

Diseño de una red WAN para una compañía nacional.

Autor: Belén Colmenar Pavón

Tutor: Jose Luis López Vicario

Área: Integración de redes telemáticas

E.T.T. Telemática

Fecha entrega: Junio 2012



Universitat Oberta
de Catalunya

**Diseño de una red WAN para
una compañía nacional**

Junio 2012

A mi pareja, por la ayuda y paciencia
durante todos estos años de estudio.

Índice de contenidos

Índice de contenidos.....	3
Índice de figuras.....	5
Capítulo 1. Introducción.....	6
1.1. Descripción del proyecto.....	6
1.2. Objetivos del proyecto.....	7
1.3. Planificación del trabajo.....	8
Capítulo 2. Tecnologías actuales de redes WAN en el mercado.....	9
2.1. Introducción a las redes WAN.....	9
2.2. Servicio MacroLAN.....	10
2.3. VPN.....	12
2.3.1. Protocolo IPSec.....	12
2.3.2. Fases para el establecimiento del túnel encriptado.....	13
2.3.3. Parámetros a configurar en el EDC.....	14
2.3.4. Red VPN – IP	15
2.4. ADSL.....	16
Capítulo 3. Situación de las sedes.....	18
3.1. Decisión de las características de las sedes.....	18
3.2. Elección de la red principal y de backup de cada sede.....	20
3.3. Escenario 1 – CPD.....	21
3.3.1. Despiece de equipos CPD.....	22
3.3.2. Cableado.....	25
3.4. Escenario 2 – Oficinas Centrales.....	26
3.4.1. Despiece de equipos Oficinas Centrales.....	27
3.4.2. Routing entre EDCs y PEs en la topología de oficinas centrales:.....	31
3.5. Escenario 3 – Oficinas Medianas.....	33
3.5.1. Despiece de equipos Oficinas.....	33
3.5.2. Routing topología oficinas.....	34
3.6. Escenario 4 – Pymes.....	35
3.6.1. Despiece de equipos Pymes.....	35
3.7. Escenario 5 – servidor alojado en cliente.....	37
3.7.1. Despiece de equipos “Servidor alojado en cliente”.....	38
3.8. Mapa general de la red WAN.....	40
Capítulo 4. Presupuesto de implantación de la red WAN.....	41
Capítulo 5. Conclusiones y consideraciones futuras.....	42
Glosario de términos.....	44
Bibliografía.....	52

Anexos.....	53
Servicio MacroLAN ofrecido por TdE.....	53
Plantilla de configuración servicio MacroLAN.....	55
Configuración VPN – LAN2LAN.....	61
Protocolo RIPv2.....	64
Protocolo HSRP.....	65
Protocolo BGP.....	66
Protocolo MPLS.....	68

Índice de figuras

Figura 1. Red MacroLAN.....	11
Figura 2. Línea ADSL y DSLAM.....	17
Figura 3. Central ADSL.....	17
Figura 4. Distintos tipos de sedes en la empresa.....	18
Figura 5. Ejemplo de mapa nacional con los diferentes tipos de sedes.....	19
Figura 6. Topología de los CPDs.....	22
Figura 7. Cisco 7604.....	24
Figura 8. Cisco 3560.....	24
Figura 9. Cableado CPD.....	25
Figura 10. Topología de las oficinas centrales.....	26
Figura 11. Cisco 2801.....	28
Figura 12. Cisco 1921.....	30
Figura 13. Topología de las oficinas	33
Figura 14. Topología de las pymes.....	35
Figura 15. Cisco 1701.....	36
Figura 16. Topología de los servidores en cliente.....	37
Figura 17. Mapa de la red WAN de la empresa.....	40

Capítulo 1. Introducción.

1.1. Descripción del proyecto

Este proyecto pertenece al área de Integración de Redes Telemáticas y en concreto se trata del diseño y desarrollo de una red WAN para una empresa nacional que interconectará a las diferentes sedes repartidas por toda la península. Se puede ubicar bien dentro de la necesidad de una nueva empresa que necesita crear toda una infraestructura en el país o bien sobre un replanteo de una compañía ya consolidada.

Esta red WAN se apoyará en la infraestructura ya preparada de los ISPs existentes en el mercado de las telecomunicaciones.

Las sedes de la compañía tendrán un volumen de datos variable en cada una de ellas y, según esta característica, dispondrán de tipos de redes diferentes para intercomunicarse, ofreciendo a las más grandes un ancho de banda de banda mejor y más dedicado que a otras sedes más pequeñas donde las necesidades serán menores.

Parte del trabajo consistirá en hacer un estudio para determinar qué tecnología se adapta mejor a las necesidades individuales de cada oficina y qué equipamiento es necesario para llevarlo a cabo con lo que una vez estudiados los tipos de redes que hay en el mercado se diseñará el mapa de red y se decidirá qué equipos son más apropiados, y el gasto que llevan asociado.




También, un aspecto importante a tener en cuenta es la seguridad ya que viajará información confidencial y sensible entre las diferentes oficinas.

Una vez finalizada la parte de estudio y diseño de la red WAN estaría disponible para su puesta en desarrollo donde las siguientes fases serían: petición de alta de líneas y permiso al Ayuntamiento en caso de que sea necesario hacer obra para llegar a la sede, compra de equipos al proveedor y su posterior configuración.

1.2. Objetivos del proyecto.

- El objetivo principal de este TFC es la interconexión de las diferentes sedes de una compañía a través de una red WAN.
- Cada una de las sedes tendrá diseñada y configurada una red LAN propia que se conectará a la red WAN propuesta en este proyecto. Uno de los hitos del proyecto será estudiar el tamaño y acceso de cada una de las sedes para determinar que tecnología de red se adecua mejor y comparar las opciones que hay en el mercado.
- Cada sede dispondrá de dos líneas de acceso a la red WAN, una principal y otra de backup, siendo la segunda de un ancho de banda menor.
- Una vez elegida la tecnología de red será necesario ver que hardware es apropiado para cada uno de los tipos de red elegidos, así como su coste. Dentro de este equipamiento se tendrá que disponer de routers, switches, firewalls, etc.
- Cada una de las líneas pasará por la estructura de alguno de los ISPs nacionales que hay disponibles actualmente en el mercado.

1.3. Planificación del trabajo

		Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1		Decisión del TFC	5 días?	jue 01/03/12	mié 07/03/12	
2		▢ PAC 1	9 días?	jue 08/03/12	mié 21/03/12	1
3		Descripción del proyecto	3 días?	jue 08/03/12	lun 12/03/12	
4		Objetivos	2 días?	mar 13/03/12	mié 14/03/12	3
5		Índice	2 días?	jue 15/03/12	vie 16/03/12	4
6		Planificación	2 días?	mar 20/03/12	mié 21/03/12	5
7		▢ PAC 2	23 días?	jue 22/03/12	mié 25/04/12	6
8		Estudio de las características de las sedes	6 días?	jue 22/03/12	jue 29/03/12	
9		Estudio de las tecnologías actuales	10 días?	vie 30/03/12	lun 16/04/12	8
10		Elección de la red principal y backup	4 días?	mar 17/04/12	vie 20/04/12	9
11		Elección de equipamiento y coste	2 días?	lun 23/04/12	mar 24/04/12	10
12		formato entrega PAC 2	1 día	mié 25/04/12	mié 25/04/12	11
13		▢ PAC 3	22 días?	jue 26/04/12	mié 30/05/12	12
14		Diseño del mapa de red	5 días?	jue 26/04/12	vie 04/05/12	12
15		Rediseño del mapa de red + equipamiento	5 días?	lun 07/05/12	vie 11/05/12	14
16		Glosario	22 días?	jue 26/04/12	mié 30/05/12	
17		Bibliografía	22 días?	jue 26/04/12	mié 30/05/12	
18		Anexos	22 días?	jue 26/04/12	mié 30/05/12	
21		formato entrega PAC 3	5 días?	jue 24/05/12	mié 30/05/12	
22		▢ Entrega del proyecto	17 días?	jue 31/05/12	vie 22/06/12	15
23		Entrega de la memoria	12 días?	jue 31/05/12	sáb 16/06/12	
24		Entrega de la presentación	5 días?	lun 18/06/12	vie 22/06/12	

Capítulo 2. Tecnologías actuales de redes WAN en el mercado

2.1. Introducción a las redes WAN.

Una WAN define la forma en que los datos se desplazan a través de una zona geográficamente extensa. Las WAN interconectan diferentes LANs utilizando los servicios de un proveedor. Las tecnologías de señalización y transporte que utilizan estos proveedores de servicios suelen ser transparentes para los usuarios finales.

Dentro de la nube WAN se dan tres tipos de conexiones:

- Líneas alquiladas: también se llaman líneas punto a punto o líneas dedicadas. Ofrecen una comunicación por un medio exclusivo para el cliente. Estas líneas eliminan los problemas de conexión/desconexión de llamada y aportan mayor privacidad y seguridad. Suelen emplearse en conexiones serie síncronas manteniendo constante la utilización del ancho de banda. Son las líneas más costosas económicamente hablando.
- Circuitos conmutados: sólo se establece comunicación entre el emisor y el receptor durante el tiempo que dura la transmisión y las sucesivas conexiones pueden o no utilizar la misma ruta u otra diferente. Este tipo de conexiones suele emplearse para entornos que tengan un uso esporádico, enlaces de respaldo o enlaces bajo demanda. También es posible aprovecharse de los servicios de telefonía básicos mediante una conexión asíncrona conectada a un módem, como por ejemplo una línea RDSI.
- Paquetes conmutados: es un método de conmutación donde los dispositivos comparten un único enlace punto-a-punto o punto-multipunto para transportar paquetes desde un origen hacia un destino a través de una red portadora. Este tipo de redes utilizan circuitos virtuales para ofrecer conectividad de forma permanente o conmutada (PVC o SVC)

2.2. Servicio MacroLAN.

MacroLAN es un servicio de Red Privada Virtual de Banda Ancha que permite la conexión de redes de área local remotas con prestaciones similares a las que se obtendrían si estuvieran dentro de un mismo edificio, con elevada fiabilidad, escalabilidad y simplicidad.

MacroLAN se sustenta de Redes Ethernet de Telefónica de España (MAN) como medio de acceso a la Red de Banda Ancha y requiere de accesos Ethernet ópticos proporcionados por el proveedor del servicio.

La comunicación entre sedes se realiza a través de la MetroLAN mediante VLANs nacionales donde todas las oficinas con acceso MacroLAN estarán dentro de la misma VLAN. Estas VLANs no tienen ningún caudal asignado ya que lo regula la propia MetroLAN que tiene diferentes valores de caudales contrastables:

- Acceso de 10 Mbps: 1 a 10 Mbps en saltos de 1 Mbps.
- Accesos de 100 Mbps: 10 a 100 Mbps en saltos de 10 Mbps más los valores de acceso a 10 Mbps.
- Accesos de 1Gbps: 100 a 1000 Mbps en saltos de 100 Mbps más los valores de acceso a 10 Mbps y 100 Mbps.

MacroLAN es un servicio de RPV en el que parte de la infraestructura sobre la que se sustenta es exclusiva de un cliente y otra parte es compartida por varios clientes. Se utilizan dos tecnologías para separar el tráfico entre diferentes clientes: VLANs de entorno metropolitano (IEEE 802.1Q) y el protocolo MPLS IP VPN a nivel nacional (RFC 2547).

La arquitectura básica del servicio es la distribución de las VLANs:

- VLAN Metro: sólo interconecta los equipos que están en la misma MAN.
- VLAN Nacional: comunica con EDCs situados en otras MAN remotas y en los diferentes Pes se mapea esta VLAN a la VPN-IP del cliente.

Esta tecnología trabaja a nivel de capa 2 y apoyándose en el nivel e capa 3 para utilizar VPN-IP.

Los equipos hardware que se utilizan para este servicio son routers/switch, que trabajan en las capas 2 y 3 y tienen capacidad de conmutación acorde a las velocidades manejadas en el servicio y posibilidad de ampliación del caudal contratado sin tener que cambiar el EDC.

En MacroLAN se definen tres clases de servicio contratables por el cliente y una adicional para el tráfico de gestión del EDC que es transparente al cliente.

- **Clase de Servicio Multimedia:** Orientada al tráfico de cliente muy sensible al retardo y al jitter (VoIP, Multimedia, etc...), al cual se le da máxima prioridad. Ofrece unos SLAs (Acuerdos de Nivel de Servicio) más exigentes que los del resto de Clases.

- **Clase de Servicio Oro:** Orientado al tráfico Intranet del cliente de aplicaciones críticas. Garantiza un caudal a este tipo de tráfico y da unos SLAs más exigentes de retardo y pérdida de paquetes que los de la Clase de servicio Plata.

- **Clase de Servicio Plata:** Orientado al tráfico Intranet de cliente, al que se le garantiza un caudal determinado. Es la clase por defecto cuando un cliente no contrata QoS.

- **Clase de Servicio Gestión:** Clase de servicio asociada al tráfico de gestión de los EDCs.



Figura 1. Red MacroLAN

2.3. VPN

Una VPN (Red Privada Virtual) se utiliza principalmente para conectar dos redes privadas a través de una red pública de datos mediante túneles encriptados. Un túnel es un método para encapsular un protocolo en otro donde se aprovecha esta característica, principalmente cuando hay protocolos no enrutables y hacen que el uso de una VPN sea imprescindible para enviar tráfico.

El funcionamiento característico de las VPNs consiste en que los routers encapsulan los paquetes IP con la etiqueta GRE¹ y los envía por la red al router de destino, en el otro extremo del router, que desencapsula los paquetes quitándoles la etiqueta GRE y dejándolos listos para enrutarlos localmente. Aunque el paquete GRE haya cruzado un gran número de routers a través de una gran red intermedia, para éste tan sólo ha efectuado un único salto a destino.

Las VPN deben proporcionar: confidencialidad, integridad y autenticación.

