DEPARTAMENTO DE INGENIERÍA TELEMÁTICA

Diseño de una Solución de Outsourcing de Infraestructuras basado en Tecnologías TIC

Proyecto Fin de Carrera

Autor: Miguel Raso Prado

Tutor: Antonio de la Oliva Delgado

Leganés, Junio de 2012

"Es mejor saber después de haber pensado y discutido que aceptar
los saberes que nadie discute para no tener que pensar."

Fernando Savater

Agradecimientos

Aunque el nombre de uno mismo siempre es el primero en aparecer en la portada, la verdad es que este proyecto de Fin de Carrera no podría existir sin la participación (a veces, incluso inconsciente) de mucha gente que ha estado a mi alrededor apoyándome, aconsejándome y acompañándome.

Y como no siempre he sido todo lo agradecido que debía con esas personas, aprovecho estas líneas para dar GRACIAS con mayúsculas a todos los que han creído en mí, incluso cuando yo ya no lo hacía:

A mi mujer, que ha seguido mi carrera a mi lado, como los buenos entrenadores: vitoreando mis aciertos, criticando mis fallos, ayudándome en las decisiones difíciles y aportándome aquellas cosas que he podido necesitar, a veces, sin ni siquiera pedírselo, y nunca me abandona, gane o pierda.

A mi familia, porque ellos más que nadie creyeron en mí desde que era un niño, siempre "dando caña", y porque ellos siempre supieron hasta donde podía y puedo llegar, y así me lo han hecho ver.

A mis amigos de la Universidad los que se fueron antes de tiempo, los que ya se han ido y los que quedan, porque nadie más que ellos puede entender lo que supone alcanzar esta meta, después de haber compartido incontables terapias de grupo en El Callejón, ahogando las penas o regando las alegrías con cerveza.

A mis amigos de toda la vida, del barrio, del colegio, porque nos hemos visto crecer y hemos compartido noches de fiesta y noches de estudio en la biblioteca.

A mis compañeros del grupo, porque con ellos he conseguido liberar mis tensiones, disfrutar de mi hobby e ilusionarnos con un proyecto compartido.

A Antonio y Albert, tutores de este proyecto, que me han ayudado con todo lo que he necesitado para llevar a cabo esta idea, a pesar de mi evidente desastre de agenda…

A los profesores de la Universidad y, por qué no, de toda mi vida estudiantil, que me han dado los conocimientos necesarios para llegar hasta donde estoy.

Y a todos aquellos que me haya dejado en el tintero, porque el que me conozca, sabe que soy de frágil memoria, pero nunca malintencionado.

RESUMEN

Palabras Clave: Solución empresarial, virtualización, servicios, outsourcing, IaaS, RPV (Red Privada Virtual), navegación segura, backup remoto.

A través del presente proyecto trataremos de desarrollar una solución práctica a las necesidades de una empresa actual, en la que se verán implicadas diferentes tecnologías, todas ellas punteras, que permitirán a través de las telecomunicaciones un ahorro en costes y una eficiencia superior a los modelos tradicionales.

Basándonos principalmente en las tecnologías de virtualización y aprovechando las economías de escala, podremos disponer de servidores de alta capacidad, integrados en un entorno de control avanzado, además de una provisión en muy corto tiempo en caso de necesitar un aumento en las capacidades de la planta, y una comunicación entre sedes de alta velocidad, a pesar de la distancia geográfica real. Estos servicios se ven complementados además con una navegación segura por internet y un backup a distancia de los equipos que, por necesidades legales, no pueden ser sacados de las sedes de la empresa. Como ventaja principal, cabe destacar el hecho de que no será necesaria una inversión elevada para la modernización de la planta, dado que los servicios se basan en un pago por uso.

Aunque se trata de un escenario ficticio, el documento está elaborado siguiendo un índice muy similar al que suelen seguir las ofertas presentadas a los clientes en el mundo empresarial.

Para conseguir cumplir los requerimientos del cliente recurriremos a los servicios de catálogo que ofrece la empresa española de telecomunicaciones Telefónica, aún a pesar de que no es la única presente en el sector capaz de cumplir las necesidades planteadas, pero si una de las que puede conseguir mejores precios debido a su nivel de negocio, sus economías de escala y a que es la única que lo puede hacer desde la posición de operadora.

ABSTRACT

Key Words: Business Solution, virtualization, services, outsourcing, Iaas, VPN, safe navigation, remote backup.

Through this Project, I have tried to develop a practical solution to the current needs on a fictional company. It involves different edge technologies, enabling cost saving and a higher efficiency compared to traditional models.

Mainly based on virtualization technologies and scale economies, we can be provided with high capacity servers, embedded in an advanced control environment and a short provision time in case of requirements. It also provides a high speed communication between locations, even though large geographical distances.

These services are completed with safe internet navigation and online remote backup services, for those computers which cannot be removed from the company's headquarters due to law reasons.

As these services are based on "pay per use" models, no great investments are needed to carry out a modernization plan, which is this environment's main advantage.

Although this is a fictional scenario, this document is based on similar indexes used on commercial bids.

In order to accomplish customer's requirements, we are drawing on Telefonica's services catalogue.

Telefónica is a Spanish telecommunication company, which is not the only one capable to acquire proper results, but the one that could provide best prices. This position is obtained thanks to their great economy scales and due to its operator position.

Índice General

Índice de figuras

Índice de Tablas

1. INTRODUCCIÓN

La empresa TRANSACCIONES INMOBILIARIAS S.A. pretende modernizar su planta de servidores. Actualmente dispone de 3 servidores totalmente amortizados en sus instalaciones centrales de Madrid, conteniendo su ERP, su servidor de correo y el sistema de ficheros compartidos. Análogamente, en Barcelona disponen de 2 servidores conteniendo el ERP de los empleados situados en aquella oficina y su sistema de ficheros.

Todos los servidores se hallan en salas re aprovechadas, es decir, no están diseñadas para servir como Centro de Procesamiento de Datos (CPDs), con las carencias en seguridad y disponibilidad eléctrica que esto supone. Cada vez que necesitan compartir información entre oficinas, recurren a los correos electrónicos, con las desventajas asociadas a este tipo de intercambio, como son la falta de seguridad o la dependencia de una capacidad en los buzones.

Además, dado el creciente número de clientes y con intención de ampliar su ámbito geográfico abrirán dos nuevas sedes en Sevilla y Zaragoza.

Por ello, esta empresa requiere un servicio que les permita compartir un solo servidor ERP para las cuatro oficinas, además de un repositorio común donde compartir la información de manera síncrona y sin recurrir al correo electrónico, con el añadido de asegurar una alta disponibilidad. Además, dado que se van a colocar datos importantes en la red privada, y la comunicación con el exterior a través de internet es vital para la continuidad del negocio, es necesario que en la salida a Internet prevista disponga de una seguridad lo suficientemente alta como para poder evitar errores y caídas tanto en los servidores como en los equipos personales de cada trabajador.

Se presentan además dos inconvenientes, que son la existencia de datos que por requerimientos de seguridad propia de la empresa, no pueden ponerse en común en la red compartida, y deben almacenarse en servidores situados dentro de las instalaciones de cada oficina pero aún así, necesitan un backup periódico,

Por otro lado, el hecho de abrir nuevas oficinas implica una alta inversión, por lo que la actualización de la planta debe suponer el mínimo impacto inicial.

