Solución de conectividad ante fallos para una red WAN empresarial

Presentación del proyecto

TRABAJO FIN DE CARRERA
Ingeniería Técnica de Telecomunicaciones
Primer semestre del curso 2013/14

UOC
Universitat Oberta de Catalunya

Alumno: José María Martín Manjón-Cabeza
Consultor: José López Vicario

APARTADOS

1. Introducción
2. Planificación del proyecto
3. Estudio Técnico
4. Diseño de la solución
5. Propuesta tecnológica
6. Estudio económico
7. Laboratorio de pruebas
8. Conclusiones

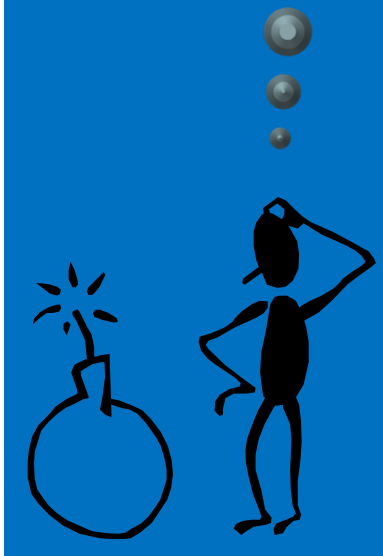
1. Introducción

¿QUÉ VAMOS A HACER?

Necesitamos crear una red WAN de respaldo…

¿Y si aprovechamos la infraestructura existente en nuestra red?

¡¡Hagamos una WAN bajo demanda con los enlaces RDSI!!

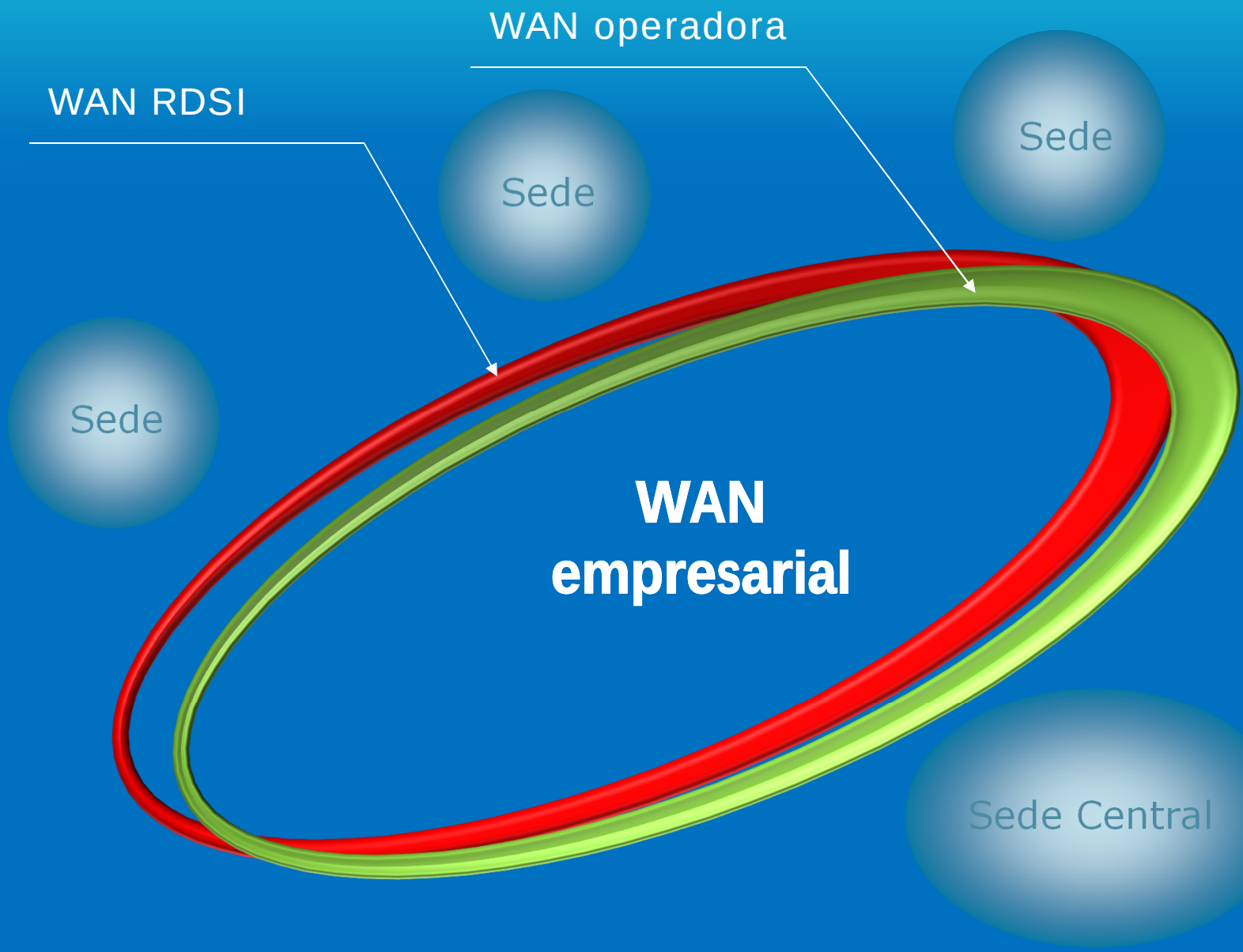


- Disponibilidad
- Convergencia
- Rendimiento
- Escalabilidad
- Baja inversión

- Gestión de tráfico
- Gestión de red
- Gestión de equipos
- Gestión de uso
- Ahorro de costes

1. Introducción

¿QUÉ VAMOS A HACER?