2.3.1. Protocolo IPSec.

IPSec es un conjunto de protocolos y algoritmos de seguridad diseñados para la protección del tráfico de red de modo transparente o modo túnel. Su característica principal es la independencia algorítmica que le permite efectuar cambios de algoritmos si fuese necesario, por ejemplo, en el caso de un fallo de seguridad o si se tiene que encontrar un algoritmo más eficaz.

Este protocolo está diseñado para proporcionar seguridad sobre la capa IP lo que beneficia el transporte de protocolos o aplicaciones inseguras logrando un alto nivel de seguridad.

Las funcionalidades de IPSec son: encriptar el tráfico de manera segura para que no pueda ser visto excepto cada uno de los extremos, validar la integridad de los datos asegurando que el tráfico no ha sido modificado, autenticar a cada uno de los extremos y anti-repetición evitando la repetición de la sesión segura.

1 Existen variantes para los túneles VPN pero en este caso se utilizarán los túneles GRE

IPSec utiliza dos protocolos importantes de seguridad:

- AH (Authentication Header) que incluye un sistema de autenticación criptográfico en el encabezado del paquete IP y que permite verificar que el tráfico no ha sido manipulado.
- ESP (Encapsulation Security Payload) que proporciona encriptación a la carga útil del paquete para el envío seguro de datos. Se utiliza para proteger tanto la conexión como los datos.

2.3.2. Fases para el establecimiento del túnel encriptado

Inicialmente se deben definir los parámetros que se usarán para establecer el túnel VPN. Para establecer un túnel VPN es necesario que se lleven a cabo dos fases de negociación IKE (Internet Key Exchange) Fase 1 y fase 2.

1. **IKE fase 1:** Esta fase es la encargada de establecer un canal autenticado de comunicación. Para esto utiliza el Algoritmo de Diffie-Hellman el cual es asimétrico y permite el intercambio seguro de llaves simétricas como DES, 3DES, AES o SEAL que son utilizadas para encriptar el tráfico entre los pares en la fase 2.

La autenticación para este protocolo se puede realizar por medio de claves Pre-Compartidas (Pre-Shared Key) o de Certificados.

Puede operar en *Main Mode* o en *Aggressive Mode*, donde la primera protege la identidad de los pares, la segunda no.

Parámetros disponibles para IKE phase 1:

- Authentication: Pre-Shared Keys, RSA-Encryption, RSA-Signature
- Encryption Algorithm: DES, 3DES, AES [128, 192, 256]
- Key Exchange: DH-Group1 [768-bit], DH-Group 2 [1024-bit], DH-Group 5 [1536-bit]
- Hashing: MD5, SHA-1.

2. **IKE fase 2:** En esta fase los pares hacen uso del canal seguro establecido en la fase 1 para compartir las claves simétricas con las cuales se encriptará el tráfico.

Parámetros disponibles para IKE ph2:

- Encryption Algorithm: esp-des, esp-3des, esp-aes [128,192,256], esp-seal, esp-null.
- Authentication: ah-md5-hmac, ah-sha-hmac, esp-md5-hmac, esp-sha-hmac.

2.3.3. Parámetros a configurar en el EDC

Crypto-map: En este bloque de configuración se define la estructura de la conexión.

Habrà un *crypto-map* por cada conexión que se quiera realizar (IPSec estático). En cada uno se define:

- Destino del túnel.
- Nombre de la transformada IPSec que se va a utilizar.
- Caracterización del tráfico a cifrar, por referencia una *Access-list*.
- Origen ip que asumirán los paquetes cifrados.

Transformada IPSec: aquí se definen los protocolos estándar a emplear en la negociación IPSec y que una vez consensuados entre los 2 EDCs servirán para el cifrado de paquetes.

Access-list: las funciones del Access-list en el crypto-map son:

- Seleccionar tráfico a cifrar
- Cada entrada en la Access-list genera su propia SA (Asociación de seguridad)
- Procesar el tráfico entrante, descartando el que llega no cifrado y debería estarlo (si está definido en salida como cifrable, lo tendrá que estar a la entrada).
- Determinar si una petición entrante de SA recibida desde otro peer, debe ser aceptada o no, en base a los datos aportados en la negociación IKE. La entrada del Access List del peer remoto tiene que estar coordinada con alguna de las entradas del Access-list local.

Secreto compartido: clave que utilizará para la autenticación en el momento de la generación del túnel. Ambos extremos tendrán que tener el mismo secreto para que el túnel IPSec se pueda establecer.

2.3.4. Red VPN – IP

Como se ha comentado antes, la red VPN crea túneles IP de extremos a extremo, sin embargo en la Red VPN – IP se van a crear túneles MPLS dentro de una nube virtual dentro de cualquier red pública.

Las redes VPN-IP nos ofrecerán:

- Tráfico solo visible para las sedes pertenecientes a la VPN - *Virtual Path Network* -.
- Direccionamiento independiente para cada una de las VPNs.
- Posibilidad de emplear distintos tipos de acceso según las necesidades de nuestro cliente.
- Posibilidad de priorizar o garantizar cierto nivel de tráfico mediante QoS y definiendo entre los caudales de tráfico ofrecidos: multimedia, oro y plata.
- Existencia de alternativas para proporcionar redundancia a los accesos VPN-IP.
- Posibilidad de utilizar cifrado entre distintas sucursales.

Las dos clases de acceso a la red VPN-IP más utilizadas son ATM - *Asynchronous Transfer Mode* - y FR - *Frame Relay* -.

2.4. ADSL

ADSL (Línea de abonado digital simétrica) es un tipo de línea perteneciente al grupo de la línea DSL que realiza una transmisión analógica de datos digitales a través del par simétrico de cobre por donde se transmite la línea telefónica. Establece tres canales de comunicación: voz, envío y transmisión de datos.

La separación de los tres canales se consigue mediante una modulación de las señales de datos en una banda de frecuencias más alta que la utilizada en las conversaciones telefónicas convencionales (300-3400 Hz), función que realiza el enrutador ADSL. Para evitar distorsiones en las señales transmitidas, es necesaria la instalación de un filtro (llamado *splitter* o microfiltro) que se encarga de separar la señal telefónica convencional de las señales moduladas de la conexión mediante ADSL.

Se denomina asimétrica debido a que la transmisión de datos desde la central hacia el usuario es de mayor ancho de banda que la transmisión de subida, desde el usuario hacia la central.

Al comunicarse mediante el par de cobre, o par de abonado, utiliza la infraestructura existente de la red de telefonía básica por lo que los operadores no han tenido que implantar una nueva tecnología, con el consiguiente ahorro de costes y rapidez en el despliegue y disponibilidad del servicio.

Cada circuito entre abonado y central es único y exclusivo para ese usuario, es decir el cable de cobre que sale del domicilio del abonado llega a la central sin haber sido agregado, y por tanto evita cuellos de botella por canal compartido, lo cual sí ocurre en otras tecnologías que utilizan el cable.

También existen una serie de inconvenientes en la línea ADSL como la limitación de servicio si el usuario se encuentra a una distancia mayor a 5,5 km de distancia de la central ya que la línea va perdiendo calidad debido a la atenuación, al ruido, a las interferencias en el cable y a la degradación de la señal según aumenta la distancia a la central, al no existir repetidores entre estos dos puntos.

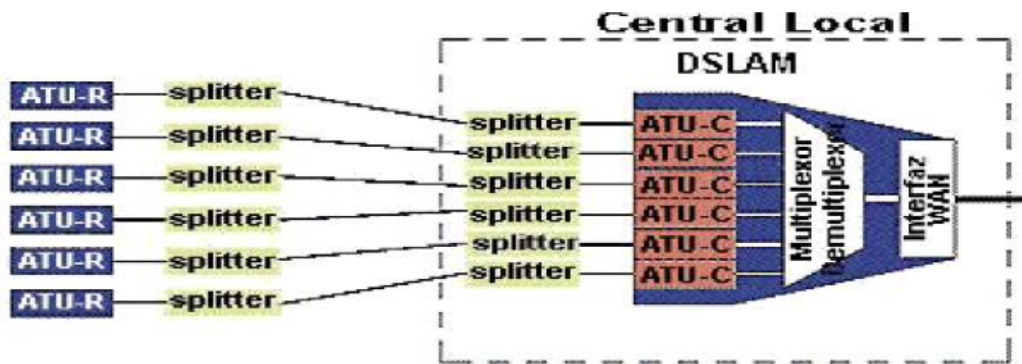


Figura 2 . Línea ADSL y DSLAM

DSLAM es un chasis que agrupa gran número de tarjetas, cada una de las cuales consta de varios módems ATU-C, y que realiza las siguientes funciones:

- Concentra en un mismo chasis los módems de central de varios usuarios.
- Concentra el tráfico de todos los enlaces ADSL hacia una red WAN.
- Realiza funciones de nivel de enlace (protocolo ATM sobre ADSL) entre el módem de usuario y el de central.

Es necesario un protocolo de nivel de enlace entre el ATU-R y el ATU-C.

Las redes de comunicaciones emplean el protocolo ATM ("Asynchronous Transfer Mode") para la conmutación en banda ancha. La transmisión ATM se puede realizar sobre un gran número de medios físicos, entre ellos, fibras ópticas y líneas de cobre. En este último caso, la solución más adecuada es el empleo de células ATM para transmitir la información sobre el enlace ADSL.

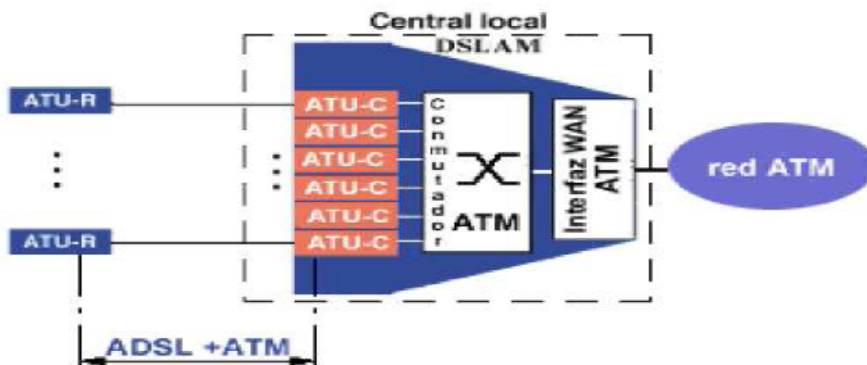


Figura 3: Central ADSL

Capítulo 3. Situación de las sedes.

3.1. Decisión de las características de las sedes.

En primer lugar, se describe el escenario en el que se va a situar a esta empresa:

Se trata de una compañía nacional con dos sedes principales (máximo 50 personas), varias sedes medianas (entre 5 y 20 personas), varias sedes pequeñas (1-10 personas), oficinas de clientes con un servidor que se conecta a nuestra empresa y teletrabajadores.

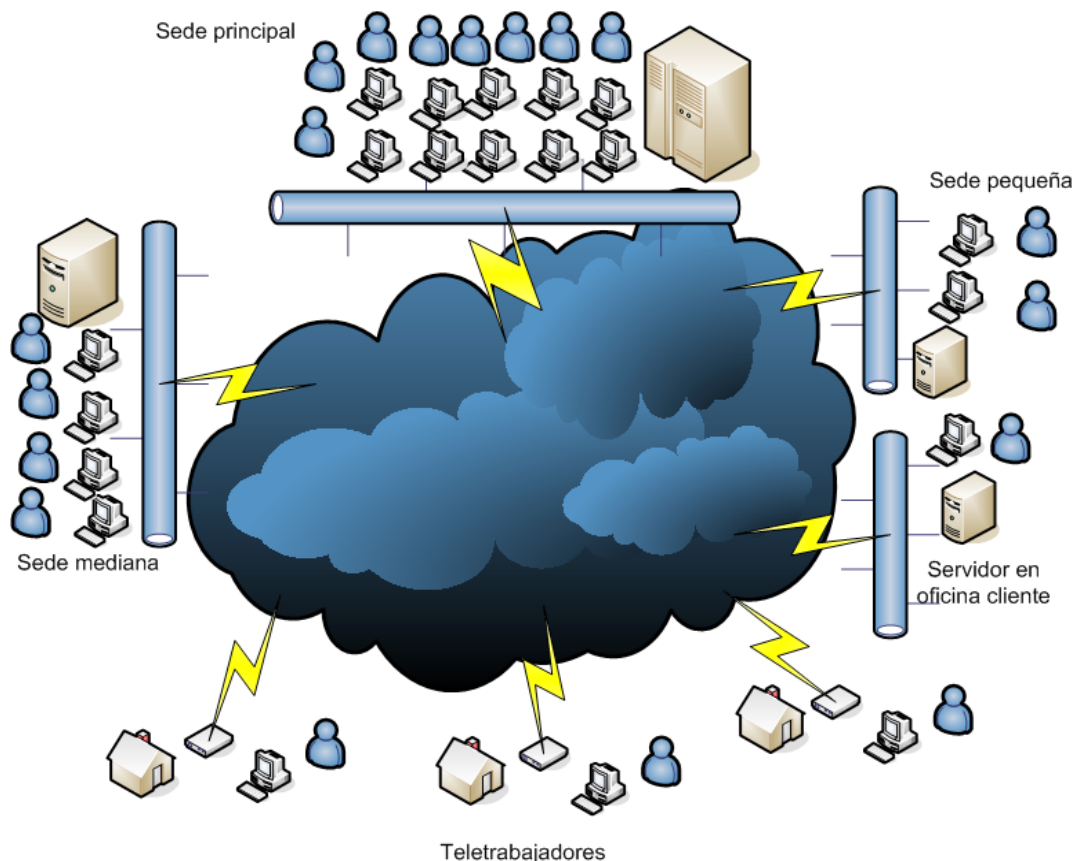


Figura 4. Distintos tipos de sedes en la empresa

Habrán dos sedes principales que alojarán un CPD cada una y enrutarán el tráfico principal de la compañía, éstas actuarán de sede principal y backup, para que en el caso de que falle el acceso de las línea de una de los CPDs podrá haber conectividad a través del otro y de esta forma no se quedará la compañía incomunicada.