Por ello, a modo de RFP (Request For Proposal), la empresa requiere los siguientes servicios, cumpliendo las condiciones indicadas:

- La virtualización de sus servidores en un hierro compartido, de manera que el alojamiento de este hierro pueda ofrecer unos niveles de servicio lo más elevados posibles, permitiendo así a la empresa desentenderse de los problemas asociados a sus plataformas informáticas. Además, es importante que aun siendo servidores virtuales, tiene que ser posible aplicar políticas de backup y recuperación en dichos servidores. Estos servidores deben ser accesibles también a través de internet, ya que en ellos se alojará también la página web y la atención a incidencias.

- Se necesita también conexiones privadas punto a punto de datos entre las sedes de la empresa, así como con los nuevos servidores virtuales de la empresa, para poder mantener una

comunicación fluida y de alta velocidad, formando así una solo red. Debido a que cierta información pública es vital para el correcto funcionamiento del negocio, los usuarios tienen que poder navegar por internet a través de esta red. Por supuesto, esta navegación debe cumplir con criterios de seguridad que eviten infecciones informáticas, de alto riesgo para la continuidad del negocio.

- Para los servidores que no pueden ser externalizados, se requiere una solución de backup, ya sea con el suministro del equipamiento necesario (cabinas y discos), como a través de cualquier otro servicio que permita realizar estas tareas.

Para conseguir dar un servicio adecuado y de una alta calidad, vamos a recurrir a las soluciones de servicios existentes en catálogo en la empresa Telefónica de España, concretamente en su división Telefónica Soluciones.

La decisión tomada responde a su dilatada experiencia en el sector, su posición como operadora y sus alianzas como Partner Tecnológico con diversas y potentes compañías, como son Oracle, EMC, CISCO y similares.

Los servicios a utilizar son los siguientes:

- **Servicio de Hosting Virtual**, para poder proveer los servidores virtuales necesarios, a través de una plataforma compartida en un Centro de Datos Gestionado (CDG), también llamado Centro de Procesado de Datos (CPD), que cuentan con las condiciones de seguridad y alojamiento más avanzadas disponibles. Además también se provee un portal de auto provisión para poder solicitar recursos extra en caso de ser necesarios, por ejemplo, en campañas extraordinarias.

- **Servicio Macrolan**, para el requerimiento de las conexiones punto a punto entre sedes.

- **Servicio Tráfico limpio,** para proveer una salida de navegación a Internet de los usuarios a través de una plataforma que ejecuta tareas de Anti-Spam, Anti- Malware, filtrado de URLs y similares, que garantizan una navegación completamente segura.

- **Servicio de Backup Remoto** para poder realizar backups y restores a distancia de servidores que no se encuentran físicamente en los CDGs, evitando así una inversión en equipos propios, como podrían ser cabinas de almacenamiento, por lo general de precios de suministro y soporte muy elevados.

A lo largo de este proyecto, describiremos el estado del arte y la evolución de los diferentes servicios que compondrán la oferta, para después describir la oferta integrada que se presentaría al cliente, intentando explicar las decisiones tomadas en el diseño de la solución. Estos datos se acompañarán de un pequeño presupuesto y algunas capacidades añadidas que se pueden contratar para completar los servicios ofrecidos.

2. ESTADO DEL ARTE

2.1 SERVICIO DE HOSTING VIRTUAL

2.1.1 ANTECEDENTES HISTÓRICOS

En estos últimos años, una de las tecnologías de computación de las que más se habla y que más ha evolucionado es la virtualización. Hace algunos años la virtualización no era tomada en cuenta como una alternativa real al momento de instalar servidores y otros equipos de producción en la mayoría de los Centros de Computación, debido mayormente a que era una tecnología poco probada, demasiado costosa, o por el ya conocido "miedo al cambio" en donde simplemente se le teme a lo que no se conoce o es diferente. Sin embargo, actualmente la virtualización se ha posicionado en el mercado de la informática como una opción económica y efectiva al momento de diseñar, ampliar, y actualizar tecnología de Centros de Computación, al punto de que en muchos casos si no se elige la virtualización, se estaría perdiendo dinero y/o la implementación podría ser menos efectiva. [1]

¿Qué es Virtualización?

Aunque este es un tema el cual se ha ampliado grandemente en estos últimos años, básicamente virtualización es una tecnología que te permite instalar y configurar múltiples computadoras y/o servidores completamente independientes (conocidas como "virtual machines" o "maquinas virtuales") en una sola "caja" física, ya sea una computadora, servidor, "appliance", etc. A pesar de que estas maquinas virtuales comparten todos los recursos de un mismo "hardware", cada una trabaja de manera totalmente independiente (con su propio sistema operativo, aplicaciones, configuraciones, etc.). En otras palabras, en lugar de utilizar 5 servidores físicos, cada uno de ellos corriendo una aplicación que solo utiliza el 10% de los recursos de su servidor; podemos instalar 5 maquinas virtuales, cada una con su propia aplicación y configuraciones específicas, en un solo servidor y utilizar el 50-60% de los recursos del mismo.

Cabe señalar que cada una de estas maquinas virtuales, con la debida configuración, deberá funcionar exactamente igual que un servidor o PC física (puede ser conectado a una red, ingresar a un dominio, aplicar políticas de seguridad, conectar de manera remota, reiniciar de manera independiente, etc.). Al final obtenemos una implementación que será [2]:

- Más económica – Requiere menos hardware, menos electricidad, menos enfriamiento, menos espacio, menos infraestructura, y menos tiempo de administración. Todo esto al final se traduce en menor coste económico
- Menos compleja – Por las mismas razones mencionadas en el punto anterior.
- Más segura – Con los niveles de seguridad adecuados, una red virtual cuenta con menos puntos de ataque físicos, lo que la hace más segura. En adición a esto, la vitalización es una excelente estrategia de seguridad al momento de elaborar un "backup plan" o un "disaster recovery plan".
- Más fácil de administrar – Con el debido conocimiento de virtualización y evitando el conocido "temor al cambio", administrar una red virtual es más sencillo que administrar una red regular.

Breve historia de la virtualización

Durante la década de los 60 los equipos de informática de muchas empresas y entidades tenían un problema similar: contaban con super-computadoras o "mainframes" de alto rendimiento que deseaban "particionar lógicamente", o utilizar para múltiples tareas simultaneas (lo que hoy conocemos como "multitasking", trabajar más de una aplicación o proceso simultáneamente). Es por esto que IBM desarrolló un método para crear múltiples "particiones lógicas" (similar a lo que conocemos hoy como "maquinas virtuales") las cuales trabajaban independientemente una de las otras, y cada una utilizando los recursos provistos por el "mainframe".

Ya para la década de los 80 y con la llegada de las relativamente económicas maquinas x86, comenzó una nueva era de micro computadoras, aplicaciones cliente-servidor, y "computación distribuida"; en donde los enormes y potentes "mainframes" con mil y una tareas y utilidades en una sola caja gigantesca se comenzaron a cambiar por relativamente pequeños servidores y computadoras personales de arquitectura x86, con "una caja diferente para cada uso", lo que se convirtió rápidamente en el estándar de la industria.

