Solución de conectividad ante fallos para una red WAN empresarial

Memoria técnica 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

Agradecimientos:

Este trabajo culmina el esfuerzo realizado durante varios años, donde he tenido que superar diversas dificultades, tanto en el plano laboral como en el personal. Con él se pone fin a un camino donde ha habido que sacrificar "de todo".

Quisiera dedicar este trabajo y mostrar mi agradecimiento, en especial, a mi entorno familiar, el cual ha sido mi compañero de viaje durante este tiempo, me ha apoyado en todo momento y me ha animado a seguir siempre adelante.

Hay muchas personas con nombre y apellidos: compañeras y compañeros de trabajo y de estudios, amigas y amigos, consultoras y consultores de determinadas asignaturas, etc. Me gustaría agradecerles a todos ellos su colaboración para mantener mi motivación siempre al máximo.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

PRIMERA PARTE: ¿QUÉ VAMOS A HACER?

1 INTRODUCCIÓN

Dentro de las distintas posibilidades que ofrece la **especialidad en Telemática** de la **Ingeniería Técnica de Telecomunicaciones** se ha seleccionado el **diseño WAN**[1] como área donde englobar el trabajo final de carrera.

Las redes WAN son aquellas que engloban una zona geográfica amplia y nos sirven para interconectar lugares remotos. Para esta conexión necesitamos contar con los enlaces que contratamos a un proveedor u operador, por lo tanto supone un coste periódico por su uso.

1.1 Oportunidad de proyecto.

En la actualidad las empresas invierten mucho dinero en tecnología, y gran parte de esa inversión va dirigida a redundar sus redes de comunicaciones. No se concibe disponer de una red con un sólo punto de acceso, lo que supone un riesgo elevado de quedarse sin comunicación ante un fallo. Las empresas contratan a las operadoras soluciones de comunicación de larga distancia para interconectar sus sedes y delegaciones. Estas operadoras proponen una solución redundante incrementando el coste total de la misma; coste que en muchos casos puede no ser asumible por una empresa.

La empresa ficticia que utilizamos para el proyecto tiene desplegada a nivel nacional una sede central y 10 sedes remotas. Hasta ahora la red empresarial contaba con soluciones de tipo ATM[2] alquiladas a operadora para transmitir datos en su entorno WAN y con una centralita por sede con primarios RDSI[3] para transmitir voz.

Actualmente han contratado un servicio VPN-IP[4] (MPLS[5]) a una operadora sobre el que descansa su conectividad WAN principal. A través de ella disponen de servicios de tráfico de datos y voz sobre IP entre las distintas sedes y la central.

Con la premisa de conseguir un ahorro de costes, quieren estudiar la posibilidad de reutilizar sus infraestructuras existentes con el fin de disponer de un sistema de conectividad de respaldo a su red WAN y no tener que contratar más enlaces a la operadora.

Con este proyecto se pretende desarrollar el estudio y diseño de una solución de conectividad alternativa a la WAN principal, para salvar el tráfico de datos y voz de una sede remota que pierda acceso a la WAN. Asimismo, se hará uso de las facilidades del enrutamiento sobre protocolo IP, tanto estático como dinámico.

[1] Red de área extensa.
[2] Modo de transferencia asíncrona.
[3] Red digital de servicios integrados.
[4] Sistema para interconectar diferentes sedes a través de redes privadas virtuales.
[5] Conmutación multiprotocolo mediante etiquetas.

1.2 Objetivos el proyecto.

El proyecto pretende proponer una solución bajo demanda y de bajo coste para poder mantener la disponibilidad de las comunicaciones de las distintas sedes de una empresa hacia el resto de la WAN corporativa ante un fallo de alguno de sus enlaces principales de la WAN contratada a la operadora.

1.2.1 Alternativas de conectividad posibles.

En la actualidad contamos con un gran abanico de tecnologías para realizar este cometido, diferenciadas sobre todo por su fiabilidad, velocidad y coste (tanto de acceso como de distancia y de uso). Entre ellas podemos enumerar las siguientes: ATM, Frame Relay, RDSI, TDM, MPLS, Metro Ethernet, Fibra oscura, DWDM, Wireless, xDSL, SONET/SDH, enlaces vía satélite,...

De todas ellas, hemos discriminados aquellas donde la inversión económica en equipamiento, el tiempo necesario para el despliegue del material y el capital humano a utilizar para conjuntar todo excede de las posibilidades de una empresa del tamaño de la que estamos tratando. Por lo tanto, hemos seleccionado las posibilidades de conectividad para el objetivo del proyecto que se ajustan más. Serían las siguientes:

- *Contratar una línea de respaldo a la operadora que nos sirve los enlaces principales.*
  En este caso las posibilidades de acceso a la red VPN-IP de la operadora serían a través de Giga Ethernet, ATM, Frame Relay o xDSL. Nos ofrecen por el mismo servicio que dan por el enlace de respaldo a un coste similar al enlace principal.

- *Conectividad basada en enlaces xDSL de salida a Internet.*
  Se utilizarían Internet como medio para levantar enlaces VPN entre los enrutadores de respaldo de las distintas sedes. Tiene el riesgo de usar un medio inseguro como es Internet para transmitir, aunque sea cifrado, tráfico que puede ser sensible para la empresa.

- *Conectividad mediante enlaces punto a punto para conectar las sedes.*
  Esta opción, además de ser de muy alto coste obligaría a la existencia de una conexión dedicada entre dos sedes, lo que haría que cada una de ellas necesitase diez enlaces para conectar con toda la empresa.

- *Conectividad con enlaces vía Satélite.*
  Son conexiones de gran retardo para comunicaciones de audio o video. Además requieren un coste de material y mantenimiento elevado ya que es necesario disponer de antenas y otros dispositivos.

- *Conectividad basada en enlaces primarios RDSI.*
  Son conexiones simétricas ideales para transmisión de voz y de datos. Nos permite usar 30 canales enlazados para transmitir datos por un primario alcanzando velocidades de hasta 2 Mbps por primario. Las conexiones pueden ser implementadas bajo demanda, por lo que el uso de las líneas será nulo cuando no haya problemas en los enlaces principales.

En nuestro caso nos decantaremos por el uso de la tecnología RDSI debido a que la empresa dispone en propiedad de una centralita en cada sede, además de los primarios RDSI conectados a

ellas. Por tanto, el coste económico se basará en el mantenimiento de la centralita y de la numeración contratada a la operadora. Esta situación además permite al personal técnico de la empresa gestionar extremo a extremo la infraestructura, lo que facilita en gran medida la monitorización y la intervención ante cualquier anomalía.

Figura 1. Necesidad del proyecto.

1.2.2 Ventajas e inconvenientes de la solución elegida.

Como todas las soluciones que afectan a las redes, ésta también presenta una serie de ventajas y desventajas. La decisión de utilizar el acceso telefónico para implementar unos enlaces de respaldo a priori puede parecer una opción no muy clara. Pero si una característica particular es una ventaja o una desventaja depende de la aplicación que se le dé.

Algunas de las ventajas y desventajas más importantes son las siguientes:

- *La velocidad de respuesta ante fallo.*

Cuando se configura correctamente, el sistema debe responder inmediatamente a un fallo del enlace principal. En nuestro caso, el enrutamiento DDR[6] convergerá tan pronto como la pérdida de la conectividad sea detectada por el protocolo de enrutamiento que utilizamos en el enlace principal.

[6] Enrutamiento de llamada bajo demanda.

Como desventaja, si no se detectase el fallo de enlace principal, la interfaz de respaldo nunca desencadenará la llamada de backup[7].

- *La confiabilidad de la respuesta al fallo.*

El sistema dispondrá del ancho de banda necesario valiéndose del uso de los 30 canales de los primarios RDSI trabajando simultáneamente, lo que nos dará anchos de banda de 2 Mbps.

Como desventaja, en caso de que no se levantan alguno de los canales configurados, dispondremos de menor ancho de banda del que teníamos en la situación del enlace principal. Esto afectará al rendimiento total, tanto del tráfico operativo como el que intercambian los protocolos de enrutamiento y enlace.

- *La estabilidad de la llamada telefónica.*

El interfaz de respaldo se mantendrá continuamente en fase de espera. La correcta configuración del enrutamiento DDR establecerá en qué condiciones se establecerán las llamadas. Si hay que procesar tráfico interesante que deba lanzar las llamadas RDSI de los enlaces de respaldo; de la misma manera que se colgarán esas llamadas pasado un tiempo sin utilización del enlace. Es una gran ventaja a nivel económico ya que sólo se activará la línea de respaldo cuando el tráfico así lo requiera.

- *La capacidad de testar el enlace.*

La prueba de la conexión de la línea de respaldo puede requerir entrar en modo de configuración en el enrutador remoto, teniendo que modificar la configuración para testar el enlace de respaldo, para después volver a restaurar la configuración. Este procedimiento, desde un puesto de vista de seguridad y operativa es un riesgo, ya que la mala praxis puede desembocar en una interrupción del tráfico de producción.

Una ventaja de la solución elegida es que un simple comando ping es lo único necesario para testar el enlace de respaldo. No se requiere ningún privilegio en el enrutador para realizarlo, ni el tráfico de producción puede verse afectado, además las pruebas se pueden automatizar.

- *El rendimiento del enlace.*

El interfaz de respaldo tiene la ventaja de que el enlace primario RDSI que utiliza puede ser usando para realizar la llamada al enrutador destino y también para el aumento del ancho de banda. Incluso se puede usar el enrutamiento DDR para levantar la línea de respaldo sobre múltiples enlaces primarios.

- *La facilidad de implementación.*

La implementación de los interfaces de respaldo es trivial por lo que no se requieren excesivas habilidades ni conocimientos para realizarla. Esto puede ser una desventaja ya que esa sencillez podría ocultar problemas de funcionalidad de la solución. Por ejemplo, los usuarios de enlaces F*rame Relay* deben configurar mensajes *keepalive*[8] extremo a extremo para evitar el tiempo de caída por fallos típicos de este tipo de enlaces. En el caso del uso de enrutamiento DDR es más compleja la configuración para que funcione de una forma fiable, ya que la línea por defecto no estará activa.

[7] Backup y respaldo se usan indistintamente a lo largo del documento.
[8] Son mensajes que se envían para mantener activa la línea.

1.3 Descripción del proyecto.

Con este proyecto se pretende desarrollar el estudio y diseño de una solución de conectividad alternativa a la WAN principal, para salvar el tráfico de datos y voz de una sede remota que pierda acceso a la WAN. Se utilizará la infraestructura RDSI existente para lograr este fin. Asimismo, se hará uso de las facilidades del enrutamiento sobre protocolo IP, tanto estático como dinámico.

Como hemos indicado en el apartado anterior, la red de respaldo propuesta se basará en conexiones RDSI que se lanzarán automáticamente desde la sede central cuando cualquier sede remota se quede aislada de la WAN principal. El número de canales que se levanten dependerá el tráfico y tipo de sede y se utilizarán las facilidades del enrutamiento dinámico en la red de interconexión con la WAN para hacer converger el tráfico por el camino alternativo vía RDSI.

La sede central será la que tiene la inteligencia para desencadenar las acciones necesarias para conectar con la sede remota, por lo tanto, será la única que dispondrá de una solución redundante de conectividad con la operadora.

El siguiente esquema muestra a alto nivel la arquitectura planteada donde podemos ver dos sistemas de conexión paralelo: uno principal y uno de respaldo:

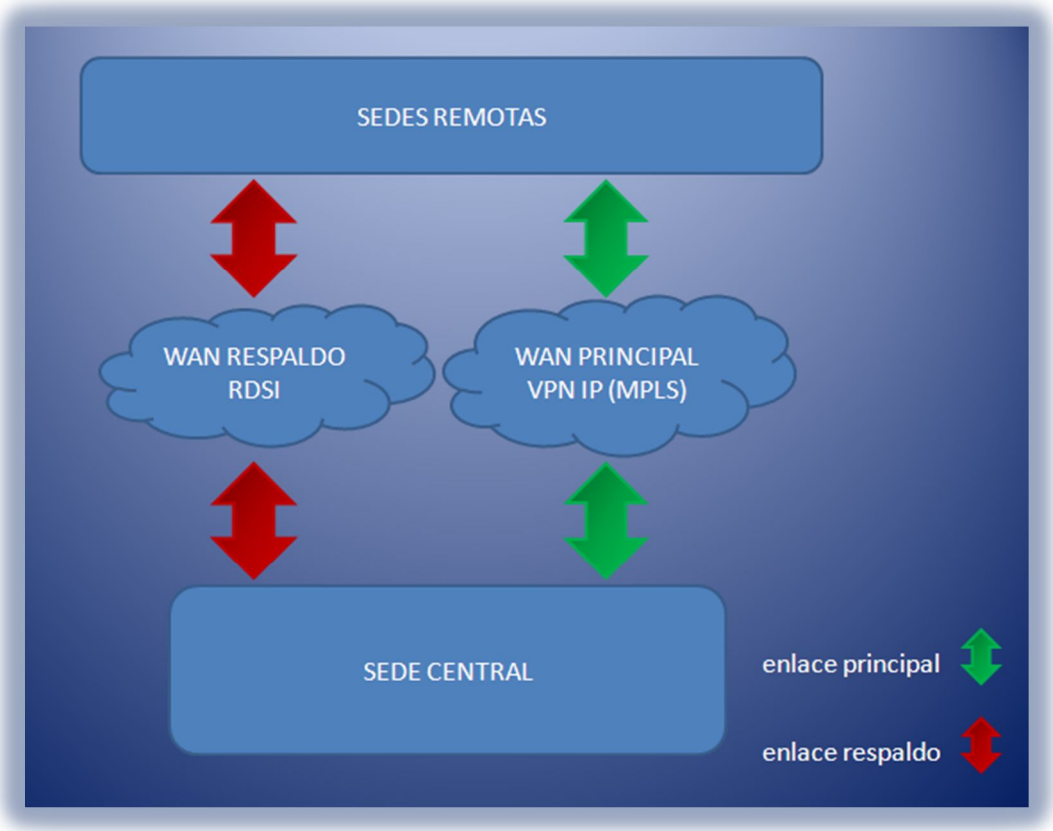


Figura 2. Esquema genérico del proyecto.

El estudio de la solución que plantea el proyecto recorrerá distintas tareas que al final complementen una definición de especificaciones de hardware y configuraciones que se adapten a la solución buscada. La red WAN de respaldo será una red real y aplicable en cualquier empresa que precise de una solución de conectividad similar.

El objetivo de la WAN de respaldo será garantizar el 75-100% del servicio haciendo un cálculo del promedio de uso de la red. Para ello nos valdremos para ello de la información que podamos extraer de los gestores de ancho de banda.

El análisis de las tecnologías de enrutamiento IP y de distintos dispositivos tales como enrutadores, gestores de ancho de banda, centralita nos permitirán conformar una estructura que cubra las necesidades de disponibilidad, rendimiento y redundancia de la WAN secundaria.

SEGUNDA PARTE: ¡NECESITAMOS UN PLAN!

2 PLANIFICACIÓN DEL PROYECTO

El trabajo que comprenderá el proyecto se desarrollará en 121 días, coincidiendo con el inicio de cuatrimestre y finalizando con la fecha de la entrega de la presentación del proyecto, que es la última a efectuar.

Los apartados principales en los que se desglosa el plan de trabajo son:

1. Decisión del proyecto

En este primer apartado se decidirá y definirá el proyecto sobre el que se va a trabajar, haciendo una descripción de la solución a adoptar que se pretende y estableciendo los objetivos a alcanzar.

2. Planificación del proyecto

Engloba todas las tareas e hitos a realizar que se plantean necesarios para acometer con éxito el proyecto. Se realizará un diagrama de Gantt donde se visualizará de una forma cronológica las distintas acciones que se vayan desarrollando durante la vida del proyecto.

3. Estudio técnico

3.1. Análisis de situación actual

El trabajo en este punto consistirá en realizar una foto de la arquitectura de red existente en la empresa, tanto de la sede central como de las distintas sedes remotas, para acceder a la WAN.

3.2. Diseño de la solución

Con todos los datos en la mano se deberá realizar un estudio de la tecnología que se va a proponer para lograr el objetivo. Una vez definido se investigará sobre el hardware necesario para implementar la solución. Con todo ello se obtendrá la propuesta tecnológica a implementar.

4. Estudio económico

Se debe concretar la cantidad de material que se debe adquirir y el precio que se debería desembolsar.

5. Laboratorio de pruebas

Se montará un laboratorio de pruebas donde se intentará emular la solución propuesta. Estas pruebas se realizarán en base a un plan previamente establecido y se justificarán los resultados de la manera más clara posible.

6. Entregables finales de proyecto

Esta última fase se dedicará a revisión de toda la información obtenida durante el proyecto para la realización de la memoria final y la presentación del proyecto.

A continuación presentamos el desglose de tareas con sus periodos de aplicación y su duración asignada:

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 de la memoria	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

Tabla 1. Plan de trabajo.

2.1 Diagrama de Gantt.

A continuación presentamos el diagrama de Gantt donde se pueden comprobar las tareas e hitos a alto nivel con sus periodos de ejecución:

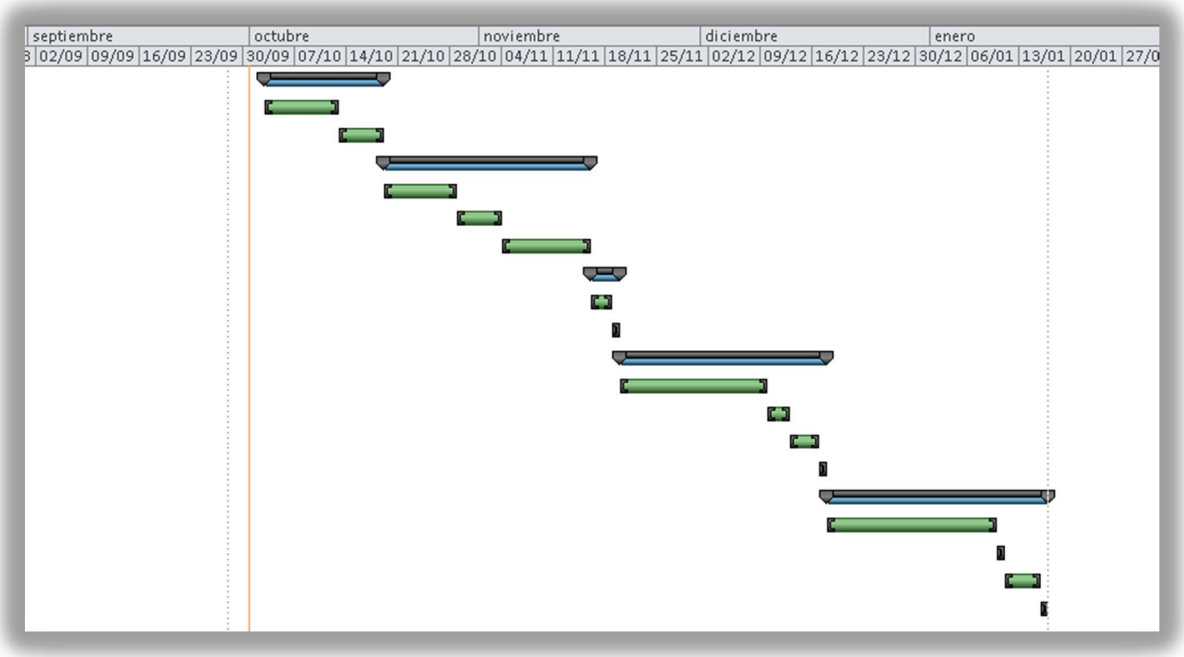


Figura 3. Diagrama de Gantt.

TERCERA PARTE: ¿QUÉ TENEMOS AHORA?

3 ESTUDIO TÉCNICO

En este apartado se hará un análisis detallado de la situación actual de la red empresarial, haciendo hincapié en la conexión de acceso a la red WAN. Se definirá un esquema de red que permita asimilar de una manera clara la estructura de la red en las distintas sedes. Se estudiarán su direccionamiento, las tablas de enrutamiento de los dispositivos actuales y se hará un cálculo medio de uso de los enlaces hacia la WAN para poder dimensionar la WAN de respaldo. Finalmente serán descritos los elementos hardware involucrados en la red.

3.1 Análisis de la WAN Corporativa.

La WAN corporativa interconecta las distintas redes de la empresa a través del servicio VPN-IP contratado a una operadora de ámbito estatal. Este servicio VPN-IP se apoya en una infraestructura IP que está basada en tecnología MPLS.

Este sistema facilita la creación de redes privadas virtuales, que de cara a una empresa sería como conectar sus sedes en una red privada independiente, con la posibilidad de aumentar el rendimiento y con un coste más bajo.

Además este servicio permite establecer distintas calidades de tráfico adaptando los caudales a las necesidades concretas del usuario:

- *Prioritario*
  Tráfico crítico.
- *Normal*
  Tráfico corriente en la empresa.
- *Multimedia*
  Pensado para transmisión de voz sobre IP.

La WAN contratada a la operadora se basa en 3 elementos fundamentales:

1. *El tipo o **método de acceso** a la red MPLS del proveedor de acceso.*
   La arquitectura de acceso a la WAN de la operadora permite el acceso a través de xDSL, ATM, Frame Relay, Ethernet, etc. Este último será el medio elegido para interconectar todas las sedes. Enlaces de fibra a 1 Gbps hacia el punto de interconexión de la WAN de la operadora.

2. *El **equipamiento** (CE[9]) que conecta la red de usuario con el proveedor.*
   Concretamente el CE es un Cisco Catalyst 3560-V2.En la sede central se instalan dos equipos con el rol de enrutador WAN primario y enrutador WAN secundario o de backup.

[9] Customer Edge.

En el resto de sedes se monta un único enrutador para conectar con la WAN de la operadora.

3. ***Tipos de servicio y anchos de banda*** *necesarios en cada sede.*
   El estudio de necesidades de tráfico de aplicaciones que se realizó antes de la migración dio como resultado las necesidades de cada sede. Por tanto, se contrataron caudales superiores en previsión de futuras necesidades.

Presentamos los siguientes cuadros donde se presentan esquematizados los datos que muestran la asignación de los 3 elementos por cada tipo de sede: la sede central y las sedes remotas.

SEDE CENTRAL		
Método de acceso	Fibra Ethernet 1Gbps	
Equipamiento	2 x Cisco Catalyst 3560-v2	
Tipos de servicio y anchos de banda	Normal (datos)	50 Mbps
	Multimedia (voz)	5 Mbps

Tabla 2. Servicio WAN para sede central.

SEDES REMOTAS		
Método de acceso	Fibra Ethernet 1Gbps	
Equipamiento	1 x Cisco Catalyst 3560-v2	
Tipos de servicio y anchos de banda	Normal (datos)	5 Mbps
	Multimedia (voz)	5 Mbps

Tabla 3. Servicio WAN para sedes remotas.

Estos valores contratados se basan en un estudio de tráfico de las aplicaciones y en el momento de mayor uso de la red. Al valor obtenido se le incremento un porcentaje para tener un ancho de banda holgado en previsión de aumentos de necesidades a corto plazo.

3.1.1 Mapa Conceptual.

Una vez expuestas las particularidades de la red WAN presentamos una foto global de la situación actual de la red. Tenemos 10 sedes que se interconectan entre ellas y con una sede central a través de la red MPLS de la operadora, la que nos facilita la comunicación en base a unos criterios de tipologías tráfico y ancho de banda contratada para cada una de ellas en cada sede.

En cada sede se cuenta con un enrutador WAN propiedad de la operadora, ubicado en el propio CPD de la sede y conectado por un lado a la red LAN y por otro mediante fibra al punto de presencia de la operadora (llamado POP) en el edificio.

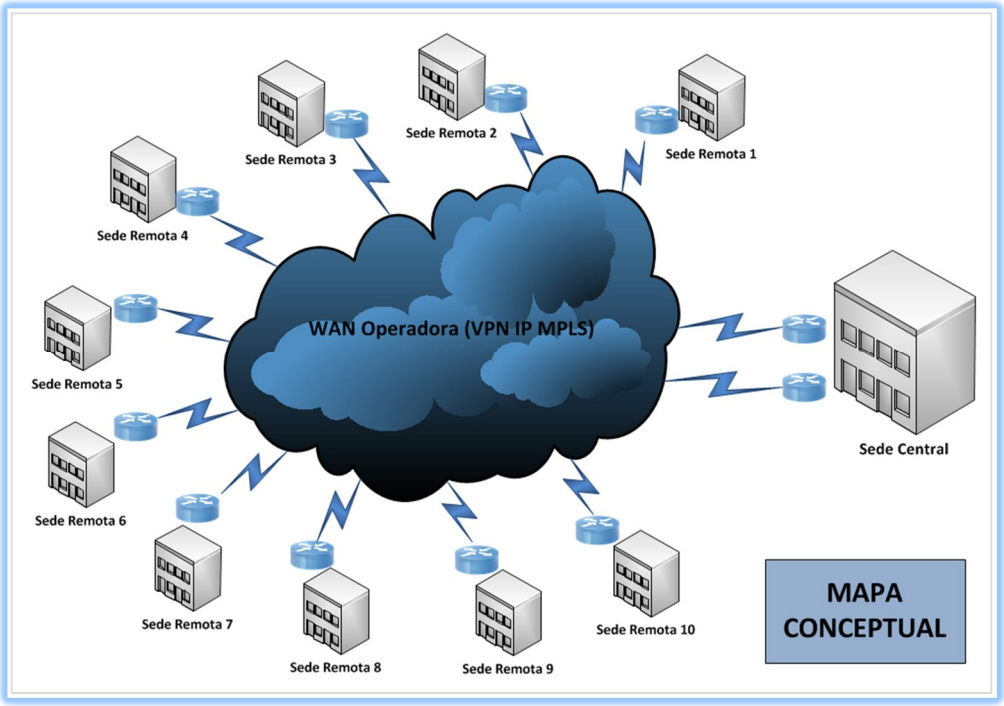


Figura 4. Esquema de red actual.