Todas las sedes dispondrán de dos líneas de conectividad con el exterior, una principal y una de backup, siendo la principal de mayor ancho de banda que la secundaria; excepto en el caso de las pymes y el caso del servidor alojado en las oficinas de clientes, que dispondrá de una única conexión “VPN Lan2Lan” con la empresa. En el caso de los teletrabajadores, se conectarán mediante su red ADSL y creando un túnel VPN mediante la herramienta “open source” OpenVPN.

El escenario general de la empresa quedaría como se muestra en la siguiente figura. De esta forma, si la empresa crece o disminuye en el número de sedes se podrían sumar o restar fácilmente. Del mismo modo el número de teletrabajadores puede variar sin problemas.



Figura 5. Ejemplo de mapa nacional con los diferentes tipos de sedes

3.2. Elección de la red principal y de backup de cada sede

La empresa va a contar con dos tipos de oficinas: las oficinas tipo1, que van a disponer de dos líneas de datos -una principal y otra de backup-, y las oficinas tipo 2 que sólo van a tener una línea de datos. En el primer caso se encuentran las oficinas nombradas como “Sede Principal” y las de tamaño mediano, que se llamarán “Oficinas” simplemente.

Las oficinas tipo 1 dispondrán de una línea principal con mayor caudal de datos y capacidad y además de una línea de respaldo, de menor capacidad, que convergerá en el caso de que la primera pierda la conectividad. Además, existe la excepción de los CPDs donde se ha optado por dos líneas exactamente iguales y redundantes pero que actuaran como las oficinas tipo 1

Las oficinas tipo 2, entre las que se encuentran las pymes, las conexiones de teletrabajo y los servidores alojados en oficinas de cliente no tendrán líneas secundarias ya que no supone una situación crítica la pérdida de servicio. No se descarta que en un futuro se amplíe y se instale una línea de backup también en este tipo de sedes.

A continuación se hará una descripción de los cinco tipos de escenarios posibles para cada una de las sedes.

3.3. Escenario 1 – CPD.

La idea principal de conexión de esta empresa es la de tener dos CPDs alojados en dos oficinas centrales que proporcionarán enlaces redundantes al resto de las oficinas desplazadas por la geografía nacional, para tal propósito, existirá una conexión desde cada CPD a Red mediante fibras totalmente diversificadas en ruta desde origen a destino. Todas las oficinas del banco, los servidores alojados en cliente y los teletrabajadores saldrán por estos CPDs que serán la clave de la interconexión nacional junto con el apoyo del proveedor de la red de datos.

Los EDC de fibras en los CPDs harán funciones de switching para el tráfico entre las oficinas, las pymes y los servidores en clientes. Con esta arquitectura se dispone de un backup para la red de oficinas por los distintos CPDs, de manera que si el enlace del CPD 1 cae automáticamente convergerán y saldrán las rutas por el CPD 2.

Las sedes principales, que albergan los CPDs, tendrán el mismo tratamiento que cualquier otro tipo de oficina media de otra provincia, proporcionando una solución de red homogénea.

En este entorno se va a utilizar unos equipos agregadores de rutas MPLS para todas las conexiones que llegan desde las oficinas y además se utilizarán otros dos agregadores en el siguiente nivel, para unir todas las conexiones de todas las oficinas y que serán enviadas a los correspondientes PEs del proveedor.

Los routers Cisco Catalyst 3560 se utilizan como extremo, también de manera redundante, a todas las conexiones VPN IP que provienen de las oficinas pymes y éstas se conectarán a los agregadores de rutas que se conectarán a los PEs del proveedor.

3.3.1. Despiece de equipos CPD

Los equipos descritos son iguales en ambos CPDs:

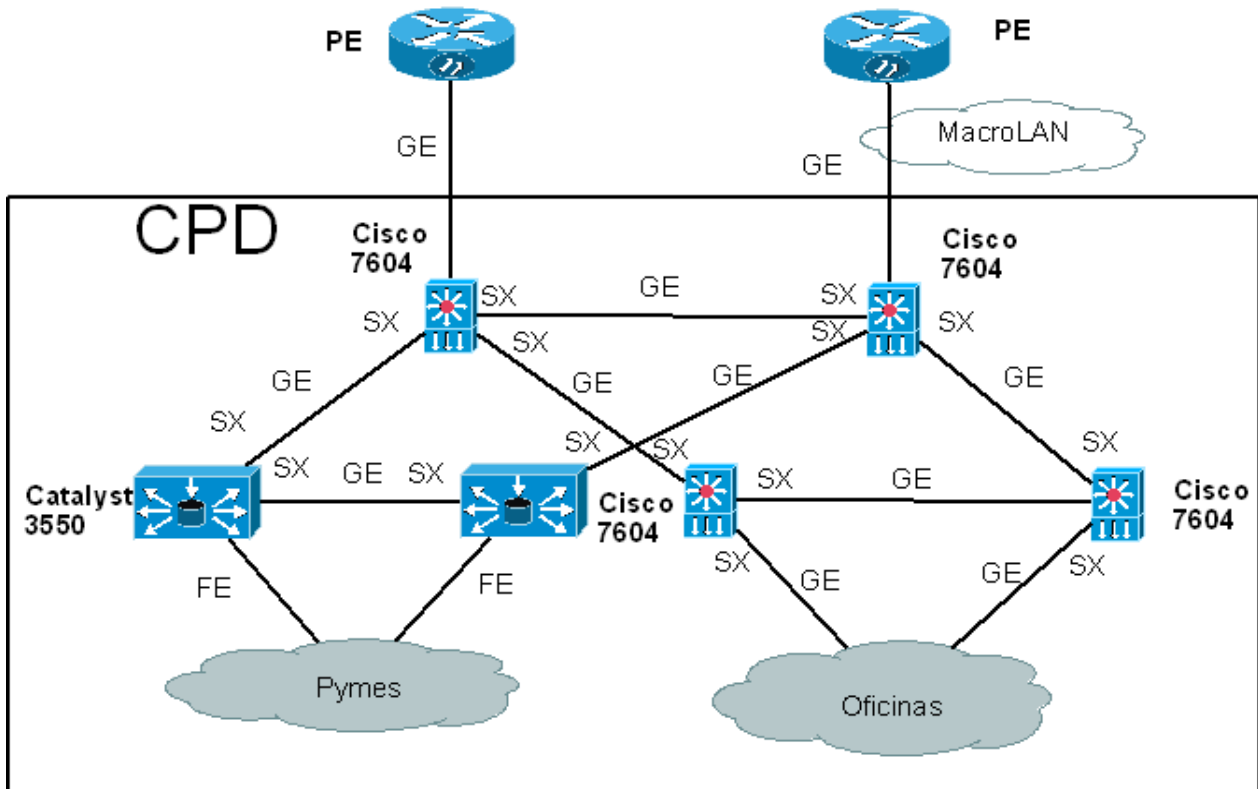


Figura 6. Topología de los CPDs

Tanto los routers Catalyst como los routers Cisco 7604 se encargan de recoger todo el tráfico que llega de todas las oficinas al CPD encontrándose en una jerarquía de primer nivel y, al mismo tiempo, éstos transfieren el tráfico a un segundo nivel donde se concentran todas las rutas y que son los otros dos routers Cisco 7604 y son el paso previo antes de la conexión con los PEs del ISP.

Los agregadores de rutas trabajan, como su propio nombre indica, agregando el tráfico que llega de los distintos nodos de acceso de de los agregadores del primer nivel y enviándolo hacia otros equipos superiores. Realizan tareas de conmutación desde los diferentes servicios configurados en los distintos escenarios utilizando VLANs.

Los PEs son los equipos en el extremo del ISP y que proporcionan la entrada a la red de tránsito del tráfico IP/MPLS.

Agregadores (Cisco 7604)

Agregador conexión a Fibra Directa

Product	Description	Quantity
Configuración base		
CISCO7604	Cisco 7604 Chassis Bundle	1
FAN-MOD-4HS	High-Speed Fan Module for 7604/6504-E	1
7604-S323B-8G-P	Cisco 7604 Chassis, 4-slot, SUP32-8GE-3B, PS	1
SUP32-GE3B	SUP32 8GE3B	1
MEMX-CEF720-256M	Catalyst 6500 256MB DDR, xCEF720 (67xx interface, DFC3A)	1
MEM-C6K-CPTFL128M	Cat6500 Sup720/Sup32 Compact Flash Mem 128MB	1
MEM-MSFC2-256MB	Catalyst 6500 256MB DRAM on the MSFC2	1
S7632IS-12218SXF	Cisco 7600-SUP32 IOS IP SERVICES	1
PWR-2700-AC/4	2700W AC Power Supply for Cisco 7604/6504-E	1
2700W-AC	2700W AC Power Supply for Cisco 7604	1
CAB-GSR16-EU	Cisco 12016 GSR AC Power Supply Cord, Europe	1
GLC-ZX-SM	1000BASE-ZX SFP	1
GLC-SX-MIM	GE SFP, LC connector SX transceiver	3
Fuente de alimentación redundante		
PWR-2700-AC/4	2700W AC Power Supply for Cisco 7604/6504-E	1
CAB-GSR16-EU	Cisco 12016 GSR AC Power Supply Cord, Europe	1

Conexión a la Fibra. Conexión WAN

Conexión local al Catalyst C3560 de Pymes

Conexión local al Router C7604 de Oficinas

Conexión local al Catalyst C7604 Agregador

Producto	Descripción	Cantidad
Configuración base		
CISCO 7604	Cisco 7604 Chasis Bundle	1
FAN-MOD-4HS	High-Speed Fan Module for 7604/6504-E	1
7604-SUP7203B-PS	Cisco 7604 Chasis, 4 slot, SUP720-3B, PS	1
SUP 720-3B	Supervisor Engine 720-3B	
MEM-S2-512MB	Catalyst 6500 512MB DRAM on the supervisor (SUP2 or SUP720)	1
MEM-C6K-CPTFL 128M	Cat6500 Sup720/Sup32 Compact Flash Mem 128	1
MEM-MSFC2-512MB	Catalyst 6500 512MB DRAM on the MSFC2	1
S7632IS-12218SFX	Cisco 7600-SUP32 IOS IP SERVICES	1
PWR-2700-AC/4	2700W AC Power Supply for Cisco 7604/6504-E	1
2700W-AC	2700W AC Power Supply for Cisco 7604	
CAB-GSR16-EU	Cisco 12016 GSR AC Power Supply Cord, Europe	1
GLC-SX-MIM	GE SFP, LC connector SX transceiver	2
Fuente de alimentación redundante		
PWR-2700-AC/4	2700W AC Power Supply for Cisco 7604/6504-E	1
CAB-GSR16-EU	Cisco 12016 GSR AC Power Supply Cord, Europe	1
Puertos GE WAN		
7600-SIP-400	Cisco 7600 Series SPA Interface Processor-400	1
SPA-2X1GE	Cisco 2-port Gigabit Ethernet Shared Port Adapter	1
SFP-2X1GE	1000BASE-SX SFP (DOM)	2
7600-SPA	SPA for cisco 7600; No physical Part for tracking only	1



Figura 7. Cisco 7604

Producto	Descripción	Cantidad
Configuración base		
WS-C3560-24TS-E	Catalyst 3560 24 10/100 + 2 SFP Enhanced Image	1
CAB-ACE	Power Cord Europe	1
GLC-SX-MM	1000BASE-SX, LC Connector y SX Transceiver	2



Figura 8. Cisco 3560

3.3.2. Cableado.

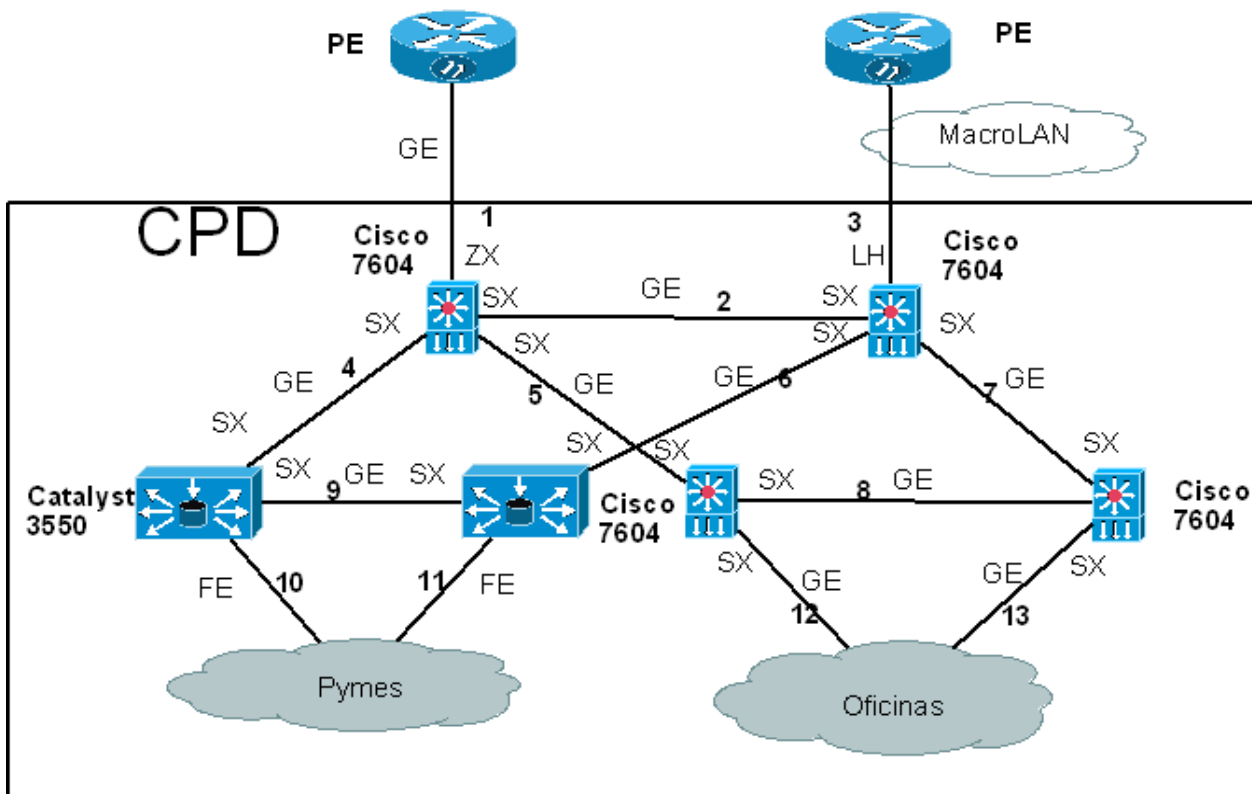


Figura 9. Cableado CPD

El cableado necesario para los equipos del CPD se explica en la siguiente tabla:

Ubicación en dibujo	Producto	Descripción	Unidad	Enlace
1y 3	Agregadores	Latiguillo de fibra monomodo 10m. LC/PC-SC(APC)	2	x2
2,4,5,6 y 7		Latiguillo de fibra multimodo 10m. LC/PC-LC-PC	2	x5
8, 12 y 13	Routers entorno oficinas	Latiguillo de fibra multimodo 10m. LC/PC-LC-PC	2	x3
9	Routers entorno pymes (es recto porque va a otro catalyst)	Latiguillo de fibra multimodo 10m. LC/PC-LC-PC	2	x1
10 y 11		Latiguillo UTP clase 5, RJ45 recto 10m.	1	x2

3.4. Escenario 2 – Oficinas Centrales.

Este tipo de oficinas serán las oficinas centrales del Banco que albergarán un máximo de 50 personas pero que causarán el mayor tráfico y tendrán mayor criticidad en el desarrollo del negocio por lo que se ha elegido como línea principal el servicio MacroLAN de 10Mb y como línea de backup un MacroLAN de 2Mb, donde ambas ofrecen conectividad simétrica a través de fibra óptica. El tráfico será enviado cifrado.