Debido a esto, una vez más, el tema de la virtualización vuelve a quedar prácticamente en el olvido y no es hasta finales de la década de los 90 que gracias al alto desarrollo del hardware volvemos a caer en un predicamento similar al que estábamos en los años 60: el hardware existente es altamente eficiente, y utilizar cada "caja" para una sola aplicación seria un desperdicio de recursos, espacio, energía y dinero; y tampoco es conveniente asignarle múltiples usos o instalar varias aplicaciones en un solo servidor convencional, por más de una razón (ej. estas aplicaciones podrían ser conflictivas entre sí, o podrían requerir diferentes configuraciones e inclusive diferentes sistemas operativos, o tener diferentes requerimientos de seguridad, entre otras variables que podrían causar problemas al ejecutar estas funciones simultáneamente). Es por esto que vuelve a resurgir la idea de dividir el hardware, de manera tal que funcione como múltiples servidores independientes pero compartiendo los recursos de un mismo servidor físico. Y es de aquí que nace lo que hoy todos conocemos como "Virtualización".

Actualmente existen diferentes compañías que se dedican al desarrollo de aplicaciones y soluciones de virtualización.

2.1.2 DESCRIPCIÓN DEL SERVICIO

El servicio Hosting Virtual suministra infraestructuras como servicio (IaaS), no sólo servidores sino almacenamiento, red, seguridad,… El objetivo es llegar a virtualizar la capa de infraestructuras de servicios de Tecnologías de la Información (TI) en su totalidad confiando en la fiabilidad, flexibilidad, seguridad y eficiencia en costes que presenta el servicio.

El servicio se basa en el concepto de virtualización por el que la infraestructura base del servicio es consumida por los clientes bajo un paradigma de dedicación de recursos, seguridad garantizada y escalabilidad ilimitada

La figura 1 representa gráficamente el esquema de aprovechamiento de los recursos de un cluster de servidores virtuales frente a un servidor físico.

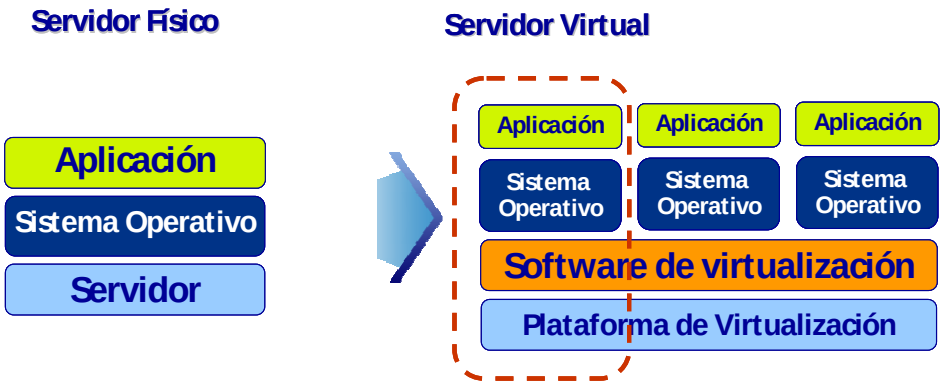


Figura 1: Servidor físico vs servidor virtual

La finalidad del servicio es suministrar al cliente todas las piezas para que pueda desplegar su propia infraestructura ajustada en todo momento a sus necesidades como se puede apreciar en la figura 2.

Figura 2: Infraestructuras basadas en servidores virtuales

Asociado a los componentes centrales del servicio, los servidores virtuales, se muestra un extenso abanico de componentes adicionales para facilitar al cliente la elección de todas y cada una de las piezas que intervienen en su entorno operativo (figura 3).

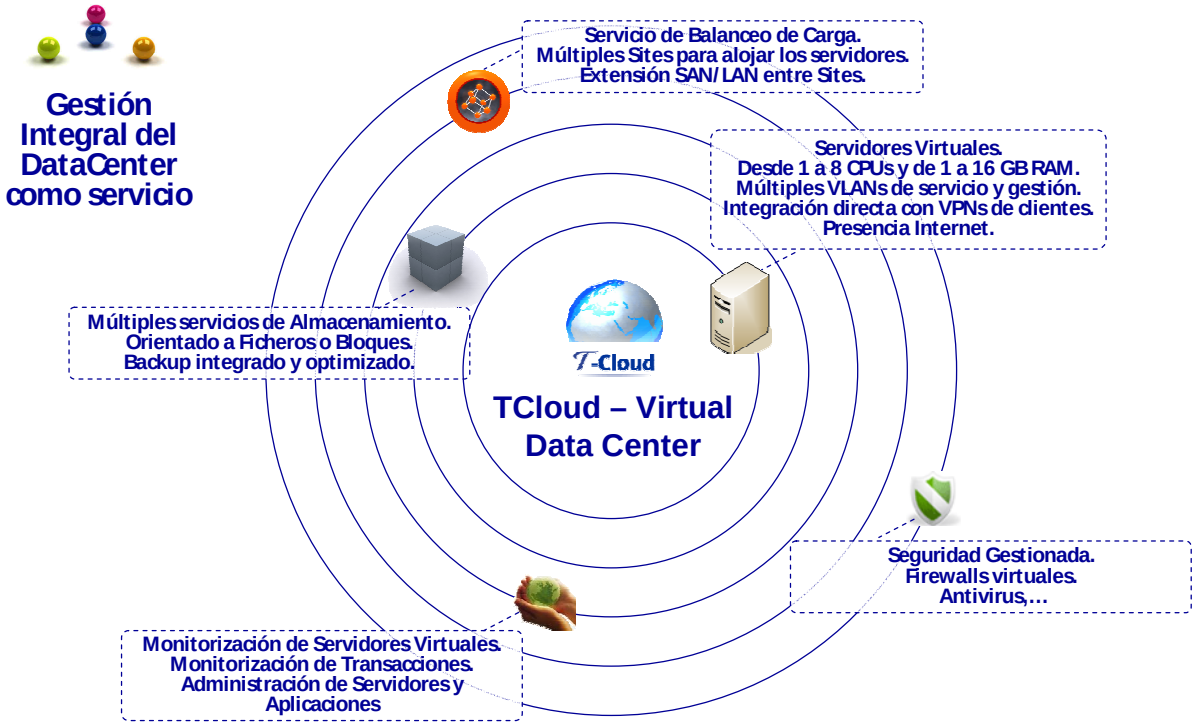


Figura 3: Servicios complementarios Hosting Virtual

2.1.3 VENTAJAS DEL SERVICIO

Las principales ventajas de este tipo de servicios son:

- Ahorro de costes. Este es sin duda una de los grandes valores del servicio y se muestra representado en muchos aspectos altamente valorados por nuestros clientes [3]:
  - Evitar inversiones al optar por un modelo de servicio basado en pago por uso o gasto (opex).
  - Ahorros de costes significativos frente a soluciones basadas en elementos dedicados apalancándonos en nuestras capacidades y economías de escala que trasladamos de forma directa a nuestros clientes.
  - Ajustar el coste a las necesidades puntuales del negocio. Total flexibilidad para el crecimiento de recursos TI ante picos de carga de trabajo o incluso a la inversa, reducción flexible de los recursos contratados para ajustarse a periodos de menor intensidad de trabajo, sin penalizaciones.
  - Servicio totalmente modular en el que el cliente va eligiendo las piezas que necesite para cada periodo de tiempo o funcionalidad concreta de la infraestructura que requiera desplegar.