3.2 Análisis de la sede central.

La sede central es la ubicación más importante de toda la infraestructura de red de la empresa. En ella se albergan los sistemas más críticos de la organización de los que se nutren las sedes remotas así como aquellos sistemas de gestión centralizada. Tales como:

- Correo electrónico.
- Servidores DNS, LDAP, FTP, etc.
- Acceso a Internet.
- Aplicaciones y BBDD corporativas.
- Videoconferencia.
- Servidores de gestión de logs y alertas.
- Servidores de control de red vía SNMP.
- Otros.

Dispone de una red LAN para dar servicio de voz y datos a 300 usuarios y de una DMZ donde tiene ubicados aquellos servicios accesibles desde el exterior, en concreto desde Internet:

- Servidor HTTP con la página web empresarial.
- Servidores de aplicaciones.

- Servidor SMTP de correo electrónico.
- Servidores DNS públicos.
- Servidor proxy Internet.
- Nodos de acceso VPN-SSL.
- Otros.

La sede central es la red más grande y más importante de toda la malla empresarial. Está compuesta por 3 equipos cortafuegos que enrutan y protegen el tráfico:

1. EL cortafuegos bastión controla los accesos y ataques a la DMZ[10].
2. El cortafuegos interno controla el tráfico entre la DMZ y las redes o VLANs[11] de CPD[12] donde están los servidores internos de la empresa.
3. EL cortafuegos WAN controla las conexiones que se producen desde/hacia otras sedes y desde/hacia las propias redes o VLANs de usuarios o servidores del CPD.

La arquitectura cuenta con dos enrutadores para acceso a la WAN de la operadora. Un equipo hace de primario y otro de secundario. Son equipos que presentan una única IP hacia la red de la sede. Esto lo consiguen utilizando un protocolo propietario llamado HSRP[13] que hace un chequeo de comunicación a través de sus interfaces para saber que el otro enrutador está activo y que facilita que automáticamente el secundario se ponga activo cuando el primario falle.

Ambos enrutadores WAN conocen todo el direccionamiento de las distintas sedes remotas y sede central. Cuando desconocen un destino entregan el tráfico en el salto de entrada en la sede central, es decir, su cortafuegos WAN. En el resto de sedes esta forma de operar será distinta. Se comentará en el apartado siguiente.

La sede central cuenta con una centralita que da servicio tanto a teléfonos IP como a teléfonos tradicionales. A esta centralita están conectadas, por un lado, las VLANs que dan servicio de voz a los usuarios, y por otro lado, un cable directo que conecta al enrutador WAN para dar el servicio de telefonía IP entre las sedes y en la propia sede central.

La centralita dispondrá de varios primarios conectados a la infraestructura de la operadora (PSTN[14]) para cursar llamadas de voz y de datos a través del exterior.

El diagrama siguiente presenta el mapa de red de las sedes remotas. Aquí podemos identificar claramente lo expuesto anteriormente:

[10] Zona desmilitarizada es la ubicación en la LAN que ofrece servicios a la red pública o Internet.
[11] Segmentos de red LAN (nivel 2 OSI).
[12] Centro de proceso de datos.
[13] Hot Standby Redundancy Protocol.
[14] Red telefónica pública.

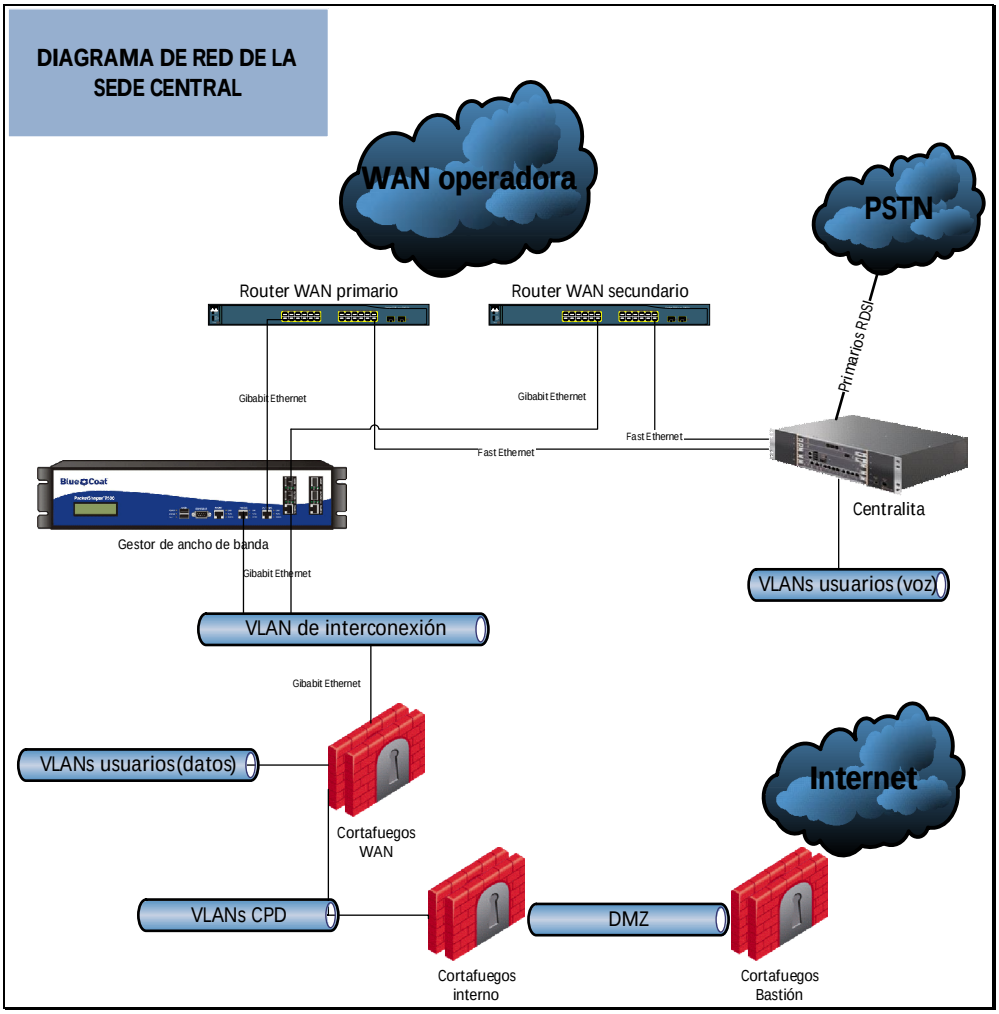


Figura 5. Mapa actual de la sede central.

El cuadro siguiente muestra el mapa de direccionamiento de la red de la sede central. En ella aparecen los elementos existentes en la red. Se utilizan subredes de clase C para la red de interconexión, que aunque nos da 254 hosts y puede parecer excesivo, nos permite escalar dentro de esa subred sin temor a quedarse sin direcciones IP. Vemos que la red LAN está formada por una subred de clase B que aparece sumarizada, ya que luego internamente la subred se subdivide en otras más pequeñas según las necesidades y así direccionar las distintas VLANs que se vayan a usar.

Direccionamiento sede central		
Datos	VLAN de interconexión	192.170.0.0/24
	Router WAN primario	192.170.0.252
	Router WAN secundario	192.170.0.253
	Cortafuegos WAN	192.170.0.3
	DMZ	192.224.177.0/27
	Resto LAN de datos	172.16.0.0/16
Voz	Conexión centralita-router WAN	192.171.0.0/24
	Router WAN	192.171.0.252
	Centralita	192.171.0.100
	Resto LAN de voz	172.17.0.0/16

Tabla 4. Direccionamiento IP sede central.

Por otra parte, se hace imprescindible conocer la configuración de enrutamiento que hay en los distintos dispositivos que conforman la estructura de la VLAN o red de interconexión WAN. Conocer el detalle de estas tablas de enrutamiento es esencial, principalmente para controlar que el tráfico que quiera llegar a cualquier destino de la red empresarial tiene un camino por el que discurrir hacia el destino.

El siguiente cuadro muestra las partes esenciales de la tabla de enrutamiento de los equipos que interactúan con el acceso a la WAN:

1. *El cortafuegos WAN* que es responsable de pasar el tráfico de la LAN a la WAN y viceversa.
2. *La centralita* para el uso de la telefonía, IP y no IP.
3. Y finalmente *el enrutador WAN* que debe conocer los segmentos de red e cada sede y saber encaminarlos.

Importante recordar que la WAN de la operadora entrega todo el tráfico de cualquier sede que no conoce en el cortafuegos WAN de la sede central. Por ello, este cortafuegos debe conocer y tener medios para poder dirigir el tráfico por algún medio hacia el destino solicitado. De hecho, éste es el punto clave del proyecto.

En el caso de la sede central también se enruta el tráfico hacia la DMZ a través de otro cortafuegos. Por ejemplo, las conexiones al proxy de salida a Internet ubicado en esta zona desmilitarizada.

Comentar que la tabla indica la subred de la LAN de usuarios de datos de manera sumarizada[15]. A nivel 2 OSI[16] se dividiría en varias subredes más pequeñas pertenecientes cada una a un sub-interface del cortafuegos WAN.

Enrutamiento en interconexión WAN en la sede central

	Destino	Máscara de red	Salto	Interface / VLAN
Router WAN	0.0.0.0 (ruta por defecto)	0.0.0.0	192.170.0.3	Gigabit Ethernet 1 / VLAN interconexión
	192.170.0.0	255.255.255.0	Directamente conectada	Gigabit Ethernet 1 / VLAN interconexión
	192.171.0.0	255.255.255.0	Directamente conectada	Fast Ethernet 0
	192.224.177.0	255.255.255.224	192.170.0.3	Gigabit Ethernet 1 / VLAN interconexión
	172.16.0.0	255.255.0.0	192.170.0.3	Gigabit Ethernet 1 / VLAN interconexión

	Destino	Máscara de red	Salto	Interface
Cortafuegos	0.0.0.0 (ruta por defecto)	0.0.0.0	192.170.0.252	Gigabit Ethernet 1 / VLAN interconexión
	192.170.0.0	255.255.255.0	Directamente conectada	Gigabit Ethernet 1 / VLAN interconexión
	192.224.177.0	255.255.255.224	192.16.0.50	Gigabit Ethernet 2 / VLAN interconexión DMZ
	172.16.0.0	255.255.0.0	Directamente conectada	Gigabit Ethernet 3-8 / varias VLANs (usuarios y CPD)

	Identificador	Salto	Interface	Descripción
Centralita	Ruta 51	192.171.0.252	Fast Ethernet 0	Telefonía interna IP
	Ruta 1		tarjetas primario a operador	Telefonía externa PSTN

Tabla 5. Enrutamiento interconexión WAN en la sede central.

Los gestores de ancho de banda analizan el tráfico de datos que se envía y se recibe de la WAN. El tráfico de voz no cruza estos dispositivos ya que hay suficiente ancho de banda para realizar las comunicaciones de telefonía IP. Recordemos que la centralita está conectada por un cable directo a un puerto del enrutador WAN. Esto es así en la sede central y en el resto de sedes.

[15] Se usan subredes que engloben otras subredes de orden menor.
[16] Modelo de interconexión de sistemas abiertos.

Para poder valorar el caudal mínimo necesario que ha de cubrir la solución WAN de respaldo se ha realizado un análisis de tráfico de 3 días consecutivos, y el gestor de ancho de banda a dado los resultados que se pueden apreciar en la siguiente gráfica:

Figura 6. Promedio de tráfico de entrada a la sede central.

De la misma forma, a continuación se presenta la misma gráfica pero con el tráfico proveniente de la WAN que ha cruzado el gestor de ancho de banda.

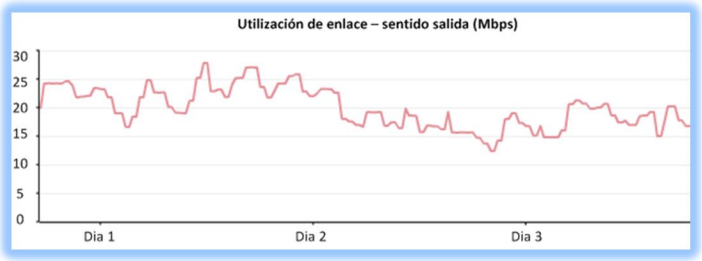


Figura 7. Promedio de tráfico de salida de la sede central.

Podemos concluir que los enlaces WAN hacen un uso medio, sin contar los picos de tráfico, de unos 30Mbps en los momentos de más uso y alrededor de 15 Mbps cuando menos.

3.3 Análisis de las sedes remotas.

Las sedes remotas disponen de una infraestructura de red más reducida puesto que tienen que dar servicio a un número de usuarios no mayor de 200. Estas sedes se surten de los servicios centralizados en la sede central aunque también disponen de servicios ubicados localmente en ellas. Por ejemplo:

- Controlador de dominio Microsoft Windows (Active Directory)
- Servidores de aplicaciones y BBDD locales
- Servidores de gestión de red (electrónica de red, cortafuegos, etc)
- Servidor NTP para sincronización horaria.
- Servidores para aplicaciones conectadas a BBDD de la sede central
- Otros

Respecto a su arquitectura de red, si realizamos un barrido desde el interior de la red LAN hacia la interconexión con la red WAN nos encontraremos con diversas VLANs o segmentos de usuarios y una correspondiente al CPD, donde se albergan los servidores. Todas ellas están protegidas y comunicadas a través de un cortafuegos que da acceso a la VLAN de interconexión con los dispositivos que dan acceso a la WAN.

Paralelamente se dispone de una centralita a la que están conectadas, por un lado, las VLANs que dan servicio de voz a los usuarios, y por otro lado, un cable directo que conecta al enrutador WAN para dar el servicio de telefonía IP entre las sedes. En estos segmentos de usuarios de voz estarán incluidos mayormente los teléfonos.

La centralita dispondrá de varios primarios conectados a la infraestructura e la operadora para cursar llamadas de voz y de datos a través del exterior.

El diagrama siguiente presenta el mapa de red de las sedes remotas. Aquí podemos identificar claramente lo expuesto anteriormente:

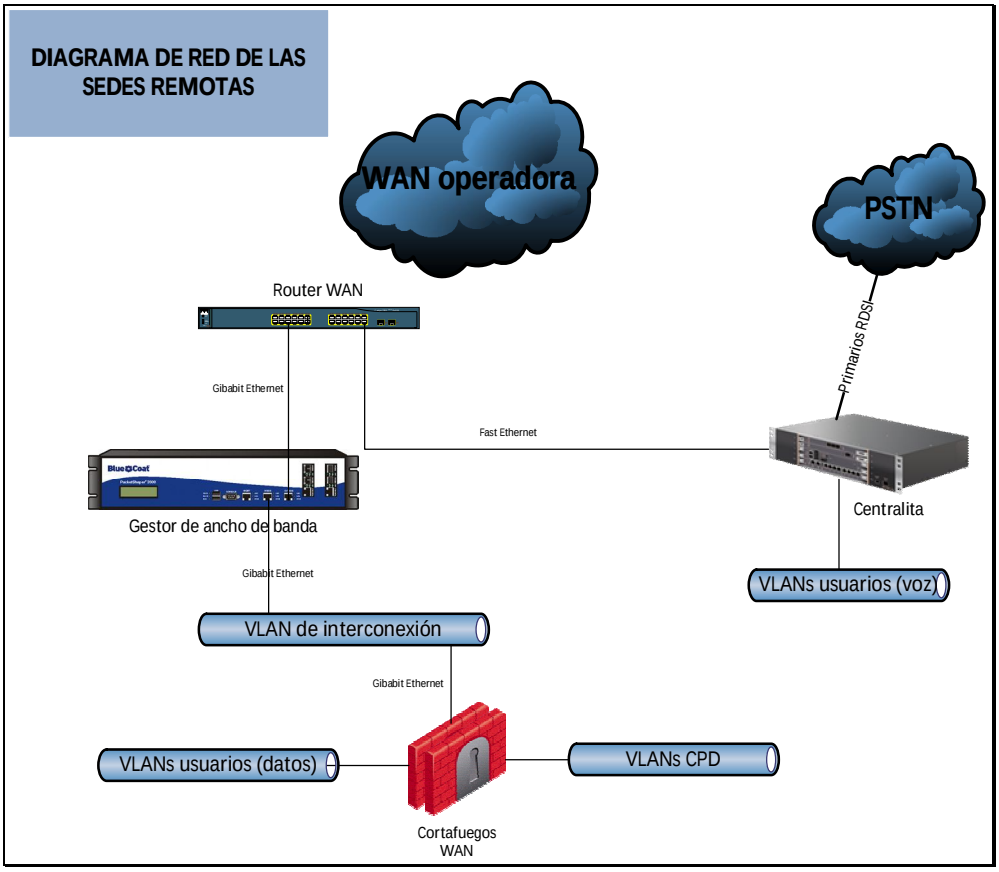


Figura 8. Mapa actual de las sedes remotas.

El cuadro siguiente muestra el mapa de direccionamiento de la red de las diez sedes remotas. Se ha querido detallar principalmente la parte del segmento de red que interconecta con la WAN, que es donde se van a desarrollar todas las tareas de la solución propuesta. El resto de la LAN de usuarios y de voz sólo participa como subredes que han de ser accesibles desde cualquier punto de la malla de red empresarial, tanto por la vía de la WAN principal como por la de la WAN de enlaces RDSI.

Direccionamiento sedes remotas

		Sede 1	Sede 2	Sede 3	Sede 4	Sede 5
Datos	VLAN de interconexión	192.170.1.0/24	192.170.2.0/24	192.170.3.0/24	192.170.4.0/24	192.170.5.0/24
	Router WAN	192.170.1.252	192.170.2.252	192.170.3.252	192.170.4.252	192.170.5.252
	Cortafuegos WAN	192.170.1.3	192.170.2.3	192.170.3.3	192.170.4.3	192.170.5.3
	Resto LAN de datos	172.21.0.0/17	172.22.0.0/17	172.23.0.0/17	172.24.0.0/17	172.25.0.0/17
Voz	Conexión centralita-router WAN	192.171.1.0/24	192.171.2.0/24	192.171.3.0/24	192.171.4.0/24	192.171.5.0/24
	Router WAN	192.171.1.252	192.171.2.252	192.171.3.252	192.171.4.252	192.171.5.252
	Centralita	192.171.1.100	192.171.2.100	192.171.3.100	192.171.4.100	192.171.5.100
	Resto LAN de voz	172.21.128.0/17	172.22.128.0/16	172.23.128.0/17	172.24.128.0/17	172.25.128.0/17

		Sede 6	Sede 7	Sede 8	Sede 9	Sede 10
Datos	VLAN de interconexión	192.170.6.0/24	192.170.7.0/24	192.170.8.0/24	192.170.9.0/24	192.170.10.0/24
	Router WAN	192.170.6.252	192.170.7.252	192.170.8.252	192.170.9.252	192.170.10.252
	Cortafuegos WAN	192.170.6.3	192.170.7.3	192.170.8.3	192.170.9.3	192.170.10.3
	Resto LAN de datos	172.26.0.0/17	172.27.0.0/17	172.28.0.0/17	172.29.0.0/17	172.30.0.0/17
Voz	Conexión centralita-router WAN	192.171.6.0/24	192.171.7.0/24	192.171.8.0/24	192.171.9.0/24	192.171.10.0/24
	Router WAN	192.171.6.252	192.171.7.252	192.171.8.252	192.171.9.252	192.171.10.252
	Centralita	192.171.6.100	192.171.7.100	192.171.8.100	192.171.9.100	192.171.10.100
	Resto LAN de voz	172.26.128.0/17	172.27.128.0/17	172.28.128.0/17	172.29.128.0/17	172.30.128.0/17

Tabla 6. Direccionamiento IP sedes remotas.

Otro punto a tratar es la configuración de enrutamiento que hay en los distintos dispositivos que conforman la estructura de la VLAN o red de interconexión WAN. Conocer el detalle de estas tablas de enrutamiento es esencial, principalmente para controlar que el tráfico que quiera llegar a cualquier destino de la red empresarial tiene un camino por el que discurrir hacia el destino.

El siguiente cuadro muestra las partes esenciales de la tabla de enrutamiento de los equipos que intervienen en la interconexión de las LAN de las distintas sedes, el cortafuegos WAN; de la interconexión para el uso de la telefonía, IP y no IP, como es la centralita y finalmente el propio enrutador WAN que debe conocer los segmentos de red e cada sede y saber encaminarlos.

Comentar que la tabla indica la subred de la LAN de usuarios de datos de manera sumarizada. A nivel 2 OSI se dividiría en varias subredes más pequeñas pertenecientes cada una a un sub-interface del cortafuegos WAN.

Enrutamiento en interconexión WAN en la sede remota 5

	Destino	Máscara de red	Salto	Interface / VLAN
Router WAN	192.170.5.0	255.255.255.0	Directamente conectada	Gigabit Ethernet 1 / VLAN interconexión
	192.171.5.0	255.255.255.0	Directamente conectada	Fast Ethernet 0
	172.25.0.0	255.255.128.0	192.170.5.3	Gigabit Ethernet 1 / VLAN interconexión

	Destino	Máscara de red	Salto	Interface
Cortafuegos	0.0.0.0 (ruta por defecto)	0.0.0.0	192.170.5.252	Gigabit Ethernet 1 / VLAN interconexión
	192.170.5.0	255.255.255.0	Directamente conectada	Gigabit Ethernet 1 / VLAN interconexión
	172.25.0.0	255.255.128.0	Directamente conectada	Gigabit Ethernet 2-8 / varias VLANs (usuarios y CPD)

	Identificador	Salto	Interface	Descripción
Centralita	Ruta 51	192.171.5.252	Fast Ethernet 0	Telefonía interna IP
	Ruta 1		tarjetas primario a operador	Telefonía externa PSTN

Tabla 7. Enrutamiento interconexión WAN en la sede remota 5.

El análisis de tráfico actual en los gestores de ancho de banda nos presenta el uso medio de caudal de tráfico que se realiza en las sedes remotas. Se ha recogido los datos de aquella sede de mayor tránsito para, a partir de ahí, realizar un cálculo estimativo de las necesidades de tráfico real de las distintas sedes.

El gráfico siguiente muestra la media en 3 días consecutivos de la cantidad de tráfico enviado hacia redes que no forma parte de la red remota. Por lo tanto, es tráfico que cursa hacia la WAN.

Figura 9. Promedio de tráfico de entrada a una red remota.

De la misma forma, a continuación se presenta la misma gráfica pero con el tráfico proveniente de la WAN que ha cruzado el gestor de ancho de banda.

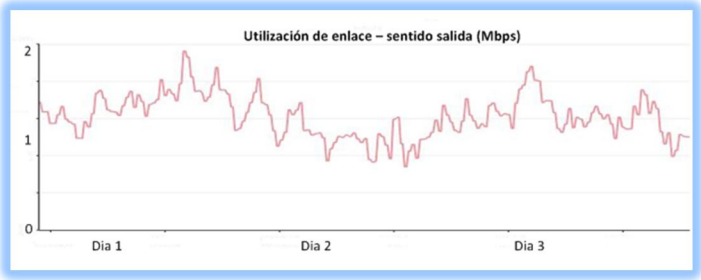


Figura 10. Promedio de tráfico de salida de una red remota.

Podemos concluir que los enlaces WAN hacen un uso medio, sin contar los picos de tráfico, de unos 2 Mbps en los momentos de más uso y de poco más de 1 Mbps cuando menos.

3.4 Análisis de dispositivos.

A continuación realizaremos un barrido informativo del hardware actual en las redes de las sedes. Mostraremos las características fundamentales de cada dispositivo en lo que hace referencia al proyecto, en concreto, su rol en la red.

También se incluirán en el apartado de apéndices los enlaces a las páginas web de los fabricantes donde se puede ampliar la información de las características de cada dispositivo.

3.4.1 Enrutador WAN.

Este equipo es propiedad de la operadora y su gestión y mantenimiento es responsabilidad de ella.

El dispositivo (CE) instalado por la operadora en cada sede es el siguiente:

Figura 11. Cisco Catalyst 3560-V2.