El EDC de la línea de backup estará conectado a una de las bocas del EDC de la línea principal y hablando el protocolo HSRP, por lo que cuando la segunda línea detecte que no hay conectividad desde la primera dejará de su estado de *standby* para pasar a ser la línea principal.

El esquema de red será el siguiente:

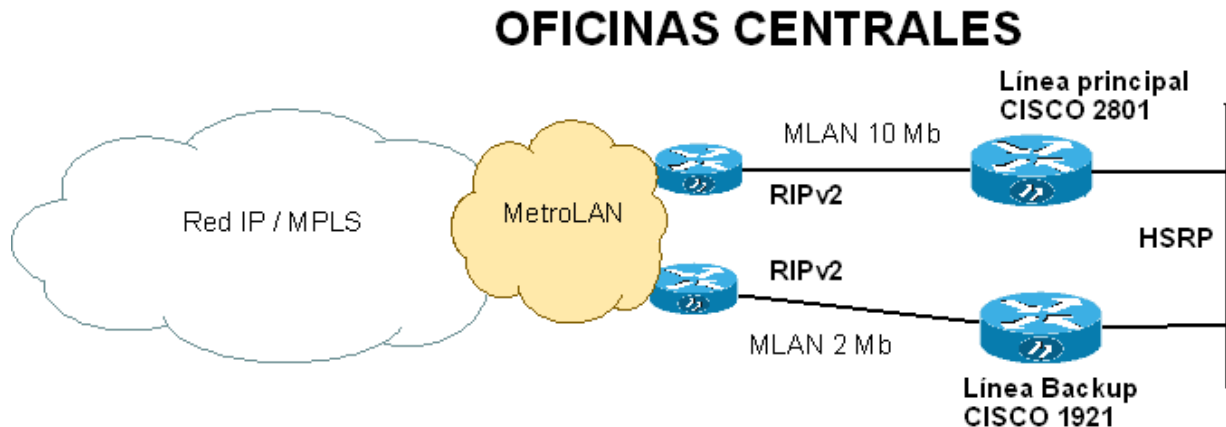


Figura 10. Topología de las oficinas centrales

3.4.1. Despiece de equipos Oficinas Centrales

1. Línea Principal MacroLAN 10Mb:

Se ha elegido el router Cisco 2801 ofrecen las siguientes características configurables:

Models Comparison

Model	Onboard DSP Slots	Fixed LAN Ports	Optional Power over Ethernet	Slots for Interface Cards	Slots for Network Modules	Size
2801	2	2 FE	120W	2 HWIC/WVIC/WIC/VIC 1 VWIC/WIC/VIC 1 VWIC/VIC (voice only)	0	1 RU

Se utiliza este equipo ya que el cliente no precisa caudales superiores a los máximos permitidos para poder utilizar este equipo. Las restricciones del mismo son las siguientes:

- Caudales hasta 10 Mbps;
- Escenarios con acceso Metrolan único por EDC²;
- Escenarios sin facilidad de transporte transparente Ethernet;
- Escenarios con un solo interfaz físico hacia el cliente;
- Preferentemente para conexiones Metrolan 2Mbps, aunque no se prohíbe su utilización sobre accesos de fibra de 10Mbps o 100Mbps, siempre que se respete la limitación del caudal

Y el despiece elegido es el siguiente:

CÓDIGO	DESCRIPCIÓN	CANTIDAD
<i>Cisco 2801</i>		
CISCO2801	2801 Router/ AC PWR, 2FE, 4slots(2HWICs), 2 AIMS, 64F, 128DRAM W/ Cisco IOSIP Software	1
CAB-ACE	Power Cord Europe	1
<i>Cisco 2801. IO S IP Base – 12.3T</i>		
S280IPB-12308T	Cisco 2801 Series IOSIP Base	1

² Es decir, escenarios de EDC simple y acceso simple o con redundancia de EDC y acceso doble (un acceso por cada EDC).



Figura 11. Cisco 2801

Este despiece incluye:

- Chasis 2801 con 128MB de DRAM y 64MB de FLASH
- Cable de alimentación europeo
- 1 Latiguillo Ethernet cruzado de 10 metros
- 1 Latiguillo Ethernet recto de 10 metros
- Dado que este equipo no va a hablar BGP, sino RIPv2 hacia la WAN, el paquete software utilizado es IOS IP Base.

Características a nivel interface:

- 2 puertos Fast Ethernet 10/100 (10 BaseT/100BaseTX)
- 4 slots externos libres que admiten:
 - 2 módulos HWIC, WIC, VIC
 - 1 admite módulos WIC, VIC o VWIC
 - 1 admite módulos VIC o VWIC
- 2 slots internos AIM (Advance Interface Module)
- Encriptación hardware integrada
- 1 puerto de consola
- 1 puerto asíncrono auxiliar
- 1 puerto USB

2. Línea de backup MacroLAN 2Mb:

Se ha elegido el router Cisco 1921 por las siguientes características configurables:

- 2 puertos integrados *Ethernet* 10/100/1000.
- Dos *slots* para tarjetas de interface WAN de alta velocidad (EHWIC).
- Distribución de alimentación totalmente integrada s módulos que soportan *802.3af Power over Ethernet (PoE)* y *Cisco Enhanced PoE*
- Seguridad:
 - Integrado por aceleración por hardware de encriptación VPN.
 - Comunicaciones de seguridad altamente colaborativas con *Group Encrypted Transport VPN, Dynamic Multipoint VPN, o Enhanced Easy VPN.*
 - Control de amenazas integrado usando *Cisco IOS Firewall, Cisco IOS Zone-Based Firewall, Cisco IOS IPS y Cisco IOS Content Filtering.*
 - Gestión de indentidad con autenticación, autorización e integridad (AAA); e infraestructura de clave pública.

Se utiliza este equipo ya que el cliente no precisa caudales superiores a los máximos permitidos para poder utilizar este equipo. Las restricciones del mismo son las siguientes:

- Caudales hasta 10 Mbps;
- Escenarios con acceso Metrolan único por EDC³;
- Escenarios sin facilidad de transporte transparente Ethernet;
- Escenarios con un solo interfaz físico hacia el cliente;
- Preferentemente para conexiones Metrolan 2Mbps, aunque no se prohíbe su utilización sobre accesos de fibra de 10Mbps o 100Mbps, siempre que se respete la limitación del caudal.

Para este tipo de accesos se utilizá el router Cisco 1921 con el siguiente despiece:

CÓDIGO	DESCRIPCIÓN	CANTIDAD
<i>Cisco 1921</i>		
CISCO1921	Modular Router w/ 2xFE, 2 WAN slots, 32 FL/ 128 DR w/ Cisco IOS IP Software	1
CAB-ACE	Power Cord Europe.	1
<i>Cisco 1921. IO S IP Base – 12.3T</i>		
S184IPB-12308T	Cisco 1921 Series IOSIP Base	1

³ Es decir, escenarios de EDC simple y acceso simple o con redundancia de EDC y acceso doble (un acceso por cada EDC).

Este despiece incluye:

- Chasis 1921 con 128 MB de DRAM y 32 MB de FLASH
- Cable de alimentación europeo
- 1 Latiguillo Ethernet cruzado de 10 metros
- 1 Latiguillo Ethernet recto de 10 metros
- Dado que este equipo no va a hablar BGP, sino RIPv2 hacia la WAN, el paquete software utilizado es IP Base.



Figura 12. Cisco 1921

3.4.2. Routing entre EDCs y PEs en la topología de oficinas centrales:

El protocolo de routing a utilizar como estándar del servicio entre EDCs y PEs, así como entre EDCs (sobre la VLAN Metro), es RIP v2. Se aplicarán los siguientes criterios:

- Se modificarán los temporizadores de RIP, tanto en los PEs como en los EDCs, para reducir el tiempo de convergencia del protocolo RIP. En concreto, el temporizador “invalid” se reducirá a 90 segundos⁴.
- Se deberán configurar los EDCs y los PEs de forma que cuando el destino sea metropolitano el tráfico vaya por la VLAN_METRO y no por la VLAN_NACIONAL, aunque pueda existir visibilidad de la misma red a través de ambas VLANs. Para ello, se crearán filtros para filtrar los anuncios de RIP recibidos por la VLAN_NACIONAL, aceptando sólo los procedentes de los PEs.
- Por defecto, el EDC sólo anunciará hacia la Red de Banda Ancha, las direcciones de las LANs del cliente directamente conectadas. Para lograr esto habrá que aplicar el filtro correspondiente en el proceso de RIP.
- Si el cliente necesita anunciar más redes que la directamente conectada, independientemente de si el EDC las aprende de forma dinámica o no, el cliente deberá informar de cuales son.
- estas redes para añadirlas en el filtro anteriormente mencionado y asociado con la información que se anuncia hacia la Red.
- Se desactivará la funcionalidad de “poison reverse” para disminuir el tráfico de *routing* sobre la MAN.
- No habrá routing dinámico hacia la LAN del Banco.

El escenario de Redundancia de estas oficinas está basado en una configuración de Doble EDC en modo Respaldo o Backup. Este escenario se constituye con dos EDCs y una conexión doble a la MAN (una conexión simple en cada EDC).

⁴ Los valores concretos a configurar se especificarán en la documentación de plantillas. En los EDCs de Riverstone no es posible modificar estos temporizadores.

Los dos accesos funcionan en modo **respaldo**, cursándose todo el tráfico, en condiciones normales, por uno sólo de ellos. Este funcionamiento se consigue mediante la configuración de *routing* en los EDCs. La MAN mantiene siempre activos ambos enlaces.

Características a destacar en este escenario:

- El tráfico de cliente se cursa por uno sólo de los accesos. El acceso de respaldo cursará, en condiciones normales, una cantidad mínima de tráfico de control (*routing*) o de gestión del propio EDC.
- La selección de EDC/ Acceso primario y de respaldo se realiza mediante configuración de *routing* en los EDCs, anunciando con peor métrica las redes desde el EDC de respaldo.
- La configuración de VLAN de ambos accesos es idéntica, tanto en red como en el EDC.
- No se hace uso del *Spanning Tree* en los EDCs.
- La caída del enlace o EDC primario provoca una pérdida total de conectividad de la oficina afectada, que se resolverá una vez converjan los protocolos de *routing* implicados y el tráfico comience a fluir por el acceso de respaldo.
- La doble conexión se debe contratar como un MetroLAN con acceso diversificado en modo respaldo.
- Para enrutar correctamente el tráfico procedente de la LAN del cliente, se configurará HSRP ya que estamos en un escenario sin *routing* dinámico sobre dicha LAN.

3.5. Escenario 3 – Oficinas Medianas.

Este tipo de oficinas acogerán a un rango de entre 20 – 100 personas. Se ha optado por una línea principal MacroLAN de 2 Mb y una línea de *backup* ADSL. El tráfico será cifrado en ambas líneas por lo que para el caso de la línea de *backup* se debe optar por utilizar túneles IPsec a través de la red VPN.

El EDC de la línea de backup estará conectado a una de las bocas del EDC de la línea principal y hablando el protocolo HSRP, por lo que cuando la segunda línea detecte que no hay conectividad desde la primera dejará de su estado de *standby* para pasar a ser la línea principal.

El esquema de red será el siguiente:

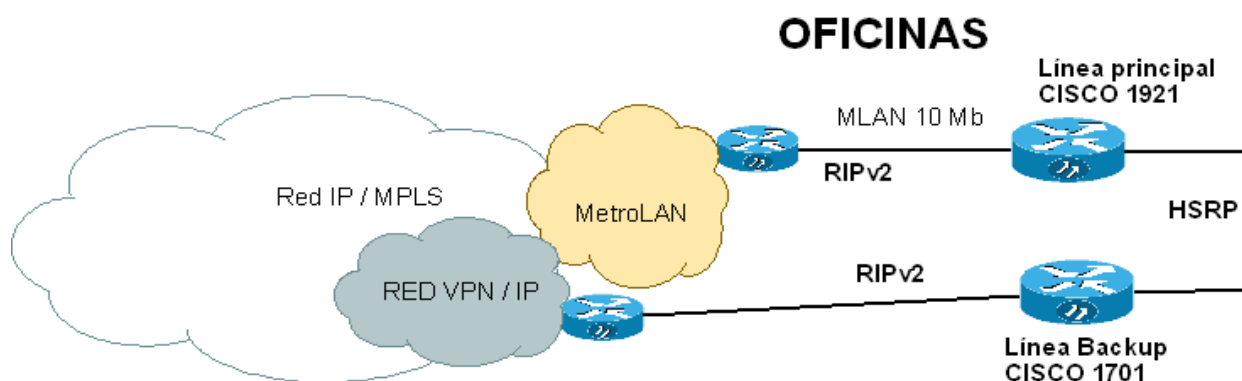


Figura 13. Topología de las oficinas

3.5.1. Despiece de equipos Oficinas

La línea principal será de las mismas características que las descritas en el apartado anterior para la línea de backup. El equipo a utilizar será un router CISCO 1921.