- Evitar el sobredimensionamiento de plataformas al poder crecer de forma flexible y sin impacto en el negocio.
- Permite a los clientes mantener el rigor y un férreo control financiero de sus servicios sabiendo en todo momento el origen de los costes y el impacto en su negocio.

- Agilidad. Los tiempos de provisión se reducen prácticamente a minutos facilitando al cliente una rápida respuesta a sus necesidades de soporte al negocio. El cliente podrá realizar todas las tareas de provisión de forma totalmente autónoma a través de un portal de auto provisión.

- Calidad de Servicio Garantizada. Telefónica gestiona de extremo a extremo el servicio prestado al cliente final, incluyendo comunicaciones y servicios TI. Esta gestión unificada TI+C (Tecnología de la Información + Comunicaciones) brinda a los clientes las garantías de servicio más elevadas del mercado.

- El cliente se acostumbra a consumir este tipo de servicios bajo una ilusión de capacidad infinita y enteramente al alcance de su mano.

- Un profundo conocimiento de los servicios y problemática de nuestros clientes. Hemos aprendido de las referencias ya consolidadas, poniendo foco en la industrialización y el empaquetamiento de soluciones integrales.

- Eliminación de activos y los problemas de su gestión, amortizaciones, valores residuales, desmantelamientos cumpliendo normativas de seguridad y calidad medioambiental, …

- Acceso a recursos y niveles de especialización tecnológica. Asesoramiento continuo.

En resumen, “Cloud Computing” es para Telefónica la apuesta por ser un operador integrado de TI+C. Es un entorno con amplia experiencia en el que las economías de escala, la calidad de servicio y las comunicaciones integradas con servicios TI son las claves diferenciadoras.

El Cloud Computing permite recuperar la esencia de cada empresa y dedicarse realmente a su razón de ser y no a los problemas ligados a las TIC.

2.1.4 COMPONENTES DEL SERVICIO

La unidad básica del servicio es el Servidor Virtual. Para cada Servidor Virtual contratado, los siguientes componentes se encuentran incluidos en el servicio, configurables para adaptarse a las necesidades del cliente:

- CPUs virtuales.
- Memoria RAM.
- Almacenamiento en disco.
- Interfaces de red virtuales.
- Sistema Operativo.

Otras facilidades incluidas por defecto:

- Servidores en HA (alta disponibilidad). Recuperación menor de 15 minutos en caso de caída del servidor físico.
- Soporte en horario de 24x7 en el CDG.
- Panel de Control: Interfaz web a través de la cual es posible realizar solicitudes de operaciones básicas, cambios así como disponer de diversa información relacionada con el servicio

Adicionalmente, es posible contratar **funcionalidades opcionales** que mejoran la solución y valor añadido del servicio contratado, son:

- Direccionamiento IP
- Funcionalidad de Respaldo de la Información (Backup).
- Funcionalidad de Almacenamiento.
- Funcionalidad de Monitorización.
- Funcionalidad de Administración.
- Funcionalidad de Balanceo de Carga.

Todos los componentes se detallan en los apartados siguientes.

2.1.4.1 DETALLE DE COMPONENTES

SERVIDORES VIRTUALES

La parte central del servicio lo conforman los servidores virtuales fácilmente seleccionables, siendo posible cualquier combinación de procesadores desde 1 hasta 8 y memorias RAM desde 1 Gb hasta 16 Gb.

La vCPU equivale a cada uno de los cores de una CPU física entre 2GHz y 2,8GHz. Debido a las herramientas de virtualización y la selección de microprocesadores de última generación el rendimiento de una vCPU llega a superar a las CPUs físicas [4].

En fase de funcionamiento, el software de virtualización asigna de forma dinámica la memoria física del servidor físico a los servidores virtuales en función de las necesidades de memoria de cada uno, hasta el máximo de memoria configurado en el servidor virtual.

En el caso de que se desee modificar el número de CPUs o GB RAM asignado a un servidor, basta con un cambio de configuración y, en ocasiones, no es necesario tan siquiera un reinicio del servidor virtual.

Limitaciones de uso.

Por defecto los servidores virtuales no podrán tener asociados componentes físicos en modo dedicado (tarjetas X25, tarjeta directa a nodo macrolan, discos RDM físico,…). Sin embargo casi la totalidad de las necesidades pueden suplirse con mecanismos alternativos.

En el servicio de Hosting Virtual no se define de forma estándar dispositivos removibles (CD-ROM, floppy, etc.) en los servidores virtuales. Sólo durante el proceso de instalación del servidor, se podrán configurar temporalmente CD-ROM virtuales asociados a imágenes ISO.

Estas imágenes ISO deberán estar disponibles a través de la red de almacenamiento SAN (Storage Area Network), bien en un espacio contratado de cliente, o bien en un espacio de almacenamiento del servicio de Hosting Virtual NG donde podrá ser ubicada la imagen ISO del cliente para tal fin, siendo eliminada una vez realizada la instalación y desconfigurado el CD-ROM virtual.

En cualquier caso, si el cliente tiene que realizar la instalación de software en el servidor, el procedimiento recomendado es que proceda a volcar vía red (p.ej. mediante una carpeta compartida) la información en el servidor, y desde el mismo se ejecuten los paquetes de instalación.

SERVIDORES EN HA. RECUPERACIÓN ANTE CAÍDAS DEL SERVIDOR FÍSICO.

La plataforma de virtualización está organizada en cluster de servidores físicos con redundancia al menos de n+1. Esto permite que en caso de caída de un servidor físico, exista siempre capacidad ociosa para absorber los servidores virtuales que se ejecutaban en el servidor caído. Esta redundancia siempre es local, dentro del mismo CDG.

A través del proceso de Gestión de la Capacidad se garantiza que la plataforma puede en todo momento asumir la caída de un servidor físico y la migración de sus servidores virtuales sin degradación de rendimiento en el resto de servidores virtuales de la plataforma.

Los servidores virtuales “alojados” en el servidor físico afectado podrán restablecerse de forma casi inmediata, minutos, dependiendo del volumen de recursos que gestionen (CPU, memoria, almacenamiento,…).

INTERFACES VIRTUALES

El software de virtualización permite definir dentro de cada servidor físico interfaces virtuales a los que se conectan los distintos servidores virtuales.

Por cada servidor virtual, se definen de forma estándar dos interfaces virtuales incluidos por defecto. Uno de estos interfaces se asocia a la red de servicio, y el segundo a la red de gestión del CDG. Para el mapeo de los interfaces virtuales sobre las conexiones Gigabite Ethernet (GbE) de los servidores físicos, cada interfaz irá asociado a una VLAN (Virtual-LAN) distinta y específica del cliente en el ámbito de direccionamiento del CDG.

Los interfaces virtuales de cliente son definidos en todos los servidores físicos de la plataforma de virtualización, con objeto de permitir el funcionamiento de los servidores virtuales en cualquier servidor físico de la plataforma.