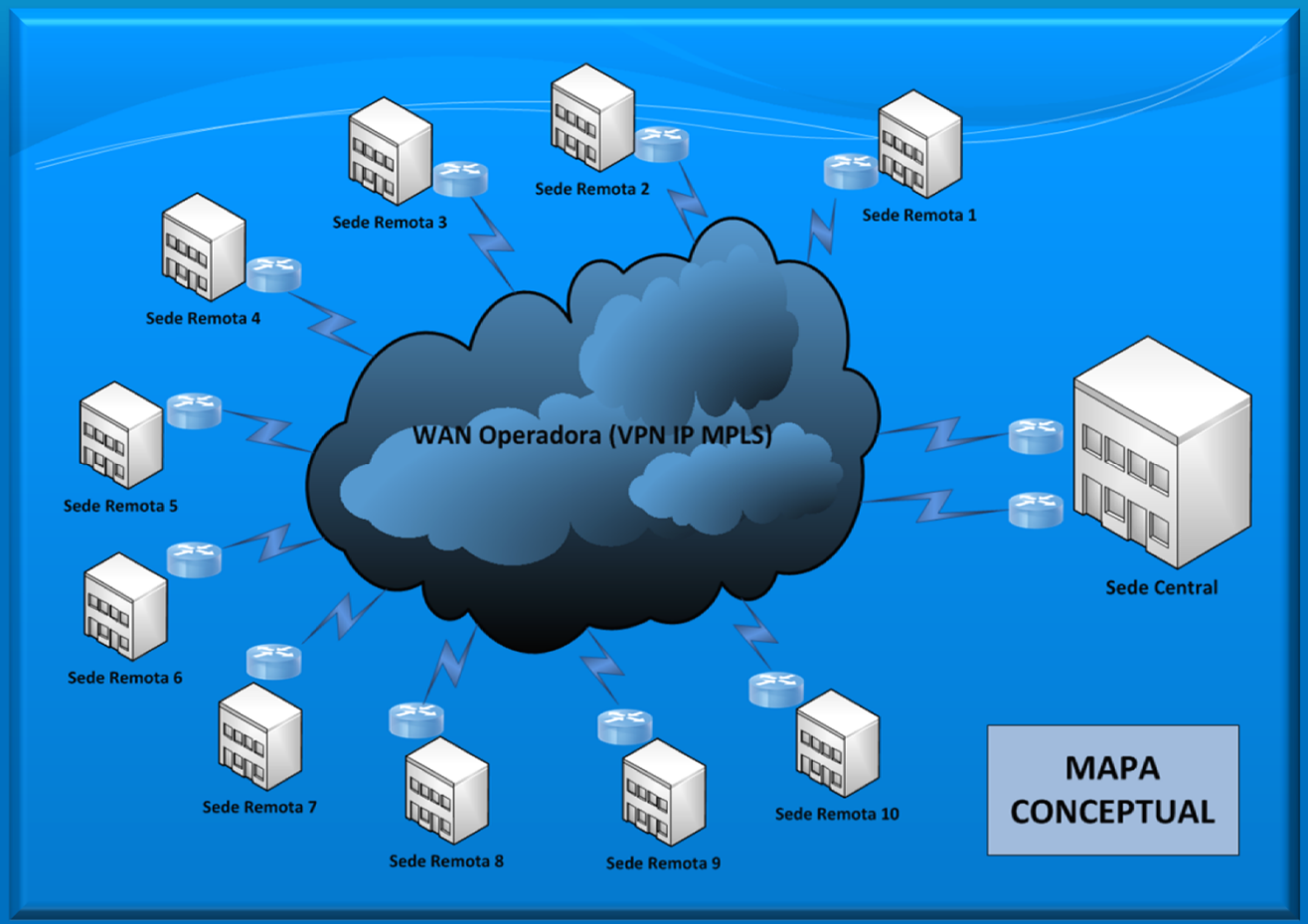
2. Planificación del proyecto

¡NECESITAMOS UN PLAN!

Nombre de tarea	Duración	Comienzo	Fin
Trabajo fin de carrera	**121 días**	**mié 18/09/13**	**jue 16/01/14**
Decisión del proyecto	**8 días**	**mié 18/09/13**	**mié 25/09/13**
Oportunidad de proyecto	1 día	mié 18/09/13	mié 18/09/13
Definición de objetivos	3 días	jue 19/09/13	sáb 21/09/13
Descripción de la propuesta	3 días	dom 22/09/13	mar 24/09/13
Comunicación del proyecto al consultor	1 día	mié 25/09/13	mié 25/09/13
Planificación del proyecto	**7 días**	**jue 26/09/13**	**mié 02/10/13**
Definición de fases y tareas	3 días	jue 26/09/13	sáb 28/09/13
Creación de diagrama de Gantt	1 día	dom 29/09/13	dom 29/09/13
Creación del índice	2 días	lun 30/09/13	mar 01/10/13
PEC 1 Entrega de la planificación del trabajo	1 día	mié 02/10/13	mié 02/10/13
Estudio técnico	**48 días**	**jue 03/10/13**	**mar 19/11/13**
Análisis de situación actual	**16 días**	**jue 03/10/13**	**vie 18/10/13**
Análisis sede central	10 días	jue 03/10/13	sáb 12/10/13
Análisis sedes remotas	6 días	dom 13/10/13	vie 18/10/13
Diseño de la solución	**28 días**	**sáb 19/10/13**	**vie 15/11/13**
Estudio de tecnologías a emplear	10 días	sáb 19/10/13	lun 28/10/13
Requisitos hardware	6 días	mar 29/10/13	dom 03/11/13
Propuesta tecnológica	12 días	lun 04/11/13	vie 15/11/13
Estudio económico	**4 días**	**sáb 16/11/13**	**mar 19/11/13**
Coste proyecto	3 días	sáb 16/11/13	lun 18/11/13
PEC 2 Primera entrega del proyecto	1 día	mar 19/11/13	mar 19/11/13
Laboratorio de pruebas	**28 días**	**mié 20/11/13**	**mar 17/12/13**
Preparación de laboratorio	20 días	mié 20/11/13	lun 09/12/13
Plan de pruebas	3 días	mar 10/12/13	jue 12/12/13
Análisis de resultados	4 días	vie 13/12/13	lun 16/12/13
PEC 3 Segunda entrega del proyecto	1 día	mar 17/12/13	mar 17/12/13
Entregables finales de proyecto	**30 días**	**mié 18/12/13**	**jue 16/01/14**
Realización de la memoria final	23 días	mié 18/12/13	jue 09/01/14
Entrega de la memoria final	1 día	vie 10/01/14	vie 10/01/14
Realización de la presentación	5 días	sáb 11/01/14	mié 15/01/14
Entrega de la presentación	1 día	jue 16/01/14	jue 16/01/14