Para la línea de backup se utilizará el router CISCO 1701 que está descrito en el apartado siguiente “Topología entornos Pymes”.

3.5.2. Routing topología oficinas

Los escenarios de routing para la implementación de línea MacroLAN y acceso backup directo a la red VPN-IP es el siguiente:

- Los EDCs MacroLAN y VPN IP anunciarán mediante RIPv2 la red local directamente conectada y/o las redes configuradas estáticamente que se quieran hacer visibles hacia el resto de la VPN.
- Se habilitará HSRP como mecanismo de redundancia LAN entre ambos EDCs.
- En los PEs principal y secundario de MacroLAN, las redes recibidas desde los EDCs se redistribuyen al mBGP con LP 200 y 100 respectivamente.
- En el PE de VPN IP, las redes recibidas desde el EDC se redistribuyen al mBGP con LP 50.
- En el PE de VPN IP se empeora la distancia administrativa de los anuncios RIPv2 recibidos por la conexión de backup.
- Para el envío de tráfico hacia la red por la conexión MacroLAN principal, el EDC recibirá routing en abierto desde los Pes de MacroLAN.
- Para el envío de tráfico hacia la red por la conexión VPN IP de backup, se procederá de la siguiente manera:
 - Ya que en el EDC no es necesario configurar una interfaz 0/0 hacia la LAN del cliente, entonces en el EDC de VPN IP se dispondrá de una ruta estática por defecto apuntando a la interfaz WAN. Por la conexión VPN IP no se recibirá routing del PE.

En estas situaciones, para cubrir aquellos casos de fallo en los que no se conmute el HSRP, en el EDC de MacroLAN se configurará una ruta estática por defecto flotante apuntando a la IP LAN del EDC VPN IP.

3.6. Escenario 4 – Pymes.

Las pymes son oficinas del banco con un número reducido de trabajadores y que no realizan el mismo trabajo que las oficinas normales de la empresa, como las “sedes principales” y las “oficinas medianas”. Su trabajo diario es atender a ciertos clientes tanto dentro como fuera de la oficina por lo que el tráfico demandado es relativamente bajo y por esta razón se ha optado por ofrecerles una línea ADSL con 20Mb de bajada y 1Mb de subida. Además, como van a tener que estar conectados con la red del banco con la que intercambiarán datos sensibles necesitan conectarse a la Red VPN IP.

El esquema de la red será el siguiente:

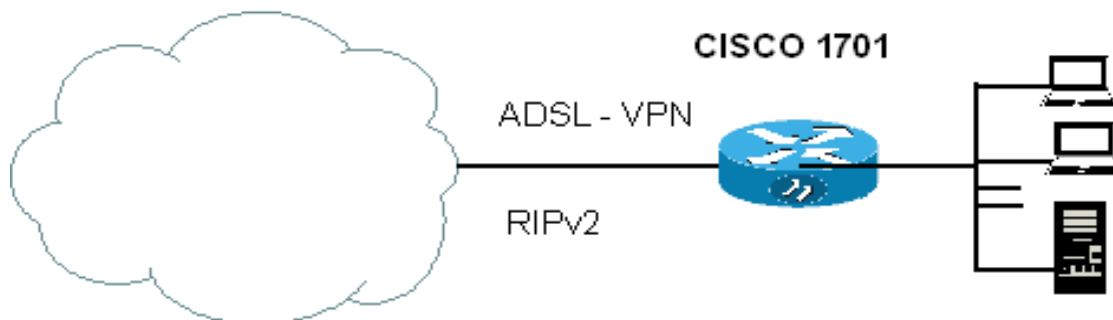


Figura 14. Topología de las Pymes

3.6.1. Despiece de equipos Pymes.

En este entorno es necesario un equipo que sea un router ADSL con boca WAN para conectarse a la red ADSL2 de la red Telefónica y acceso LAN cableado mediante RJ45 para conectar equipos en red tanto para usuarios como para conectar equipos en red, como la impresora, por ejemplo, así como acceso *WiFi* para que los trabajadores puedan conectarse a la WLAN.

Se ha elegido el router Cisco 887 porque dispone de conexión WAN a la línea ADSL2 e incluye IPSec 3DES para VPNs y está indicado para pequeñas y medianas empresas, también ofrece configuración avanzada de políticas de QoS.

Los routers Cisco 887VA Routers soportan líneas DSL multimodo, incluyendo VDSL2 y ADSL2+ en un único interface WAN.

Los routers Cisco 887VA aportan las siguientes características:

- Soporte DSL multimodo, VDSL2, ADSL2 y ADSL2+ sobre línea de teléfono básica.
- Continuidad de negocio con conexiones primarias y de backup.
- VPNs a velocidades de banda ancha de hasta 20 túneles.
- Construido para capacidades de seguridad tales como NAT y firewall.
- Cuatro puertos switch de 10/100 Mbps Fast Ethernet.
- Fácil despliegue con *Cisco Configuration Professional*.
- Gestión centralizada.
- Imagen de software universal para una fácil expansión con la activación de software.
- Funciones de seguridad avanzada incluyendo prevención de intrusiones, encriptado VPN y VPN dinámica multipunto (DMVPN).
- *Power over Ethernet* (PoE) en dos de los puertos switch.



Figura 15. Cisco 1701

3.7. Escenario 5 – servidor alojado en cliente



Figura 16. Topología de los servidores en cliente

En este caso particular, la oficina va a disponer de servidores alojados en clientes que necesitan realizar conexiones a la empresa principal pero que son independientes de la red. Por esto mismo se les ha proporcionado un servidor con el cual se pueden conectar y realizar operaciones como si estuviesen dentro de nuestra empresa.

Para ofrecer mayor seguridad a la comunicación entre el servidor y la red WAN se va a configurar una VPN – LAN2LAN con independencia del router y el tipo de línea a la que va a estar conectado el servidor y la conexión se va a realizar a través de una VPN que encriptará todos los datos enviados y recibidos.

Se ha optado por este tipo de configuración ya que así es posible colocar de una manera rápida y efectiva el servidor en cualquier partner asociado con independencia del tipo de comunicación que tenga contratada ya que la VPN se realizará a nivel de aplicación y conectará con un router borde de nuestra empresa que lo introducirá dentro de la red. Además también se ahorra costos ya que tan sólo es necesario disponer de un servidor Linux que se va a configurar con herramientas de software libre con la aplicación IPsec-Tools.

La configuración que se debe realizar es la siguiente:

- Añadir políticas de entrada de seguridad *forward* and *reverse* a la base de datos de políticas de seguridad (definidas en `/etc/ipsec-tools.conf`)
- Reiniciar el proceso “setkey” para asegurar que las nuevas políticas son cargadas dentro del kernel SDP (definido en `/etc/init.d/setkey restart`)
- Añadir las rutas de los hosts que queremos enrutar por el túnel encriptado (definido en `/etc/network/interfaces`)

El paquete IPsec-Tools viene con los servicios:

- `ibipsec`
Librería con la implementación de PF_KEY.
- `setkey`
Herramienta para manipular el kernel *Security Policy Database* (SPD) y *Security Association Database* (SAD).
- `racoon`
Demonio Internet Key Exchange (IKE) para enlazar mediante claves automáticamente las conexiones IPsec.
- `racoonctl`
Una herramienta de control shell-based para racoon

3.7.1. Despiece de equipos “Servidor alojado en cliente”

Se ha elegido un servidor que va a estar gestionado por el sistema operativo con licencia GNU/Linux Ubuntu 10.04 TLS. Este equipo almacenará todas las aplicaciones administrativas para que los empleados de la pyme trabajen en red.

Las especificaciones del servidor son las siguientes:

Número de catálogo / Descripción	Código del producto	Qty	SKU	Id.
Base: PowerEdge R320	513108	1	[210-39851]	1
Configuración de chasis: 3.5" Chassis with up to 4 Cabled Hard Drives and Embedded SATA	513118	1	[350-11190][470-13052]	1530
Procesador: Intel® Xeon® E5-1410 2.80GHz, 10M Cache, 6.4GT/s , Turbo, 4C, 80W	513172	1	[213-15772][412-10171]	1550
Tipo de configuración de memoria: Performance Optimized	511811	1	[370-22145]	1562
Tipo y velocidad de los DIMM de memoria: 1333 MHz UDIMMs	511970	1	[370-22271]	1561
Capacidad de memoria: 4GB UDIMM, 1333 MHz, Low Volt, Dual Rank, x8	511801	1	[370-22135]	1560
Servicios de asistencia: 1Yr Basic Warranty - NBD Included - No Upgrade Selected	137003	1	[710-10767]	30
Sistema operativo instalado de fábrica: No Operating System	65590	1	[611-10036]	1650
Kits de medios del OS: No Media Required	511784	1	[605-11443]	1652
Configuración RAID: C1 - No RAID for Embedded SATA, 1-4 SATA HDDs, Cabled Chassis	513131	1	[780-13381]	1540
Controlador RAID: Embedded SATA	511832	1	[405-12067][405-12088]	1541
Discos duros: 2TB, SATA, 3.5in, 7.2k HD (Cabled)	704117	1	[400-25658]	1570
Configuración del BIOS (administración de energía): Performance BIOS Setting	393135	1	[223-10221]	1533
Fuente de alimentación: Single Cabled Power Supply 350W	513188	1	[450-18240]	1620
Cables de alimentación: Rack Power Cord, C13 to C14, PDU Style, 12A, 2M/6.5Ft	204752	1	[450-12466]	1621
Gestión de sistemas integrada: Basic Management	513112	1	[528-10000]	1515
Add-in Network Adapter: On-Board Broadcom 5720 Dual Port 1GBE	702617	1	[540-11217]	1514
Rack Rails: No Rack Rails or Cable Management Arm	509807	1	[770-11315]	1610
Unidad óptica interna: No Internal Optical Drive for 4HD Chassis	257400	1	[429-14168]	1600
Garantía básica: 1Yr Basic Warranty - Next Business Day - Minimum Warranty	686917	1	[709-11184][709-11185]	29
Dell Servicios: Instalaciones: No Installation Service Selected (Contact Sales rep for more details)	58267	1	[683-11870]	1290

3.8. Mapa general de la red WAN.

Como ya se ha especificado en los puntos anteriores cómo van a estar conectadas las sedes, a continuación se muestra un esquema general a modo de resumen donde se muestra un ejemplo de cada uno de los escenarios ya descritos.

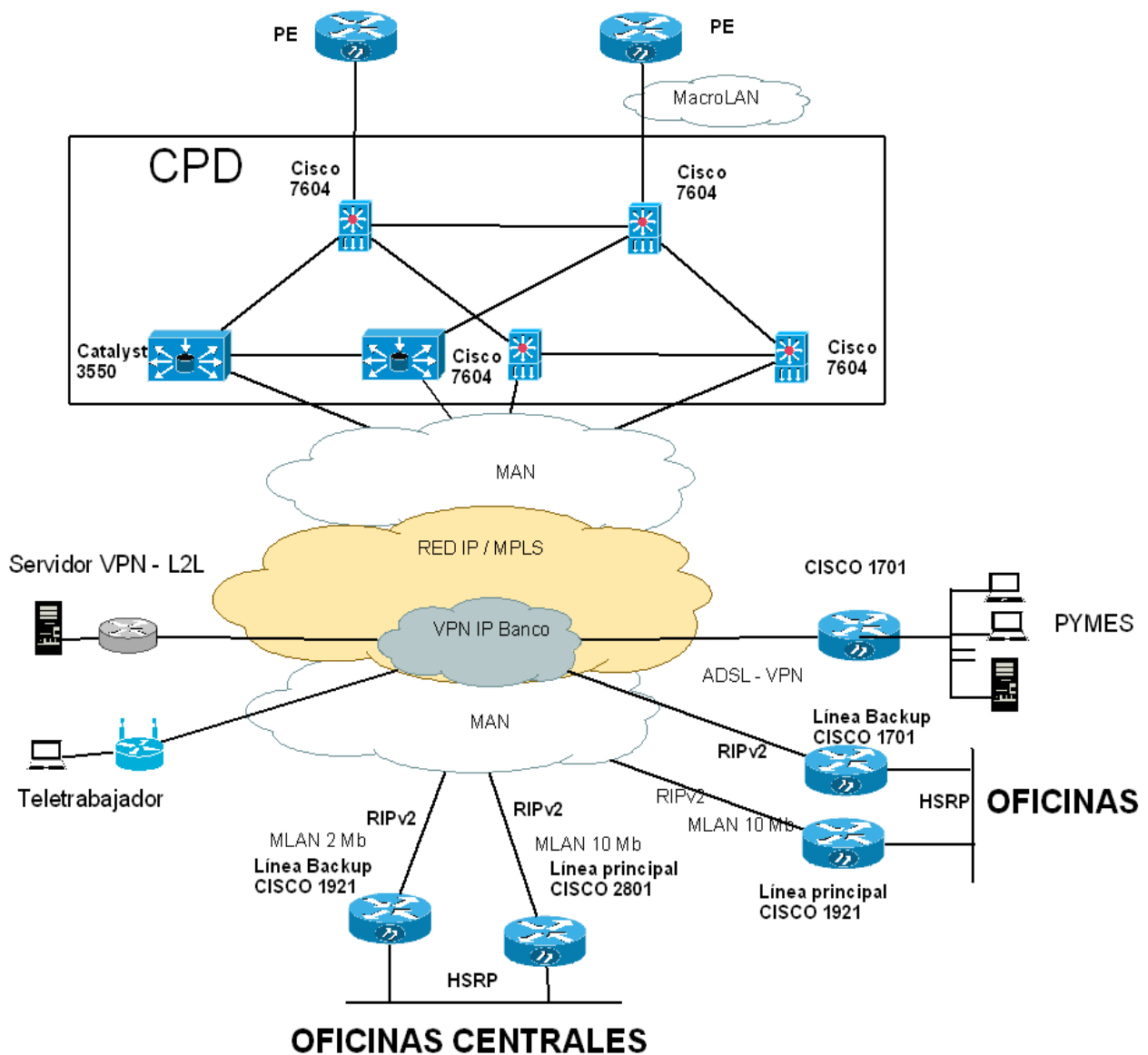


Figura 17. Mapa de la red WAN de la empresa

Capítulo 4. Presupuesto de implantación de la red WAN.