Es un conmutador (nivel 2 OSI) con facilidades de enrutador (nivel 3 OSI) gracias a la versión del software que lleva implementada (Cisco IOS Software Release 12.1(11)EA1 o superior). Por lo tanto implementa las características de un enrutador.

Estos dispositivos deberán conocer la red empresarial a nivel IP para poder enrutar el tráfico entre las sedes.

Físicamente tiene configurados dos puertos: uno para conectar nuestro enlace de datos y otro para conectar nuestro enlace de voz.

3.4.2 Cortafuegos

El equipo cortafuegos que utiliza la empresa es un *appliance*[17] modelo 4400 de la empresa de seguridad CheckPoint. Destacar entre sus características que soportan 5 Gbps de tráfico global, 1.2 millones de sesiones y 40000 conexiones por segundo.

Figura 12. Cortafuegos CheckPoint 4600.

Este equipo es gestionado por la empresa y alberga la política de seguridad de accesos entre redes. De otra manera dicha, controla quién (direcciones IP) puede acceder hacia dónde (direcciones IP) y a qué (protocolo o servicio) y le permite o deniega el acceso.

Está montado en alta disponibilidad con dos equipos, uno activo y uno pasivo, los cuales se sincronizan a través de un sistema propietario llamado *ClusterXL*. Estos dispositivos son los enrutadores principales de la red, por consiguiente, reencaminar el tráfico dirigido al exterior de la red hacia el enrutador WAN.

Cuentan con un sistema de enrutamiento avanzado que permite implementar soluciones de protocolos de enrutamiento dinámico como son RIP, OSPF, PIM, etc.

3.4.3 Gestor de Ancho de Banda

Este equipamiento es el responsable de controlar el uso del ancho de banda de las distintas aplicaciones y usuarios (direcciones IP) que conforman las distintas redes de cada sedes de la red.

[17] Dispositivo enracable que conjunta hardware y software de propósito específico.

Este elemento se introduce en la red situándolo en el camino por el que pasa el tráfico de la red. La instalación es simple ya que sería como cortar el cable en dos y conectarlo a equipo en sus puertos de entrada y salida.

Por defecto es capaz de visualizarlo y categorizarlo sin afectar a su discurrir. Pero una vez que se define y se aplica una política de uso de ancho de banda dará más prioridad a las aplicaciones o IPs que se hayan definido en su política.

En las sedes remotas nos encontramos el modelo 3500 que entre sus características más importantes está que soporta 60000 flujos (40000 TCP y 20000 UDP) y que puede identificar hasta 512 tipos de tráfico distintos.

Tiene contratada con el fabricante una licencia para gestionar 10 Mbps de tráfico.

Figura 13. Bluecoat Packetshaper 3500.

En la sede central hay un equipo de mejores prestaciones, el modelo 7500, el cual tiene la funcionalidad de soportar hasta 300000 flujos IP e identificar 1024 clases de servicio.

Este dispositivo tiene una licencia para poder gestionar hasta los 100 Mbps de tráfico.

Figura 14. Bluecoat Packetshaper 7500.

Ambos equipos soportan la inclusión de dos tarjetas de expansión LEM (LAN Expansión Module) para gestionar el tráfico de otros segmentos de red. Será un elemento clave de nuestra solución.

3.4.4 Centralita

Las distintas sedes cuentan con sistemas de telefonía modelo MX-ONE Lite de la marca Aastra.Esta centralita está diseñada para soportar principalmente extensiones IP y accesos RDSI. Ocupa el espacio de 3U en un armario de comunicaciones. Vemos una imagen de la centralita:

Figura 15. Centralita Aastra MX-ONE Lite.

Proporciona un conmutador que permite la conexión de tarjetas para la conexión de terminales y redes no IP como pueden ser las extensiones analógicas, digitales, enlaces BRI RDSI y enlaces analógicos.

Dispone de una tarjeta llamada MGU (Media Gateway Unit) que cuyas características más destacadas son:

- Puertos Ethernet redundantes. Cualquiera de los dos puertos Ethernet soporta señalización y media.
- (8 x PRI[18] (RDSI E1/T1).
- Extensiones móviles.
- Extensiones IP (H.323).
- Extensiones IP (SIP, incluyendo IP DECT y Wi-Fi).
- Enlaces IP (H.323, SIP).
- IP networking con otras PBXs.
- QSIG networking con otras PBXs.
- Softphone.
- 3 posiciones disponibles para tarjetas.

Esta centralita da servicio de voz sobre IP a las distintas sedes. Cuando la red IP falla se conmuta para usar la telefonía a través de los primarios RDSI contratados con la operadora y que salen por la red pública de telefonía (PSTN).

[18] Enlaces primario RDSI.

CUARTA PARTE: ¿QUÉ NECESITAMOS?

4 DISEÑO DE LA SOLUCIÓN

4.1 Tecnologías a emplear.

En este apartado definimos las tecnologías de las que nos vamos a valer para llevar a cabo el proyecto: ¿de qué manera nos vamos a conectar?, ¿qué protocolos van a servir para reencaminar el tráfico?, ¿qué dispositivos se adaptan a nuestras necesidades?.

También establecemos el hardware que necesitaremos para hacer el despliegue de la solución.

4.1.1 Método de acceso a la WAN de respaldo.

Como se comentó en la introducción, se ha decido usar la tecnología RDSI por encima de otras tecnologías de enlace como xDSL, punto a punto, vía satélite, etc, debido a que la empresa ya tiene desplegada en todas sus sedes una arquitectura basada en enlaces primarios RDSI y además cuenta con la gestión de la centralita de cada sede a la que están conectados directamente los primarios que tiene contratados con la operadora de telefonía.

4.1.1.1 RDSI.

La red digital de servicios integrados (RDSI o ISDN) es una tecnología WAN orientada a conexión que usa la telefonía digital para digitalizar vos , datos, video y otro tipo de información a través de la línea telefónica existente. Actualmente, muchas operadoras telefónicas ofrecen RDSI como servicio de suscripción digital a los usuarios para el acceso a Internet, las llamadas telefónicas de voz y la videoconferencia. El resultado de la creación de una red RDSI es la capacidad de los dispositivos RDSI de realizar llamadas de teléfono a través de la red de la portadora telefónica que lleva muchos tipos de datos. Podemos decir que la RDSI es un modem digital que puede transportar muchos tipos de datos.

Los dispositivos que se conectan a la red RDSI son terminales. Los dos tipos de terminales son los que comprenden los estándares RDSI, que se denominan equipo del terminal tipo 1 (TE1) y los que preceden a los estándares RDSI, que se denominan equipo del terminal tipo 2 (TE2). Los TE2 se conectan a la RDSI usando un adaptador de terminal (*terminal adapter*, TA). Los TE1 no necesitan TA.

El siguiente paso a la hora de hablar de la red RDSI es conectarse a uno dispositivo de terminación de red tipo 1 (NT1) o de terminación de red tipo 2 (NT2). Los dos tipos de dispositivos de terminación de la red convierten el cable que se utiliza en la red de la portadora telefónica (cuatro hilos) en el cableado más frecuente de uso en las casas y las empresas (bucle local de dos hilos).

En España la operadora telefónica proporciona en NT1; no forma parte del dispositivo RDSI situado en las instalaciones del usuario. EL NT2, que añade funcionalidad de capa de enlace de

datos y de capa de red a un NT, suele utilizarse con dispositivos de Intercambio privado de rama (*Private Branch Exhange*, PBX[19]).

La relación entre estos componentes RDSI se muestra a continuación de forma gráfica.

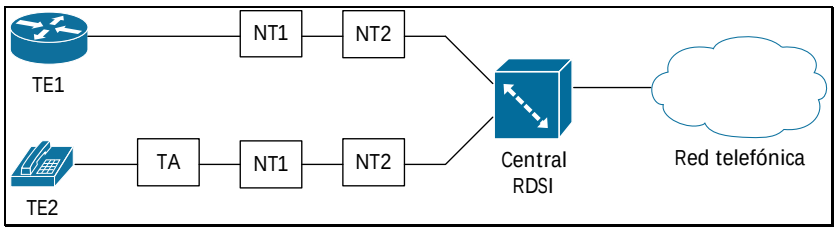


Figura 16. Componentes de una red RDSI.

RDSI ofrece a los dispositivos dos tipos de servicio:

1. Interfaz de acceso básico (*Basic Rate Interface*, BRI)

   Una interfaz RDSI de acceso básico ofrece dos canales B y un canal D (2B+D). El servicio del canal B, que funciona a 64 Kbps full-duplex, se usa para transportar los datos de usuario y no contiene información de señalización. El servicio del canal D, que funciona a 16 Kbps o 64 Kbps full-duplex, transporta la información de señalización entre el usuario y la red. Contiene la señalización para controlar las llamadas asociadas a los canales B. El canal D puede configurarse de manera que transporte datos del usuario en forma de paquetes de baja velocidad.
   Utilizando un único canal B, una interfaz BRI puede transferir datos a 64 Kbps, utilizando 2 canales B puede alcanzar los 128 Kbps. Si además se transfiere datos por el canal D puede llegar a alcanzar tasas de transferencia de 160 Kbps.

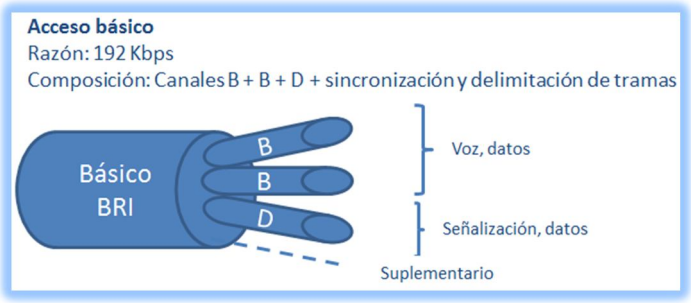


Figura17. Estructura de canal RDSI BRI.

2. Interfaz de acceso primario (*Primary Rate Interface*, PRI)

   El acceso primario PRI está destinado a usuarios con necesidades de más capacidad de transmisión, como oficinas con PBX, LAN o bases de datos. En Europa la velocidad estándar del acceso primario es de 2048 Mbps de la trama E1. Está formado por 30 canales B de 64 Kbps y una canal D de 64 Kbps (30B+D).

[19] Centralita autónoma conectada a la red pública.

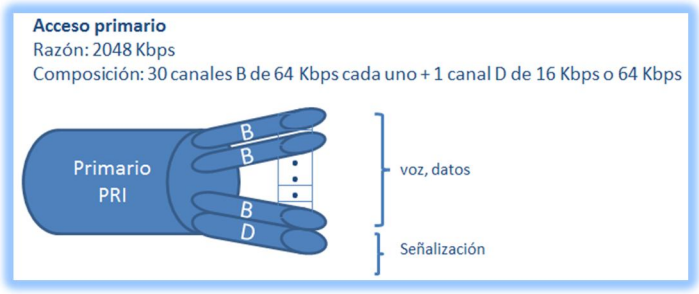


Figura 18. Estructura de canal RDSI PRI.

El proceso de establecimiento de una conexión RDSI se inicia cuando por el canal D, que siempre está activo, se envía el número al que se quiere llamar al conmutador RDSI. Este tráfico del canal D emplea el protocolo de la capa de enlace llamado LAPD, que está basado en HDLC. EL conmutador local utiliza el protocolo SS7 (Sistema de Señalización 7) para establecer la ruta al conmutador de terminación que es quién finaliza la comunicación sobre el canal D en destino.

Una vez establecida esta comunicación, el canal B se conecta en modo extremo a extremo para transmitir voz o datos por cada canal o por todos a la vez.

Los dispositivos conectados deberán finalmente negociar que protocolo de enlace de datos común utilizarán. Un ejemplo puede ser el uso de PPP.

Debido a que en este proyecto se necesita disponer de un ancho de banda suficiente para que las sedes se puedan comunicar ante un fallo de la WAN de la operadora, se utilizarán enlaces primarios PRI. Los interfaces RDSI PRI se proveen en líneas arrendadas T1 o E1. Nos valdremos de la funcionalidad RDSI implementada en los enrutadores llamada DDR (Enrutamiento por llamada telefónica bajo demanda) para poder levantar los enlaces RDSI que gestiona el enrutador cuando éste considere que es necesario. La implementación de este sistema es interesante para enlaces de utilización esporádica, como es el objetivo del proyecto.

DDR es un proceso en el que se define el destino del tráfico para desencadenar la llamada del enrutador RDSI hacia un sitio remoto. Este proceso se resume en los siguientes pasos:

1. El enrutador recibe tráfico, efectúa la búsqueda en sus tablas de enrutamiento para determinar si existe ruta hacia el destino.
2. El enrutador identifica el siguiente salto y realiza la marcación:
    - Si el interface está conectado al destino se envía el tráfico sin marcación y se restablece el temporizador de inactividad.
    - SI el interface no está conectado al destino remoto, el enrutador envía la información de llamada (canal D) al equipo remoto y levanta los canales B que tenga configurados.
    - Una vez que el enlace está activo el enrutador envía todo el tráfico.
    - La llamada finaliza tras alcanzar el tiempo definido de inactividad.

4.1.2 Introducción al enrutamiento IP

Antes de adentrarnos en los temas de enrutamiento haremos una introducción al rol que desempeña un enrutador o enrutador en la red y a lo que son las tablas de enrutamiento.

La función principal de un enrutador es enviar los paquetes hacia sus redes de destino, la dirección IP del destino del paquete. Para ello, un enrutador tiene que buscar en la información de enrutamiento almacenada en su tabla de enrutamiento.

Una *tabla de enrutamiento* es un archivo almacenado en la memoria RAM del enrutador cuya finalidad es almacenar la información de las rutas sobre redes conectadas directamente y redes remotas. La tabla de enrutamiento contiene asociaciones red/siguiente salto que le dicen al enrutador que un destino (identificado por el concepto "red") puede alcanzarse enviando el paquete hacia otro enrutador (que representa el concepto "siguiente salto") en el camino al destino final.

El concepto "red", hablando de redes IP, puede referirse a una red, subred o a un host y el concepto "siguiente salto" puede ser otro enrutador o uno de los interfaces del propio enrutador si este lleva directamente al destino final porque está directamente conectada al enrutador.

Diferenciemos lo que son redes directamente conectadas y redes remotas:

- Una *red directamente conectada* es aquella que está directamente conectada a uno de los interfaces del enrutador. Cuando una de los interfaces del enrutador se configura con una dirección IP y una máscara de subred se convierte en un host de esa red conectada.
- Una *red remota* es aquella que no está conectada directamente al enrutador, por lo tanto, para alcanzarla, el enrutador deberá enviar el tráfico a otro enrutador.

Una vez que está clara esta diferenciación de redes podemos hablar del concepto de tipos de rutas:

- *Rutas directamente conectadas*.
  Son aquellas rutas a redes que de la que forman parte alguno de los interfaces del enrutador.
- *Rutas estáticas*.
  Son rutas a redes que pueden ser configuradas manualmente por el administrador del enrutador.
- *Rutas dinámicas*.
  Son rutas a redes remotas que son aprendidas automáticamente por el enrutador usando un protocolo de enrutamiento dinámico. Algún ejemplo de este tipo de protocolo sería RIP, OSPF, BGP, PIM,...

Cuando el enrutador tiene que decidir qué ruta ha de aplicar a un tráfico con un destino concreto necesita tener un criterio para poder resolver esa situación de decisión. Para concluir definiremos dos conceptos fundamentales del enrutamiento que nos ayudan a solventarlo: la métrica y la distancia administrativa.

- *La métrica.*

Los protocolos de enrutamiento utilizan métricas para determinar qué ruta es la mejor. Hay casos en que un protocolo de enrutamiento aprende más de una ruta al mismo destino. Para seleccionar la mejor ruta, el protocolo de enrutamiento debe poder evaluar y diferenciar entre las rutas disponibles. Para este propósito se utiliza la métrica. Una métrica es un valor que los protocolos de enrutamiento utilizan para asignar los costes de alcanzar redes remotas.

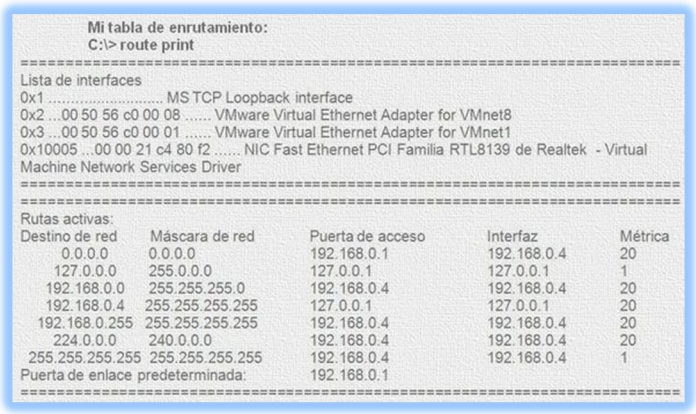
Los diferentes protocolos de enrutamiento utilizan métricas distintas. La métrica utilizada por un protocolo de enrutamiento no es comparable con la de otro protocolo de enrutamiento. Dos protocolos de enrutamiento diferentes pueden elegir rutas distintas al mismo destino debido a que usan unas métricas diferentes.

Las métricas utilizadas en los protocolos de enrutamiento IP son las siguientes:

- Conteo de saltos: es una métrica sencilla que cuenta el número de enrutadores que un paquete debe atravesar para llegar al destino. Es la que usa el protocolo RIP.
- Ancho de banda: influye en la selección de la ruta al preferir la que tiene el ancho de banda más alto. Usada en algunas implementaciones del protocolo OSPF y por EIGRP y IGRP.
- Carga: considera la utilización de tráfico de un cierto enlace. Usado por EIGRP y IGRP.
- Retraso: considera el tiempo que un paquete tarda en atravesar una ruta. Utilizada por el protocolo EIGRP y por el protocolo IGRP.
- Fiabilidad: evalúa la probabilidad de un fallo en el enlace, y se calcula a partir del conteo de errores de un interface o de los fallos anteriores del enlace. Usado por IGRP y EIGRP.
- Coste: es un valor por defecto o determinado a priori por el administrador de la red para indicar la preferencia de una ruta. Por ejemplo usado por IS-IS y OSPF.

La tabla de enrutamiento muestra la métrica para cada ruta dinámica y estática. Los protocolos de enrutamiento determinan la mejor ruta basándose en la ruta con la métrica más baja. Las rutas estáticas siempre tienen la métrica 0 para darles mayor prioridad.

La siguiente imagen muestra la tabla de utas de un PC donde se pueden apreciar los valores de las métricas:



Mi tabla de enrutamiento:
C:\> route print

Lista de interfaces
0x1 ..... MS TCP Loopback interface
0x2 ...00 50 56 c0 00 08 ..... VMware Virtual Ethernet Adapter for VMnet8
0x3 ...00 50 56 c0 00 01 ..... VMware Virtual Ethernet Adapter for VMnet1
0x10005 ...00 00 21 c4 80 f2 ..... NIC Fast Ethernet PCI Familia RTL8139 de Realtek - Virtual Machine Network Services Driver

Rutas activas:

Destino de red	Máscara de red	Puerta de acceso	Interfaz	Métrica
0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.4	20
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.0.0	255.255.255.0	192.168.0.4	192.168.0.4	20
192.168.0.4	255.255.255.255	127.0.0.1	127.0.0.1	20
192.168.0.255	255.255.255.255	192.168.0.4	192.168.0.4	20
224.0.0.0	240.0.0.0	192.168.0.4	192.168.0.4	20
255.255.255.255	255.255.255.255	192.168.0.4	192.168.0.4	1

Puerta de enlace predeterminada: 192.168.0.1

Figura 19. Métricas en la tabla de enrutamiento.

- *La distancia administrativa.*

La distancia administrativa define la preferencia de un origen de enrutamiento. Cada origen de enrutamiento (incluyendo protocolos de enrutamiento específicos, rutas estáticas y redes conectadas directamente) se prioriza de más a menos preferible utilizando un valor de distancia administrativa. Los enrutadores la utilizan para seleccionar la mejor ruta cuando aprenden sobre la misma red desde dos o más orígenes de enrutamiento diferentes. La distancia administrativa es un valor entero de 0 a 255. Cuanto más pequeño sea el valor, más fiable es el origen de ruta. Una distancia administrativa de 0 es la que será más fiable. Sólo una red directamente conectada tiene una distancia administrativa de 0, la cual no puede variarse. Si es posible variar el valor de la distancia administrativa en rutas estáticas y protocolos de enrutamiento dinámico. Una distancia

administrativa de 255 significa que el enrutador no creerá en el origen de esa ruta y no se instalará en la tabla de enrutamiento.

Origen de la ruta de distancia administrativa	Distancia por defecto
Interface directamente conectada	0
Ruta estática	1
Ruta sumaria EIGRP	5
BGP externo	20
Ruta interna EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
Ruta externa EIGRP	170
BGP interno	200
Desconocido	255

Tabla 8. Tabla distancia administrativa.

4.1.2.1 Enrutamiento estático.

Las rutas estáticas se definen administrativamente y establecen rutas específicas que han de seguir los paquetes para pasar de un puerto de origen hasta un puerto de destino. Se establece un control preciso del enrutamiento según los parámetros del administrador.

Las rutas por defecto especifican un Gateway (puerta de enlace) de último recurso, a la que el enrutador debe enviar un paquete destinado a una red que no aparece en su tabla de enrutamiento, es decir, que desconoce.

Las rutas estáticas se utilizan habitualmente en enrutamientos desde una red hasta una red de conexión única, ya que no existe más que una ruta de entrada y salida en una red de conexión única, evitando de este modo la sobrecarga de tráfico que genera un protocolo de enrutamiento. La ruta estática se configura para conseguir conectividad con un enlace de datos que no esté directamente conectado al enrutador.

Para conectividad de extremo a extremo es necesario configurar la ruta en ambas direcciones. Las rutas estáticas permiten la construcción manual de la tabla de enrutamiento.

La sintaxis de la configuración de una ruta estática tendría los siguientes campos:

- Red: es la red o subred de destino.
- Máscara: es la máscara de subred.
- Dirección: es la dirección IP del enrutador del siguiente salto.
- Interface: es el nombre de la interfaz que debe usarse para llegar a la red de destino.
- Distancia: es un parámetro opcional que define la distancia administrativa.
- Métrica: es un parámetro opcional que nos permite indicar la métrica de la ruta.

El enrutamiento estático tiene varios usos principales, incluyendo los siguientes:

- Ofrece facilidad de mantenimiento de la tabla de enrutamiento en las redes más pequeñas y que no se espera que crezcan significativamente.
- Enrutamiento a y desde redes internas de la LAN.
- Uso de una ruta predeterminada sencilla (ruta por defecto), que se utiliza para representar una ruta de cualquier red que no tiene una coincidencia más específica con otra ruta de la tabla de encaminamiento.

Las ventajas del enrutamiento estático son las siguientes:

- Mínimo procesamiento de la CPU del enrutador.
- Facilidad de comprensión para el administrador.
- Sencillez en la configuración.

Los inconvenientes del enrutamiento estático son los siguientes:

- La configuración y el mantenimiento consumen mucho tiempo.
- La configuración es propensa a los errores, especialmente en las redes muy grandes.
- La intervención del administrador es necesaria para mantener la información de rutas que deban variar.
- No escala bien con redes que crecen; el mantenimiento puede llegar a ser difícil.
- Requiere un conocimiento completo de la red entera para una implementación apropiada.

4.1.2.2 Enrutamiento dinámico.

Los cambios que una red puede experimentar hacen poco factible la utilización de rutas estáticas, el administrador se vería forzado a reconfigurar los enrutadores ante cada cambio. El enrutamiento dinámico permite que los enrutadores actualicen conocimientos ante posibles cambios sin tener que recurrir a nuevas configuraciones. Un protocolo de enrutamiento permite determinar dinámicamente las rutas y mantener actualizadas sus tablas.

Un protocolo de enrutamiento es el utilizado por los enrutadores para mantener tablas de enrutamiento y así poder elegir la mejor ruta hacia un destino. Algunos de ello son: RIP, EIGRP, IGRP, OSPF,...

Los protocolos de enrutamiento se pueden clasificar en diferentes grupos de acuerdo a sus características:

- ✓ IGP o EGP.
- ✓ Por vector de distancia o por estado de enlace.
- ✓ Con clase o sin clase.

Existen dos grandes núcleos de protocolos de enrutamiento:

- Protocolos de Gateway interior (IGP)
  Se usan para intercambiar información de enrutamiento dentro de un sistema autónomo. Como ejemplo RIP e IGRP.
- Protocolos de Gateway exterior (EGP)
  Se usan para intercambiar información de enrutamiento entre sistemas autónomos Un ejemplo sería el protocolo BGP.

Un sistema autónomo (AS) es un conjunto de red bajo un dominio administrativo común.