3. Estudio Técnico

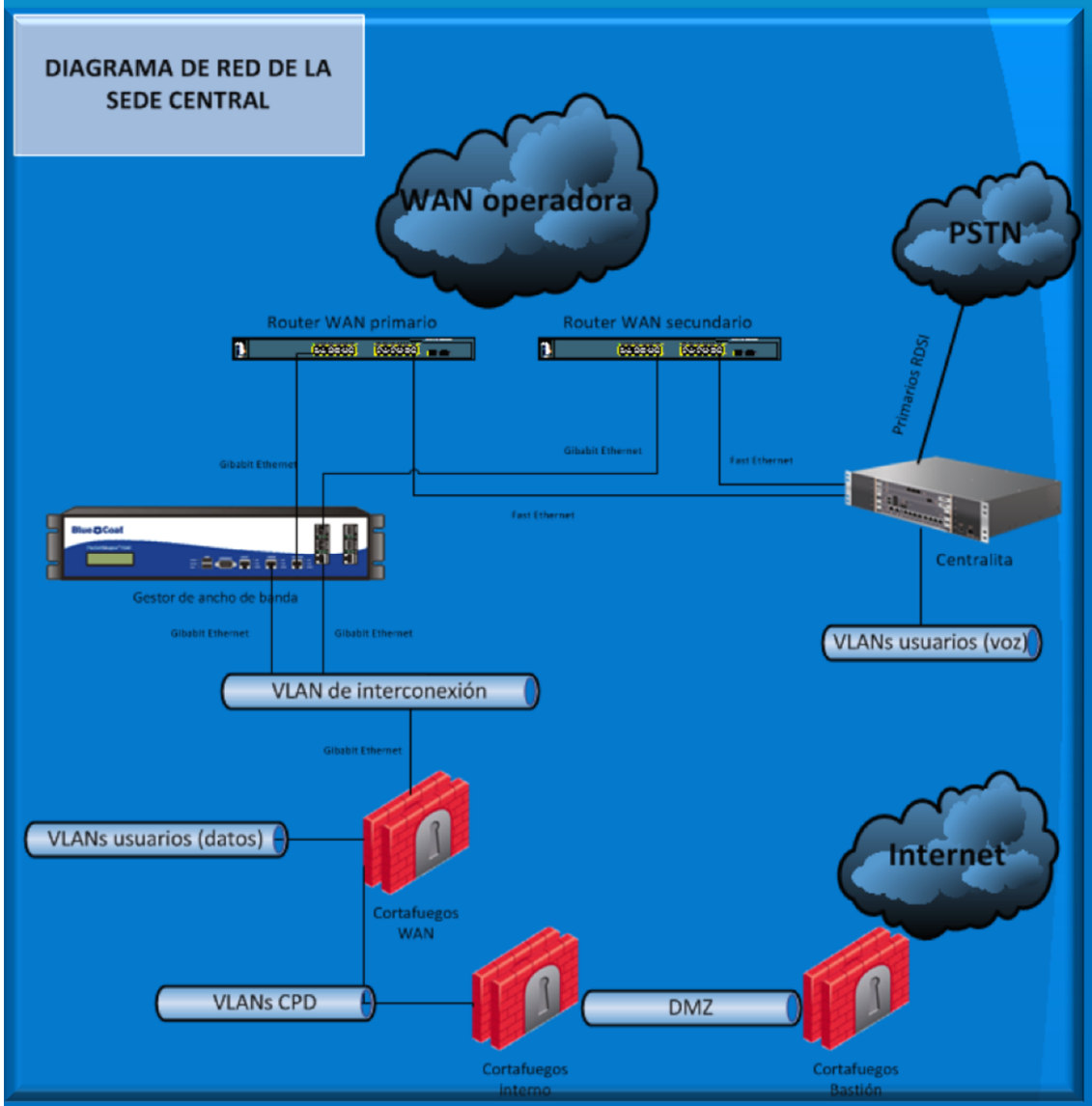
¿QUÉ TENEMOS AHORA?



La empresa cuenta con diversas sedes interconectadas a través de enlaces a la WAN de una operadora. Debido al alto coste que oferta la operadora para los enlaces de respaldo, se busca una solución alternativa para evitar que un fallo pueda aislar una o varias sedes.

3. Estudio Técnico

¿QUÉ TENEMOS AHORA?