COMUNICACIONES LAN

Las conexiones de los CDGs a Internet garantizan la seguridad, disponibilidad y velocidad de los servicios prestados. El CDG da conectividad a estas redes de alta disponibilidad mediante un anillo de fibra diversificado y desde dos nodos de red redundantes, presentando de esta forma el suficiente nivel de redundancia de forma que no es necesaria la contratación de líneas de backup con otros operadores.

En el diseño de la infraestructura LAN del CDG existe una red independiente de la de servicio para realizar tareas de administración de los servidores, monitorización y backup, junto con una tercera red independiente para la plataforma de almacenamiento. Este hecho separa las redes permitiendo aumentar el tráfico, la seguridad de los servicios prestados y el rendimiento esperado, viéndose fortalecido mediante el aislamiento de las redes de los clientes en distintas VLANs.

ACCESO INTERNET

Los CDGs en los que se alojaran los equipos, que son propiedad de la empresa Telefónica Soluciones, disponen de excelentes infraestructuras de comunicación que unidos a una gran experiencia en gestión de infraestructuras, permiten ofrecer servicios de alta calidad y disponibilidad. Entre otras, e incluyendo las certificaciones de los centros de datos, algunas capacidades de comunicaciones son:

- Anchos de banda disponibles:
  - 40GB en Tres Cantos
  - 40GB en Julián Camarillo
  - 5GB en Terrasa

- Otros elementos de comunicaciones gestionados:
  - +140 switches
  - +75 balanceadores
  - +270 Firewalls
  - +17.600 puertos (puertos LAN de cobre y fibra)

Todo ello convierte a los Centros de Datos Gestionados en un punto central de las comunicaciones de los clientes. En la actualidad hay más de 90 bastidores de Comunicaciones WAN/MAN de clientes alojados en los diferentes CDGs proporcionando servicios avanzados de Comunicaciones, adicionalmente a la conectividad a Internet que se proporciona desde los CDGs.

Telefónica puede proporcionar los servicios de DNS (Domain Name Server) primario o secundario con Internet siempre que se contrate el servicio de conectividad a Internet. La asignación del direccionamiento dentro del CDG será realizada por nuestros empleados.

Opcionalmente, se puede contratar salida a Internet bajo Firewall compartido con un caudal mínimo de 1Mpbs. En caso que el caudal contratado supere los 10 Mbps, se deberá contratar un Firewall en modalidad de uso dedicado para poder absorber todo el tráfico generado.

DIRECCIONAMIENTO IP

El cliente podrá contratar direcciones IP públicas, usar direccionamiento privado del CDG o de su red interna (solventando solapamientos si fuera necesario) o utilizar direccionamiento independiente de proveedor PI (si técnicamente se puede direccionar el segmento correspondiente de forma correcta).

La asignación de direccionamiento IP en este caso, es la misma que en el caso del servicio de Hosting físico.

Además, se le podrán proporcionar al cliente direcciones privadas compatibles con el direccionamiento del CDG.

SISTEMA OPERATIVO

El servicio Hosting Virtual facilita un catálogo de plantillas para la rápida implantación de imágenes de servidores virtual ya pre configurados. Los sistemas operativos (SO en adelante) incluidos son:

- Windows NT, 95, 98, 2000, Server 2003, 2008
- Linux Red Hat
- Linux SuSE

En este caso se entregará un servidor virgen (Blank Server) y el cliente deberá instalarse el SO. En caso de que el cliente solicite que sea Telefónica quien instale el SO se realizará la valoración económica oportuna.

Las licencias del SO por defecto serán suministradas por el cliente. Ahora bien, debido a las condiciones especiales de licenciamiento de del SO Windows Server Datacenter, existe un pack especial en el que este SO se proporciona con el servidor virtual.

Las licencias de SO puestas a disposición de los clientes son las siguientes:

- Windows Server 2003 R2 Standard
- Windows Server 2003 R2 Enterprise (para entornos autenticados)
- Windows Server 2008 R1 Standard
- Windows Server 2008 R1 Enterprise (para entornos autenticados)

Los servidores virtuales se suministran por defecto con un sistema operativo preinstalado.

El sistema operativo se instala desde un conjunto de plantillas tipo que pueden incluir exclusivamente el S.O. y las VMWare Tools o incluso agentes necesarios para la prestación de servicios adicionalmente contratados como pueden ser la monitorización y el backup.

Dentro de los procedimientos operativos se va a incluir la actualización periódica y publicación de un documento con las versiones de S.O. con plantillas creadas y las características de éstas. Por defecto existirán plantillas para la mayor parte de los Sistemas Operativos (S.O.) comercialmente más difundidos (y sus 'releases' oportunas). En caso de no existir plantilla para alguno de estos S.O. (extendido comercialmente) se generará en fase de provisión por el Centro de Competencia Tecnológica de Virtualización (previa aceptación en fase de oferta del gestor de producto y responsable del servicio en Explotación) y pasará a ser parte de la biblioteca de plantillas.

El S.O. se instala en las unidades de sistema por defecto ("C:" para entornos Windows, "/" para entornos linux,…) creando una partición o file system de un tamaño determinado dependiendo del S.O. y agentes empaquetados (24 GB,…).

Una vez instalado, el administrador del S.O. podrá acceder al mismo ya sea desde consola o a través de los mecanismos de administración típicos (terminal server, SSH,…) y configurar el resto de espacio de disco inicialmente en bruto y sin asignar como unidades o filesystems adicionales, aplicable tanto a el espacio incluido con el servidor virtual como el almacenamiento adicional. Los mecanismos para ello serán los estándares dependiendo del S.O., "Disk Management" en Windows, "mkfs/fdisk" en linux, etc.

El cliente puede hacer estas gestiones en remoto pero si lo prefiere, a efectos operativos, puede acceder a la sala de clientes del CDG, con conectividad con el resto de CDGs. Esta opción puede ser recomendada para la carga de ISOs específicas del cliente o carga masiva de contenidos ya que en remoto (Internet/VPN) podría llevarle un tiempo elevado.

Limitaciones de uso.

Se podrá instalar SO compatibles con VSphere 4 de acuerdo con la matriz de compatibilidad de disponible en su web [5].

SERVIDORES DE PROPÓSITO ESPECÍFICO (VAPPS)

Las VApps son servidores virtuales (1 ó varios) pre-empaquetados de propósito específico, aplicaciones “enlatadas de serie (miniS.O.+Aplicación)” en servidores virtuales [6].

El tratamiento de estos componentes difiere según la finalidad del servicio:

- vApps en modo Gestionado. El servicio incluye:
    - Procedimiento para la importación de VAppliances certificadas por VMWare. Las no certificadas no podrán ser implantadas en el servicio.
    - Existe un mercado libre de VApps con o sin licencias, certificadas o no con VMWare,… Muy orientadas a disponibilidad de servicios.
    - Sin monitorización.

- Sin backup.
- Modelo de Precios.
  - Alta por instalación de VApps soportadas.
  - Los recursos que consuma las VApps deberán contratarse como servidores virtuales básicos encajándolo en las características correspondientes del servicio. Ej. un VApp que despliega 2 VMs (Virtual Machines) de 1,2 cores y 512 MB RAM se traduce en la contratación de 2 SVB de 2 cores y 1 GB RAM, al no existir configuraciones de prestaciones inferiores. Así mismo aplicará el tamaño de disco: en principio 50 GB por defecto y ampliaciones de disco en caso necesario.