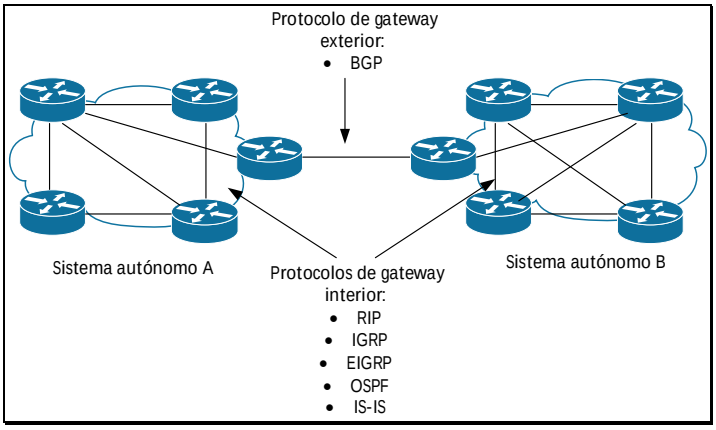


Figura 20. Protocolos IGP y EGP.

Los protocolos de enrutamiento IGP se pueden separar en dos tipos:

- Vector de distancia.
  Este tipo de protocolo determina la dirección y la distancia a cualquier red. RIP e IGRP son dos ejemplos.
- Estado de enlace.
  Estos protocolos tienen una idea exacta de la topología de la red y no efectúan actualizaciones a menos que ocurra un cambio en la topología. OSPF e IS-IS son protocolos de este tipo.

La siguiente tabla nos presenta las ventajas y desventajas de los protocolos de enrutamiento de estado de enlace:

Ventajas	Desventajas
Tiempos de convergencia rápidos, dado que elorigen afectado anuncia los cambios inmediatamente.	Impone demandas significativas sobre los recursos de memoria y CPU.
Ofrece solidez contra los bucles de enrutamiento.	Requiere un diseño de red muy estricto.
Los routers conocen la topología.	Requiere un administrador de red experto.
Los paquetes de estado de enlace se secuencian y se calcula su tiempo de existencia.	La inundación de red inicial puede reducir el desempeño de la red.
La base de datos de estado de enlace se puede minimizar al diseñar la red con cuidado.	

Tabla 9. Comparativa protocolos de estado de enlace.

Los protocolos de enrutamiento también se pueden clasificar como:

- *Protocolos de enrutamiento con clase*.
  No envían información de máscara de subred en las actualizaciones de enrutamiento. Sólo existen 3 tipos de redes con una máscara prefijada, clase A, B o C. La máscara de red puede determinarse con el primer octeto de la dirección de red. Ejemplos de este tipo de protocolos son RIPv1 e IGRP.

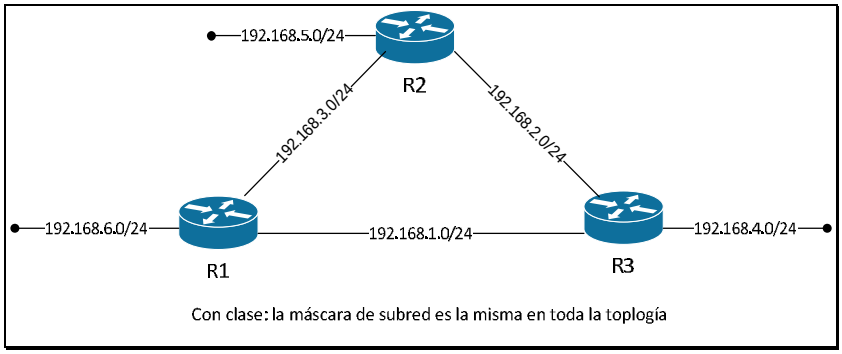


Figura 21. Enrutamiento con clase.

- *Protocolos de enrutamiento sin clase*.
  Sí envían la información de la máscara de subred con la dirección de red en las actualizaciones de enrutamiento. Las redes actuales ya no se signan basándose en clases y la máscara de subred no puede determinarse por el valor del primer octeto. Los protocolos de enrutamiento sin clase son necesarios en la mayoría de las redes actuales debido a que soportan VLSM[20], las redes discontinuas, etc...
  Este tipo de protocolos son RIPv2, EIGRP, OSPF, IS-IS y BGP.

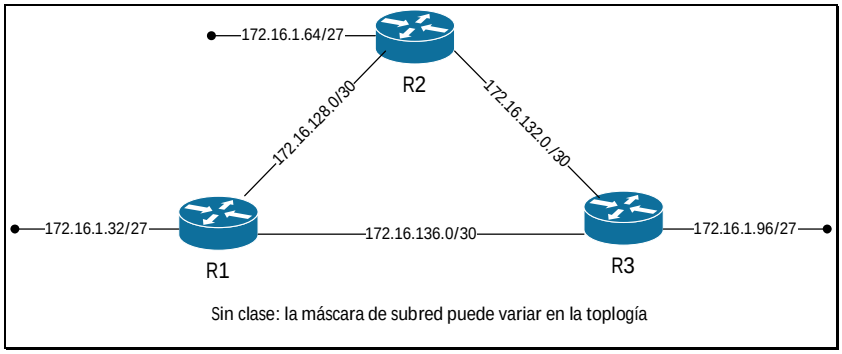


Figure 22. Enrutamiento sin clase.

Otro punto a destacar cuando se habla de protocolos de enrutamiento es la convergencia. Esta es una característica importante cuando sucede un cambio de topología en la red.

La convergencia es cuando las tablas de enrutamiento de todos los enrutadores se encuentran en un estado de consistencia. La red converge cuando todos los enrutadores tienen información completa y exacta sobre la red. El tiempo de convergencia es el tiempo que invierten los enrutadores en compartir información, calcular las mejores rutas y actualizar sus tablas de encaminamiento. Una red no es completamente operable hasta que la red ha convergido; por tanto, la mayoría de redes requieren tiempos de convergencia cortos.

La convergencia es tanto cooperativa como independiente. Los enrutadores comparten información entre sí, pero deben calcular independientemente los efectos de un cambio en la topología en sus propias rutas. Como ellos desarrollan un acuerdo independientemente con la topología nueva, se dice que convergen en este consenso.

[20] Máscara de subred de longitud variable.

Las propiedades de convergencia incluyen la velocidad de propagación de la información de enrutamiento y el cálculo de las rutas óptimas. Los protocolos de enrutamiento se pueden evaluar basándose en la velocidad de convergencia. Generalmente, RIP e IGRP son de convergencia lenta, mientras que EIGRP, OSPF e IS-IS son más rápidos a la hora de converger.

El cuadro siguiente muestra una comparativa de las características de los protocolos de enrutamiento de tipo IGP:

Protocolo	RIPv2	IGRP	EIGRP	IS-IS	OSPF
Vector distancia	X	X	X		
Estado de enlace				X	X
Resumen automático de ruta	X	X	X	X	
Resumen manual de ruta	X	X	X	X	X
Soporte VLSM	X		X	X	X
Propietario de fabricante		X	X		
Convergencia	120	100	90	115	110
Distancia administrativa	Lento	Lento	Muy rápido	Muy rápido	Muy rápido
Tiempo de actualización	30	90			
Métrica	Saltos	Compuesta	Compuesta	Coste	Coste

Tabla 10. Comparativa de protocolos de enrutamiento IGP.

Las ventajas del enrutamiento dinámico son las siguientes:

- Al administrador le supone menos trabajo mantener la configuración cuando añade o elimina redes.
- Los protocolos reaccionan automáticamente a los cambios de topología.
- La configuración es menos propensa a los errores.
- Más escalable; el crecimiento de la red normalmente no presenta problemas.

Los inconvenientes del enrutamiento dinámico son los siguientes:

- Se utilizan los recursos del enrutador (ciclos de CPU, memoria y ancho de banda del enlace).
- El administrador debe tener un mayor conocimiento para las tareas de configuración, verificación y resolución de problemas.

Para concluir se muestra una tabla comparativa entre el enrutamiento dinámico y el enrutamiento estático.

Característica	Enrutamiento dinámico	Enrutamiento estático
Complejidad de configuración	Generalmente independiente del tamaño de la red	Aumenta con el tamaño de la red
Conocimientos requeridos por parte del administrador	Requiere un conocimiento avanzado	No requiere conocimientos extra
Cambios en la topología	Se adapta automáticamente a los cambios de la topología	Requiere la intervención del administrador
Escalado	Adecuado para topologías sencillas y complejas	Adecuado para topologías sencillas
Seguridad	Menos seguro	Más seguro
Uso de recursos	Utiliza CPU, memoria y ancho de banda del enlace	No necesita resursos adicionales
Pronosticación	La ruta depende de la topología actual	La ruta al destino es siempre la misma

Tabla 11. Enrutamiento dinámico vs estático.

En este proyecto se va a utilizar RIPv2 debido a los siguientes motivos:

1. Pretendemos tener una configuración lo más simple posible.
2. El campo de actuación del protocolo es sólo la VLAN de interconexión de cada sede. El resto de enrutamiento de cada sede es estático.
3. El enrutador WAN es gestionado por la operadora y por lo tanto en caso de problemas será más complicada la resolución en un tiempo razonable. RIPv2 es más sencillo de analizar para resolver problemas.
4. Al ser un protocolo de vector distancia hacemos que los equipos de enrutamiento carguen menos su CPU.
5. El tiempo de convergencia es más alto que en protocolos de estado de enlace, pero en nuestro caso se depende también del tiempo de convergencia de la WAN de la operadora.
6. No queremos casarnos con protocolos de un fabricante concreto. En la VLAN de interconexión tenemos equipos enrutadores de dos fabricantes distintos.

4.1.2.2.1 RIP v2.

Uno de los protocolos de *gateway* interior más utilizado es el *Routing Information Protocol* (RIP). RIP es una implementación de un algoritmo de vector de distancia, o del algoritmo de Bellman–Ford. RIP clasifica los enrutadores en activo y pasivo (silencio) .Los enrutadores activos anuncian sus rutas (información de accesibilidad) a los demás, los enrutadores pasivos escuchan y actualizar sus rutas basado en anuncios, pero no anuncian. Normalmente, los enrutadores ejecutan RIP en modo activo, mientras los equipos usan el modo pasivo.

Un enrutador que ejecuta RIP en modo activo envía actualizaciones a intervalos establecidos. Cada actualización contiene pares de valores, donde cada par se compone de una dirección IP y un valor entero que indica la distancia a esa red. RIP utiliza la métrica de número de saltos para medir la distancia a un destino. En las métricas de RIP, un enrutador anuncia redes directamente conectadas con una métrica de 1 por defecto. Las redes que son accesibles a través de otra puerta

de enlace son 2 saltos, etc. Por lo tanto, el número de saltos o número de saltos a lo largo de un camino desde una fuente dada hasta un destino determinado se refiere al número de puertas de enlace que un datagrama se encontraría a lo largo de ese camino. El uso de la cantidad de saltos para calcular los caminos más cortos no siempre produce resultados óptimos. Por ejemplo , una ruta de acceso con un número de saltos 3 que atraviesa tres redes Ethernet puede ser sustancialmente más rápido que un camino con una cuenta de saltos 2 que cruza dos líneas en serie de baja velocidad. Para compensar las diferencias en tecnología, muchos enrutadores anuncian mayores métricas para enlaces de conexiones lentas.

RIP se reconstruye dinámicamente usando la información recibida a través de actualizaciones de RIP. Cuando se pone en funcionamiento, RIP emite una solicitud de información de enrutamiento y luego escucha las respuestas a la solicitud. Si un sistema configurado para suministrar RIP oye la petición, responde con un paquete de respuesta basado en la información en su base de datos de enrutamiento. El paquete de respuesta contiene las direcciones de red de destino y la métrica de enrutamiento para cada destino.

Cuando se recibe un paquete de respuesta RIP, el demonio de enrutamiento toma la información y vuelve a generar la base de datos de enrutamiento, agregando las nuevas rutas y también modifica las "mejores" (inferiores métricas) rutas a destinos que ya figuran en la base de datos. RIP también borra rutas de la base de datos si el enrutador siguiente a ese destino informa de que la ruta contiene más de 15 saltos, o si se elimina la ruta. Todas las rutas a través de una puerta de entrada se eliminan si no se reciben las actualizaciones de esa puerta de entrada durante un período de tiempo especificado. En general, las actualizaciones de enrutamiento se emiten cada 30 segundos. En muchas implementaciones, si una puerta de enlace no se oye durante 180 segundos, todas las rutas de esa puerta de entrada se eliminan de la base de datos de enrutamiento. Los 180 segundos de intervalo también se aplica a la eliminación de rutas específicas.

RIP versión 2 añade funciones adicionales a RIP. Algunas de estas funciones son compatibles con RIPv1 y otras no lo son. Algunas de las mejoras más notables RIPv2I son:

- *Siguiente salto*.
  Con RIPv2, un enrutador puede anunciar un próximo salto que no sea él mismo. EL siguiente salto es útil cuando se advierte de una ruta estática a un enrutador que tiene RIP, porque evita tener paquetes que se transmiten a través de este enrutador y así se evita que crucen la red dos veces.

- *Máscara de red.*
  RIP que supone que todas las subredes de una red dada son con clase (clase A, B o C). RIPv1 utiliza esta suposición para calcular las máscaras de red para todas las rutas recibidas. Este supuesto impide subredes con máscaras de red sin clase que se incluyan en los paquetes RIP. RIPv2 añade la posibilidad de especificar la máscara de red entre la red en un paquete.

- *Autenticación.*
  Paquetes RIPv2 pueden contener uno de los dos tipos de cadenas de autenticación que pueden ser utilizados para verificar la validez de los datos de encaminamiento suministrados. El primer método es una contraseña simple en el que una clave de autenticación de hasta 16 caracteres se incluye en el paquete. Si esta clave no coincide con

lo que se espera, se descartará el paquete. Este método proporciona muy poca seguridad, ya que es posible aprender la clave de autenticación observando paquetes RIP.

El segundo método utiliza el algoritmo MD5 para crear un *cripto-checksum*[21] de un paquete RIP y una clave de autenticación de hasta 16 caracteres. El paquete transmitido no contiene la clave de autenticación en sí, sino que contiene una suma de comprobación criptográfica, llamado el "*digest*". El enrutador receptor realizará un cálculo utilizando la clave de autenticación correcta y descartará el paquete si el resumen no coincide. Además, un número de secuencia se mantiene para evitar el reenvío de paquetes antiguos. Este método proporciona una seguridad mucho más fuerte ya que los datos de encaminamiento se originaron en un enrutador con una clave de autenticación válida.

Ambos métodos de autenticación pueden ser especificados por interface. Los paquetes se envían siempre utilizando el método principal, pero los paquetes recibidos se comprueban con los dos métodos primarios y secundarios antes de ser desechados. Además, una clave de autenticación separada se utiliza para las consultas que no sean de un enrutador.

La siguiente tabla nos presenta las características más importantes del protocolo RIPv2:

Características RIPv2
Es un protocolo de enrutamiento por vector-distancia.
Utiliza el número de saltos como métrica para la selección de rutas.
Si el número de saltos es superior a 15, el paquete se descarta.
Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 30 segundos.
Capacidad para transportar mayor información relativa al enrutamiento de paquetes.
Mecanismo de autenticación para la seguridad de origen al hacer actualizaciones de tablas.
Soporta enmascaramiento de subredes de longitus variable (VLSM).
Elimina una ruta no actualizada a los 180 segundos.

Tabla 12. Tabla resumen características RIPv2.

El uso del protocolo RIPv2 nos servirá para hacer converger hacia la red WAN de respaldo. Es la inteligencia que desencadenará todo el proceso que hará el tráfico fluya por la WAN de respaldo.

4.1.3 Gestión de Ancho de Banda.

Al ser un dispositivo que proporciona visibilidad de aplicaciones, detección y clasificación de tráfico en tiempo real para cientos de aplicaciones; la información que presenta es útil para que los administradores pueden configurar límites de ancho de banda para aplicaciones y contenido problemáticos, reservar ancho de banda para aplicaciones operativas clave o garantizar una asignación equitativa de ancho de banda entre los usuarios de computadores de escritorio virtuales. En definitiva, se puede supervisar y controlar el rendimiento de las aplicaciones.

Algunos tipos de tráfico de red hacen un uso ineficiente del ancho de banda disponible. Al optimizar el tráfico en tiempo real, el módulo de compresión aumenta de manera instantánea la capacidad de la WAN, lo cual mejora el rendimiento de las aplicaciones y los tiempos de respuesta

[21] Para certificar que el mensaje original no ha sido modificado.

de los usuarios. Con una arquitectura simétrica con inteligencia para aplicaciones, el módulo de compresión identifica el tráfico comprimible y aplica la tecnología de compresión adecuada, lo cual aumenta la capacidad de dos a cuatro veces, para reducir el uso de ancho debanda y disminuir la latencia de WAN.

Los gestores de ancho de banda administran el caudal de tráfico de datos con el objetivo de dar mayor priorizar a aquellos flujos de aplicaciones más importantes. Estos equipos descuben el tráfico de red y lo categorizan atendiendo a los tipos de servicio o protocolo que vean (ICMP, UDP, TCP, RIP; Oracle,...). También es posible asignar un ancho de banda concreto e incluso un ancho de banda variable, que adapte a las necesidades del flujo concreto de la aplicación.

Nos serviremos de ellos para poder analizar el tráfico actual de la red y así poder dimensionar las necesidades de la WAN de respaldo. De igual manera aplicaremos la misma política de gestión de ancho de banda al tráfico que fluya por la WAN de los enlaces RDSI.

Como vemos en el cuadro siguiente correspondiente a los dos modelos que existen en las podemos usar en cada uno de ellos una o dos tarjetas de expansión para conectar más segmentos de red que se quieran analizar o aplicar QoS[22] al tráfico que curse por el enlace.

3500 & 7500	Network Interfaces:	Copper 10/100/1,000 Mbps
	LAN Expansion Modules (LEM):	Copper 10/100/1,000 Mpbs, Fiber SFP
	Integrated Backup Ports:	None
	Out-of-Band Management Port:	Yes
	Console Port:	RS-232 (AT-compatible) with male DB-9 connector

Figura 23. Características físicas de los modelos.

Se añade una captura para facilitar la comprensión del método de conexión del dispositivo a la red que se va a gestionar.

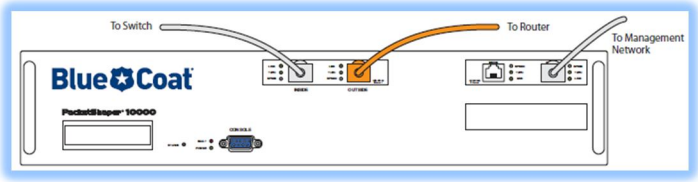


Figura 24. Esquema conexión física.

4.1.4 Cortafuegos.

El cortafuegos existente en la red cuenta con un proceso de enrutamiento avanzado que soporta protocolos de enrutamiento dinámico tales como RIPv1, RIPv2, OSPF y BGP.

CheckPoint utiliza una red de sincronización y un protocolo propietario para mantener el estado de las tablas de conexiones y de las tablas de enrutamiento en ambos nodos del *cluster*[23]. Por ello, cuando el cortafuegos conmuta (un nodo pasa de estado activo a estado pasivo y viceversa) debido a algún problema, el otro nodo mantendrá actualizada las tablas necesarias para su funcionamiento.

[22] Calidad de servicio.
[23] Dispositivos montados en parejas o más para dotar de alta disponibilidad o balanceo de carga.

Cuando utilizamos un protocolo de enrutamiento dinámico como RIPv2, configuramos un interface para que utilice este protocolo. Pero será solamente el nodo que está activo el que se comunica a través del protocolo con la red en ese interface. El otro nodo actualizará su tabla de rutas con la información obtenida por RIP que le facilitará por el nodo activo a través de la red de sincronismo del *cluster* del cortafuegos.

Este componente es fundamental en la conmutación a la red WAN de respaldo ya que será quien iniciará todo el proceso al perder por RIP la ruta a la sede remota que ha quedado aislada de la WAN de la operadora.

4.2 Hardware necesario

4.2.1 Análisis de posibles enrutadores.

Para la comunicación de las sedes central con la WAN RDSI se han barajado dispositivos de diferentes fabricantes, buscando aquellos que dispusiesen de interfaces PRI RDSI y que soportasen enrutamiento DDR.

Entre los que se han analizado están:

- *Juniper serie J*
  Estos dispositivos soportan primarios RDSI pero va a ser descontinuados y sustituidos por la serie SRX que contará con este tipo de interfaces sólo para enviar voz. Por tanto, descartamos esta opción.
- *Cisco serie ISR2911 y serie ISR3925*
  Estos equipos soportan interfaces ISDN PRI y funcionalidad de enrutamiento DDR. Son líderes en el mercado y se encuentra fácilmente gran cantidad de información sobre configuraciones en Internet.
- *HP serie MSR*
  Aun teniendo posibilidad de usar un interface RDSI no deja claro si es PRI o BRI y tampoco si tiene la funcionalidad de enrutamiento DDR. Igualmente, descartamos esta opción.
- *Huawei serie AR2220 y serie AR2240*
  Soporta interfaces RDSI PRI e implementa en su software la posibilidad de encaminar el tráfico levantando enlaces RDSI bajo demanda. A esa tecnología le llaman DCC (Dial Control Center). Es una solución con un precio ligeramente menor a el equipamiento Cisco.
- *Allied Telesis serie AT-ARxx*
  Siendo una solución de bajo coste, soporta enlaces RDSI PRI y configuración para llamada bajo demanda.

La decisión final ha venido influenciada mayormente por los posibles problemas que podrían dar la interoperabilidad de usar distintos fabricantes. Ya que el equipo enrutador que suministra la operadora es de la compañía Cisco se ha optado por adquirir equipamiento del mismo fabricante. Aun siendo la opción más cara de todas las que cumplen con los requerimientos, se ha pensado que esta inversión inicial será recompensada al dotar a la red de una solución más fiable, estable, escalable y contrastada, que evite que se produzcan costos ocultos tales como caídas de red con el consecuente impacto para la productividad de la empresa.

4.2.1.1 Enrutadores seleccionados.

Concluida la elección, se han seleccionado enrutadores de la nueva hornada de productos de *Cisco*, los ISR (*Integrated Services Enrutador*). Concretamente los modelos *Cisco ISR 2911* para las sedes remotas y el modelo *ISR 3925* para la sede central.

Debido a que es una plataforma de alto rendimiento y altamente modular que cuenta con varios tipos de ranuras diseñadas para incorporar módulos de conectividad y servicios que permiten satisfacer los diversos requisitos de red de las sucursales, entre ellas T1/E1, T3/E3, xDSL y Gigabit Ethernet en cobre y fibra óptica.

Por otra parte estos equipos ofrecen una variedad de opciones de conectividad LAN y WAN para poder efectuar cambios futuros sin necesidad de cambiar toda la plataforma.

Para el equipo 2911 se ha añadido un interface para conectar un primario RDSI: HWIC-1CE1T1-PRI - 1-port Channelized E1/T1/ISDN PRI HWIC

A continuación mostramos una foto de equipo:

Figura 25. Enrutador Cisco 2911 – sedes remotas.

Para la sede central se ha seleccionado dentro de la mima familia de productos un enrutador de una gama superior debido a que en un momento dado puede tener que soportar el enrutamiento y conectividad con varias sedes a la vez.

Por lo tanto se le ha añadido al equipo 2 tarjetas de expansión de doble enlace para poder soportar hasta 4 primarios RDSI: HWIC-2CE1T1-PRI - 2-port Channelized E1/T1/ISDN PRI HWIC

El modelo de enrutador es el Cisco ISR 3925, el cual se puede ver en la imagen adjunta:

Figura 26. Enrutador Cisco 3925 – sede central.

4.2.2 Componentes para la centralita.

Para la centralita no es necesario adquirir ningún dispositivo ya que cuenta con una tarjeta MGU (*Media Gateway Unit*) que tiene soporte para conectar 8 enlaces primarios RDSI. De los 8 puertos unos irán conectados como primarios con el operador de telefonía y otros nos servirán para conectar las tarjetas de primario de los enrutadores RDSI. El siguiente esquema nos muestra como es la tarjeta de la MGU y donde irán conectados los primarios RDSI.

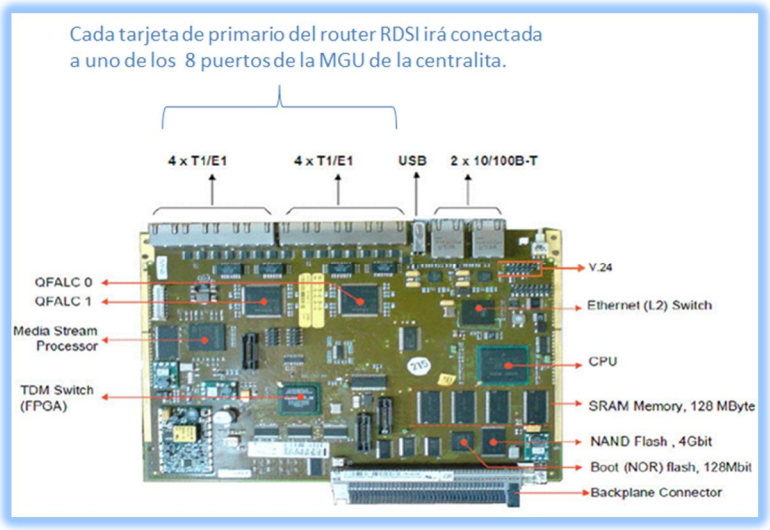


Figura 27. Conexión del enrutador RDSI a la MGU de la centralita.