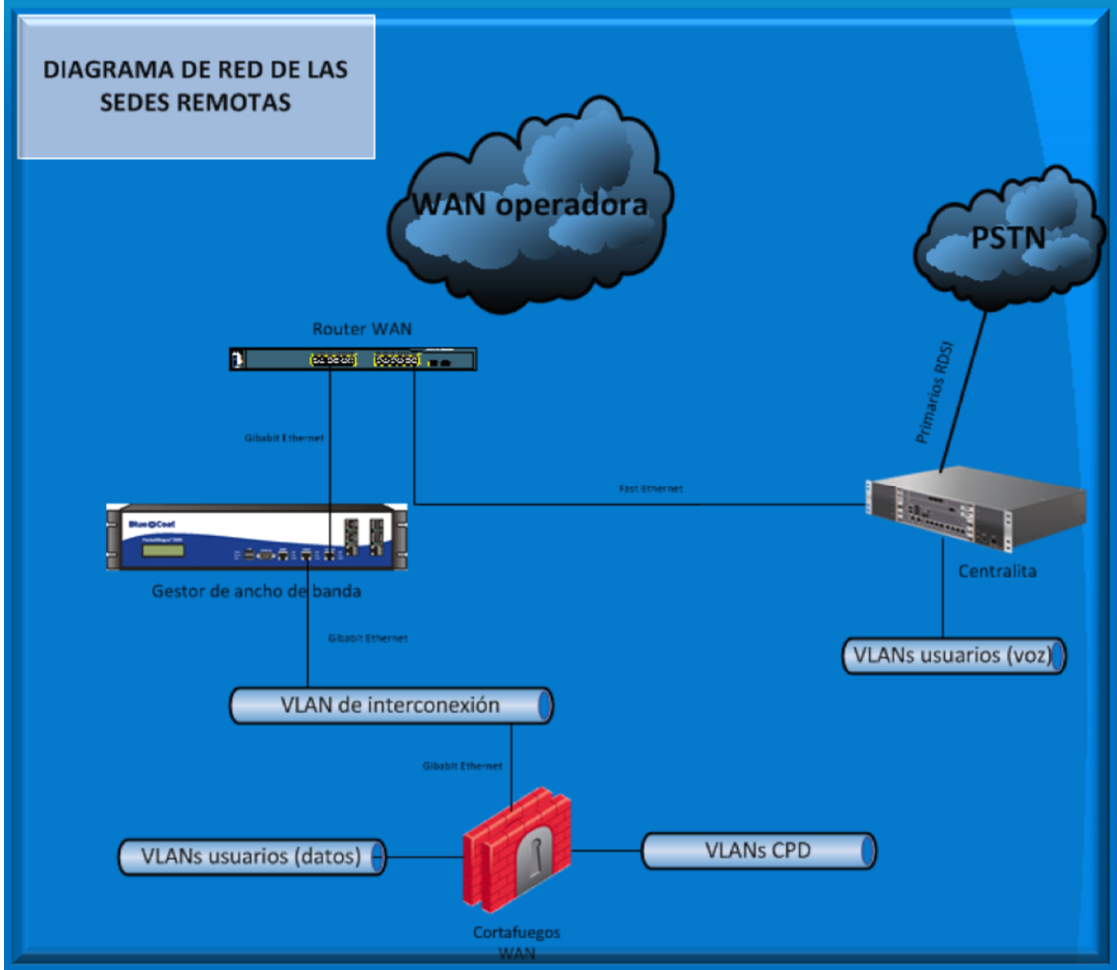


Arquitectura de la sede central:

- 2 enrutadores Cisco Catalyst 3560-v2 para conectar a la red MPLS de la operadora y dar acceso a la WAN. Son propiedad de la operadora. Uno funciona como activo y otro como pasivo.
- 1 gestor de ancho de banda que garantiza el caudal necesario para el tráfico crítico entre las sedes. El modelo usado en esta sede es el Packetshaper 7500 de Bluecoat.
- 1 centralita Aastra MX-ONE Lite para las comunicaciones de voz tanto IP como tradicional. Tiene conexiones de primarios RDSI para hacer las llamadas por la red pública.
- 3 cortafuegos en alta disponibilidad para proteger el acceso a la DMZ, a la WAN y a los CPDs. Los dispositivos empleados son CheckPoint 4600.

3. Estudio Técnico

¿QUÉ TENEMOS AHORA?



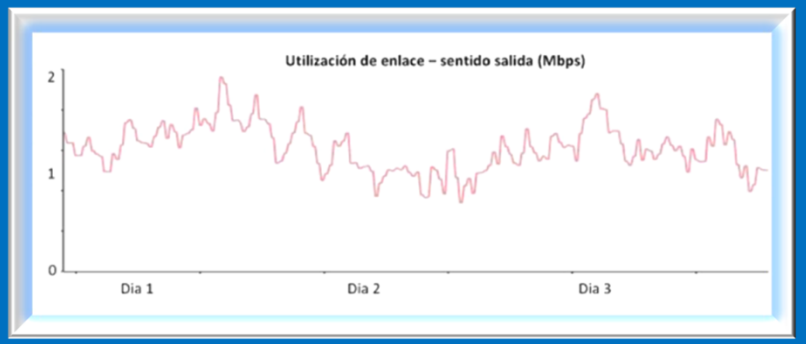
Arquitectura de las sedes remotas:

- 1 enrutador Cisco Catalyst 3560-v2 para conectar a la red MPLS de la operadora y dar acceso a la WAN. Son propiedad de la operadora.
- 1 gestor de ancho de banda que garantiza el caudal necesario para el tráfico crítico entre las sedes. El modelo usado en esta sede es el Packetshaper 3500 de Bluecoat.
- 1 centralita Aastra MX-ONE Lite para las comunicaciones de voz tanto IP como tradicional. Tiene conexiones de primarios RDSI para hacer las llamadas por la red pública.
- 1 cortafuegos en alta disponibilidad para proteger el acceso a la WAN y al CPD. Los dispositivos usados son CheckPoint 4600.

3. Estudio Técnico

¿QUÉ TENEMOS AHORA?

- La solución debe cubrir el ancho de banda necesario en las sedes remotas.
- Las políticas de los gestores de ancho de banda no deberán sufrir ninguna variación ya que el caudal de las conexiones de respaldo cubrirá totalmente las necesidades de la red.
- Las gráficas de uso de ancho de banda en la sede remota con más carga de tráfico no presenta picos superiores a los 2 Mbps.



4. Diseño de la solución

¿QUÉ NECESITAMOS?

Primarios RDSI para conectar las sede central con el resto de las sedes remotas.

RIPv2 como protocolo de enrutamiento entre cortafuegos y enrutador WAN principal.

Técnica de enrutamiento Dial on Demand Routing para la convergencia de la WAN principal a la WAN de respaldo.

Gestión de ancho de banda para asegurar el tráfico en la WAN de respaldo.

4. Diseño de la solución

¿QUÉ NECESITAMOS?

Enrutador Cisco 3925 con 2 tarjetas para conectar 4 enlaces primarios RDSI.

Sede Central

- Tarjetas de expansión LEM para los modelos Bluecoat Packetshaper 3500 y 7500.
- En ellas se conectarán el cortafuegos y el enrutador RDSI de cada sede.