- vApps administrados

  - Tomando como base la definición de vApps en modo Gestionado se incluirá la administración de SO y aplicativos correspondientes atendiendo a:

    - Se tratarán vía Desarrollo de Servicios. En este alcance inicial tan sólo se incluye la administración de un servicio de balanceo de carga basado en ZXTM LB, enlatado como un vApp se ha incluido dentro del desarrollo de un servicio de Balanceo (recogido en este mismo Manual de Marketing).

    - En caso de que el cliente traiga un VApp y desee que Telefónica lo administre se tratará como un proyecto a medida y se designará el Centro de Competencia correspondiente para su administración.

Sólo se podrán alojar vApps soportadas en VMWare vSphere y con VMWare Tools.

SERVIDORES ON/OFF.

El servicio de Hosting Virtual podrá tener servidores arrancados o parados, sin distinción de costes operativos.

Si el cliente desea parar sus servidores durante periodos largos (más de 1 mes natural) el servicio incluye la posibilidad mediante solicitudes de servicio de crear una imagen de ese servidor y almacenarlo en disco de bajo coste (Almacenamiento orientado a ficheros – Gama Silver) para posteriormente restaurarlo de forma rápida. Para periodos prolongados el servidor virtual no será objeto de facturación pero si las solicitudes realizadas sobre él y el almacenamiento que ocupe su imagen.

Limitaciones de uso.

El cliente deberá notificar adecuadamente la parada de las máquinas con una antelación de al menos 24h (preferentemente 48h), en caso contrario, no aplicarán los acuerdos de nivel que se vean afectados por dicha parada realizada sin previo aviso.

MONITORIZACIÓN

MONITORIZACIÓN DE ALARMAS Y RENDIMIENTO SERVIDORES VIRTUALES

Los servidores virtuales podrán incluir opcionalmente la monitorización de sistemas y de rendimiento – Monitorización:

- Contratación de monitorización de sistemas y rendimiento empaquetado sin poder solicitar la contratación por separado.
- Preconfigurado en las plantillas de distribución con el SO lo que simplifica la puesta en marcha de los agentes y los servicios.

Monitorización de Alarmas

Este componente permite la monitorización de los sistemas o servidores, tanto hardware como Sistema Operativo. Para la monitorización de sistemas es necesaria la instalación y configuración en la máquina del cliente del agente SNMP (Simple Network Management Protocol) estándar de sistema operativo y un agente específico de gestión.

Estos agentes permiten recoger gran cantidad de información de los equipos y servidores, tales como: Variables y traps SNMP, ficheros de log de sistemas, scripts o aplicaciones del entorno, realizando un refresco en la monitorización cada 5 minutos. Los agentes de monitorización suman funcionalidades adicionales gracias al resto de componentes de la suite HP Openview, así como otros desarrollos propios para la monitorización.

Las alarmas se representan mediante el código de colores representado en la figura 4.

	Alarma Crítica.
	Alarma de aviso Importante.
	Alarma de aviso Menor.
	Alarma de aviso de Información.
	Sin Alarmas.

Figura 4: Monitorización de alarmas

El detalle de las alarmas producidas podrá consultarse en el módulo Alarmas que en todo momento está sincronizado con el módulo Vista de Servicio. Se puede ver un ejemplo en la figura 5.

Figura 5: Detalle en la monitorización de alarmas

Cualquier alarma que se produzca en alguno de los objetos monitorizados y representados en el nivel más bajo se propaga por el árbol de servicio hacia arriba reflejando el estado de los objetos, servidores, servicios o el propio identificador asociado al cliente.

Las alarmas estándar configuradas son las siguientes:

- Ocupación de discos o sistemas de ficheros.
- Estado de los discos.
- Estado de las tarjetas de red.
- Estado de los servicios y procesos.
- Vigilancia de logs y eventos del sistema.
- Existencia de ficheros vitales.
- Crecimiento ilimitado de ficheros de logs.
- Alarmas de seguridad (log, eventos 'Security', etc.).
- Vigilancia del estado del cluster.

Conjuntamente a las alarmas se muestra una visión de servicio que permite al cliente conocer de un vistazo el estado del servicio y las máquinas con problemas. Esta vista de servicio se construye formando un árbol invertido (figura 6) en el que la raíz es el propio cliente y cada una de las ramas son los servicios gestionados que ha contratado con Telefónica. Las hojas son cada uno de los objetos que se están monitorizando de cada máquina (sistema de ficheros, procesos, ficheros de logs, etc.).

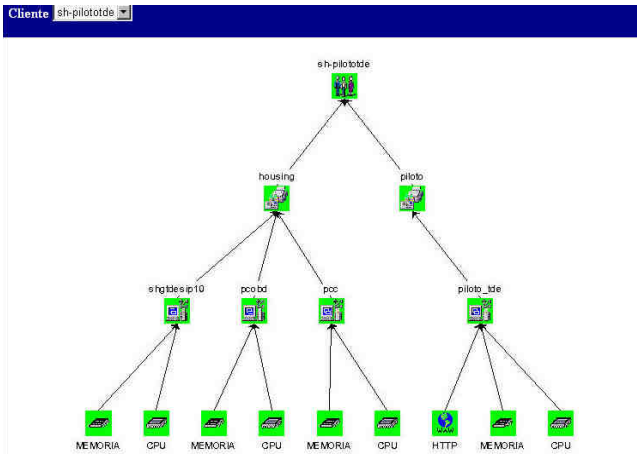


Figura 6: Visión de servicio

Los eventos detectados serán notificados a los grupos de Operación 24x7 pudiendo, si así se ha especificado, tener asociados acciones correctivas básicas. También puede asociarse al evento una notificación e-mail para su gestión por el grupo de administradores del servicio.

Monitorización de Rendimiento

La gestión de rendimiento es quizá el concepto más importante para alcanzar el éxito en la gestión proactiva de los sistemas. La gran mayoría de las situaciones anómalas en un sistema podrían evitarse realizando una correcta y eficiente gestión de rendimiento.

Actualmente, las aplicaciones Internet son cada vez más potentes y consumen más recursos del sistema, siendo frecuente detectar que un servidor web o de correo se han quedado “colgados” por no poder consumir más recursos. Un estudio a posteriori del rendimiento muestra como el sistema ha ido degradando su rendimiento hasta dejar inoperativas algunas funciones y aplicaciones.

Esta modalidad permite que los clientes obtengan una serie de informes sumamente detallados del rendimiento de sus sistemas. Analizando estos informes se identifican cuellos de botella y tendencias de los sistemas, permitiendo así tomar acciones para la mejora del rendimiento de la plataforma empleada de forma proactiva.

Es requisito para la contratación de esta monitorización la contratación también de la monitorización de sistemas de alarmas.

MONITORIZACIÓN DE SERVICIOS INTERNET Y TRANSACCIONES

Al contrario que el resto de las monitorizaciones anteriormente descritas esta monitorización es no intrusiva, es decir, no se utiliza un agente interno a los sistemas de los clientes sino que toda la monitorización se realiza desde el exterior. Se trata de una simulación de tráfico real para comprobar el funcionamiento de los servicios. Esta simulación puede ser básica (acceso a una IP y puerto) o más avanzada (simulación de transacciones).