El presupuesto que se detalla a continuación es orientativo ya que de manera particular no es posible conseguir precios exactos. Por un lado, Cisco no vende equipos directamente a los particulares y tampoco ofrece un listado de precios en su web ya que éste vende a través de partners, incluido el proveedor de servicios Telefónica. Por otro lado, Telefónica ofrece la posibilidad de alquilar o comprar los equipos junto con sus líneas que se tramitan a través de un comercial.

Cada cliente puede conseguir precios diferentes ya que hay que negociar con Telefónica sus propios descuentos.

De modo orientativo, el presupuesto de todo el despliegue del hardware es el siguiente:

Producto	Precio Unitario	Unidades	Precio final
Cisco 7604 MLAN	\$ 27.695	4	\$ 110.780
Cisco 7604 Agregadores	\$ 89.800	4	\$ 359.200
Catalyst 3560 Pymes	\$ 5.990	4	\$ 23.960
Cisco 2801 MLAN 10Mb	\$ 1.995	2	\$ 3.990
Cisco 1921 MLAN 2Mb	\$ 636	22	\$ 13.992
Cisco 1701 VPN- IP	\$ 735	27	\$ 19.845
		subtotal \$	\$ 531.767
		subtotal €	430.000 €
Servidor	1591,82 €	7	11142,74 €
		TOTAL	441.142,74 €

Capítulo 5. Conclusiones y consideraciones futuras.

En este proyecto se ha expuesto el caso del diseño de una red WAN para una empresa nacional, en concreto se trata de un banco. Esta empresa tendrá oficinas repartidas por toda la geografía nacional por lo que se ha tenido que definir la conexión entre ellas teniendo en cuenta el tamaño y características de cada una de ellas.

Se han definido cinco escenarios con dos características principales: oficinas que tienen línea principal y de backup, y oficinas con sólo una línea principal. Además, se ha diseñado que los datos telemáticos de todas las sedes pasen a través de un CPD con líneas redundantes para que en el caso de que se quede incomunicada uno de los CPDs se conmute al segundo CPD y éste ofrezca el servicio de datos.

Se ha optado por equipamiento Cisco por el amplio rango de hardware que ofrece, en su mayoría con posibilidad de obtener routers modulares y poder construir el dispositivo a medida, además del eficaz y consolidado funcionamiento para el tipo de redes que el cliente necesita. Por otro lado, se ha optado por contratar el servicio de datos al ISP de Telefónica ya que ofrece tecnologías de red de alta velocidad y con servicios de seguridad apropiados para los datos delicados que pueden pasar a través de las comunicaciones del banco.

El protocolo de enrutamiento elegido para transportar todas las conexiones es MPLS porque converge con todas las redes definidas en el esquema general de la figura 17, y además ofrece las siguientes ventajas:

- Soporta VLSM (máscaras de subred de tamaño variable).
- Se pueden crear VPNs a través de los enlaces troncales (backbone) sin encriptación.
- Utiliza QoS tanto en la red IP como en la red ATM y permite conjuntar las dos redes.
- Permite una conmutación más rápida en comparación con las redes IP ya que los routers no han de calcular la cabecera cada vez que llega un paquete IP y tampoco

consultar la mejor ruta en la tabla de enrutamiento sino que basándose en la etiqueta de entrada ya sabe cual es la interfaz de salida y por dónde ha de conmutar el paquete, incorporando una nueva etiqueta de salida a su cabecera para que sea interpretada por el siguiente router intermedio.

Finalmente, como línea futura de la propuesta actual se puede ampliar el caudal contratado de las líneas de fibra óptica de MacroLAN si el tamaño de las oficinas lo requieren así como el de la línea ADSL, en el caso de las oficinas con este tipo de tecnología. También, es posible aportar una conexión de backup a las sedes que están trabajando solamente con un único enlace principal, como en el caso de las pymes. Respecto al equipamiento, sería posible ver el hardware equivalente que ofrece la compañía Juniper y migrar los equipos ya que están tomando relevancia en el mercado y poniéndose a la altura de su competencia.

Glosario de términos

A:

ADSL (Asymmetric Digital Subscriber Line). Una de las cuatro tecnologías DSL. ADSL entrega mayor ancho de banda hacia abajo (desde la oficina central al cliente) que hacia arriba (desde el cliente a la oficina central). Las transmisiones a través de ADSL funcionan a distancias de hasta 5.488 metros sobre un único par trenzado.

Ancho de banda. Diferencia entre las frecuencias más altas y más bajas disponibles para las señales de red. Así mismo, la capacidad de rendimiento medida de un medio o protocolo de red.

Anillo. Conexión de dos o más estaciones en una topología circular lógica. La información se pasa de forma secuencial entre las estaciones activas. Ejemplos de anillo: Token Ring, FDDI y CDDI.

B:

BGP (protocolo de gateway fronterizo). Protocolo de enrutamiento interdominios que reemplaza a EGP. BGP intercambia información de accesibilidad con otros sistemas BGP y se define en el protocolo RFC 1163.

BRI (Interfaz de acceso básico). Interfaz RDSI compuesta por dos canales B y uno D para la comunicación de un circuito conmutado de voz, videos y datos.

Bucle local: también llamada la última milla. Es el cableado desde la demarcación hasta la oficina central del proveedor.

C:

Carrier. Compañía de servicios privada que suministra servicios de comunicación al público, con tarifas reguladas.

CIR. Velocidad de información suscrita. Velocidad en bits por segundo, a la que el switch Frame-Relay acepta transferir datos.

CO (Oficina Central). Oficina local de la compañía telefónica en la cual todos los pares locales en una área determinada se conectan y donde ocurre la conmutación de circuitos de las líneas del suscriptor.

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

Conmutación de circuitos. Sistema de conmutación en el que un circuito físico dedicado debe existir entre el emisor y el receptor durante la llamada. Se usa ampliamente en la red de telefonía.

Conmutación de paquetes. Método de networking en el cual los nodos comparten el ancho de banda entre sí enviando paquetes.

CPE (Customer premises equipment). Dispositivo de red ubicado físicamente en el cliente.

CSU (Unidad de servicio de canal). Dispositivo de interfaz digital que conecta el equipamiento del usuario final al par telefónico digital local.

D:

DCE (equipo de transmisión de datos). Dispositivo usado para convertir los datos del usuario del DTE en una forma aceptable para la instalación de servicios de WAN.

Demarcación: punto en el que finaliza el CPE y comienza el bucle local en las redes WAN.

DLCI (identificador de conexión de enlace de datos). Valor que especifica un PVC o un SVC en una red Frame Relay. Son significativos localmente, para Frame Relay, ya que usan diferentes valores para especificar la misma conexión y; significativos globalmente para LMI, puesto que los DLCI especifican dispositivos de extremos individuales.

DSL (Digital Subscriber Line, Línea Digital del Suscriptor). Tecnología de red que permite conexiones de banda ancha sobre el cable de cobre a distancias limitadas. Hay cuatro tipos de DSL: ADSL, HDSL, SDSL y VDSL. Todas estas tecnologías funcionan a través de pares de módems, uno localizado en la oficina central y otro en la casa del cliente. DSL no utiliza todo el ancho de banda del par trenzado.

DSU (unidad de servicio de datos). Ver CSU.

DTE (Equipo terminal de datos). Dispositivo en el extremo del usuario de una interfaz de usuario de red que sirve como origen de datos, destino o ambos. DTE se conecta a una red de datos a través de un dispositivo DCE y utiliza normalmente señales de

sincronización generadas por el DCE. DTE incluye dispositivos tales como computadores, traductores de protocolo y multiplexores.

E:

Encapsulamiento. Colocación en los datos de un encabezado de protocolo en particular, con información sobre la capa que ha hecho la encapsulación.

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. Canal de comunicaciones de red que se reserva indefinidamente para transmisiones , en lugar de conmutarse según lo requiera la transmisión.

Enlace punto a punto. Enlace que proporciona una sola ruta preestablecida de comunicaciones de WAN desde el cliente a través de una red de *carrier*, a una red remota.

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.

Ethernet. El protocolo de conexión más común en las LAN. Todas las estaciones del segmento comparten el ancho de banda total, que es 10 Mbps, 100 Mbps para Fast Ethernet o 1000 Mbps para Giga Ethernet.

F:

FECN

Frame-Relay. Protocolo conmutado de la capa de enlace de datos que administra varios circuitos virtuales utilizando un encapsulamiento HDLC entre dispositivos conectados. Frame Relay es más eficiente que X.25.

G:

GRE (Generic Routing Encapsulation). Túnel VPN que soporta protocolos de capa 3 como IP e IPX. GRE no utiliza TCP ni UDP, trabaja directamente con IP, identificado con el número 47. Posee características propias de verificación e integridad.

H:

HDLC (Control de Enlace de Datos de Alto Nivel). Protocolo síncrono de la capa de enlace de datos, orientado a bit. Desarrollado por ISO. HDLC especifica un método de

encapsulamiento de datos en enlaces síncronos seriales que utiliza caracteres de trama y sumas de autocomprobación.

HDSL (High-data-rate digital Subscriber Line). Línea Digital del Suscriptor de alta velocidad. Una de las cuatro tecnologías de DSL. HDSL entrega 1.544 Mbps de ancho de banda de bajada (de la oficina central al cliente) y de subida (del cliente a la oficina central), sobre dos pares de cobre trenzado. Está limitado a un rango de distancia de 3658,5 metros.

Horizonte dividido. Técnica de enrutamiento en la cual se impide que la información acerca de los routers salga de la interfaz del router a través de la cual se recibió la información. Esta técnica es útil para evitar bucles de enrutamiento.

Host: Computador en una red. Similar a nodo excepto que el host normalmente implica un ordenador y nodo se aplica a cualquier sistema de red, incluyendo servidores y router.

I:

Internetwork. Industria dedicada a la conexión de redes entre sí. Agrupamiento de redes interconectadas por routers y otros dispositivos que funciona como una sola red.

IP (Protocolo Internet). Protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetwork de redes no orientada a conexión. El IP da funciones de direccionamiento, especificación del tipo de servicio, fragmentación y reensamblaje, y seguridad. Se define en el RFC 791.

IPSec (Protocolo de Internet Seguro). Es un conjunto de protocolos y algoritmos de seguridad diseñados para la protección del tráfico de red para trabajar con IP de modo transparente o modo túnel que soporta una gran variedad de encriptaciones y autenticaciones.

L:

LAN (red de área local). Red de datos de alta velocidad y bajo nivel de errores que cubre un área geográfica relativamente pequeña. Las LAN conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un sólo edificio y otra área geográficamente limitada. Los estándares de LAN especifican el cableado y señalización en las capas físicas y de enlace de datos del método OSI. Ethernet, FDDI y Token Ring son tecnologías LAN ampliamente utilizadas.

LMI (Interfaz de Administración Local). Conjunto de mejoras a las especificaciones básicas Frame-Relay. LMI incluye soporte para un mecanismo de actividad, que verifica que los datos están fluyendo; un mecanismo de multicast, que le ofrece al servidor de red su DLCI local y DLCI de multicast; direccionamiento global, que le ofrece a los DLCI significado global en lugar de local en las redes Frame-Relay; y un mecanismo de estado, que proporciona un informe de estado constante sobre los DLCI que el switch conozca.

M:

Multiplexión: Esquema que permite que varias señales lógicas se transmitan de forma simultánea a través de un canal físico exclusivo.

MPLS, Multiprotocol Label Switching (Switching de etiquetas multiprotocolo). MPLS es un estándar de la industria sobre el cual se basa la conmutación (switching) de etiquetas, las cuales identifican los diferentes tipos de información sobre la red. La tecnología MPLS le permite a un proveedor de servicio montar sobre su red servicios diferenciados a los cuales se tiene acceso a través del protocolo IP. MPLS permite que los usuarios tengan acceso a la red y se registren a algunos servicios específicos, sin que esto implique tener acceso a toda la red, es decir, se garantiza la privacidad y seguridad de la información mediante la creación de redes virtuales privadas, VPN.

N:

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

O:

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. OSPF ofrece enrutamiento de menor costo, el enrutamiento de múltiples rutas y el balanceo de carga.

P:

Paquete: Agrupación lógica de información que incluye un encabezado que contiene la información de control y (generalmente) los datos del usuario. Los paquetes se usan a menudo para referirse a las unidades de datos de capa de red.

PBX (central telefónica privada). Conmutador de un teléfono analógico o digital ubicado

en las instalaciones del suscriptor y que se usa para conectar redes telefónicas privadas y públicas.

PVC (circuito virtual permanente). Circuito virtual que se establece de forma permanente. Los PVC ahorran el ancho de banda relacionado con el establecimiento y desmantelamiento del circuito en situaciones en las que ciertos circuitos virtuales deben existir de forma permanente. Comparar con SVC.

R:

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 de pago. Grupo de dispositivos y recursos de red que se encuentran dentro de la nube.

Router: Dispositivo de capa de red que usa una o más métricas para determinar cuál es la ruta más óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes de una red a otra basándose en la información de capa.