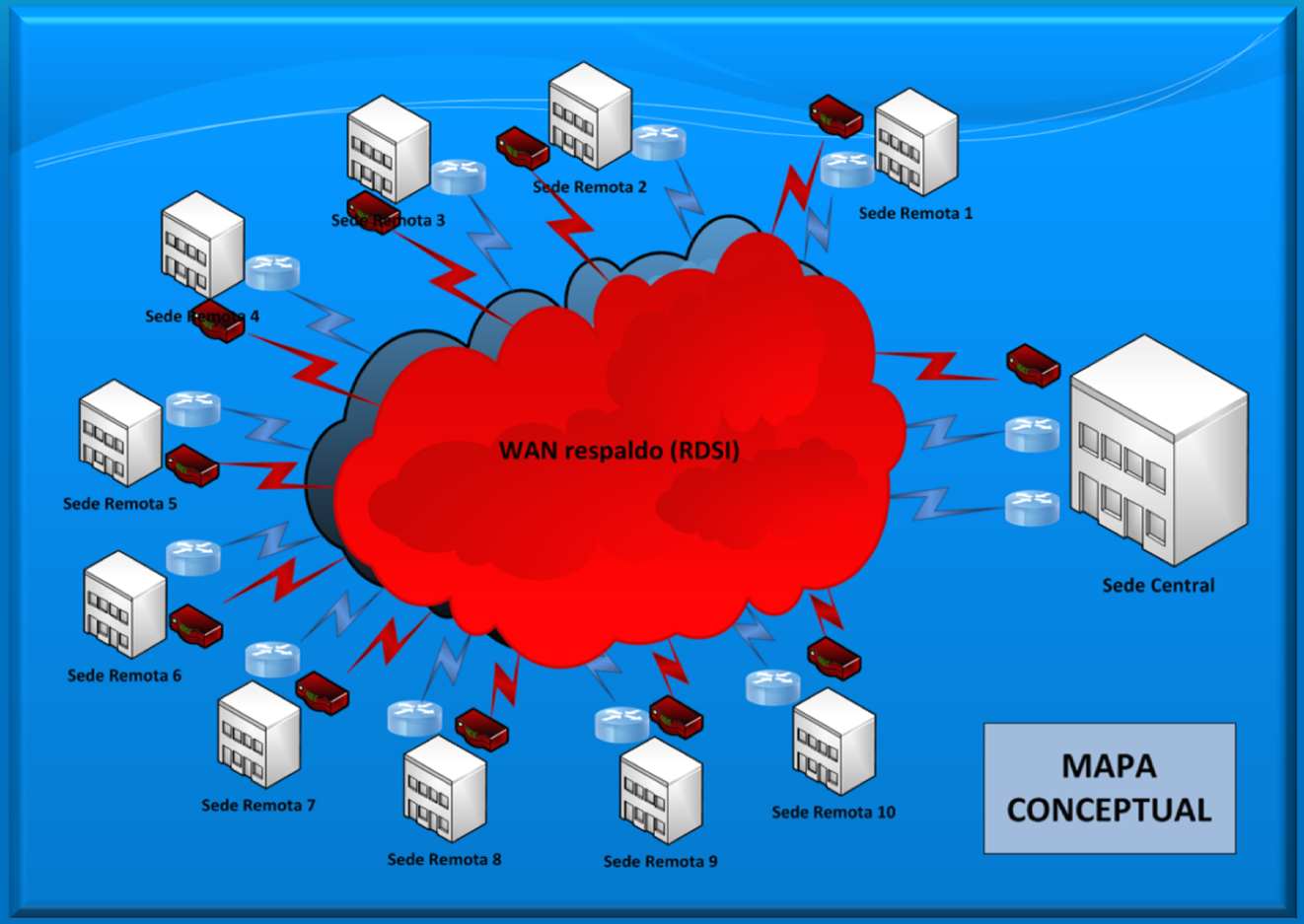
Tanto los cortafuegos como las centralitas de todas las sedes cuentan con puertos libres para implementar la solución.

Sede Remota

Enrutador Cisco 2911 con 1 tarjeta para conectar 2 enlaces primarios RDSI.

5. Propuesta tecnológica

¿CÓMO LO VAMOS A HACER?



La solución propuesta se integra sobre la arquitectura actual haciendo uso de la infraestructura RDSI existente. Destacar como características más importantes: la velocidad y confiabilidad de respuesta ante fallo, la estabilidad de la llamada telefónica, la capacidad de testar el enlace, su rendimiento y la facilidad de implementación.

5. Propuesta tecnológica

¿CÓMO LO VAMOS A HACER?