A continuación se detallan ambos tipos de monitorizaciones, pudiendo ser contratadas indistintamente:

Modalidad de protocolos.

Se emplea para comprobar la disponibilidad y tiempo de respuesta de los servicios que se prestan en una máquina desde un servidor externo en el que se localiza la herramienta de monitorización. Para ser posible este tipo de monitorización es preciso que los servidores tengan presencia en Internet.

Los protocolos monitorizables son todos los protocolos Internet, incluyendo los siguientes servicios:

- Suministro, instalación y configuración del servicio
- Monitorización 24 x 7, con chequeos periódicos en intervalos de 5 minutos.
- Notificación según los mecanismos acordados con el cliente en el "Protocolo de Mantenimiento" de situaciones de indisponibilidad o superación de umbrales en tiempos de respuesta.

Los protocolos con monitorización estándar son, incluyendo los siguientes servicios, los reflejados en la Tabla 1:

Puerto		*Descripción*
DHCP	Dynamic Host Configuration Protocol	Verifica que el servidor DHCP acepta peticiones para ello asigna una dirección IP dinámica y mide el tiempo total hasta que le servidore DHCP devuelve la dirección IP.
DNS	Domain Name Service	Verifica que el servidor DNS acepta peticiones Para ello se comprueba la confirmación de una dirección para un domino especifico y se mide el tiempo total de respuesta para resolver el host name o la dirección IP.
FTP	File Transfer Protocol	Verifica que el servidor de FTP acepta peticiones , para ello se realiza una conexión FTP se comprueba la autenticación y se confirma la recuperación de un fichero.
HTTP	HyperText Transfer Protocol (web pages on TCP port 80)	Verifica la disponibilidad y el tiempo de acceso a una determinada URL, el objeto es asegurar la disponibilidad de las páginas Web de un site , para ello se emula una petición HTTP.
HTTPS	HyperText Transfer Protocol Secure (SSL-based web pages on TCP port 443)	Verifica la disponibilidad y el tiempo de acceso a una URL determinada. El objeto es comprobar la disponibilidad de las páginas Web de un site emulando una petición HTTPS.
IMAP4	Internet Message Access Protocol	Verifica que el servidor IMAP4 funciona correctamente , para ello se estudia el recorrido y la descarga de un mensaje desde el servidor.
LDAP	Lightweight Directory Access Protocol	Verifica que el servidor LDAP funciona correctamente , para ello se establece una conexión con éste, se ejecuta una autenticación "simple"y se mide el tiempo empleado en la conexión al servidor LDAP.
NNTP	Network News Transfer Protocol	Verifica que el servidor de noticias NNTP está funcionando correctamente, para ello se establece una conexión a éste y se comprueba si los titulares de las noticias y los artículos pueden ser descargados.
POP3	Post Office Protocol	Verifica que el servidor POP3 funciona correctamente para ello se estudia el recorrido y la descarga de un email desde el servidor.
RADIUS	Remote Authentication Dial In User Service	Verifica que el servidor RADIUS está trabajando adecuadamente, para ello se envía una petición autentioada al servidor RADIUS y se mide el tiempo de respuesta.
SMTP	Simple Mail Transfer Protocol	Verifica que se el servidor de mail acepta peticiones y confirma que los mensajes pueden ser enviados , para ello se testea complatamente la función e-mail , enviando un mensaje al servidor, estudiando su recorrido y descargándolo de nuevo .
ICMP	Internet Control Message Protocol	Mide la disponibilidad de cualquier dispositivo IP.

Tabla 1: Protocolos con monitorización estándar en HV

Esta modalidad de monitorización ofrece una visualización de la disponibilidad del servicio según los intervalos que se elijan, horas o días. En la figura 7 se muestran diferentes ejemplos.

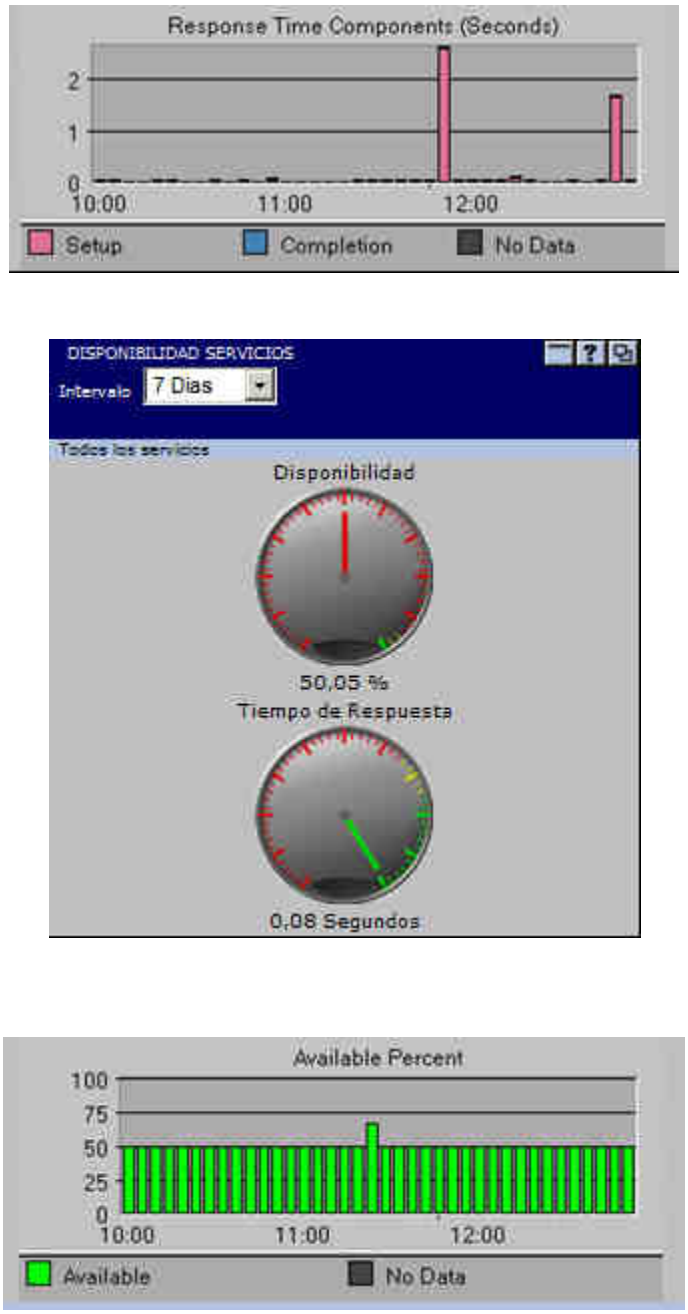


Figura 7: Monitorización disponibilidad del servicio

Adicionalmente, esta modalidad de monitorización ofrece la posibilidad de vigilar periódicamente por IP y puertos genéricos. Esta opción es muy útil para desarrollos a medida del cliente que utilizan puertos no estándares.