La centralita usará el protocolo de señalización QSIG en los enlaces primarios con los enrutadores RDSI. La señalización Q (QSIG) es un protocolo usado para llevar datos sobre líneas de alta velocidad de la red digital de los servicios integrados (ISDN). QSIG se utiliza para señalar a través de estas líneas a conectar con los intercambios de rama privados (PBXs). La señalización es la transferencia de la información a los puntos en una red. Un PBX es una red de teléfono de propiedad privada dentro del negocio, de la escuela, o de la otra entidad grande, como una oficina gubernamental.

Permite también las llamadas de las PBXs entre las líneas dentro de la compañía y que los usuarios hagan llamadas externas. QSIG se utiliza para ISDNs que usan el estándar Q.931 para transportar la información entre un usuario individual y un PBX. QSIG permite que el equipo de diversos vendedores trabaje junto tiene acceso a una red del PBX vía la línea del ISDN. Las redes que incluyen Q.931 usan el estándar Q, lo utilizan para procesar las llamadas entrantes a la red. La señalización Q proporciona las funciones esenciales en la red del estándar Q.931. Estas funciones incluyen alertar a la red que está entrando una llamada, estableciendo una conexión, y la terminación de la conexión cuando la llamada es completada. La siguiente imagen nos da una idea del concepto explicado.

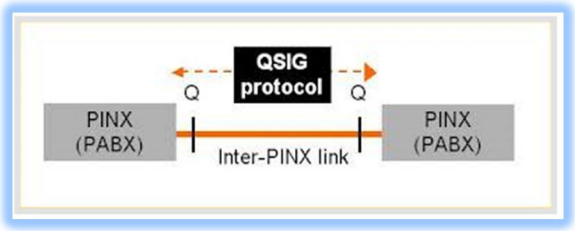


Figura 28. Protocolo QSIG.

4.2.3 Componentes para los gestores de ancho de banda.

Cuando se tienen múltiples segmentos de una LAN a los que se quiere gestionar el ancho de banda es necesario introducir un elemento que nos permita hacer esas tareas. Por lo tanto deberías tener un equipo conectado a cada segmento de red que se quiera analizar.

Las opciones que planea esta disyuntiva son dos:

1. Adquisición de un nuevo equipo gestor de ancho de banda para que aplique en el tráfico que va hacia el enlace de respaldo. Esto conlleva un desembolso y licencia de un nuevo equipo.
2. Inclusión de una tarjeta de expansión en los equipos actuales para gestionar el tráfico de respaldo. Es una opción más económica y los equipos no se ven penalizados en su rendimiento ya que tienen bahías de expansión pensadas para ello. Es la opción seleccionada.

Los equipos de gestión de ancho de banda de que dispone la red empresarial, es decir, el *Packetshaper 2500* y *7500* disponen de la opción de utilizar tarjetas de expansión para realizar la gestión del tráfico de diferentes segmentos de la red.

Por lo tanto, se ha decidido añadir una tarjeta con puertos 1000 BaseT[24] en cada dispositivo para controlar el tráfico de la WAN principal, tal y como se está realizando actualmente. Y por otro lado poder gestionar el tráfico que cursará por el enlace de la WAN de respaldo.

Además otra ventaja es que la misma política de gestión del enlace principal se usará en el enlace de respaldo, lo cual facilitará en gran medida su integración.

A nivel económico no hay que ampliar la licencia de gestión, ya que en el peor de los casos, los modelos 3500 de las sedes centrales tienen hasta 10 Mbps licenciados, lo que permitiría realizar la gestión del enlace principal y del enlace de backup.

En el siguiente dibujo se puede ver cómo es una tarjeta de expansión LEM y en que slot del equipamiento iría colocada.

Figura 29. Tarjetas de expansión LEM.

[24] Fast Ethernet (100 Mbps).

QUINTA PARTE: ¿CÓMO LO VAMOS A HACER?

5 PROPUESTA TECNOLÓGICA

Una vez analizada la arquitectura actual de la red empresarial, identificado el equipamiento necesario y las tecnologías a utilizar, se puede comenzar con el trabajo sobre el terreno. En este apartado definiremos con detalle la configuración de cada elemento interviniente. Es importante destacar que en lo que respecta a las sedes remotas, las diez tienen la misma configuración donde sólo varía el direccionamiento IP.

Se comienza presentando un mapa que presenta una foto general de la situación de la WAN de respaldo respecto a la WAN principal. Después se verá el diagrama final de ambos tipos de sedes al incluir el enrutador RDSI. Se pasará a analizar la configuración de cada dispositivo comenzando por aquella parte que gestiona la operadora.

Concluiremos esta parte haciendo una descripción del proceso de convergencia, es decir, paso a paso lo que sucede cuando una sede pierde la conexión con la WAN principal y hay que recuperar la conectividad por la WAN RDSI de respaldo.

5.1 Mapa conceptual.

Para tener una visión global e la solución propuesta se ha superpuesto la nueva arquitectura de red de respaldo a la situación existente. Como se puede apreciar en el siguiente dibujo en rojo la solución alcanza todos los puntos de la organización.

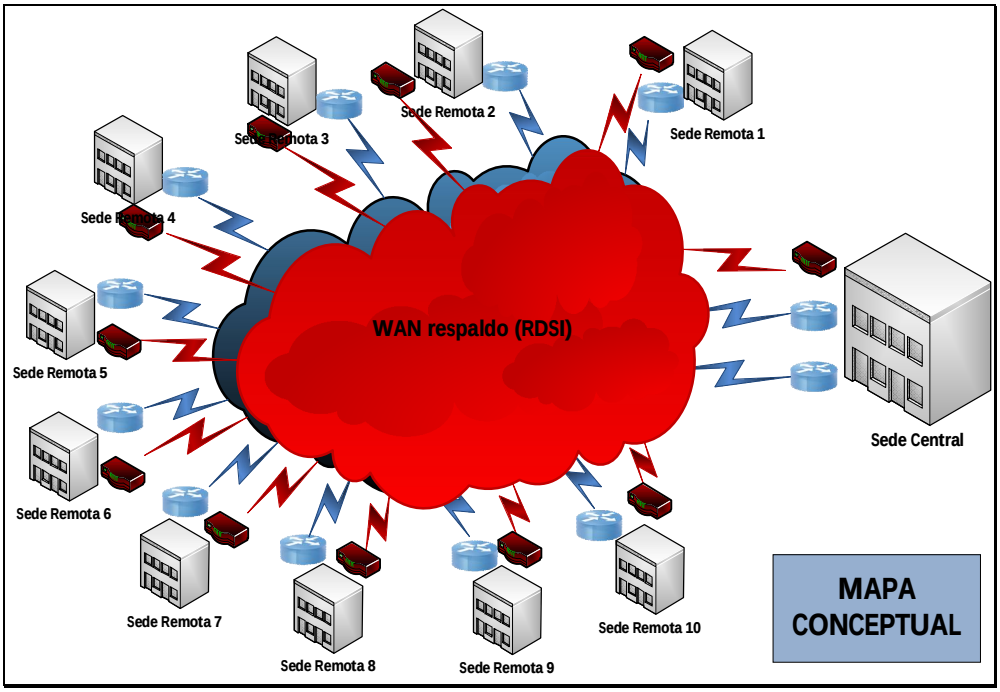


Figura 30. Esquema de red final.

5.2 Diagrama final de la sede central.

En la sede central se ubica el enrutador RDSI de mayor capacidad: tendrá que dar servicio a una o varias sedes a la vez. Por lo tanto a este enrutador, al que se le han añadido dos tarjetas de expansión de doble enlace primario, se conectarán 4 cables de pares provenientes de los puertos E1 de la MGU de la centralita.

Por otro lado este mismo enrutador irá conectado por un enlace en modo autonegociación[25] y Gigabit Ethernet a la tarjeta LEM[26] del gestor de ancho de banda, en concreto a su puerto *outside*[27].

El diagrama nos muestra esta situación final de la arquitectura de red de la sede central:

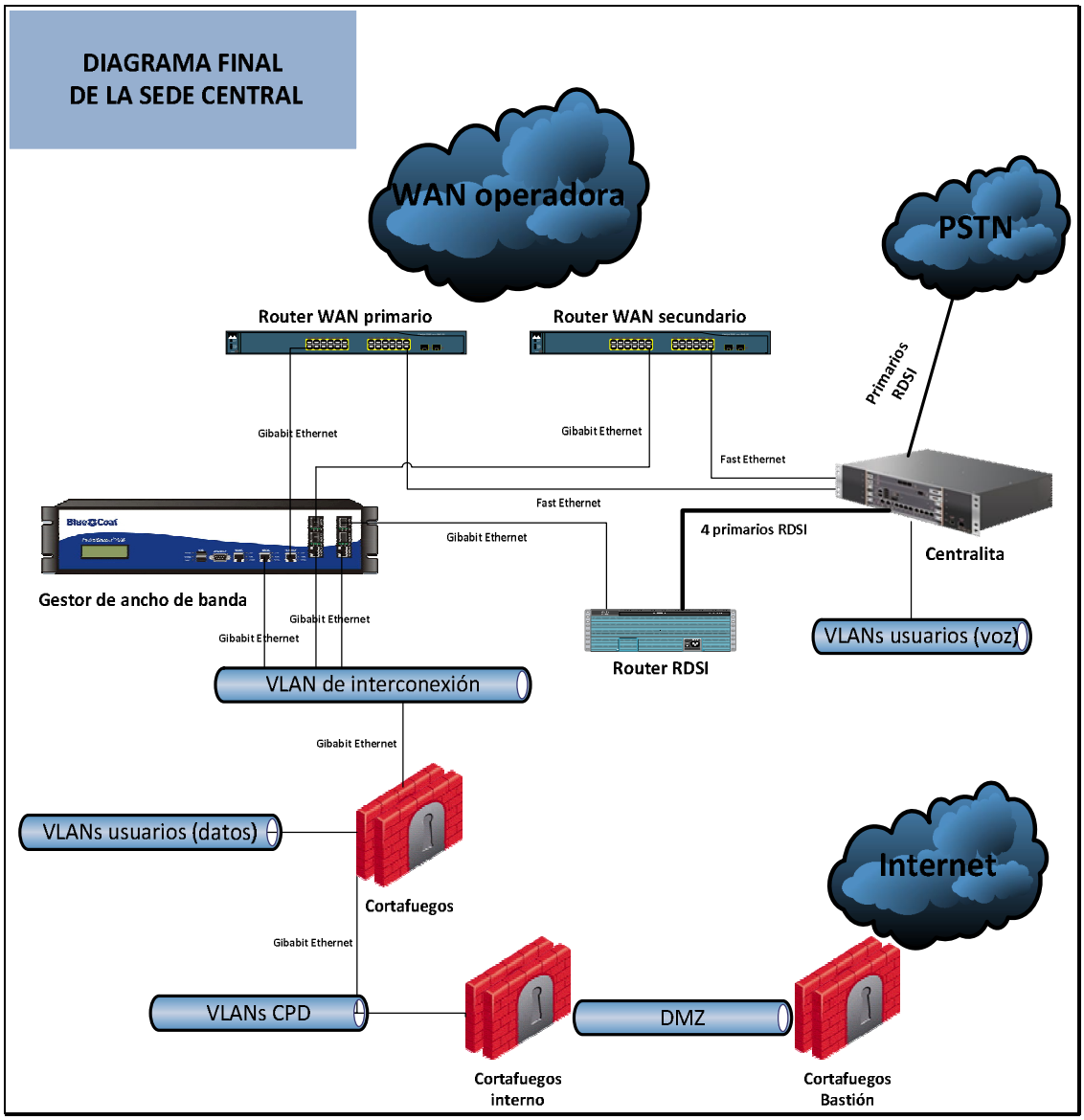


Figura 31. Mapa final de la sede central.

[25] El puerto físico del dispositivo negocia una velocidad de enlace con el puerto físico del dispositivo al que está conectado.
[26] Tarjeta de ampliación.
[27] Puerto de la tarjeta LEM que se conecta hacia la red externa.

5.2.1 Direccionamiento IP de la sede central.

	Direccionamiento sede central	
Datos	VLAN de interconexión	192.170.0.0/24
	Router WAN	192.170.0.252
	Cortafuegos WAN	192.170.0.3
	Router RDSI	192.170.0.50
	Resto LAN de datos	172.16.0.0/16
Voz	Conexión centralita-router WAN	192.171.0.0/24
	Router WAN	192.171.0.252
	Centralita	192.171.0.100
	Resto LAN de voz	172.17.0.0/16

Tabla 13. Direccionamiento IP sede central.

5.3 Diagrama final de las sedes remotas.

El esquema final de en el resto de sedes es similar al de la sede central. En este caso, las sedes remotas dispondrán de un enrutador RDSI de gama más baja ya que sólo ha de dar servicio a la sede remota donde reside. A este enrutador se le ha montado una tarjeta de expansión para conectar un primario RDSI. La conexión se hará a uno de los puertos E1 de la tarjeta MGU de la centralita.

Al igual que en el caso de la sede central se conectará un puerto Gigabit Ethernet del enrutador al puerto *outside* la tarjeta LEM que se ha añadido al gestor de ancho de banda para administrar el caudal de tráfico que pase por el enlace WAN RDSI.

El diagrama nos muestra esta situación final de la arquitectura de red de una sede remota:

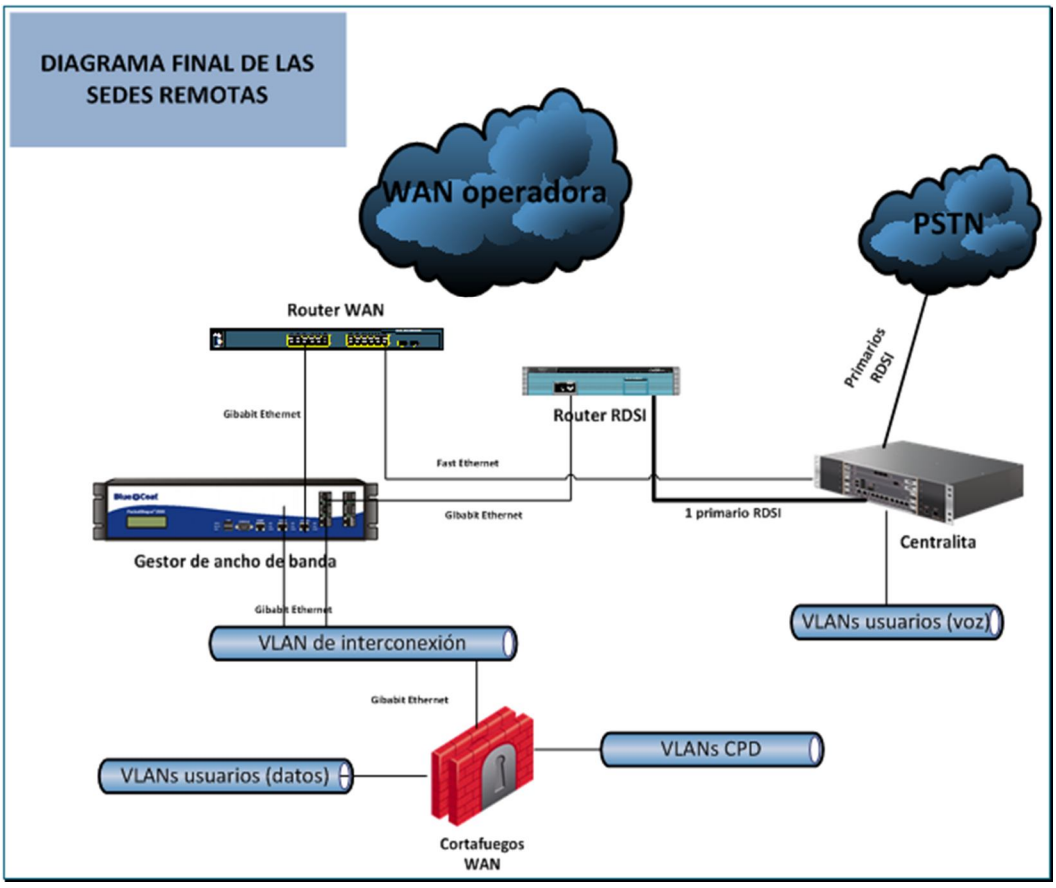


Figura 32. Mapa final de las sedes remotas.

5.3.1 Direccionamiento IP de las sedes remotas

Direccionamiento sedes remotas

		Sede 1	Sede 2	Sede 3	Sede 4	Sede 5
Datos	VLAN de interconexión	192.170.1.0/24	192.170.2.0/24	192.170.3.0/24	192.170.4.0/24	192.170.5.0/24
	Router WAN	192.170.1.252	192.170.2.252	192.170.3.252	192.170.4.252	192.170.5.252
	Cortafuegos WAN	192.170.1.3	192.170.2.3	192.170.3.3	192.170.4.3	192.170.5.3
	Router RDSI	192.170.1.150	192.170.2.150	192.170.3.150	192.170.4.150	192.170.5.150
	Resto LAN de datos	172.21.0.0/17	172.22.0.0/17	172.23.0.0/17	172.24.0.0/17	172.25.0.0/17
Voz	Conexión centralita-router WAN	192.171.1.0/24	192.171.1.0/24	192.171.1.0/24	192.171.1.0/24	192.171.1.0/24
	Router WAN	192.171.1.252	192.171.1.252	192.171.1.252	192.171.1.252	192.171.1.252
	Centralita	192.171.1.100	192.171.1.100	192.171.1.100	192.171.1.100	192.171.1.100
	Resto LAN de voz	172.21.128.0/17	172.22.128.0/16	172.23.128.0/17	172.24.128.0/17	172.25.128.0/17

		Sede 6	Sede 7	Sede 8	Sede 9	Sede 10
Datos	VLAN de interconexión	192.170.6.0/24	192.170.7.0/24	192.170.8.0/24	192.170.9.0/24	192.170.10.0/24
	Router WAN	192.170.6.252	192.170.7.252	192.170.8.252	192.170.9.252	192.170.10.252
	Cortafuegos WAN	192.170.6.3	192.170.7.3	192.170.8.3	192.170.9.3	192.170.10.3
	Router RDSI	192.170.6.150	192.170.7.150	192.170.8.150	192.170.9.150	192.170.10.150
	Resto LAN de datos	172.26.0.0/17	172.27.0.0/17	172.28.0.0/17	172.29.0.0/17	172.30.0.0/17
Voz	Conexión centralita-router WAN	192.171.1.0/24	192.171.1.0/24	192.171.1.0/24	192.171.1.0/24	192.171.1.0/24
	Router WAN	192.171.1.252	192.171.1.252	192.171.1.252	192.171.1.252	192.171.1.252
	Centralita	192.171.1.100	192.171.1.100	192.171.1.100	192.171.1.100	192.171.1.100
	Resto LAN de voz	172.26.128.0/17	172.27.128.0/17	172.28.128.0/17	172.29.128.0/17	172.30.128.0/17

Tabla 14. Direccionamiento IP sedes remotas.

5.4 Configuraciones.

En este apartado se pretende ir desgranando la configuración que habrá que aplicar a los equipos para implementar la funcionalidad requerida en cada uno de ellos.

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 cuando se converja 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 aislado tendrán que realizarlas por la red pública a los números de teléfono habituales.

5.4.1 Requerimientos de la WAN principal.

La WAN de la operadora debe conocer todo el direccionamiento IP que hay en las distintas sedes para poder asegurar la comunicación entre cualquier punto de ellas. Además, para que el sistema de respaldo se ponga operativo y la red converja, debe avisar de alguna manera al resto de las sedes de que hay alguna de ellas que se ha quedado aislada. Como ya comentamos, esto se conseguirá a través del uso de un protocolo de enrutamiento RIPv2.

Por lo tanto, a la operadora se le debe solicitar que implemente en sus enrutadores WAN la configuración enrutamiento para que realice las siguientes tareas:

1. Mediante RIPv2 publicar en la VLAN de interconexión de cada sede las rutas al resto de redes de las otras sedes.
2. Usando RIPv2 publicarse como la ruta por defecto sólo en las sedes remotas.
3. Utilizar autenticación mediante clave y modo MD5[28] para la comunicación de actualizaciones RIPv2.
4. Cuando la WAN de la operadora no conozca algún destino entregará ese tráfico en el cortafuegos WAN de la sede central.

5.4.2 Configuración de la centralita.

En primer lugar se va a describir la configuración de la centralita, ya que algunos de los datos que aquí se definan serán necesarios en la configuración de los enrutadores RDSI.

Todas las centralitas tienen enlaces de tipo QSIG (primario, 30 canales) con los diferentes enrutadores RDSI. En el caso de la sede central son cuatro y en el resto uno. En el caso de la voz IP se hace con una conexión *Fast Ethernet* al enrutador WAN. Además, cada enlace se identifica en la centralita con el nombre de una ruta. Por ejemplo, cuando se analizaron las sedes en el apartado

[28] Algoritmo de encriptación de 128 bits.

3, se mostró que la Ruta 1 correspondía a los primarios que van hacia la red pública del operador y la Ruta 51 era la que iba al enrutador WAN.

A continuación mostramos como sería la tabla de enrutamiento para la centralita de la sede central:

Tabla enrutamiento centralita en la sede central

	Identificador	Salto	Interface	Descripción
Centralita	Ruta 41		Puerto 0 E1/T1	1 primario conectado al router RDSI
	Ruta 42		Puerto 1 E1/T1	1 primario conectado al router RDSI
	Ruta 43		Puerto 2 E1/T1	1 primario conectado al router RDSI
	Ruta 44		Puerto 3 E1/T1	1 primario conectado al router RDSI
	Ruta 51	192.171.0.252	Fast Ethernet 0	Telefonía interna (Voz IP)
	Ruta 1		tarjetas primario a operador	Telefonía externa PSTN

Tabla 15. Enrutamiento centralita sede central.

Respecto a las sedes remotas, como todas son iguales, (sólo varía el tercer octeto de la dirección IP en la red de interconexión, la cual que identifica la sede) para mostrar la configuración de la centralita de la sedes remotas hemos cogido como ejemplo la de la sede 5,

Tabla enrutamiento centralita en la sede remota 5

	Identificador	Salto	Interface	Descripción
Centralita	Ruta 61		Puerto 0 E1/T1	1 primario conectado al router RDSI
	Ruta 51	192.171.5.252	Fast Ethernet 0	Telefonía interna (Voz IP)
	Ruta 1		tarjetas primario a operador	Telefonía externa PSTN

Tabla 16. Enrutamiento centralita sede remota 5.

Por tanto, cuando deba levantar la RDSI de respaldo habrá una llamada desde la sede central hacia la Ruta 1 de la sede remota y la centralita de esta sede la redirigirá hacia la Ruta 61 del enrutador RDSI.

En el siguiente punto, cuando tratemos la configuración de los enrutadores RDSI veremos cómo identificamos cada enlace primario con el nombre de la Ruta de la centralita asociada.

5.4.3 Configuración de los enrutadores RDSI.

Es importante recordar los roles que ocupan los enrutadores RDSI en cada tipo de sede:

- *El enrutador RDSI de la sede central* es el único que tiene configuración para realizar llamadas a los otros enrutadores RDSI de las sedes remotas. Para ello dispone de cuatro primarios, lo que le permite como máximo dar servicio a cuatro sedes a 2 Mbps (30 canales B).
- *El enrutador RDSI de las sedes remotas* no puede lanzar llamadas, sólo recibirlas. Para ello simplemente no incluiremos la opción de llamar *dialer string*[29]. El proceso de convergencia establece que sea el enrutador RDSI de la sede central quien desencadene las conexiones para levantar la WAN de respaldo.

Una vez aclarado este punto entraremos en la configuración propiamente dicha. Para realizar la configuración de los enrutadores la dividiremos en los siguientes apartados:

[29] Sirve para indicar el número de teléfono destino.

1. Tipo de enlace PRI.
2. Configuración de interfaces y subinterfaces.
3. Configuración de enrutamiento estático.
4. Configuración de RIPv2.