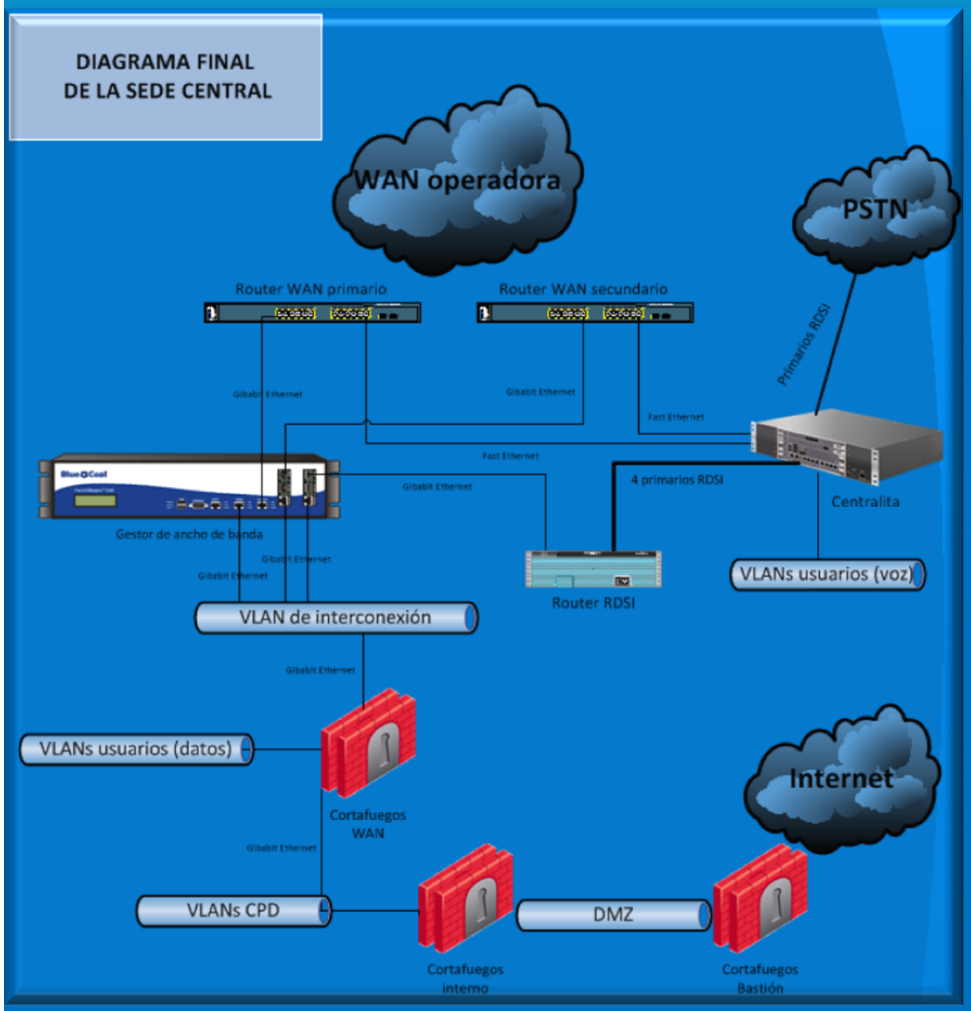
Funcionalidades y roles

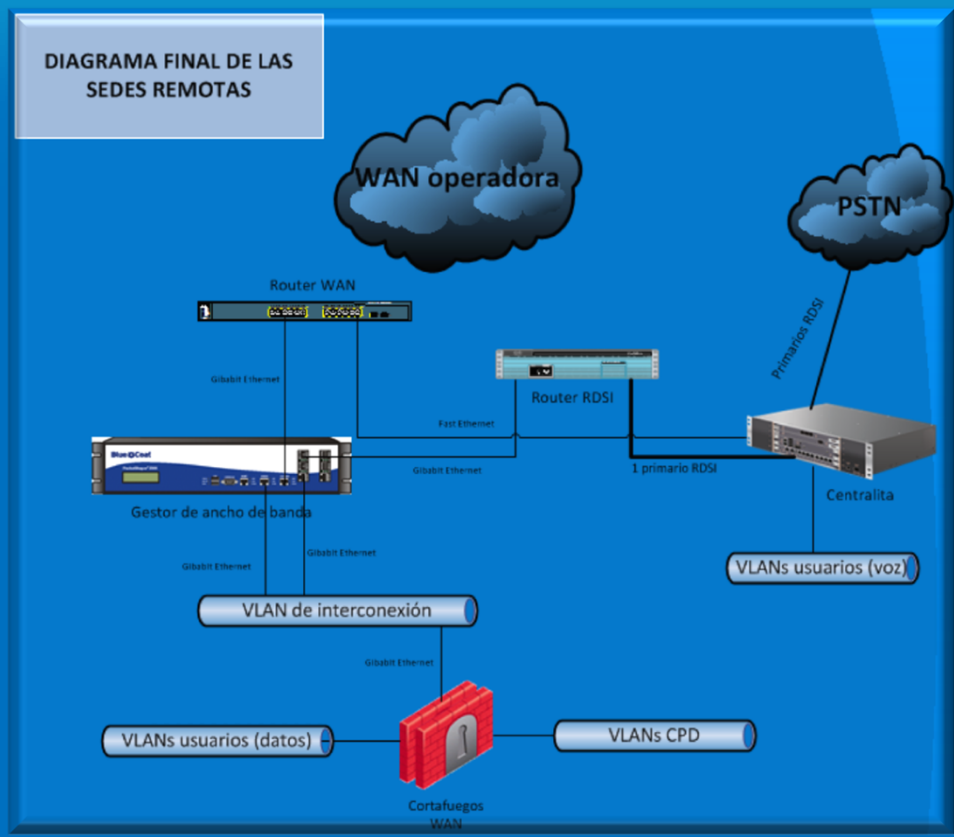
El éxito de la solución propuesta depende de la conjunción varios actores:

- **Los enrutadores WAN** interconectan las distintas sedes con la WAN de la operadora y deben "informar" a las distintas sedes de cualquier cambio de topología.
- **Los cortafuegos WAN** deben ser sensibles a cualquier cambio de topología informada por los enrutadores WAN.
- **Los enrutadores RDSI** deben lanzar la conexión a sus gemelos de las distintas sedes una vez reciban el tráfico procedente del cortafuegos.
- **El gestor de ancho de banda** asegurará que se da la misma política de prioridades tanto al tráfico de la WAN principal como, después de converger, al tráfico de la WAN RDSI.
- **Las centralitas**, cuando no puedan establecer llamadas internas de voz IP a las extensiones de la sede que se haya quedado aislada, tendrán que realizarlas por la red pública a los números de teléfono habituales.

5. Propuesta tecnológica

¿CÓMO LO VAMOS A HACER?

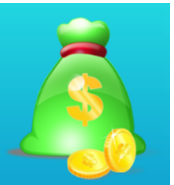




Diagramas de red

6. Estudio económico

¿CUÁNTO NOS VA A COSTAR?



PRESUPUESTO TOTAL DEL PROYECTO	
Coste de material	44.177 €
Coste de personal	22.250 €
Coste total	66.427 €

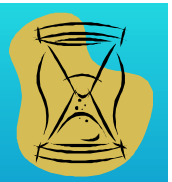
- El presupuesto de material incluye el primer año de soporte.
- El resto de años se estima un coste total de 5000 €/año en concepto de renovación de licencia y soporte de fabricante.
- El presupuesto de personal incluye un gestor de proyecto, un técnico en sede central y un técnico por sede remota.
- El responsable técnico del proyecto será el técnico de la sede central y será el único a tiempo completo en el proyecto.

- La inversión mayor se asume al principio.
- En el segundo año ya se ha rentabilizado la inversión inicial.
- El ahorro obtenido se podría dedicar a formación del personal, a la escalabilidad del sistema o a sistemas de monitorización y gestión de alertas.

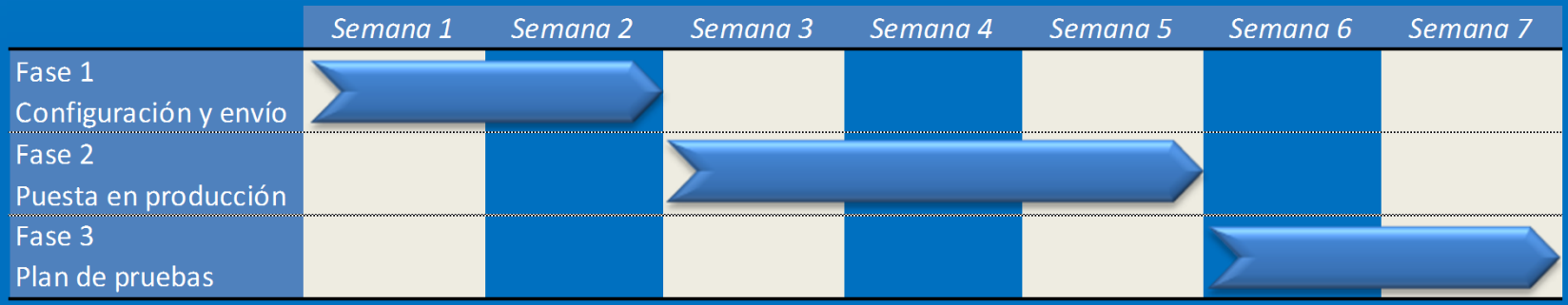
RETORNO DE LA INVERSIÓN	*Año 1*	*Año 2*	*Año 3*
Opción WAN respaldo operadora	51.000 €	51.000 €	51.000 €
Opción WAN respaldo RDSI	66.427 €	5.000 €	5.000 €
Beneficio	-15.427 €	46.000 €	46.000 €
ROI	-23,22%	920,00%	920,00%

6. Estudio económico

¿CUÁNTO TIEMPO ES NECESARIO?