S:

SDSL (very-high-data-rate digital subscriber line). Línea de velocidad de suscriptor de altísima velocidad. Una de las cuatro tecnologías de DSL. Entrega entre 13 y 52 Mbps hacia abajo (desde la central hacia el cliente) y entre 1.5 y 2.3 hacia arriba (desde el cliente hacia la central) sobre un único par trenzado. Está limitado a un rango entre 304,8 y 1372 metros.

Servidor: Hardware provisto de herramientas software que suministra servicios a los clientes o usuarios de una empresa.

SMDS (Servicio de Datos Conmutados Multimegabit). Es un servicio definido en EE.UU. capaz de proporcionar un transporte de datos transparente "no orientado a conexión" entre locales de abonado. SMDS permite implementar servicios de interconexión de redes de área local utilizando una red dorsal compartida en un ámbito de cobertura nacional, sin detrimento en las prestaciones de velocidad que siguen siendo las propias de las RALs. Ofrece distintas velocidades de acceso desde 1, 2, 4, 10, 16, 25 y hasta 34 Mb. La velocidad entre nodos de la red dorsal comienza en 45Mb y llegará a 155Mb. SMDS

ofrece un servicio de Red Metropolitana con un acceso desde el punto de vista del abonado idéntico al 802.6, con la particularidad de que no especifica la tecnología interna de la red pública, pudiéndose utilizar tanto técnicas de conmutación ATM como otras.

SVC (circuito virtual conmutado). Circuito virtual que se establece de forma dinámica a pedido y que se desconecta cuando la transmisión se completa. Los SVC se usan en situaciones en las que la transmisión de datos es esporádica. Comparar con PVC.

T:

TCP/IP (Protocolo de Control de Transmisión/Protocolo de Internet). Nombre común para el conjunto de protocolos desarrollados por el DoD de EEUU en los años 70 para promover el desarrollo de *internetwork* de redes a nivel mundial.

Token Ring. LAN de transmisión de tokens desarrollada y soportada por IBM. Token Ring se ejecuta a 4 o 16 Mbps a través de un topología de anillo.

V:

VDSL (very-high-data-rate digital subscriber line). Línea de velocidad de suscriptor de altísima velocidad. Una de las cuatro tecnologías de DSL. Entrega entre 13 y 52 Mbps hacia abajo (desde la central hacia el cliente) y entre 1.5 y 2.3 hacia arriba (desde el cliente hacia la central) sobre un único par trenzado. Está limitado a un rango entre 304,8 y 1372 metros.

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, en realidad, están ubicados en una serie de segmentos de LAN distintos. Debido a que las VLAN están basadas en conexiones lógicas en lugar de físicas, son extremadamente flexibles.

VPN (Red privada virtual). Permite establecer una conexión segura a través de una red pública o Internet. Una VPN permite que el tráfico IP viaje seguro a través de una red pública TCP/IP al encriptar el tráfico desde una red hasta la otra. Una VPN usa *tunneling* para encriptar toda la información en el nivel IP.

W:

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 *carriers* comunes. Frame-Relay, SMDS y X.25 son ejemplos de WAN.

X:

X.25. Estándar UIT-T que define la manera en la que las conexiones entre los DTE y DCE se mantienen para el acceso a la terminal remota y las comunicaciones en computadores en las redes de datos públicas. Frame-Relay ha reemplazado en cierta manera a X.25.

Bibliografía

Guía de estudio para la certificación CCNA 640-802 – Ernerto Ariganello, Editorial Rama

ISBN 978-84-7897-885-4

http://en.wikipedia.org/wiki/Cisco_Catalyst

http://es.wikipedia.org/wiki/L%C3%ADnea_de_abonado_digital_asim%C3%A9trica

http://portal.uned.es/pls/portal/docs/PAGE/UNED_MAIN/SERVICIOSGENERALES/CSI/UNIDADES/COMUNICACIONES_SEGURIDAD/ACS06/ACS0605/SERVICIO%20MACROLAN.PDF

<http://ipsec-tools.sourceforge.net/>

<http://www.netbsd.org/docs/network/ipsec/rasvpn.html>

Datasheet de los equipos:

- Cisco <http://www.cisco.com>
- Agregadores Cisco 7604
http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheets_list.html
- Cisco Catalyst 3560 – 24 EMI
http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5528/product_data_sheet09186a00801f3d7d.html
- MacroLAN 10Mb: Cisco 2801
http://www.cisco.com/en/US/prod/collateral/routers/ps5854/ps5882/product_data_sheet0900aec8016fa68_ps5854_Products_Data_Sheet.html
http://www.cisco.com/en/US/prod/collateral/routers/ps221/product_data_sheet0900aec8028aa5a_ps5854_Products_Data_Sheet.html
- MacroLAN 2 Mb: Cisco 1921
http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps7290/ps10589/data_sheet_c78-598389.html
- ADSL 20 Mb: Cisco 887
http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78_459542_ps380_Products_Data_Sheet.html

Anexos

Servicio MacroLAN ofrecido por TdE

El servicio MacroLAN es la solución de Telefónica de altas prestaciones y velocidad para la interconexión de Redes Privadas Virtuales, cuya puesta en marcha requiere la intervención de técnicos de varias áreas.

1. Instalación de la acometida de Fibra óptica:

Un técnico de Telefónica contactará con el cliente autorizado de la sede para concertar una cita en el domicilio e instalar una acometida de fibra óptica, que será un cable que llega desde la red exterior hasta un Punto de Terminación de Fibra óptica (PTRO o roseta óptica de medidas) colocado en el interior y lo más próximo posible a la ubicación de los equipos terminales (switch o router).

Los trabajos de este técnico pueden llevar más de 1 día y su labor se realiza tanto en las inmediaciones del domicilio de instalación como en el interior del mismo, siendo necesaria en ocasiones una visita previa de replanteo para preparar los trabajos.

En el caso de que ya tenga instalado algún acceso de Fibra óptica (o que haya contratado un acceso vía cobre de baja velocidad), no será necesario tender una nueva acometida, simplificándose el proceso.

2. Instalación de los equipos terminales:

Una vez instalada la acometida de fibra óptica es necesaria la intervención de otro técnico para instalar los equipos terminales, que son habitualmente un Conversor de Medios y el EDC (switch o router) que se haya seleccionado.

3. Configuración y puesta en servicio.

Una vez instalados los equipos terminales se procederá a su configuración remota desde el Centro de Gestión. Finalmente, mediante llamada telefónica, se confirmarán los datos de direccionamiento necesarios para la puesta en marcha del servicio.

Infraestructura necesaria para la instalación de los equipos

Fundamentalmente:

- Pared y suelo libres de obstáculos que impidan adosar rosetas en la pared.
- Temperatura entre 5° y 30° C, y ventilación de la Sala.
- Espacio para la operación y mantenimiento de los equipos.
- Enchufes de alimentación de 220V. y 10/16 A., con toma de Tierra inferior a 5 ohmios de resistencia.
- En caso de que tenga un switch de comunicaciones, será necesaria al menos una boca libre para la conexión con el EDC.

Además, se recomienda:

- Armario (rack) de 19 pulgadas de anchura con la altura y profundidad suficientes para albergar los equipos (incluyendo los Conversores de Medios), dotado de bandejas, puertas delantera/trasera, ventilación y alimentación preferiblemente con SAI.
- Una altura mínima de techo 220 cm.
- Iluminación mediante lámpara fluorescente.
- Suelo técnico o falso techo desmontable para facilitar la prolongación del cableado interior.

Plantilla de configuración servicio MacroLAN

- Plantilla de autodescubrimiento:

Primero hay que borrar la configuración por si tuviera ya algo preconfigurado previamente.

```

enable
erase startup-config

--- CONFIGURACIÓN ---

service password-encryption
!
enable secret <PASSWORD ENABLE>
!
no aaa new-model
ip subnet-zero
ip cef
!
interface FastEthernet0/0
shutdown
!
interface FastEthernet0/1
no shutdown
no ip address
speed auto
duplex auto
!
interface FastEthernet0/1.90
encapsulation dot1Q 90
ip address dhcp client-id FastEthernet0/1
!
ip classless
!
no ip http server
!
snmp-server community provision RW
snmp-server enable traps tty
!
line con 0
password <PASSWORD>
login
line aux 0
password <PASSWORD>
login
line vty 0 15
password <PASSWORD>
login
!
end

```

- Plantilla de configuración:

```

!
!!!!El interfaz LAN variará dependiendo del modelo de equipo, se tendrá que revisar!!!

interface Fa0/0
no ip address
ip address <ip red lan Macrolan +3> 255.255.255.x
ip address <ip red lan Interlan +1>255.255.255.x secondary
ip helper-address 10.0.203.4
standby 1 ip <ip red lan Macrolan +1>
standby 1 preempt
hold-queue 100 out
!

int serial0/0
ip route-cache
ip mroute-cache

ip classless
ip route 0.0.0.0 0.0.0.0 serial0/0.xx
ip route <IP ACCESO><MÁSCARA> Serial0/0.400
ip route <IP ACCESO><MÁSCARA WILDCARD> Serial0/0.401

ip prefix-list REDESCLIENTE seq 5 permit <ip red lan Macrolan>/<mascará formato corto>
ip prefix-list REDESCLIENTE seq 10 permit <ip red lan Interlan>/<mascará formato corto>
ip prefix-list REDESGESTION seq 10 permit <ip gestión Interlan>/32

key chain 1
key 1
key-string macrolan

interface fa0/0                                     (Dependerá del modelo de equipo)
ip rip authentication mode md5
ip rip authentication key-chain 1

router rip
version 2
timers basic 30 90 90 90
redistribute connected
passive-interface fa0/0      (Dependerá del modelo de equipo, ya que puede ser et0 o Fa0 )
distribute-list prefix REDESCLIENTE out serial0/0.xx      (Dependerá del modelo de equipo)
distribute-list prefix REDESGESTION out serial0/0.401      (Dependerá del modelo de equipo)
distribute-list prefix REDESGESTION out serial0/0.400      (Dependerá del modelo de equipo)
no auto-summary
!
service nagle
no service finger
service tcp-keepalives-in
service dhcp
ip cef
no service udp-small-servers
no service tcp-small-servers
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
no ip http server
no service config
!
!
no ip domain-lookup
no ip name-server
ip subnet-zero
no cdp run
no ip source-route
no ip bootp server
!
interface Loopback400
description Direccion IP de Gestion de EDC
no ip directed-broadcast
no ip proxy-arp
!

```



```

ip tacacs source-interface Loopback400
ip tftp source-interface Loopback400
ip ftp source-interface Loopback400
!
tacacs-server host <IP TACAS SERVER>
tacacs-server timeout 3
tacacs-server key <TACAS KEY>
!
aaa new-model
aaa authentication login default group tacacs+ enable
aaa authentication enable default group tacacs+ enable

!!!salir y volver a entrar!!!
aaa authorization exec default group tacacs+ if-authenticated
aaa authorization commands 0 default group tacacs+ if-authenticated
aaa authorization commands 1 default group tacacs+ if-authenticated
aaa authorization commands 15 default group tacacs+ if-authenticated
!
enable secret <PASSWORD>
!
clock timezone MET 1
clock summer-time METDST recurring last Sun Mar 2:00 last Sun Oct 3:00
!
logging buffered 100000
no logging console
logging rate-limit console 10 except errors
access-list 50 remark GESTION SNMP SOLO LECTURA
access-list 50 permit <IP ACCESO><MÁSCARA WILDCARD>
!
access-list 51 remark GESTION PERMISO ESCRITURA Y TFTP
access-list 51 permit <IP ACCESO><MÁSCARA WILDCARD>
!
access-list 52 remark ACCESO TELNET
access-list 52 permit <IP ACCESO><MÁSCARA WILDCARD>
access-list 52 permit <ip red lan Macrolan> < mascara Wildcard>
access-list 52 permit <Ip red wan central Interlan> < mascara Wildcard>
!

snmp-server community GESTION ro 50
snmp-server community ESCRITO rw 51
snmp-server location <Domicilio>
snmp-server contact CGP Telefonica
snmp-server trap-source Loopback400
snmp-server ifindex persist
snmp-server enable traps snmp linkup linkdown coldstart warmstart
snmp-server enable traps frame-relay
snmp-server enable traps envmon
snmp-server enable traps bgp
snmp-server enable traps atm pvc
snmp-server enable traps isdn call-information
snmp-server tftp-server-list 51

!

access-list 70 remark Lista de acceso para permitir SNMP a cliente
access-list 70 permit <IP SNMP SERVER>

snmp-server community <SNMP COMUNITY KEY>

rmon event 100 log trap GESTION description NUM_INTERFACES_HA_CAMBIADO owner config
rmon event 200 log trap GESTION description MEMORIA_LIBRE_SUPERIOR_A_500K owner config
rmon event 201 log trap GESTION description MEMORIA_LIBRE_INFERIOR_A_500K owner config
rmon event 300 log trap GESTION description SUPERADO_UMBRAL_DE_USO_DE_CPU owner config
rmon event 301 log trap GESTION description USO_DE_CPU_EN_LIMITES_ACEPTABLES owner config
rmon alarm 100 interfaces.1.0 900 delta rising-threshold 1 100 falling-threshold -1 100 owner
config
rmon alarm 200 lsystem.8.0 3600 absolute rising-threshold 500000 200 falling-threshold 500000
201 owner config
rmon alarm 300 lsystem.58.0 900 absolute rising-threshold 70 300 falling-threshold 55 301
owner config
!