Comenzamos con el enrutador RDSI de la sede central:

1. Tipo de enlace PRI.

```
card type e1 1
card type e1 2
!
isdn switch-type primary-net5
!
!
controller E1 1/0
pri-group timeslots 1-31
description Identificador Centralita: Ruta 41
!
controller E1 1/1
pri-group timeslots 1-31
description Identificador Centralita: Ruta 42
```

```
!
controller E1 2/0
pri-group timeslots 1-31
description Identificador Centralita: Ruta 43
!
controller E1 2/1
pri-group timeslots 1-31
description Identificador Centralita: Ruta 44
!
```

2. Configuración de interfaces y subinterfaces.

```
interface GigabitEthernet0/1
no ip address
 no ip redirects
 no ip route-cache cef
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1.10
description VLAN de interconexión sede central
encapsulation dot1Q 10
ip address 192.170.0.150 255.255.255.0
 no ip redirects
no ip unreachables
 no ip proxy-arp
ip rip authentication mode md5
ip rip authentication key-chain RIP
no cdp enable
!
!
interface Serial1/0:15
description Identificador Centralita: Ruta 41
no ip address
 encapsulation ppp
 dialer pool-member 1
```

```
!
interface Dialer4
description RDSI a sede 4
ip address 10.10.10.4 255.255.255.0
 encapsulation ppp
 dialer pool 2
 dialer idle-timeout 300
 dialer string <nº teléfono sede 4>
 dialer-group 1
 no cdp enable
ppp multilink
ppp multilink links maximum 30
ppp multilink links minimum 30
!
!
interface Dialer5
description RDSI a sede5
ip address 10.10.10.5 255.255.255.0
 encapsulation ppp
 dialer pool 3
 dialer idle-timeout 300
dialer string<nº teléfono sede 5>
dialer-group 1
 no cdp enable
ppp multilink
```

```
 isdn switch-type primary-net5
 isdn calling-number <nº teléfono origen>
ppp multilink
!
interface Serial1/1:15
 description Identificador Centralita: Ruta 42
 no ip address
 encapsulation ppp
 dialer pool-member 2
 isdn switch-type primary-net5
 isdn calling-number <nº teléfono origen>
 no cdp enable
ppp multilink
!
interface Serial2/0:15
description Identificador Centralita: Ruta 43
no ip address
 encapsulation ppp
 dialer pool-member 3
 isdn switch-type primary-net5
 isdn calling-number <nº teléfono origen>
 no cdp enable
ppp multilink
!
interface Serial2/1:15
description Identificador Centralita: Ruta 44
no ip address
 encapsulation ppp
 dialer pool-member 3
 isdn switch-type primary-net5
 isdn calling-number <nº teléfono origen>
 no cdp enable
ppp multilink
!
!
interface Dialer1
description RDSI a sede 1
ip address 10.10.10.1 255.255.255.0
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 300
 dialer string <nº teléfono sede 1>
 dialer-group 1
 no cdp enable
ppp multilink
ppp multilink links maximum 30
ppp multilink links minimum 30
!
!
interface Dialer2
ppp multilink links maximum 30
ppp multilink links minimum 30
!
!
interface Dialer6
description RDSI a sede 6
ip address 10.10.10.6 255.255.255.0
 encapsulation ppp
 dialer pool 3
 dialer idle-timeout 300
 dialer string <nº teléfono sede 6>
 dialer-group 1
 no cdp enable
ppp multilink
ppp multilink links maximum 30
ppp multilink links minimum 30
!
!
interface Dialer7
 description RDSI a sede7
ip address 10.10.10.7 255.255.255.0
 encapsulation ppp
 dialer pool 3
 dialer idle-timeout 300
dialer string<nº teléfono sede 7>
dialer-group 1
 no cdp enable
ppp multilink
ppp multilink links maximum 30
ppp multilink links minimum 30
!
!
interface Dialer8
description RDSI a sede 8
ip address 10.10.10.8 255.255.255.0
 encapsulation ppp
 dialer pool 4
dialer idle-timeout 300
dialer string <nº teléfono sede 8>
dialer-group 1
 no cdp enable
ppp multilink
ppp multilink links maximum 30
ppp multilink links minimum 30
!
!
interface Dialer9
 description RDSI a sede9
ip address 10.10.10.9 255.255.255.0
 encapsulation ppp
```

```
 description RDSI a sede 2
ip address 10.10.10.2 255.255.255.0
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 300
dialer string<nº teléfono sede 2>
dialer-group 1
 no cdp enable
ppp multilink
ppp multilink links maximum 30
ppp multilink links minimum 30
!
!
interface Dialer3
description RDSI a sede 3
ip address 10.10.10.3 255.255.255.0
 encapsulation ppp
 dialer pool 2
 dialer idle-timeout 300
 dialer string <nº teléfono sede 3>
 dialer-group 1
 no cdp enable
ppp multilink
ppp multilink links maximum 30
ppp multilink links minimum30
!
```

```
 dialer pool 4
 dialer idle-timeout 300
dialer string<nº teléfono sede 9>
dialer-group 1
 no cdp enable
ppp multilink
ppp multilink links maximum 30
ppp multilink links minimum 30
!
!
interface Dialer10
description RDSI a sede 10
ip address 10.10.10.10 255.255.255.0
 encapsulation ppp
 dialer pool 4
 dialer idle-timeout 300
dialer string <nº teléfono sede 10>
dialer-group 1
 no cdp enable
ppp multilink
ppp multilink links maximum 30
ppp multilink links minimum 30
!
access-list 125 remark Trafico por  RDSI
access-list 125 permit ip any any
dialer-list 1 protocol ip list 125
```

3. Configuración de enrutamiento estático.

```
ip route 0.0.0.0 0.0.0.0 null0
ip route 172.16.0.0 255.255.0.0 192.170.0.3
ip route 194.224.177.0 255.255.225.224 192.170.0.3
ip route192.170.1.0 255.255.255.0 10.10.10.11 150
ip route192.170.2.0 255.255.255.0 10.10.10.12 150
ip route192.170.3.0 255.255.255.0 10.10.10.13 150
ip route 192.170.4.0 255.255.255.0 10.10.10.14 150
ip route 192.170.5.0 255.255.255.0 10.10.10.15 150
ip route 192.170.6.0 255.255.255.0 10.10.10.16 150
ip route 192.170.7.0 255.255.255.0 10.10.10.17 150
ip route 192.170.8.0 255.255.255.0 10.10.10.18 150
ip route 192.170.9.0 255.255.255.0 10.10.10.19 150
ip route 192.170.10.0 255.255.255.0 10.10.10.20 150
ip route 172.21.0.0 255.255.128.0 10.10.10.11 150
ip route 172.22.0.0 255.255.128.0 10.10.10.12 150
ip route 172.23.0.0 255.255.128.0 10.10.10.13 150
ip route 172.24.0.0 255.255.128.0 10.10.10.14 150
ip route 172.25.0.0 255.255.128.0 10.10.10.15 150
ip route 172.26.0.0 255.255.128.0 10.10.10.16 150
ip route 172.27.0.0 255.255.128.0 10.10.10.17 150
```

```
ip route 172.28.0.0 255.255.128.0 10.10.10.18 150
ip route 172.29.0.0 255.255.128.0 10.10.10.19 150
ip route 172.30.0.0 255.255.128.0 10.10.10.20 150
```

4. Configuración de RIPv2.

```
!
key chain RIP
 key 1
  key-string 7 0393823981B38721893
  accept-lifetime 00:00:00 Jan 1 1993 infinite
  send-lifetime 00:00:00 Jan 1 1993 infinite
!
!
interface GigabitEthernet0/1.10
 description VLAN de interconexion
 encapsulation dot1Q 10
ip address 192.170.0.150 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
ip rip authentication mode md5
ip rip authentication key-chain RIP
no cdp enable
!
!
enrutador rip
 version 2
 passive-interface default
 network 192.170.0.0
 default-metric 14
no auto-summary
!
```

Para la configuración de las sedes remotas volveremos a utilizar la sede remota 5 como ejemplo. Todas las sedes tendrían la misma configuración a excepción del direccionamiento IP, el cual se puede conocer de las tablas expuestas anteriormente.

1. Tipo de enlace PRI.

```
!
card type e1 1
!
isdn switch-type primary-net5
!
!
controller E1 1/0
pri-group timeslots 1-31
```

```
!
```

2. Configuración de interfaces y subinterfaces.

```
!
interface FastEthernet0/0
 no ip address
 duplex full
 speed auto
!
interface FastEthernet0/0.10
 description VLAN de interconexion
 encapsulation dot1Q 10
ip address 192.170.5.150 255.255.255.0
 no ip redirects
no ip unreachables
 no ip proxy-arp
ip rip authentication mode md5
ip rip authentication key-chain RIP
no cdpenable
!
```

```
!
interface Serial1/0:15
 no ip address
 encapsulation ppp
 dialer pool-member 1
 isdn switch-type primary-net5
 no cdp enable
ppp multilink
!
interface Dialer0
description RDSI a sede central
ip address 10.10.10.15 255.255.255.0
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 300
 dialer-group 1
 no cdp enable
ppp multilink
ppp multilink links maximum 30
ppp multilink links minimum 30
!
dialer-list 1 protocol ip permit
```

3. Configuración de enrutamiento estático.

```
ip route 0.0.0.0 0.0.0.0 10.10.10.5 150
ip route 172.25.0.0 255.255.128.0 192.170.5.3
```

4. Configuración de RIPv2.

```
!
keychain RIP
 key 1
  key-string 7 5020B05321332312321
   accept-lifetime 00:00:00 Jan 1 1993 infinite
   send-lifetime 00:00:00 Jan 1 1993 infinite
!
interface FastEthernet0/0.10
description VLAN de interconexión sede 5
encapsulation dot1Q 10
ip address 192.17.5.150 255.255.255.0
 no ip redirects
no ip unreachables
```

```
 no ip proxy-arp
ip rip authentication mode md5
ip rip authentication key-chain RIP
no cdp enable
!
!
enrutador rip
 version 2
network 192.170.5.0
!
```

5.4.4 Configuración de los cortafuegos.

La conexión física del cortafuegos a la red la podemos visualizar en la siguiente gráfica:

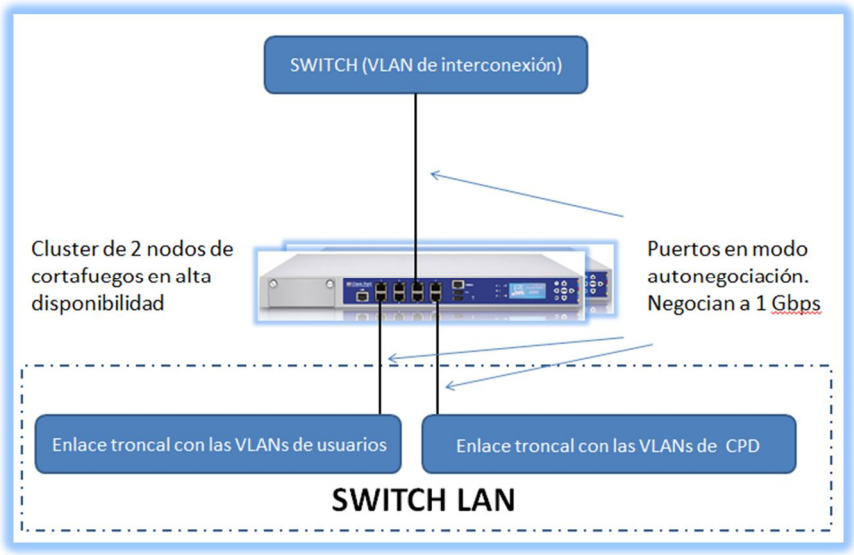


Figura 33. Esquema físico de las conexiones del cortafuegos.

La presentación de la configuración de los cortafuegos la dividiremos en los siguientes apartados:

1. Configuración de interface de la VLAN de interconexión.
2. Configuración de enrutamiento estático.
3. Configuración de RIPv2.

El cortafuegos de la sede central presenta la siguiente configuración:

1. Configuración de interface de la VLAN de interconexión.

```
NODO1
18: Lan1.10@Lan1: <BROADCAST,MULTICAST,UP,10000>mtu 1500 qdiscnoqueue
   link/ether 00:90:fb:2c:26:65 brdff:ff:ff:ff:ff:ff
inet 192.170.0.1/24 brd 192.170.0.255 scope global Lan1.10
NODO 2
18: Lan1.10@Lan1: <BROADCAST,MULTICAST,UP,10000>mtu 1500 qdiscnoqueue
   link/ether 00:90:fb:2c:26:65 brdff:ff:ff:ff:ff:ff
inet 192.170.0.2/24 brd 192.170.0.255 scope global Lan1.10
```

```
IP VIRTUAL DEL CLUSTER
Lan4.10        192.170.0.3
```

2. Configuración de enrutamiento estático.
   Se presentan aquellas rutas que afectan a la red interconexión.

```
Kernel IP enrutamiento table

Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.170.1.0     10.10.10.11     255.255.255.0   UG    150    0        0 Lan1.10
192.170.2.0     10.10.10.12     255.255.255.0   UG    150    0        0 Lan1.10
192.170.3.0     10.10.10.13     255.255.255.0   UG    150    0        0 Lan1.10
192.170.4.0     10.10.10.14     255.255.255.0   UG    150    0        0 Lan1.10
192.170.5.0     10.10.10.15     255.255.255.0   UG    150    0        0 Lan1.10
192.170.6.0     10.10.10.16     255.255.255.0   UG    150    0        0 Lan1.10
192.170.7.0     10.10.10.17     255.255.255.0   UG    150    0        0 Lan1.10
192.170.8.0     10.10.10.18     255.255.255.0   UG    150    0        0 Lan1.10
192.170.9.0     10.10.10.19     255.255.255.0   UG    150    0        0 Lan1.10
192.170.10.0    10.10.10.20     255.255.255.0   UG    150    0        0 Lan1.10
172.21.0.0      10.10.10.11     255.255.128.0   UG    150    0        0 Lan1.10
172.22.0.0      10.10.10.12     255.255.128.0   UG    150    0        0 Lan1.10
172.23.0.0      10.10.10.13     255.255.128.0   UG    150    0        0 Lan1.10
172.24.0.0      10.10.10.14     255.255.128.0   UG    150    0        0 Lan1.10
172.25.0.0      10.10.10.15     255.255.128.0   UG    150    0        0 Lan1.10
172.26.0.0      10.10.10.16     255.255.128.0   UG    150    0        0 Lan1.10
172.27.0.0      10.10.10.17     255.255.128.0   UG    150    0        0 Lan1.10
172.28.0.0      10.10.10.18     255.255.128.0   UG    150    0        0 Lan1.10
172.29.0.0      10.10.10.19     255.255.128.0   UG    150    0        0 Lan1.10
172.30.0.0      10.10.10.20     255.255.128.0   UG    150    0        0 Lan1.10
192.170.0.0     *               255.255.255.0   U     0      0        0 Lan1.10
0.0.0.0         192.170.0.150   0.0.0.0         UG    10     0        0 Lan1.10
```

3. Configuración de RIPv2.
   El cortafuegos alimenta su tabla de enrutamiento con las rutas aprendidas por RIP anunciadas por el enrutador WAN. A esas rutas le damos preferencia 5 para que tomen preferencia sobre las rutas estáticas del sistema.
   Mostramos la configuración del demonio *Gated*[30] que es el responsable del funcionamiento del protocolo RIP en el cortafuegos:

```
enrutador rip
   enable
   preference 5
   trusted-gateway 192.170.0.252
   network 192.174.0.0 0.0.0.255
   exit
interface Lan1.10
ip rip no-send
ip rip enable
ip rip version 2
```

[30] Proceso que gestiona los protocolos de enrutamiento en el cortafuegos.

```
ip rip authentication md5 1 <mypassword>
exit
```

El cortafuegos de la sede remota 5 presenta la siguiente configuración:

1. Configuración de interface de la VLAN de interconexión. Indicamos como se hizo en la sede central las IPs físicas y virtual del interface.

```
NODO1
18: Lan1.10@Lan1: <BROADCAST,MULTICAST,UP,10000>mtu 1500 qdiscnoqueue
   link/ether 00:90:fb:2c:26:65 brdff:ff:ff:ff:ff:ff
inet 192.170.5.1/24 brd 192.170.0.255 scope global Lan1.10
NODO 2
18: Lan1.10@Lan1: <BROADCAST,MULTICAST,UP,10000>mtu 1500 qdiscnoqueue
   link/ether 00:90:fb:2c:26:65 brdff:ff:ff:ff:ff:ff
inet 192.170.5.2/24 brd 192.170.5.255 scope global Lan1.10
IP VIRTUAL DEL CLUSTER
Lan4.10        192.170.5.3
```

2. Configuración de enrutamiento estático.
   En las sedes remotas le damos métrica a la ruta estática por defecto para que cuando se aprenda la de RIP tome preferencia sobre esta.

```
Kernel IP enrutamiento table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.170.5.0     *               255.255.255.0   U     0      0        0 Lan1.10
0.0.0.0         192.170.5.150   0.0.0.0         UG    10     0        0 Lan1.10
```

3. Configuración de RIPv2.
   Es similar a la del cortafuegos de la sede central variando el direccionamiento.

```
enrutador rip
   enable
   preference 5
   trusted-gateway 192.170.5.252
   network 192.174.5.0 0.0.0.255
   exit
interface Lan1.10
ip rip no-send
ip rip enable
ip rip version 2
ip rip authentication md5 1 <mypassword>
exit
```

Finalmente hemos añadido una regla a la política del cortafuegos para que acepte el tráfico RIP que proviene del enrutador WAN. Se muestra el detalle de la regla:

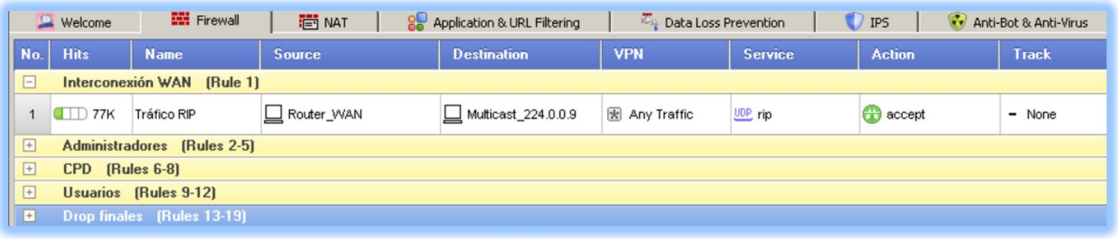


Figura 34. Regla para permitir tráfico RIP.

5.4.5 Configuración de los gestores de ancho de banda.

Respecto al gestor de ancho de banda decir que tiene dos segmentos diferenciados, uno que será el que se conectará para interferir en el flujo de tráfico de la WAN de la operadora, y otro para hacer lo mismo con el flujo de la WAN de respaldo. A continuación se muestra su conexionado físico en un dibujo. Tenemos dos interfaces de entrada y dos de salida, una pareja en puertos del chasis y otra pareja en la tarjeta de expansión LEM que hemos añadido. Se puede apreciar que el equipo tiene dos enlaces amarillos, que son los conectados hacia los dispositivos de salida y dos negros, conectados a la LAN. Describimos cada pareja:

- Un enlace amarillo, que es un cable cruzado de pares conectado al enrutador WAN y una cable normal de pares conectado a un conmutador de la electrónica de la LAN de la sede. El dispositivo administrará el tráfico que venga y vaya a la WAN de la operadora.
- Un enlace amarillo igual que el anterior conectado al enrutador RDSI y otro cable conectado a un conmutador de la LAN. Será preferible que sea distinto que el anterior.

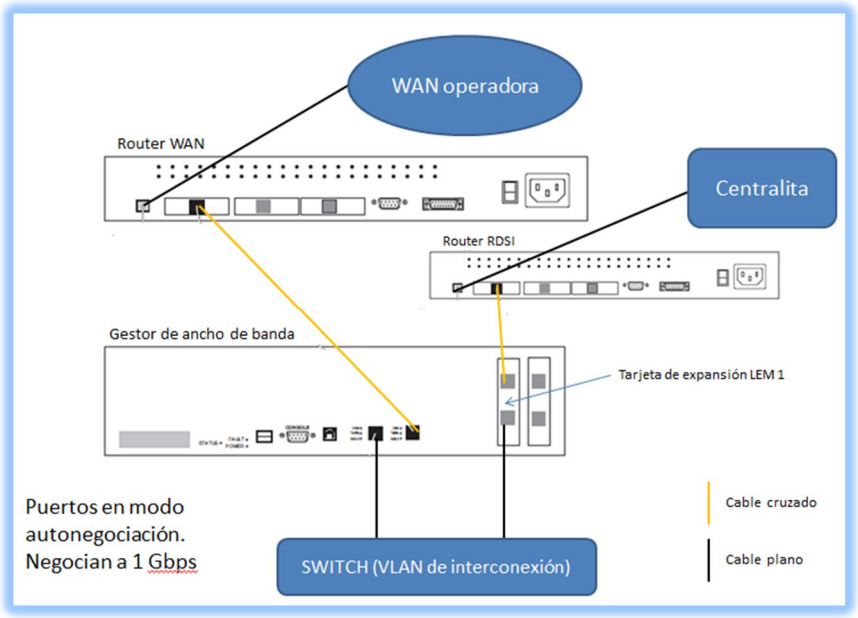


Figura 35. Esquema físico de conexiones del gestor de ancho de banda.

El gestor de ancho de banda no tiene ni direccionamiento IP ni tabla de enrutamiento. Él exclusivamente se dedica a coger el tráfico que le cruza y aplicar la política de que tiene definida.

Esta política aplica en nuestro caso al tráfico que viene desde o hacia el enrutador WAN y el tráfico que viene o va al enrutador RDSI. En la siguiente captura vemos como hay dos perfiles configurados, para tráfico de entrada (inbound) y de salida (outbound) con las configuraciones de las clases de los distintos tipos de aplicaciones para el flujo por la WAN de la operadora y por el camino alternativo por la WAN RDSI.

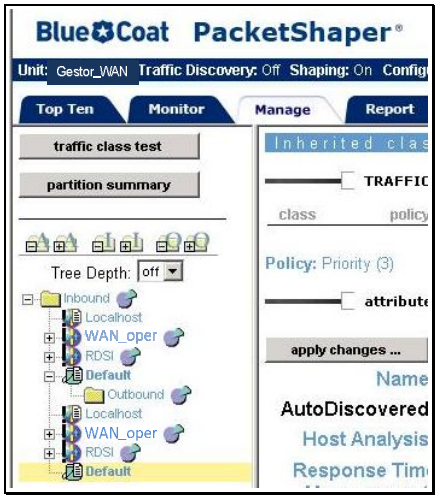


Figura 36. Tabla de clases.

5.5 Descripción del proceso de convergencia a la WAN de respaldo.

Los motivos que pueden desencadenar que la red tenga que cambiar su topología y converger hacia la WAN de respaldo son los siguientes:

- Mala configuración o problemas en la WAN de la operadora que implique que las rutas no sean correctamente propagadas a las sedes, concretamente a la sede central que es la responsable de iniciar el levantamiento de enlaces RDSI.
- Apagado o fallo en el conmutador de la red de la sede en donde esté conectado el enrutador WAN.
- Caída o fallo del puerto del conmutador o del enrutador WAN.
- Desconexión del cable que conecta con el enrutador WAN.

Aclarar que si fallase el cortafuegos porque no aprende las rutas RIP, éste derivaría el tráfico hacia el enrutador RDSI por su ruta estática por defecto. El enrutador RDSI, como también aprende RIP, sabría reencaminar el tráfico hacia donde fuere necesario.

El proceso de convergencia a la WAN de respaldo sería el siguiente:

Una vez se ha producido el aislamiento de la sede remota, la WAN de la operadora debe converger e informar al resto de sedes que una sede no es alcanzable. Esto lo realiza no

propagando por RIP, en ninguna sede, las rutas hacia las redes de esa sede problemática. Eso sucede aproximadamente en un máximo de 180 segundos. Llegados a este punto, todo el tráfico que vaya hacia esa sede será depositado en la sede central, concretamente dirigido a su cortafuegos WAN (recordar que es uno de los requisitos que debe cumplir la operadora).

Paralelamente en la sede remota que se ha quedado aislada lo que está sucediendo es que al perder la conexión con la WAN, el cortafuegos ha perdido la convergencia RIP y por lo tanto se apoya en sus rutas estáticas encaminando todo su tráfico a la ruta estática por defecto, esto es, al enrutador RDSI. Pero el enrutador RDSI no puede realizar llamadas, por lo que ha de esperar a la llamada proveniente del enrutador RDSI de la sede central. Este tráfico cruza el gestor de ancho de banda por su interface LEM.

Volviendo a la sede central, el cortafuegos WAN no tiene ruta para alcanzar la sede aislada, por lo que revierte hacia su ruta por defecto que es el enrutador RDSI. Este tráfico cruzará la tarjeta LEM del gestor de ancho de banda y aplicará la política de tráfico de ese enlace.

El enrutador RDSI también ha perdido la ruta RIP para alcanzar la sede remota. Tiene por tanto que utilizar las rutas estáticas para alcanzarla, cuya salto es la IP del enlace conectado al primario del enrutador RDSI de la sede remota. Esta configuración provoca que el enrutador desencadene una llamada hacia el destino que es el enrutador RDSI de la sede aislada y levante los 30 canales del primario RDSI que le facilitarán unos 2 Mbps de ancho de banda.

De esta manera el tráfico comenzará a cursarse y se salvará el servicio entre la sede remota y el resto de la red empresarial.

Cuando se recupere la conectividad de la sede con la WAN principal las rutas asociadas a esa sede se volverán a propagar en la interconexión de las sedes y por lo tanto la red volverá a converger hacia la WAN principal. Se caerán los enlaces RDSI que hemos levantado pasados 300 segundos de inactividad.