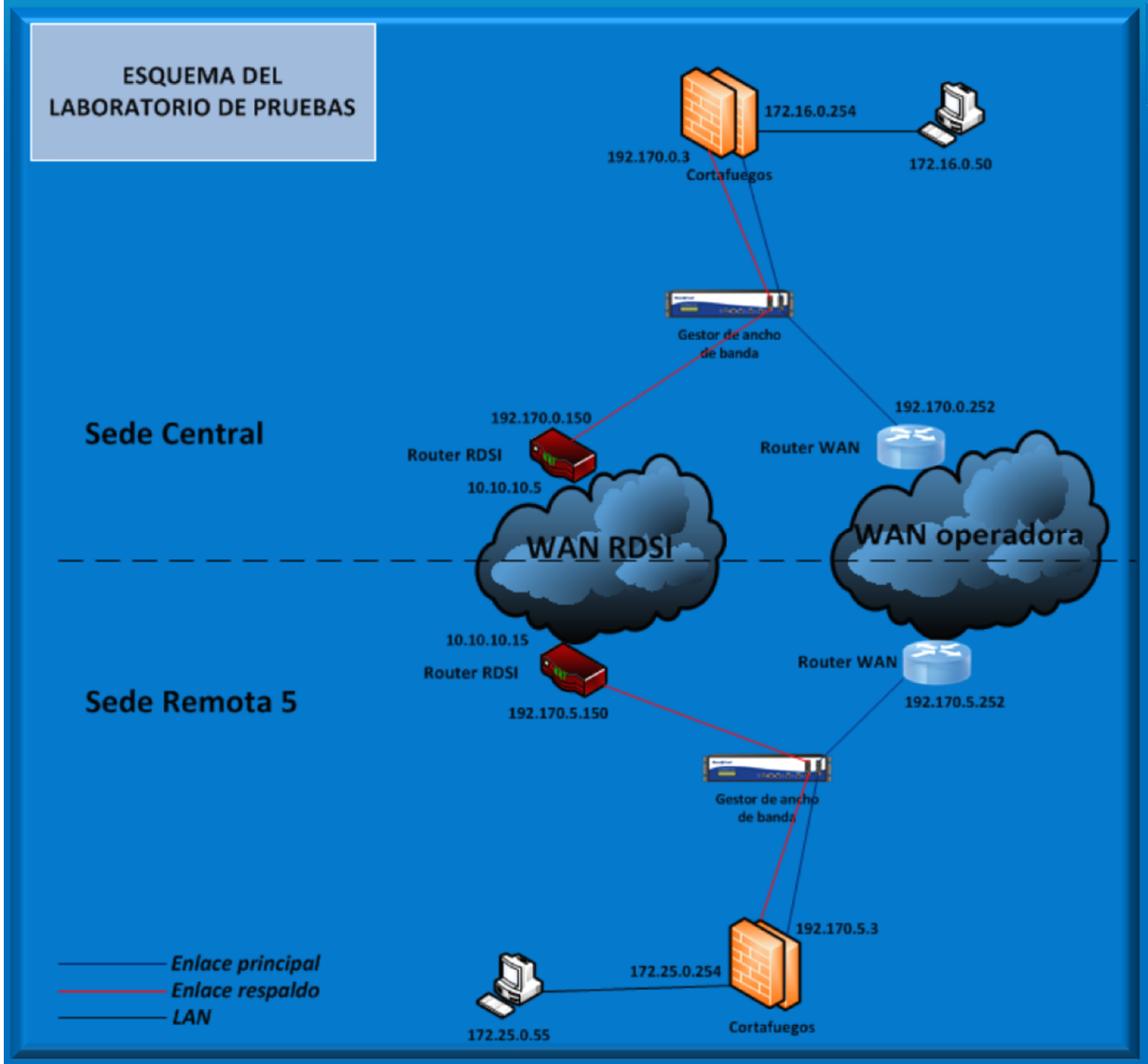
PLAN DE DESPLIEGUE



- ✓ El proyecto se desarrollará en 3 fases.
- ✓ Se han estimado 7 semanas para su implantación.
- ✓ La fase 1 se realizará completamente en la sede central.
- ✓ La fase 2 requerirá de la coordinación de los técnicos de distintas sedes.
- ✓ La fase 3 se realizará sede por sede para dar el visto bueno final.

7. Laboratorio de pruebas

¡PROBEMOS SI FUNCIONA!



Plan de pruebas

Proceso de convergencia a la WAN RDSI:

La sede remota 5 se queda aislada de la WAN de la operadora.

El enrutador WAN de la sede central deja de propagar con RIP las rutas para alcanzar las redes de la sede remota 5.

Los cortafuegos pierden esas rutas de su tabla De enrutamiento y aplican su ruta estática por defecto que son los enrutadores RDSI.

El enrutador RDSI de la sede central mediante la técnica DDR lanza las llamadas al enrutador RDSI de la sede remota 5.

