 172.3.0.2 255.255.255.0
 standby 3 ip 172.3.0.1
 standby 3 priority 200
 standby 3 preempt
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial2/0
 ip address 10.0.0.1 255.255.0.0
 encapsulation frame-relay
!
interface Serial3/0
```

```
 no ip address
 clock rate 2000000
 shutdown
!
interface FastEthernet4/0
 no ip address
 shutdown
!
interface FastEthernet5/0
 no ip address
 shutdown
!
router bgp 100
 bgp log-neighbor-changes
 no synchronization
 neighbor 10.0.1.1 remote-as 101
 neighbor 10.0.2.1 remote-as 102
 neighbor 172.1.0.3 remote-as 200
 neighbor 172.2.0.3 remote-as 200
 neighbor 172.3.0.3 remote-as 200
 network 172.1.0.0 mask 255.255.255.0
 network 172.2.0.0 mask 255.255.255.0
 network 172.3.0.0 mask 255.255.255.0
!
ip classless
!
ip flow-export version 9
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
end
```

Router operador 2 del CPD:

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname CPD_R200
!
ip cef
no ipv6 cef
!
```

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.100
 encapsulation dot1Q 100
 ip address 172.1.0.3 255.255.255.0
 standby 1 ip 172.1.0.1
 standby 1 preempt
!
interface FastEthernet0/0.200
 encapsulation dot1Q 200
 ip address 172.2.0.3 255.255.255.0
 standby 2 ip 172.2.0.1
 standby 2 preempt
!
interface FastEthernet0/0.300
 encapsulation dot1Q 300
 ip address 172.3.0.3 255.255.255.0
 standby 3 ip 172.3.0.1
 standby 3 preempt
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial2/0
 ip address 10.0.0.2 255.255.0.0
 encapsulation frame-relay
!
interface Serial3/0
 no ip address
 clock rate 2000000
 shutdown
!
interface FastEthernet4/0
 no ip address
 shutdown
!
interface FastEthernet5/0
 no ip address
 shutdown
!
router bgp 200
 bgp log-neighbor-changes
 no synchronization
 neighbor 10.0.2.2 remote-as 202
```

```
 neighbor 10.0.1.2 remote-as 201
 neighbor 172.1.0.2 remote-as 100
 neighbor 172.2.0.2 remote-as 100
 neighbor 172.3.0.2 remote-as 100
 network 172.1.0.0 mask 255.255.255.0
 network 172.2.0.0 mask 255.255.255.0
 network 172.3.0.0 mask 255.255.255.0
!
ip classless
!
ip flow-export version 9
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
end
```

ANEXO 2: Configuración de la SEDE 1

Switch de la SEDE 1:

```
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 100
 switchport mode trunk
!
interface FastEthernet1/1
 switchport access vlan 100
!
interface FastEthernet2/1
 switchport access vlan 200
!
interface FastEthernet3/1
 switchport access vlan 300
!
```

```
interface FastEthernet4/1
 switchport mode trunk
!
interface FastEthernet5/1
!
interface Vlan1
 no ip address
 shutdown
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
end
```

Router del operador 1 de la SEDE 1:

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SEDE1-R101
!
ip cef
no ipv6 cef
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.100
 encapsulation dot1Q 100
 ip address 172.1.1.2 255.255.255.0
 standby 11 ip 172.1.1.1
 standby 11 priority 200
 standby 11 preempt
!
interface FastEthernet0/0.200
 encapsulation dot1Q 200
 ip address 172.2.1.2 255.255.255.0
 standby 12 ip 172.2.1.1
 standby 12 priority 200
 standby 12 preempt
!
```

```
interface FastEthernet0/0.300
 encapsulation dot1Q 300
 ip address 172.3.1.2 255.255.255.0
 standby 13 ip 172.3.1.1
 standby 13 priority 200
 standby 13 preempt
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial2/0
 ip address 10.0.1.1 255.255.0.0
 encapsulation frame-relay
!
interface Serial3/0
 no ip address
 clock rate 2000000
 shutdown
!
interface FastEthernet4/0
 no ip address
 shutdown
!
interface FastEthernet5/0
 no ip address
 shutdown
!
router bgp 101
 bgp log-neighbor-changes
 no synchronization
 neighbor 10.0.0.1 remote-as 100
 neighbor 10.0.2.1 remote-as 102
 neighbor 172.1.1.3 remote-as 201
 neighbor 172.2.1.3 remote-as 201
 neighbor 172.3.1.3 remote-as 201
 network 172.1.1.0 mask 255.255.255.0
 network 172.2.1.0 mask 255.255.255.0
 network 172.3.1.0 mask 255.255.255.0
!
ip classless
!
ip flow-export version 9
!
line con 0
!
line aux 0
!
```

```
line vty 0 4
 login
!
end
```

Router del operador 2 de la SEDE 1:

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SEDE1-R201
!
ip cef
no ipv6 cef
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.100
 encapsulation dot1Q 100
 ip address 172.1.1.3 255.255.255.0
 standby 11 ip 172.1.1.1
 standby 11 preempt
!
interface FastEthernet0/0.200
 encapsulation dot1Q 200
 ip address 172.2.1.3 255.255.255.0
 standby 12 ip 172.2.1.1
 standby 12 preempt
!
interface FastEthernet0/0.300
 encapsulation dot1Q 300
 ip address 172.3.1.3 255.255.255.0
 standby 13 ip 172.3.1.1
 standby 13 preempt
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial2/0
 ip address 10.0.1.2 255.255.0.0
 encapsulation frame-relay
```

```
!
interface Serial3/0
 no ip address
 clock rate 2000000
 shutdown
!
interface FastEthernet4/0
 no ip address
 shutdown
!
interface FastEthernet5/0
 no ip address
 shutdown
!
router bgp 201
 bgp log-neighbor-changes
 no synchronization
 neighbor 10.0.0.2 remote-as 200
 neighbor 10.0.2.2 remote-as 202
 neighbor 172.1.1.2 remote-as 101
 neighbor 172.2.1.2 remote-as 101
 neighbor 172.3.1.2 remote-as 101
 network 172.1.1.0 mask 255.255.255.0
 network 172.2.1.0 mask 255.255.255.0
 network 172.3.1.0 mask 255.255.255.0
!
ip classless
!
ip flow-export version 9
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
end
```

ANEXO 3: Configuración de la SEDE 2

Switch de la SEDE 2:

```
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
```

```
hostname S-SEDE2
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 100
 switchport trunk allowed vlan 2-1005
 switchport mode trunk
!
interface FastEthernet1/1
 switchport access vlan 100
!
interface FastEthernet2/1
 switchport access vlan 200
!
interface FastEthernet3/1
 switchport access vlan 300
!
interface FastEthernet4/1
 switchport mode trunk
!
interface FastEthernet5/1
!
interface Vlan1
 no ip address
 shutdown
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
end
```

Router del operador 1 de la SEDE 2:

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SEDE2-R102
!
ip cef
no ipv6 cef
```

```
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.100
 encapsulation dot1Q 100
 ip address 172.1.2.2 255.255.255.0
 standby 21 ip 172.1.2.1
 standby 21 priority 200
 standby 21 preempt
!
interface FastEthernet0/0.200
 encapsulation dot1Q 200
 ip address 172.2.2.2 255.255.255.0
 standby 22 ip 172.2.2.1
 standby 22 priority 200
 standby 22 preempt
!
interface FastEthernet0/0.300
 encapsulation dot1Q 300
 ip address 172.3.2.2 255.255.255.0
 standby 23 ip 172.3.2.1
 standby 23 priority 200
 standby 23 preempt
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial2/0
 ip address 10.0.2.1 255.255.0.0
 encapsulation frame-relay
!
interface Serial3/0
 no ip address
 clock rate 2000000
 shutdown
!
interface FastEthernet4/0
 no ip address
 shutdown
!
interface FastEthernet5/0
 no ip address
 shutdown
!
```

```
router bgp 102
 bgp log-neighbor-changes
 no synchronization
 neighbor 10.0.0.1 remote-as 100
 neighbor 10.0.1.1 remote-as 101
 neighbor 172.1.2.3 remote-as 202
 neighbor 172.2.2.3 remote-as 202
 neighbor 172.3.2.3 remote-as 202
 network 172.1.2.0 mask 255.255.255.0
 network 172.2.2.0 mask 255.255.255.0
 network 172.3.2.0 mask 255.255.255.0
!
ip classless
!
ip flow-export version 9
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
end
```

Router del operador 2 de la SEDE 2:

```
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SEDE2-R202
!
ip cef
no ipv6 cef
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.100
 encapsulation dot1Q 100
 ip address 172.1.2.3 255.255.255.0
 standby 21 ip 172.1.2.1
 standby 21 preempt
!
interface FastEthernet0/0.200
```

```
 encapsulation dot1Q 200
 ip address 172.2.2.3 255.255.255.0
 standby 22 ip 172.2.2.1
 standby 22 preempt
!
interface FastEthernet0/0.300
 encapsulation dot1Q 300
 ip address 172.3.2.3 255.255.255.0
 standby 23 ip 172.3.2.1
 standby 23 preempt
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial2/0
 ip address 10.0.2.2 255.255.0.0
 encapsulation frame-relay
!
interface Serial3/0
 no ip address
 clock rate 2000000
 shutdown
!
interface FastEthernet4/0
 no ip address
 shutdown
!
interface FastEthernet5/0
 no ip address
 shutdown
!
router bgp 202
 bgp log-neighbor-changes
 no synchronization
 neighbor 10.0.0.2 remote-as 200
 neighbor 10.0.1.2 remote-as 201
 neighbor 172.1.2.2 remote-as 102
 neighbor 172.2.2.2 remote-as 102
 neighbor 172.3.2.2 remote-as 102
 network 172.1.2.0 mask 255.255.255.0
 network 172.2.2.0 mask 255.255.255.0
 network 172.3.2.0 mask 255.255.255.0
!
ip classless
!
ip flow-export version 9
!
```

```
line con 0
!
line aux 0
!
line vty 0 4
 login
!
end
```