Esta solución nos permite garantizar la conectividad, y por tanto los servicios entre la sede central y todas las delegaciones.

Respecto al tráfico de voz decir que hay un proceso que automatice que curse las llamadas por los primarios con la operadora cuando falle la comunicación IP entre centralitas. Solamente si se cayese el interfaz físico conectado a las centralitas, éstas usarían otro camino alternativo. Por tanto en la mayoría de casos será la intervención manual quien deba actuar para conmutar el servicio.

SEXTA PARTE: ¿CUÁNTO NOS VA A COSTAR?

6 ESTUDIO ECONÓMICO

A continuación veremos que el desembolso que le exigirá a la empresa implementar esta solución es del todo asumible; y aunque en un primer momento tendrá que asumir un desembolso mayor, en un periodo escaso de tiempo verá recuperada esta inversión inicial.

6.1 Plan de despliegue.

Será el personal del departamento IT el encargado de asumir el despliegue e implantación del material. La empresa cuenta con un equipo técnico para operaciones, mantenimiento y explotación del parque de comunicaciones e informática de cada sede.

En el plan de despliegue se establece que será desde la sede central desde donde se coordinarán todas las tareas. Eso se realizará así por dos motivos:

1. Es el lugar que tiene una visión global de la WAN.
2. Será el punto único de comunicación con la operadora.

Por tanto, se plantea un plan de despliegue en tres fases a llevar a cabo en siete semanas, tal como se muestra en el siguiente diagrama temporal.

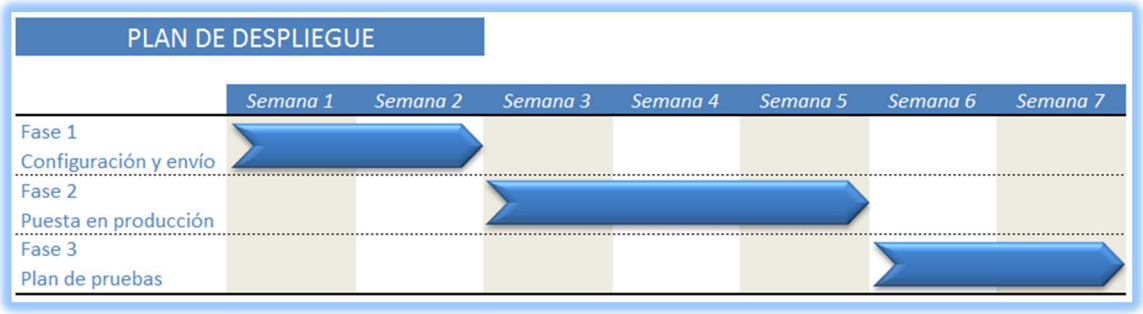


Figura 37. Plan de despliegue.

La *Fase 1* se iniciará una vez se haya recibido el material en la sede central. Durante este periodo se realizará una configuración base de cada enrutador adaptando ésta al direccionamiento de cada sede. Una vez configurado se enviará a la sede correspondiente el enrutador más la tarjeta LEM para el gestor de ancho de banda. Así se hará con las 10 sedes.

Además se configurará el enrutador de la sede central con la configuración específica para poder dar servicio a todas las sedes.

En la *Fase 2* se realizarán las siguientes tareas:

a. Se conectarán los enrutadores a la red de las distintas sedes y se conectarán los enlaces a los primarios de la centralita y se realizará la configuración específica de cada elemento.

b. Se montarán las tarjetas LEM en los gestores de ancho de banda y se adaptará la configuración para que opere con los enlaces de respaldo que cruzarán la LEM.
c. Se solicitará a la operadora que propague las rutas dinámicamente a las interconexiones con todas las sedes mediante el protocolo RIPv2 autenticado por clave.
d. Se configurarán los procesos de enrutamiento de los cortafuegos para escuchar RIPv2. Se habilitarán reglas para aceptar este tráfico proveniente del enrutador de la operadora.

Finalmente, en la *Fase 3*, se realizarán las pruebas de funcionamiento:

a. Se comprobará que la operadora propaga correctamente las rutas en todas las sedes.
b. Se harán llamadas desde el enrutador de la sede central a cada sede remota para ver que levanta los canales de la RDSI.
c. Se comprobará desconectando el enrutador WAN principal de una sede que la red converge hacia la WAN de enlaces RDSI.
d. Se comprobará la convergencia del gestor de ancho de banda cuando se activa el tráfico por el enlace de respaldo.

6.2 Coste del proyecto.

Para evaluar el coste total del proyecto primero se presentará desglosado el presupuesto del material que necesitamos.

PRESUPUESTO DEL MATERIAL

Concepto / Código producto	*Descripción*	*Unidades*	*Precio/unidad (*)*	*Precio total (*)*
Router Cisco 3925 C3925E-CME-SRST/K9	Router RDSI para la sede central.	1	$9.897	$9.897
Router Cisco 2911 C2911-CME-SRST/K9	Router RDSI para cada sede remota.	10	$2.997	$29.970
HWIC-2CE1T1-PRI	Tarjeta de 2 puertos primario RDSI para el router Cisco 3925 de la sede central.	2	$2.520	$5.040
HWIC-1CE1T1-PRI	Tarjeta de 1 puertos primario RDSI para el router Cisco 2911 de cada sede remota.	10	$1.560	$15.600
Bluecoat Packetshaper LEM-1000M-HH-T	Tarjeta de expansión con dos puertos 1000BaseT para gestionar el tráfico de los enlaces RDSI de los gestores de ancho de banda de todas las sedes.	11	$738	$8.118
		Coste total (*)		$60.507

(*) precios en dólares

Tabla 17. Presupuesto del material.

A continuación se mostrará el presupuesto de personal en el que se han definido dos perfiles y su consiguiente precio/hora:

- *Gestor de proyecto*: Estará a tiempo parcial supervisando que las tareas se van ejecutando tal como se han planificado. Dará validez a cada fase del proyecto.
- *Técnico de la sede central*: Será el encargado de realizar la configuración inicial de todo el equipamiento y su posterior envío a las distintas sedes. De igual manera coordinará las

pruebas que se realicen para confirmar la puesta a punto de la solución entre la sede central y las distintas sedes.

- *Técnicos de las sedes remotas*: Recibirán el equipamiento ya configurado, lo montará en su ubicación física y seguirá las indicaciones desde la sede central para realizar la puesta en producción y las posteriores pruebas.

PRESUPUESTO DE PERSONAL					
Rol	*Unidades*	*Jornadas*	*Horas*	*Precio/hora*	*Precio total*
Gestor de proyecto	1	10	80	60 €	4.800 €
Técnico de la sede central	1	35	280	40 €	11.200 €
Técnicos de ls sedes remotas	10	2,5	25	25 €	6.250 €
			Coste total		22.250 €

Tabla 18. Presupuesto de personal.

Respecto a los recursos humanos necesarios para hacer la implementación, serán los miembros del mismo departamento IT los encargados de configurar el equipamiento, hacer el despliegue en las sedes y realizar las peticiones a la operadora para adaptar las configuraciones de la WAN principal a las necesidades del sistema de respaldo.

Por último comentar que el material que no se indica es material que ya debe existir en la infraestructura de los CPDs de las sedes: cableado de red, tomas de corriente, espacio en los armarios de comunicaciones, etc.

Con todos estos factores y los cálculos hechos en euros se presenta el importe completo que requiere el proyecto:

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

Tabla 19. Presupuesto total del proyecto.

6.3 Viabilidad del presupuesto del proyecto.

La necesidad de abordar una solución alternativa para resolver la conectividad de la WAN empresarial ante un fallo surge por el elevado coste de la solución propuesta por la operadora para dar solución a este requerimiento.

En el siguiente cuadro se presenta el presupuesto inicial facilitado por la operadora para 3 años de duración. Si bien los datos finales serían negociables ya el cómputo anual se presenta excesivamente caro.

PRESUPUESTO WAN RESPALDO OPERADORA				PRESUPUESTO POR AÑO		
Concepto	*Unidades*	*Precio/linea*	*Cuota mensual*	*Año 1*	*Año 2*	*Año 3*
Alta de linea ADSL VPN-IP 2Mbps	10	0,00 €	0,00 €	0 €	0 €	0 €
Caudal de tráfico en la WAN (150 Mbps)	1	0,00 €	2.500,00 €	30.000 €	30.000 €	30.000 €
Cuota línea/servicio ADSL VPN-IP + mantenimiento equipamiento router	10	0,00 €	175,00 €	21.000 €	21.000 €	21.000 €
			Coste total por año	51.000 €	51.000 €	51.000 €

Tabla 20. Presupuesto de la operadora.

Por lo tanto, el proyecto que se plantea como alternativa a éste, pretende dotar de una solución de respaldo que facilite a la empresa la continuidad de su operativa ante un fallo de sus enlaces WAN principales. El coste final del mismo, que asciende a poco más de 65.000 euros, cubre estas necesidades que puede requerir la red en un momento dado, y también aporta la funcionalidades necesarias para realizar automáticamente la adaptación de la red ante una caída. La arquitectura elegida es totalmente escalar y reutilizable, ya que permite adaptarse a nuevas tecnologías de conectividad y velocidad necesitando simplemente la adquisición de tarjetas de expansión.

Ciñéndose al aspecto puramente económico comentar que en la fase inicial del proyecto se tendrá que asumir la mayor parte del desembolso, ya que habrá que adquirir todo el material. Pero una vez superado ese momento, a medida que avance el tiempo, supondrá un rápido ROI (retorno de la inversión) debido a que el coste real después de haber realizado el despliegue será el del uso de los enlaces RDSI más el mantenimiento del hardware con el soporte correspondiente contratado al fabricante; unos 5000 €/año.

El coste de mantenimiento de numeración con la operadora y de los primarios RDSI sigue siendo el mismo que la empresa tenía previamente.

Finalmente comentar, que al realizar el proyecto con recursos propios de la empresa supondrá también una inversión formación y experiencia en el trabajo con nuevas tecnologías. Esta formación que se asumirá a medida que se vaya desarrollando el proyecto será fundamental para las actuaciones reactivas y proactivas de administración, evolución y mantenimiento de la infraestructura.

Se presenta en modo esquemático una valoración del ROI que presentaría este proyecto a 3 años.

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

Tabla 21. Retorno de la inversión.

Se puede comprobar en el cuadro que en el segundo año ya se ha rentabilizado la inversión inicial.

SÉPTIMA PARTE: ¡PROBEMOS SI FUNCIONA!

7 LABORATORIO DE PRUEBAS

Una vez definido el proyecto, seleccionado los elementos que lo conforman y la configuración que precisarán, se va a emular un entorno de pruebas donde se pueda demostrar el funcionamiento de la solución propuesta. Aunque debido a la dificultad que conlleva disponer del material para simular le tráfico de voz y su comportamiento ante la caída, se ceñirá a salvaguardar al tráfico de datos. El laboratorio simulará la sede central y una sede remota.

Para el laboratorio se ha diseñado el siguiente esquema de red:

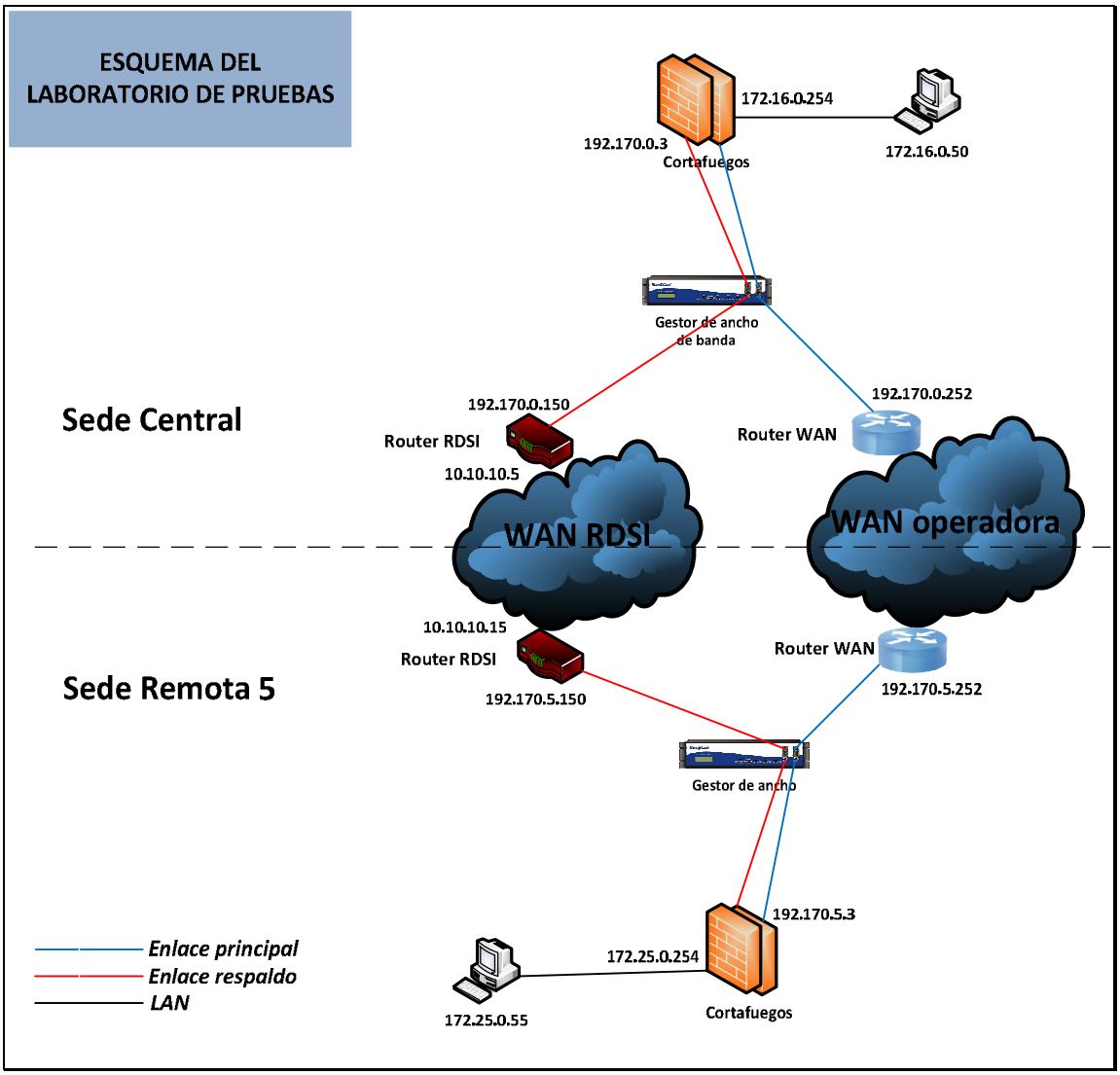


Figura 38. Esquema del laboratorio de pruebas.

7.1 Plan de pruebas.

El plan de pruebas se ha basado en la simulación de la caída de una sede remota y la consiguiente activación del proceso automatizado que conlleva a levantar la comunicación entre la sede central y esa sede remota a través de la WAN de respaldo RDSI.

Partimos de una situación inicial donde el tráfico está discurriendo con normalidad por la WAN principal. La convergencia RIPv2 entre enrutadores y cortafuegos está operativa. Se muestra la tabla de enrutamiento de ambos cortafuegos donde se puede ver que toma preferencia la ruta que apunta hacia el enrutador WAN, tanto en la sede central como en la sede remota.

```
Rutas del cortafuegos de la sede central
192.170.0.0   *              255.255.255.0  U      0     0     0    Lan1.10
0.0.0.0       192.170.0.150  0.0.0.0        UG     10    0     0    Lan1.10
0.0.0.0       192.170.0.252  0.0.0.0        UGD5 0       0 Lan1.10
Rutas del cortafuegos de la sede remota 5
192.170.5.0   *              255.255.255.0  U      0     0     0    Lan1.10
0.0.0.0       192.170.5.150  0.0.0.0        UG     10    0     0    Lan1.10
0.0.0.0       192.170.5.252  0.0.0.0        UGD5 0       0 Lan1.10
```

A continuación se simulará un fallo y el posterior proceso de convergencia paso a paso para dar mayor claridad a la prueba:

1. Se produce un fallo en la conectividad de la sede remota con la WAN de la operadora. Se ha dejado un lanzado un ping desde la estación de trabajo de la sede central a la sede remota y se ve que deja de responder.

```
C:\Users\PC_SEDE_CENTRAL>time
La hora actual es: 15:05:18,69
C:\Users\PC_SEDE_CENTRAL>ping 172.25.0.55 –n 6
Haciendo ping a 172.25.0.55 con 32 bytes de datos:
Respuesta desde 172.25.0.55: bytes=32 tiempo=82ms TTL=111
Respuesta desde 172.25.0.55: bytes=32 tiempo=64ms TTL=111
Respuesta desde 172.25.0.55: bytes=32 tiempo=68ms TTL=111
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
```

2. Seguidamente, debido a que la sede está aislada, el enrutador WAN deja de propagar rutas a esa sede y el cortafuegos , por tanto, las pierde de su tabla de rutas. A partir de aquí hará caso a su ruta por defecto que apunta hacia el enrutador RDSI.

```
Rutas del cortafuegos de la sede central
192.170.0.0   *              255.255.255.0  U      0     0     0    Lan1.10
0.0.0.0       192.170.0.150  0.0.0.0        UG     10    0     0    Lan1.10
Rutas del cortafuegos de la sede remota 5
192.170.5.0   *              255.255.255.0  U      0     0     0    Lan1.10
0.0.0.0       192.170.5.150  0.0.0.0        UG     10    0     0    Lan1.10
```

3. El enrutador RDSI de la sede central comienza a recibir tráfico proveniente del cortafuegos con destino las redes de la sede remota. Esto hace que el enrutador desencadene una serie de llamadas hacia el enrutador RDSI de la sede remota 5. Se ve en el cuadro la emisión de las llamadas desde la sede central y la recepción en la sede remota 5.

```
RDSI_SEDE_CENTRAL#show isdn active
--------------------------------------------------------------------------------
                    ISDN ACTIVE CALLS
--------------------------------------------------------------------------------
Call    Calling     Called      Remote  Seconds Seconds Seconds Charges
Type    Number      Number      Name    Used    Left    Idle    Units/Currency
--------------------------------------------------------------------------------
Out   93XXXXXXX +091XXXXXXX    RDSI_SEDE_5    8773     0     0     0
Out   93XXXXXXX +091XXXXXXX    RDSI_SEDE_5    8764     0     0     0
Out   93XXXXXXX +091XXXXXXX    RDSI_SEDE_5    8755     0     0     0
Out   93XXXXXXX +091XXXXXXX    RDSI_SEDE_5    8747     0     0     0
Out   93XXXXXXX +091XXXXXXX    RDSI_SEDE_5    8740     0     0     0

RDSI_SEDE_5#show isdn active
--------------------------------------------------------------------------------
                    ISDN ACTIVE CALLS
--------------------------------------------------------------------------------
Call    Calling     Called      Remote  Seconds Seconds Seconds Charges
Type    Number      Number      Name    Used    Left    Idle    Units/Currency
--------------------------------------------------------------------------------
In    93XXXXXXXXXXX  RDSI_PIO_A     508 Unavail   -
In    93XXXXXXXXXXX  RDSI_PIO_A     507 Unavail   -
In    93XXXXXXXXXXX  RDSI_PIO_A     507 Unavail   -
In    93XXXXXXXXXXX  RDSI_PIO_A     507 Unavail   -
In    93XXXXXXXXXXX  RDSI_PIO_A     506 Unavail   -
```

4. Una vez que los enlaces están levantados se comprueba que el tráfico se está enrutando a través de los enlaces de respaldo. El siguiente cuadro presenta una traza desde el equipo de la sede central hacia el equipo de la sede remota.

```
D:\Users\PC_SEDE_CENTRAL>tracert -d 172.25.0.55
Traza a 20.0.0.100 sobre caminos de 30 saltos como máximo.
1    <1 ms<1 ms<1 ms  172.16.0.254
 2    1 ms85ms    85ms  192.170.0.150
 4   110 ms    98 ms   100 ms  10.10.10.15
 5    97 ms    89 ms   146 ms  192.170.5.3
6    74 ms    73 ms   76 ms  172.25.0.55
Traza completa.
```

De esta manera el tráfico se ha salvado por el enlace de respaldo y la sede remota se puede seguir comunicando sin problemas. Vemos que el tiempo de corte ha sido de 1 minuto y 22 segundos. Esto engloba el tiempo de detección de error, el tiempo de convergencia de la WAN principal y el del levantamiento de los enlaces de respaldo.

```
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.25.0.55: bytes=32 tiempo=79ms TTL=111
Respuesta desde 172.25.0.55: bytes=32 tiempo=72ms TTL=111
Respuesta desde 172.25.0.55: bytes=32 tiempo=76ms TTL=111
C:\Users\PC_SEDE_CENTRAL>time
La hora actual es: 15:06:40,34
```

Una vez la conexión de la sede remota a la WAN principal se recupera, el proceso se realiza exactamente a la inversa.

1. La red vuelve a converger con las sedes mediante anuncios de rutas vía RIPv2, las tablas de rutas vuelven a estar como al principio y el tráfico vuelve a cursar los enlaces principales. Se puede ver el comportamiento repitiendo la traza del punto anterior.

```
D:\Users\PC_SEDE_CENTRAL>tracert -d 172.25.0.55
Traza a 20.0.0.100 sobre caminos de 30 saltos como máximo.
1    <1 ms<1 ms<1 ms  172.16.0.254
 2    1 ms    82 ms    82 ms  192.170.0.252
3    1 ms    1 ms     2 ms  10.128.248.1
 4    *       *       *      Tiempo de espera agotado para esta solicitud.
 5   27 ms    84 ms    71 ms  81.46.1.217
 6    *       *       *      Tiempo de espera agotado para esta solicitud.
 7    *       *       *      Tiempo de espera agotado para esta solicitud.
8   30 ms    80 ms    74 ms  81.46.16.1
 9   74 ms    73 ms   76 ms  172.25.0.55
Traza completa.
```

2. El tráfico dejar de fluir por las RDSI, y pasado el tiempo de inactividad configurado (300 s), éstas conexiones se cierran. El siguiente cuadro muestra un apunte del log del enrutador RDSI donde se puede ver que se desconecta.

```
003365: Dec8 17:41:13.957: %ISDN-6-DISCONNECT: Interface Serial1/0:15 disconnected from 913278202
RDSI_SEDE_CENTRAL, call lasted 315 seconds
003366: Dec8 17:41:13.981: %LINK-3-UPDOWN: Interface Serial1/0:15, changed state to down
003367: Dep 8 17:41:13.981: %DIALER-6-UNBIND: Interface Se1/0:15 unbound from profile Di1
003368: Dec8 17:41:14.977: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0:15, changed state to down
```

7.2 Análisis de resultados.

Después de haber realizado el plan de pruebas se puede concluir que la solución configurada ha reaccionado según lo previsto y ha resuelto correctamente la pérdida de conectividad de los enlaces principales. De la misma manera, una vez recuperada la conexión se han ido desactivando los enlaces de respaldo.

Los puntos más destacables a tratar son:

- ✓ Los tiempos de respuesta que han dado los pings y las trazas son aceptables para un entorno WAN. En esta prueba, el tiempo de inactividad desde que se ha producido el corte hasta que se ha recuperado el servicio ha sido de alrededor de 1 minuto y medio. Es un corte asumible aunque ajustando los temporizadores del protocolo RIPv2 podría llegar a reducirse. El tiempo de vida de una ruta aprendida por RIP es superior a los 3 minutos y para eliminarse depende de cuando el enrutador de la operadora deje de propagar esa ruta en sus actualizaciones, las cuales son enviadas cada 30 segundos.

- ✓ Respecto al tráfico comentar que este ha sido garantizado por los gestores de ancho de banda, tal como se muestra en las siguientes capturas que se han hecho en la sede remota. Se puede apreciar de una manera clara el momento en el que se produce el fallo y el tiempo que está operando por el enlace de respaldo hasta que se recupera la conexión principal a la WAN de la operadora.

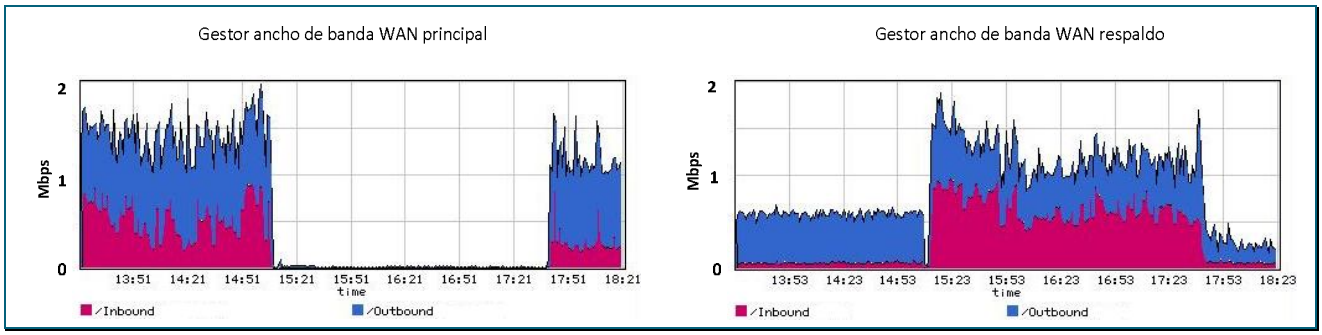


Figura 39. Gráficas de tráfico en las pruebas.