Proceso de convergencia a la WAN de operadora:

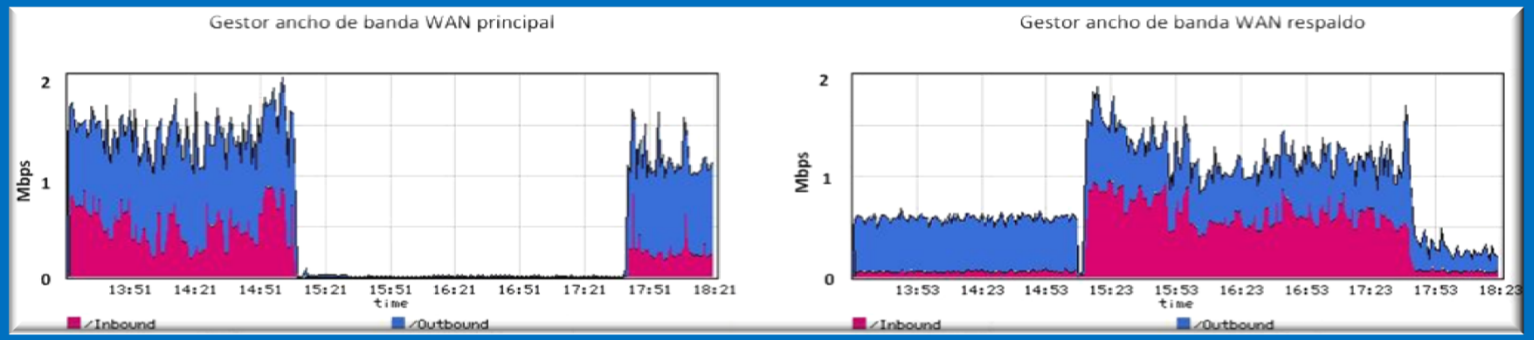
Una vez recuperado el enlace WAN principal la red convergerá de forma automática mediante la publicación de rutas con RIP y los enlaces RDSI se cortarán pasado un tiempo de inactividad.

7. Laboratorio de pruebas

¡PROBEMOS SI FUNCIONA!

¡¡¡Funciona!!!

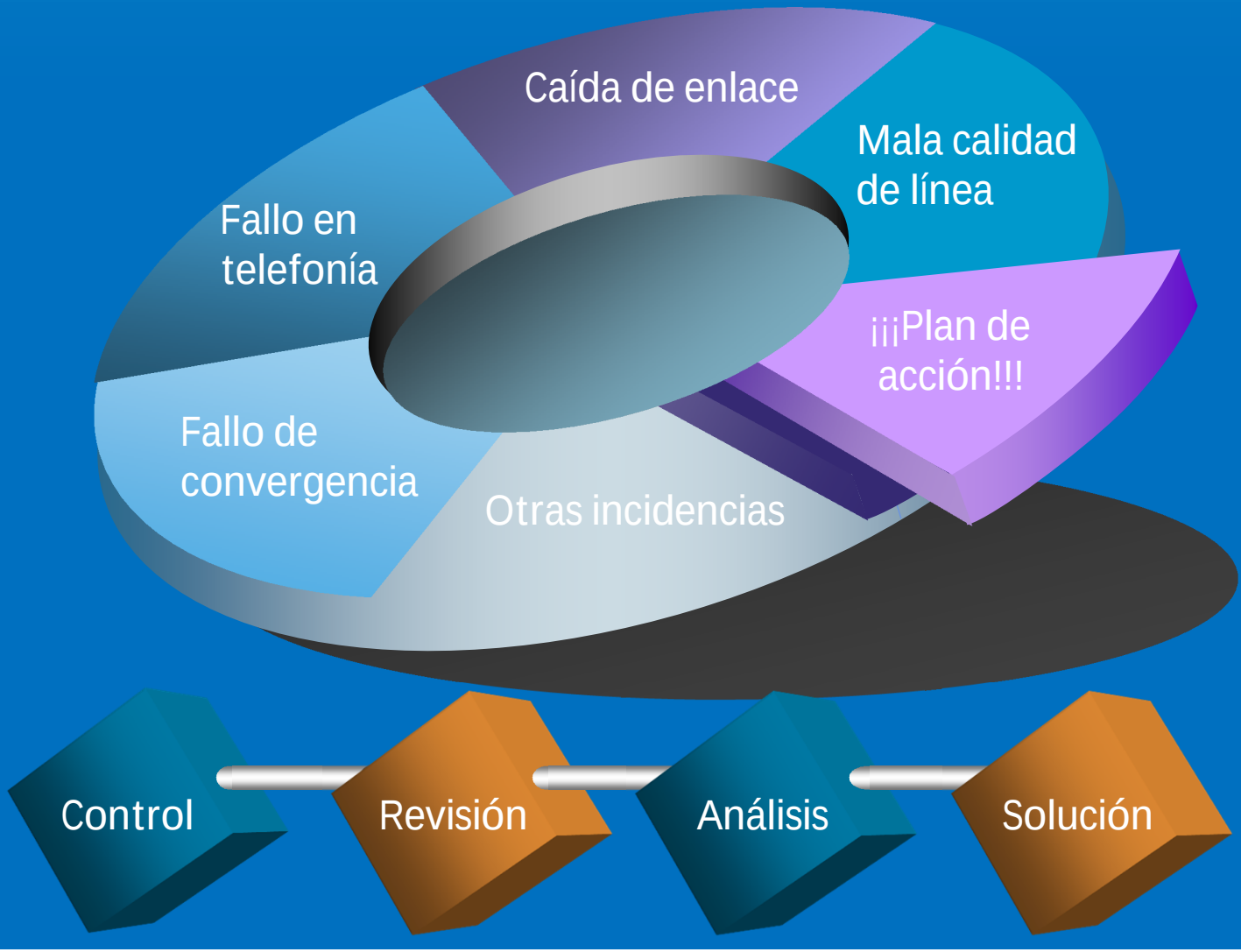
- El tiempo de convergencia es aceptable: 1 m 30 seg.
- El enrutador RDSI ha levantado los 30 canales del primario RDSI: 2 Mbps.
- La tabla de enrutamiento de los cortafuegos se han adaptado de forma dinámica, usando RIPv2, a los cambios de topología.
- El tráfico por la WAN de respaldo RDSI ha sido garantizado por los gestores de ancho de banda.
- Una vez recuperado el enlace a la WAN principal la red ha vuelto a converger automáticamente.
- Los enlaces RDSI se han desactivado pasado el tiempo de inactividad.



7. Laboratorio de pruebas

¿Y CUANDO ALGO FALLE?

Gestión de incidencias



8. Conclusiones

¿QUÉ CONCLUSIONES SACAMOS?

A favor

- Solución rentable.
- Implementación sencilla.
- Reutilización de infraestructura.
- Hardware escalable y modular.
- Gestión global de la solución.
- Procedimientos de actuación simples.
- Ampliación de conocimiento técnico.

En contra

- Escalable con limitaciones.
- Recomendable sólo como conexión secundaria.
- No permite automatizar la solución para telefonía.
- Los tiempos de convergencia podrían mejorarse con el uso de otro protocolo de enrutamiento.