```

```
!  
banner motd ^  
*****  
*****  
**      Esta usted accediendo a una maquina privada propiedad de      **  
**              TELEFONICA DATA ESPAÑA S.A.              **  
**      Necesita autorización para usar este sistema      **  
**      estando Vd estrictamente limitado al uso en dicha autorización **  
*****  
**              El acceso no autorizado a este sistema      **  
**              o el uso indebido del mismo esta prohibido      **  
**              es contrario a la Polictica de Seguridad      **  
**              y a la legislacion vigente      **  
**      Si no esta autorizado cierre inmeditamente su conexion      **  
*****  
**      Si usted revela informacion interna de      **  
**      Telefonica Data España S.A. o de sus clientes,      **  
**      sin autorizacion, podra estar incurriendo en una violacion      **  
**      que podria suponer la posible comision de una falta o delito      **  
*****  
**              Telefonica Data España S.A.      **  
*****^  
!  
line con 0  
exec-timeout 5 0  
password <PASSWORD>  
!  
line aux 0  
exec-timeout 5 0  
password <PASSWORD>  
access-class 52 in  
modem inout  
no exec  
transport input none  
stopbits 1  
flowcontrol hardware  
!  
line vty 0 4  
access-class 52 in  
password <PASSWORD>  
exec-timeout 5 0  
!  
!
```

Plantilla de configuración con VPN e IP fija

```

!
version 12.1
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname Router
!
logging rate-limit console 10 except errors
enable secret 5 xxxxxxxxxxxxxxxxxxxx
enable password 7 xxxxxxxxxxxxxxxx
!
username chatplay
ip subnet-zero
no ip finger
!
ip cef
no ip dhcp-client network-discovery
!
policy-map WFQ
class class-default
fair-queue
random-detect
!
!
!
!
interface Tunnell
ip address 192.168.50.3 255.255.255.0
tunnel source xxx.xxx.xxx.xxx
tunnel destination xxx.xxx.xxx.xxx
tunnel mode ipip
tunnel key 33493
tunnel sequence-datagrams
tunnel checksum
!
interface Ethernet0
ip address 192.168.0.xxx 255.255.255.0
ip nat inside
no ip mroute-cache
no cdp enable
!
interface ATM0
no ip address
no ip mroute-cache
no atm auto-configuration
no atm ilmi-keepalive
no atm address-registration
no atm ilmi-enable
bundle-enable
dsl operating-mode auto
hold-queue 208 in
!
interface ATM0.1 point-to-point
ip address xxx.xxx.xxx.xxx 255.255.255.224
ip nat outside
no ip mroute-cache
pvc 8/32
encapsulation aal5snap
service-policy output WFQ
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 ATM0.1
ip route 192.168.1.0 255.255.255.0 Tunnell
no ip http server
!
ip nat inside source list 101 interface ATM0.1 overload

```

```
access-list 1 permit 192.168.0.0 0.0.0.255
access-list 101 permit ip any any
no cdp run
```

```
!
line con 0
exec-timeout 120 0
transport input none
stopbits 1
line vty 0 4
exec-timeout 0 0
password 7 xxxxxxxxxxxxxxxx
login
!
scheduler max-task-time 5000
end
```

Configuración VPN – LAN2LAN

Configuración de los ficheros comentados en "Topología servidor alojado en cliente"

- /etc/ipsec-tools.conf

```
#!/usr/sbin/setkey -f

flush;

spdflush;

spdadd <IP LAN servidor cliente> <IP LAN servidor destino> any -P out ipsec esp/tunnel/<IP
publica servidor cliente>-<IP publica servidor destino>.11/unique;

spdadd <IP LAN servidor destino> <IP LAN origen servidor cliente> any -P in ipsec
esp/tunnel/<IP publica servidor destino>-<IP publica servidor cliente>/unique;
```

- /etc/racoon/psk.txt

```
<IP pública servidor destino> <Password Pre shared key>
```

- /etc/racoon/certs

- /etc/racoon-tool.conf

```
#
# Configuration file for racoon-tool
#
# See racoon-tool.conf(5) for details
#

# How to control the syslog level
global:
    log: notify

#
# Example of multiple networks to one endpoint
#
#connection(bacckdoor-doormat):
#    src_range: 192.168.223.1/32
#    dst_range: 192.168.200.0/24
#    src_ip: 172.31.1.1
#    dst_ip: 10.0.0.1
#    admin_status: enabled
#    compression: no
#    lifetime: time 20 min
#    authentication_algorithm: hmac_sha1,hmac_md5
#    encryption_algorithm: aes,3des

#connection(backdoor-outhouse):
#    src_range: 192.168.223.0/24
#    dst_range: 10.255.255.254
```

```
# src_ip: 172.31.1.1
# dst_ip: 10.0.0.1
# admin_status: no
# lifetime: time 20 min
# authentication_algorithm: hmac_sha1
# encryption_algorithm: 3des

#peer(10.0.0.1):
# verify_cert: on
# passive: off
# verify_identifier: off
# lifetime: time 60 min
# hash_algorithm[0]: sha1
# encryption_algorithm[0]: 3des
## my_identifier: fqdn backdoor.foo.bar
## peers_identifier: fqdn garden-path.foo.bar
## certificate_type: x509 bLaH.pem PrIv.pem
```

- **/etc/racoon.conf**

```
# Please read racoon.conf(5) for details, and also read setkey(8).
#
path pre_shared_key "/etc/racoon/psk.txt";
path certificate "/etc/racoon/certs";

listen {
    isakmp <IP Pública servidor cliente> [500];
}

log <LEVEL>;

remote <IP Pública servidor destino> {
    lifetime time 24 hour;
    exchange_mode main;
    my_identifier address;
    ike_frag on;
    proposal {
        encryption_algorithm 3des;
        hash_algorithm md5;
        dh_group 2;
        authentication_method pre_shared_key;
    }
}

sainfo anonymous {
    lifetime time 28800 seconds;
```

```

    encryption_algorithm 3des;
    authentication_algorithm hmac_md5;
    compression_algorithm deflate;
    pfs_group 2;

```

```

}

```

- **/etc/network/interfaces**

```

auto lo
iface lo inet loopback
    up ip addr add <IP LAN servidor cliente>/32 dev lo
    down ip addr del <IP LAN servidor cliente>/32 dev lo

auto eth0
iface eth0 inet static
    address <IP pública servidor cliente>
    netmask <Máscara>
    gateway <Gateway>
    up ip route add <IP LAN servidor destino>/32 via <IP pública servidor cliente> src <IP LAN
servidor cliente>
    down ip route del <IP LAN servidor destino>/32 via <IP pública servidor cliente> src <IP
LAN servidor cliente>

auto eth1
iface eth1 inet static
    address <IP LAN>
    netmask <MÁSCARA>

```

Protocolo RIPv2

RIP es un protocolo de vector distancia que utiliza la cuenta de saltos del router como métrica. La cuenta de saltos máxima de RIP es 15 y cualquier punto que exceda este número se declarará como inalcanzable.

En RIP, la información de enrutamiento se propaga de un router a los otros vecinos por medio de una difusión de IP usando el protocolo UDP y el puerto 520.

El algoritmo de vector distancia permite que los routers difundan periódicamente sus tablas de routing entre los routers vecinos con una periodicidad que se ha de definir previamente en los valores de los temporizadores, y éstos se pueden variar para optimizar el funcionamiento del protocolo.

El protocolo RIPv2 es un protocolo sin clase que admite CDIR, VSLM, resumen de rutas y seguridad mediante texto simple y autenticación MD5.

Algunos de los comandos RIP más útiles:

Comando	Descripción
router rip	Inicia el enrutamiento RIP
version [número de versión]	RIPv1 o RIPv2, por defecto es RIPv1
network [dirección de red]	Añade una o más redes al protocolo
distance [1-255]	Establece una distancia administrativa, por defecto 120
distribute-list	Redistribuye una lista de acceso en el protocolo
redistribute static	Redistribuye una ruta estática en el protocolo
passive-interface	Evita el envío de actualizaciones de enrutamiento sobre una interfaz determinada
timers basic	Establece los tiempos de Interval Invalid Holddwn Flush
ip rip authentication key-chan	Configura una contraseña en RIP
ip rip authentication mode text	Establece una contraseña en texto plano
ip rip authentication mode md5	Establece una contraseña en texto cifrado
show ip protocols	Muestra los parámetros RIP
Show ip route rip	Muestra la tabla de enrutamiento RIP
debug ip rip	Muestra los procesos RIP

Protocolo HSRP

HSRP (Hot standby router protocol) es un protocolo propietario de CISCO que permite redundancias automáticas entre routers conectados donde uno de ellos pertenece a la línea principal y el otro router a la línea de backup. El cambio de una línea a otra se hace de manera automática debido a que la línea secundaria está mandando paquetes multicast de “hello” a la línea principal para verificar su correcto funcionamiento y en cuanto no recibe respuesta toma el control y se convierte en línea principal.

HSRP utiliza la dirección multicast 224.0.0.2 a través del puerto 1985 de UDP para intercambiar la información de actividad entre los routers, con un intervalo de 3 segundos, donde pasados 10 segundos sin respuesta provoca la convergencia entre las redes. Estos parámetros son configurables.

Comando	Descripción
standby [0-255] ip [dirección IP virtual]	Crea un grupo HSRP y asigna una IP virtual
standby [0-255] priority [0-255]	Establece una prioridad dentro del grupo HSRP
standby mac-refresh [0-255]	Configura los tiempos de envíos de los paquetes ARP
standby [0-255] mac-address [dirección MAC]	Utiliza una MAC determinada por el administrador
Standby [0-255] preempt	Configura una preferencia de elección de router activo
Standby [0-255] priority [0-255] preempt	Configura una preferencia de elección de router activo
standby [0-255] timers [hello failover]	Configura los tiempos de saludo y caída
Standby [0-255] authentication [contraseña]	Establece una contraseña de autenticación
Show standby	Muestra información general sobre HSRP
Show standby [interface tipo][número]	Muestra la información HSRP específica en la interfaz
Show standby brief	Muestra un resumen HSRP en las interfaces

Protocolo BGP

BGP (Border Gateway Protocol) es un protocolo de gateway exterior que fue diseñado para intercambiar información sobre las redes entre sistemas autónomos. Es el protocolo más usado por las empresas y proveedores de servicio de Internet ya que garantiza el enrutamiento libre de bucles y resúmenes de rutas (CIDR).

BGP utiliza el protocolo TCP para comunicarse con sus routers vecinos, a través del puerto 179, con los que establece una sesión BGP e intercambia información de ruta y de sesión de manera incremental.

Para proporcionar mayor seguridad, en las transferencias de información, se puede utilizar firmas MD5 para verificar cada segmento TCP.

Este protocolo guarda una tabla de enrutamiento independiente a la tabla de enrutamiento IP que contiene todas las rutas de acceso posibles a las redes publicadas.

BGP seleccionará la ruta más óptima basándose en las siguientes reglas:

- La ruta óptima será la que tenga menor distancia administrativa.
- Entre dos rutas iguales:
 - se optará por la definida con mayor métrica² (LOCAL_PREF).
 - Una ruta con información AS-path será preferente ante otra que no lo disponga.
 - Entre dos rutas con AS-path se elegirá la que tenga menor valor de métrica (MULTI_EXIT_DISC)
 - Entre dos rutas con ASP-path diferentes, se preferirá la de origen IGP ante la de origen EGP.
 - Entre dos rutas con ASP-path diferente y mismo origen, se prefiere la que tenga el AS-path de menor longitud
- Se prefieren las rutas instalables en la tabla de rutas activas del equipo frente a las rutas no instalables
- Se prefiere la ruta que tenga siguiente salto con el valor de dirección IP más bajo.

Comandos	Descripción
router bgp [número de sistema autónomo]	Inicia el enrutamiento BGP y lo asocia a un sistema autónomo local
network [dirección de red] mask [máscara]	Asocia una o más redes al enrutamiento BGP
neighbor [dirección igual-grupo-nombre] remote as [número]	Identifica al router vecino o un grupo de vecinos con el que se establece una sesión y su respectivo sistema autónomo.
neighbor [igual-grupo-nombre] peer-group	Asocia al router con un nombre de grupos vecinos
synchronization	Activado por defecto, permite una convergencia más eficaz.
neighbor [dirección IP] route-reflector-client	Determina la dirección del router cliente
prefix-list-name	Nombra la lista de prefijos
[seq seq-value]	Número de secuencias de 32 bits.
{deny permit}	Acción que tomará al encontrar coincidencia
network/len	Red a cotejar
[ge ge-value] [le le-value]	Opcional, intervalo de longitud del prefijo a cotejar con el parámetro network/len

Protocolo MPLS

MPLS (Multiprotocol Label Switching) es un protocolo que trabaja entre las capas 2 y 3 de la pila OSI. Es un protocolo basado en señalización de los paquetes mediante etiquetas y la información que se tiene en la base de datos, llamada LFIB, para cada una de ellas ya que según la información que tenga enrutará por un interfaz u otro y le añadirá una etiqueta nueva, ya que la información es local y para su router vecino.

Los dos tipos de etiquetado más comunes son:

- ➔ LPD (Label Distribution Protocol): Protocolo abierto, descubre y mantiene conexión con sus vecinos mediante UDP multicast (224.0.0.2) a través el puerto 646.
- ➔ TDP (Tag Distribution Protocol): Protocolo propietario de CISCO, descubre y mantiene conexión con sus vecinos mediante UDP broadcast a través del puerto 711.

La principal ventaja que tiene este protocolo es el ahorro de consumo en los equipos ya que tan sólo tiene que consultar la base de datos, por cada paquete que llega, y no la lista de rutas que en entornos muy grandes puede llegar a realizar un gran esfuerzo de CPU.

Proporciona servicio de VPN de capa 2 y 3 sin importar desde qué tecnología provenga o incluso si es necesario atravesar otros ISP para interconectar diferentes sitios remotos.

Utiliza *Traffic Engineering* (TE) es una técnica que depende del protocolo de encaminamiento y que aprovecha enlaces poco usados, de respaldo o convergencia rápida ante cortes en algún enlace.

En la topología de la red MPLS se distinguen tres tipos de dispositivos:

- ➔ Provider (P). Son dispositivos de tránsito pertenecientes al proveedor.
- ➔ Provider Edge (PE). Son los encargados de agregar el tráfico proveniente del cliente e insertarlo en la red MPLS o viceversa. Pertenece a la red del proveedor.
- ➔ Customer Edge (CE). Son los routers o switches en el acceso, que se conectan a los PE. Pertenecen a la red del cliente.