- ✓ En la prueba realizada, los enlaces RDSI han levantado los 30 canales que tenían configurados (2 Mbps total) y una vez recuperada la conectividad principal se han desactivado pasados 5 minutos de inactividad.

- ✓ Las rutas en los cortafuegos se han eliminado/añadido atendiendo al protocolo RIPv2 y han hecho fluir el tráfico tal y como indicaba en cada momento su tabla de enrutamiento.

Como punto final, hacer notar que en estas pruebas sólo se han contemplado las comunicaciones entre una sede remota y la sede central, pero la solución permite responder de igual manera a la necesidad de conectividad de varias sedes remotas.

7.3 Posibles riesgos e incidencias.

El mantenimiento de una red de gran envergadura requiere de procedimientos de actuación para monitorizar el correcto estado de todos los dispositivos. Un equipo técnico dotado de herramientas, conocimientos y procedimientos.

Sin adentrarnos en el tema de monitorización sería conveniente disponer de alguna herramienta SNMP que pueda acceder a los diferentes dispositivos para gestionarlos, así como recibir las alarmas (traps[31]) que puedan generar. No se ha contemplado en el alcance del proyecto pero podría ser una mejora.

Es conveniente chequear periódicamente el estado de salud de los sistemas: en el caso de las conexiones RDSI bastará con lanzar un ping para obligar a levantar las llamadas y así comprobar que todos los canales se levantan correctamente.

En caso de una caída que afectase a la sede central, y pese a tener una conexión secundaria a la operadora no hubiese conectividad, sería posible reconfigurar los enrutadores RDSI y los gestores de ancho de banda para que, disponiendo de menor número de canales y por tanto menor ancho de banda, se pudiese salvar las comunicaciones más críticas. El sistema nos permite repartir los canales de los primarios RDSI entre las distintas conexiones a las sedes.

Si se produjesen problemas porque el cortafuegos no aprendiese correctamente las rutas recibidas por RIPv2 y por tanto encaminase todo el tráfico al enrutador RDSI, se podría conmutar al nodo pasivo del cortafuegos si es un problema de ese nodo únicamente u operar manualmente para introducir las rutas estáticas necesarias mientras se encontrase el origen del problema.

Si se detectase que algún tráfico más sensible se viese afectado se podría dotar de más recursos o prioridad de ancho de banda en los gestores.

La redundancia de la telefonía, en caso de caída de la WAN principal, no es salvable automáticamente. La centralita sólo responderá ante la caída física del interface. Por lo tanto el único caso en que saltará sin intervención es el apagado del conmutador de la LAN donde esté conectado. Por tanto, en el resto de casos deberá ser la actuación manual la que permita reencaminar las llamadas hacia el exterior (PSTN). Por lo tanto a nivel de llamadas, cuando falla la WAN, RUTA 51 (tenemos que detectar caída física, si no bloquear la tarjeta de la sede remota que contiene la ruta 51), las llamadas salen “por la calle” (ruta 1).

Un punto importante a tener en cuenta es salvaguardar las configuraciones de todos los dispositivos, para en caso de que alguno dejase de funcionar, hubiese que montarlo de cero o sustituirlo se pudiese aplicar la configuración que tuviese y así el tiempo de afección sería n el mínimo tiempo. Normalmente estos dispositivos permiten descargar la configuración en un servidor FTP/TFTP.

Las incidencias que sean de hardware serán resueltas a través de los contratos de garantía de adquisición de los dispositivos.

El siguiente cuadro presenta algunas de las incidencias más usuales que se podrían dar y la forma de actuar ante cada una de ellas, tanto para realizar su análisis como para orientar su posible resolución:

[31] Mensajes SNMP que emite el dispositivo ante una alerta en su sistema.

GESTIÓN DE INCIDENCIAS		
Fallo detectado	*Sintomatología*	*Análisis y acciones correctoras*
Caida de enlace.	1. Pérdida de conectividad. 2. Mensajes y LEDs de error. 3. Niveles altos de colisiones en LAN. 4. Fallo de puertos en LAN.	1. Comprobación de la energía. 2. Revisión de fallos de hardware. 3. Revisión fallos de cableado. 4. Revisión uso de CPU. 5. Análisis de logs y revisión de configuraciones de equipos. 6. Si algún enlace RDSI no levanta utilizar canales de otro primario que no esté en uso. Configurar el router RDSI para tal efecto.
Mala calidad de linea.	1. Pérdida de paquetes. 2. Excesiva lentitud. 3. Desconexiones de las aplicaciones.	1. Comprobar en los routers RDSI si se han lanzado todos los canales del primario. En caso contrario intentar usar otro primario. Reconfigurar router RDSI. 2. Si se están sobrecargando al red analizar en los gestores de ancho de banda qué equipos y qué servicios están saturando los enlaces. Adaptar la configuración para no afectar al servicio.
Fallo en la convergencia de la red.	1. Destinos no alcanzables. 2. Tráfico intermitente. 3. Excesiva lentitud.	1. Revisión de fallos en los puertos del router WAN, cortafuegos y conmutadores LAN donde estén conectados. 2. Revisión de las tablas de enrutamiento del cortafuegos. 3. Capturar tráfico con un analizador de red (tcpdump o wireshark) en la VLAN de interconexión para ver si el router WAN está enviando tráfico RIP y éste es correcto. 4. Incluir rutas estáticas con un coste alto para alcanzar la sede afectada a través de los routers RDSI. 5. Comprobar que la sede afectada enruta el tráfico vía enlace RDSI hacia la sede central.
Fallo de aplicación.	1. Error en la aplicación. 2. La aplicación no alcanza el servidor. 3. Excesiva lentitud. 3. Desconexiones de las aplicaciones.	1. Comprobación del enrutamiento extremo a extremo (*traceroute*). 2. Comprobación mediante ping de los elementos involucrados. 3. Si fuese necesario ampliación de tráfico garantizado en el gestor de ancho de banda. 4. Revisión y si aplica, adaptación de políticas del cortafuegos.
Fallo en la telefonía.	1. No es posible hacer llamadas internas. 2. No es posible hacer llamadas externas. 3. Primario caido. 4. Puerto caido. 5. Centralita inaccesible.	1. Comprobación de la energía. 2. Revisión de fallos de hardware. 3. Revisión fallos de cableado. 4. Revisión uso de CPU. 5. Análisis de logs y revisión de configuraciones de equipos. 6. Bloquear la ruta 51 (LAN/WAN) para que la centralita reencamine el tráfico hacia la ruta 1 (PSTN). 7. Si algún primario está caido intentar reubicar otro que no esté en uso en ese momento y adaptar la configuración.

Tabla 22. Gestión de incidencias.

OCTAVA PARTE: ¿QUÉ NOS HA PARECIDO?

8 CONCLUSIONES

Como colofón al desarrollo del proyecto se puede afirmar que la reutilización de infraestructura, la reducción de costes y la aplicación de tecnologías, que a priori podrían pensarse desfasadas, como es la RDSI, pueden facilitarnos una solución sencilla y adaptable en coste y funcionamiento para cualquier organización que requiera de conexiones alternativas de gran alcance para unir sus diferentes emplazamientos. El proyecto demuestra que es una solución aceptable para ser usada de segunda conexión orientada a respaldar la WAN principal.

En nuestro caso, el modularidad del hardware que se ha adquirido permite la posibilidad de escalar con las tecnologías elegidas o portar a otras soluciones de mayor velocidad o capacidad con un desembolso menor.

El rápido avance tecnológico hace que el parque de dispositivos de red se quede obsoleto en poco tiempo, lo cual obliga a pensar en inversiones que a la larga sean rentables y permitan, de una forma equilibrada, hacer un desembolso comedido.

A nivel personal este proyecto ha abierto las posibilidades de investigar un abanico de dispositivos y tecnologías orientadas al entorno LAN y WAN. Desde el estudio de diferentes dispositivos con sus idiosincrasias específicas y su forma de intercomunicarse entre ellos hasta elementos más avanzados de filtrado y gestión de tráfico, segmentación de redes IP y protocolos de nivel de enlace.

El único pero que comentar ha sido la imposibilidad de conseguir que la solución redundase de una forma automática la salvaguarda de la voz. Por lo tanto esta será un área donde se profundizará en busca de alguna alternativa.

Como punto final decir que este proyecto, aunque ha logrado cumplir su objetivo, permite la ampliación de posibilidades de interconexión y comunicación, incluso pudiéndose abarcar el diseño de una red WAN principal donde tomarían presencia otro tipo de dispositivos de mayor rendimiento y capacidad y de otros protocolos de enrutamiento y conmutación.

APÉNDICES

9 APÉNDICES

9.1 Glosario.

Actualización de enrutamiento: Mensaje que se envía desde el enrutador para indicar si la red es accesible y la información de costo asociada.

Administración de red: Uso de sistemas o acciones para mantener. Caracterizar o realizar el diagnóstico de una red.

ATM (Modo de Transferencia Asíncrono): Norma internacional para la retransmisión de celdas, en el cual se transmiten múltiples tipos de servicio (como voz, video o datos), en celas e longitud fija (53 bytes).

Ancho de banda: Diferencia entre las frecuencias más altas y más bajas disponibles para las señales de red.

Autenticación: Con respecto a la seguridad, la verificación de la identidad de una persona o proceso.

Banda ancha: Técnica de transmisión de alta velocidad y alta capacidad que permite la transmisión integrada y simultánea de diferentes tipos de señales (voz, datos, imágenes, etc.).

BRI (Interfaz de Acceso Básico): Interfaz RDSI compuesta por dos canales B y un canal D para la comunicación por un circuito conmutado de voz, video y datos.

Cable de fibra óptica: Medio físico que puede conducir una transmisión de luz modulada.

Confiabilidad: Proporción entre los mensajes de actividad esperados y recibidos de un enlace. Si la relación es alta a línea es confiable.

Congestión: Tráfico que supera la capacidad de la red.

Conmutación: Proceso de tomar una trama entrante de una interfaz y enviarla a través de otra interfaz.

Conmutación de circuito: Sistema de conmutación en el que el circuito físico dedicado debe existir entre el emisor y el receptor durante la “llamada”.

Convergencia: Velocidad y capacidad de un grupo de dispositivos de interconexión de red que ejecutan un protocolo de enrutamiento específico para concordar sobre la topología de una interconexión de redes luego de un cambio de topología.

Costo: Valor arbitrario, basado normalmente en el número de saltos, ancho de banda del medio, u otras medidas, que es asignado por el administrador de red y utilizado para comparar diversas rutas a través de un entorno de interconexión de redes.

DDR (Enrutamiento por llamada telefónica bajo demanda): Técnica utilizada para que un enrutador inicie y cierre dinámicamente sesiones conmutadas por circuito a medida que las estaciones finales las necesiten.

Dirección de red: Dirección de capa de red que se refiere a un dispositivo de red lógico.

Dirección de subred: Parte de una dirección IP especificada como la subred por la máscara de subred.

Dirección del salto siguiente: Dirección IP del siguiente enrutador en una ruta hacia un determinado destino.

Dirección destino: Dirección de un dispositivo de red que recibe datos.

Dirección IP: Dirección de 32 bits asignada a los hosts mediante TCP/IP. Se escribe en forma de 4 octetos separados por un punto.

Dirección origen: Dirección de un dispositivo de red que envía datos.

DNS (Sistema de nombres de dominio): Sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones.

DWDM (Dense Wavelenght Division Multiplexing): DWDM es una tecnología que emplea múltiples ondas para transmitir señales sobre una sola fibra óptica.

E1: Es quema de transmisión digital de área amplia utilizado especialmente en Europa, que lleva datos a una velocidad de 2048 Mbps.

Enlace: Canal de comunicaciones de red que se compone de un circuito o ruta de transmisión y todo el equipo relacionado entre un emisor y un receptor.

Enlace dedicado: Enlace de comunicaciones que se reserva indefinidamente para transmisiones, en lugar de conmutarse según requiera la comunicación.

Enlace punto a punto: Enlace que proporciona una sola ruta preestablecida de comunicaciones de WAN desde las instalaciones del cliente a través de red.

Enlace WAN: Canal de comunicaciones de WAN que se compone de un circuito o ruta de transmisión y todo el equipo relacionado entre un emisor y un receptor.

Enrutamiento: Proceso de descubrimiento de una ruta hacia el host destino.

Enrutamiento dinámico: Enrutamiento que se ajusta automáticamente a la topología de la red o a los cambios de tráfico.

Enrutamiento estático: Ruta que se ha configurado e introducido explícitamente en la tabla de enrutamiento.

Escalabilidad: Capacidad de una red para aumentar el tamaño sin que sea necesario realizar cambios importantes en el diseño general.

Estándar: Conjunto de reglas o procedimientos de uso generalizado o de carácter oficial.

Ethernet: El método de conexión más común en las redes de área local, LANs.

Full-duplex: Capacidad de transmisión simultánea de datos entre una estación emisora y una estación receptora.

Fast Ethernet: Cualquiera de las especificaciones de Ethernet de 100 Mbps.

Fibra óptica: Fibra basada en el vidrio, que sustituye a los cables de cobre y permite transmitir un gran volumen de información a alta velocidad y a gran distancia. Atendiendo al número de frecuencias de luz y la distancia de propagación las hay multimodo y monomodo.

Regla de cortafuegos: Determina si debe enviar o descartar ese tráfico basándose en los criterios establecidos.

Cortafuegos: Enrutador o servidor de acceso, o varios enrutadores o servidores de acceso, designados para controlar el tránsito del tráfico entre distintas redes, normalmente redes de conexión pública y una red privada.

Flujo: Corriente de datos que viajan de un punto a otro.

Frame-Relay: Protocolo conmutado de la capa de enlace de datos, que administra varios circuitos virtuales.

FTP (File Transfer Protocol): Protocolo de aplicación, parte de la pila de protocolo TCP/IP, utilizado para transferir archivos entre nodos de red.

Gateway: Dispositivo con capacidades de enrutamiento de una red IP tal como son los enrutadores o los cortafuegos. Elemento que interconecta diferentes redes.

Gbps (Gigabit por segundo): Medida de velocidad de transferencia de aproximadamente 1000 millones de bits.

Estación de trabajo: Computador de una red.

HTTP (Protocolo de transferencia de hipertexto): Protocolo utilizado por los navegadores y servidores de la Web para transferir archivos, como archivos de texto y de gráficos.

Interfaz: Conexión entre dos sistemas o dispositivos. En terminología de enrutamiento, una conexión de red.

Interoperabilidad: Capacidad de los equipos de diferentes fabricantes para comunicarse entre sí en una red.

IP (Protocolo Internet): Protocolo de capa de red de la pila TCP/IP que ofrece un servicio de interconexión de redes no orientado a conexión.

Kbps (Kilobit por segundo): Medida de velocidad de transferencia de aproximadamente 1000 bits.

LAN (Red de área local): red de datos de alta velocidad y bajo nivel de errores que cubre un área geográfica relativamente pequeña.

LAPD (Procedimiento de acceso al enlace en el canal D): Protocolo de la capa de enlace de datos RDSI para el canal D.

Latencia: Retardo entre el momento en que un dispositivo solicita acceso a una red y el momento en que se le concede permiso para transmitir.

Línea de acceso telefónico: Circuito de comunicaciones estableció por una conexión conmutada por circuito que usa la red de la compañía telefónica.

Máscara de subred: Máscara utilizada para extraer información de red y subred de la dirección IP.

Mbps (Megabit por segundo): Medida de velocidad de transferencia de aproximadamente 1 millón de bits.

Métrica de enrutamiento: Método mediante el cual un protocolo de enrutamiento determina que una ruta es mejor que otra.

Modelo de referencia OSI: Modelo de arquitectura de red desarrollado por ISO e UIT-T. El modelo está compuesto por siete capas, cada una de las cuales especifica funciones de red individuales, tales como el direccionamiento, el control de flujo, el control de errores, el encapsulamiento y la transferencia confiable de mensajes.

MPLS (Multiprotocol Label Switching): MPLS es un estándar de la industria sobre el cual se basa la conmutación de etiquetas, las cuales identifican los diferentes tipos de información sobre la red.

Nodo: Punto final de la conexión de red o una unión que es común para dos o más líneas de una red.

NT1 (terminación de red de tipo 1): Dispositivo que conecta el cableado RDSI del suscriptor de cuatro hilos a la instalación de bucle convencional local de dos hilos.

NT2 (terminación de red de tipo 2): Dispositivo que dirige el tráfico hacia y desde distintos dispositivos del suscriptor y el NT1. El NT2 es un dispositivo inteligente que realiza conmutación y concentración.

Número de saltos: Métrica de enrutamiento utilizada para medir la distancia entre un origen y un destino.

OSPF (Primero la ruta libre más corta): Protocolo de enrutamiento por estado de enlace jerárquico, que se ha propuesto como sucesor de RIP en la comunidad de Internet.

Ping: mensaje de eco ICMP y su respuesta. Se suele usar en redes IP para probar el alcance de un dispositivo de red.

POP (punto de presencia): Punto de interconexión entre las instalaciones de comunicación suministradas por la compañía telefónica y el servicio de distribución principal del edificio.

PPP (protocolo punto a punto): Es un protocolo que suministra conexiones enrutador a enrutador y host a red través de circuitos síncronos y asíncronos.

PRI (Interfaz de acceso primario): Interfaz RDSI de acceso primario. El acceso primario consta de un canal D de 64 kbps más 30 canales B (E1) para voz y datos.

Protocolo de enrutamiento: Protocolo que logra el enrutamiento mediante la implementación de un protocolo de enrutamiento específico. Entre los ejemplos están RIP y OSPF.

Protocolo de enrutamiento por estado de enlace: Protocolo de enrutamiento en el cual cada enrutador realiza un broadcast o multicast de información referente al costo de alcanzar cada uno de sus vecinos a todos los nodos de interconexión de redes.

Protocolo de enrutamiento por vector distancia: Protocolo que utiliza el número de saltos en una ruta para encontrar la ruta de destino.

Protocolo exterior: Protocolo utilizado para intercambiar información de enrutamiento entre redes que no comparten una administración común.

Protocolo interior: Protocolo utilizado para enrutar redes que se encuentran bajo una administración de red común.

Puerto: Interfaz de un dispositivo de interconexión.

Q.931: Protocolo que recomienda una capa de red entre el extremo final de la terminal y el conmutador RDSI local.

QoS (Calidad de servicio): Medida de desempeño de un sistema de transmisión que refleja se calidad de transmisión y disponibilidad de servicio.

RDSI (Red digital de servicios integrados): Protocolo de comunicaciones que ofrecen las compañías telefónicas y que permite que las redes telefónicas transmitan datos, voz y tráfico de otros orígenes.

Red empresarial: La red de una asociación comercial, agencia, escuela u otra organización que une sus datos, comunicaciones, informática y servidores de archivo.

Red interna: Red interna a la que tienen acceso los usuarios con acceso a la LAN interna de la organización.

Redundancia: En la terminología de redes, es la duplicación de dispositivos, servicios o conexiones, de modo que, en caso de que se produzca un fallo, los dispositivos, servicios o conexiones redundantes puedan realizar el trabajo de aquellos en los que se produce el fallo.

Rendimiento: Velocidad de la información que llega a, y pase a través de un punto determinado del sistema de red.

RIP (Protocolo de información de enrutamiento): EL protocolo de Gateway Interior (IGP) más común de Internet. RIP utiliza el número de saltos como métrica de enrutamiento.

Enrutador (o enrutador): Dispositivo de la capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red.

Ruta por defecto: Una entrada de la tabla de enrutamiento que se utiliza para dirigir las tramas para las cuales el próximo salto no está de una forma explícita mencionado en la tabla de enrutamiento.

Salto: Paso de un paquete de datos entre dos nodos de red (por ejemplo, entre dos enrutadores).

Segmento: Sección de una red que está rodeada de puentes, encaminadores o conmutadores.

Señalización: En el contexto RDSI, el proceso de configuración de llamada utilizado, establecimiento de la llamada, terminación de la llamada, información y mensajes varios, incluyendo configuración, conexión, liberación, información del usuario, cancelación, estado y desconexión.

SNMP (Protocolo simple de administración de redes): Protocolo que brinda una forma de monitorizar y controlar los dispositivos de red y de administrar configuraciones, recolección de estadísticas,

Subinterfaz: Se refiere a una serie de interfaces que dependen de un mismo interfaz físico.

Subred: Red segmentada por una serie de redes más pequeñas.

Conmutador (o switch): Dispositivo que interconecta computadoras de forma inteligente. Puede agregar ancho de banda, acelerar el tráfico de paquetes y reducir el tiempo de espera.

Tabla de enrutamiento: Tabla almacenada en un dispositivo con capacidad de interconexión que realiza un seguimiento de las rutas hacia destinos de red específicos y las métricas asociadas a esas rutas.

TE1 (equipo terminal tipo 1): Dispositivo compatible con la red RDSI. TE1 se conecta a una terminación de tipo 1 o tipo 2.

TE2 (equipo terminal tipo 2): Dispositivo no compatible con la red RDSI que requiere un adaptador de terminal.

TFTP (Protocolo de Transferencia de Archivos Trivial): Versión simplificadas de FTP que permite la transferencia de archivos de un computador a otro a través de una red.

Topología: Disposición físicas de los nodos y medios de red de una estructura de interconexión a nivel empresarial.

xDSL (x Digital Subscriber Line): Línea Digital del Suscriptor. Tecnología de red que permite conexiones de banda ancha sobre el cable de cobre a distancia limitadas. Las cuatro tecnologías xDSL: ADSL, HDSL, SDSL, VDSL.

VoIP (Voice over IP): La habilidad de transportar voz telefónica normal sobre una red de datos basada en el protocolo Internet, con la misma funcionalidad, confiabilidad y calidad de voz que ofrecen las empresas telefónicas tradicionales.

VLAN (LAN virtual): Grupo de dispositivos de una LAN que están configurados de tal modo que se pueden comunicar como si estuvieran conectados al mismo cable, cuando realmente están ubicados en segmentos de LAN distintos.

VPN (Red privada virtual): Es una red que permite establecer una conexión segura a través de una red pública o Internet.

WAN (Red de área amplia): Red de comunicación de datos que sirve a usuarios dentro de un área geográfica extensa y a menudo usa dispositivos de transmisión suministrados por operadoras de comunicaciones.

9.2 Bibliografía.

- *WILLIAM STALLINGS*. Comunicaciones y redes de computadoras. 7ª edición. Pearson Educación (2004).
- *ERNESTO ARIGANELLO*. Redes Cisco. Ra-Ma (2005).
- *VACHON Y GRAZIANI*. Acceso a la WAN. Pearson Educación (2009).
- *GRAZIANI Y JOHNSON*. Conceptos y protocolos de enrutamiento. Pearson Educación (2008).
- *WAYNE LEWIS*. LAN inalámbrica y conmutada. Pearson Educación (2009).
- *TOM SHAUGHNESSY*. Manual de Cisco. McGraw-Hill (2006).
- *LEINWAND Y PINSKY*. Configuración de enrutadores Cisco. 2ª edición. Cisco Press (2001).
- *DR. SIDNIE FEIT*. TCP/IP. McGraw-Hill (2006).
- *ROBERT L. ZIEGLER*. Firewalls Linux. Prentice Hall (2004).
- *MIQUEL FONT / EDUARD LARA / RENÉ SERRAL / XAVIER VILAJOSANA*. Telemática. UOC (2011).
- *PERE BARBERÁN Y ENRIC LÓPEZ*. Redes y servicios. UOC (2008).

9.3 Enlaces.

- Listas de precios - PEPPM National Cooperative Purchasing Contracts
  http://www.peppm.org/
- Cisco Catalyst 3560 V2
  http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5528/data_sheet_c78-530976.pdf
- Cisco ISR 2911
  http://www.cisco.com/en/US/products/ps10540/index.html
- Cisco ISR 3925
  http://www.cisco.com/en/US/products/ps10542/
- CheckPoint 4000 appliances
  http://www.checkpoint.com/products/4000-appliances/index.html
- Bluecoat Packetshaper
  http://www.bluecoat.com/es/products/packetshaper
- Aatra MX-ONE Lite
  http://www.aastra.es/cps/rde/aareddownload?file_id=5815-13193-_P11_XML&dsproject=www-aastra-es&mtype=pdf
- Protocolo QSIG
  http://elastixtech.com/protocolo-qsig/
- RFC RIPv2
  http://tools.ietf.org/html/rfc2453
- Interconexión de redes usando DDR
  http://docwiki.cisco.com/wiki/Internetwork_Design_Guide_--_Designing_DDR_Internetworks#Designing_DDR_Internetworks
  http://www.net130.com/attestation/jsh/ccs.pdf