Modalidad de transacciones

Esta modalidad de monitorización permite:

- Verificar que un Servidor Web y sus procesos asociados se están ejecutando correctamente.
- Verificar la disponibilidad y los tiempos de acceso a URLs específicas para asegurarse de que las páginas web están disponibles para los usuarios en un intervalo de tiempo razonable.
- Verificar que las múltiples actividades asociadas a una transacción on-line son completadas satisfactoriamente.
- Simular la sesión de un usuario a través de distintas páginas web.

Funcionalmente, esta monitorización es una simulación de las transacciones a ser monitorizadas en la que se pretende simular el comportamiento más típico de un navegante o usuario que accede al servicio desde Internet. De esta forma, cuando se detecte un fallo de disponibilidad en uno de los chequeos, además de mostrarlo gráficamente, se generará una alarma que notificará el fallo en la operación realizada.

Las alarmas que se produzcan estarán configuradas con correlación de eventos, es decir, la llegada de una notificación de vuelta al estado normal del chequeo realizará de forma automática un borrado de las alarmas anteriores.

SERVICIO RESPALDO DE LA INFORMACIÓN

El servicio estándar de Backup Centralizado del CDG permite realizar backup y sus correspondientes restores de la información alojada en los Servidores Virtuales en plataformas compartidas de almacenamiento, a través de la red interna desplegada en nuestro CDG, como se muestra en la figura 8.

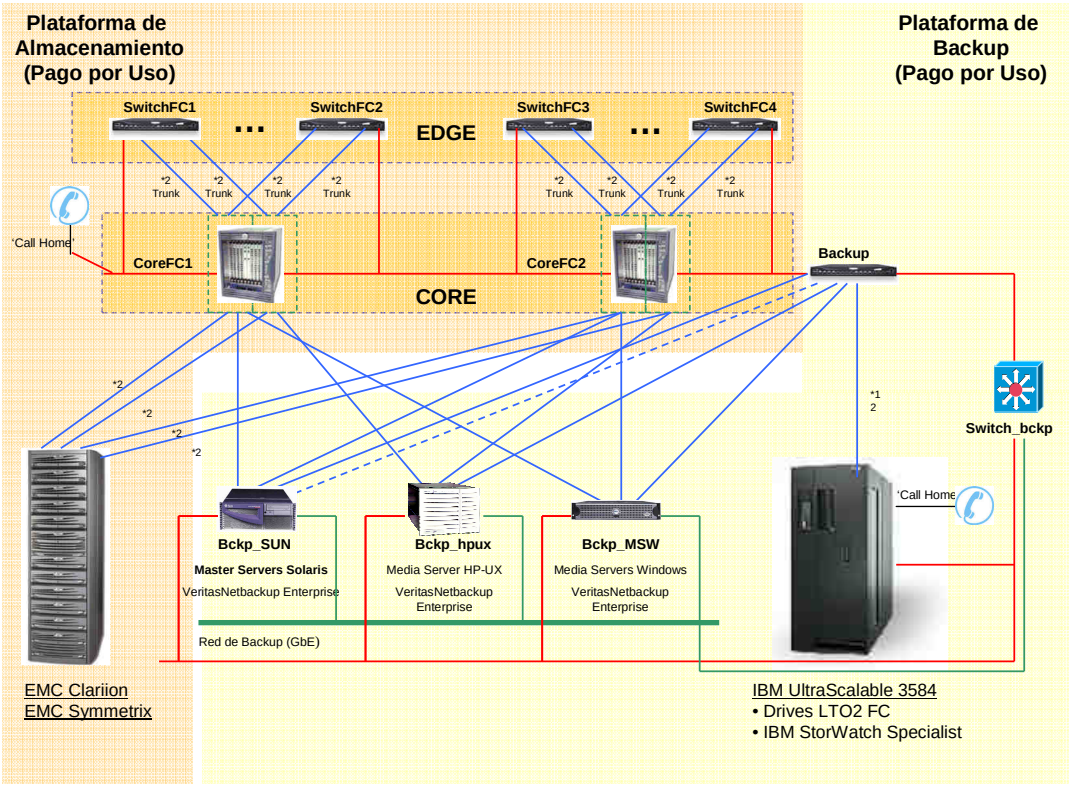


Figura 8: Esquema plataforma backup y almacenamiento compartido

La plataforma de backup está basada en:

- Software de backup de Veritas, Veritas NetBackup.
- Servidores de Backup (Media server, SAN server,...) para todas las tecnologías.
- Robótica de IBM (IBM Ultrascalable 3584 o similar).
- Soportes magnéticos: LTO-X (200/400 GB).

Los requisitos mínimos necesarios para poder realizar backup de un equipo son los siguientes:

- Direcciones IP: el direccionamiento debe ser del rango asignado por Telefónica.
- Requiere la instalación de agentes dentro de los equipos. Telefónica es responsable de instalar y mantener los agentes de backup en los servidores del cliente.
- Compatibilidad del software de los equipos del cliente, especialmente por el tipo y versión del Sistema Operativo, con el sistema de backup del CDG.
- Una interfaz virtual asignada a tal efecto en el servidor del que se quiera realizar Backup.

Las actuaciones contempladas dentro de este servicio son las siguientes:

- Administración de los servidores de Backup.

- Operación y vigilancia de la correcta ejecución del Backup.
- Implementación de las políticas de backup y la rotación de cintas.
- Instalación y mantenimiento de los agentes de backup en los servidores del cliente.
- Provisión del Portal de Cliente o link a "Backup Reporter", donde el cliente podrá:
    - Solicitar peticiones de backup o/y restore bajo demanda, así como modificaciones en la política de backup y especificaciones programadas.
    - Disponer de una serie de informes, en los que se muestra el detalle de información de cada backup o restore realizado, indicando la fecha de dicho informe y la cantidad de información transferida (en bytes)

Las políticas estándar definidas por Telefónica que podrán aplicarse son las reflejadas en la Tabla 2:

	Oro	**Plata**	**Bronce**
Backup Diario	Total. 30 días retención.	Incremental. 14 días retención.	Incremental. 7 días retención.
Backup Semanal	Total. 12 semanas retención.	Total. 8 semanas retención.	Total. 4 semanas retención.
Backup Mensual	Total. 12 meses retención.	Total. 8 meses retención.	Total. 4 meses retención.
Backup Anual	Total. 5 años retención.	Total. 1 años retención.	No aplica.

Tabla 2: Políticas de Backup en el servicio de HV

El cliente podrá:

- Solicitar una política de backup diferente de las previamente establecidas por Telefónica (Oro, Plata o Bronce) y se le aplicarán costes por almacenamiento de datos en la plataforma de backup y por transferencia.
- Variar la política de backup a otra definida por el cliente (diferente de las estándar de Telefónica) mediante una solicitud comercial.
- Solicitar restauración de datos (restores) aplicándosele en este caso los cargos correspondientes.
- Petición de desarrollo y/o adaptación de script de integración con aplicaciones de Negocio.

CONSIDERACIONES LOPD

El servicio Hosting Virtual está preparado para soportar un nivel BÁSICO de seguridad según la LOPD [7] y se tratará como proyectos los casos en los que la naturaleza de los datos requiera un tratamiento de seguridad mayor, añadiendo en este caso el cliente/responsable de la solución técnica del proyecto, los elementos necesarios para cubrir los requisitos adicionales de seguridad requeridos (ej. encriptación de datos, encriptación de comunicaciones, etc.).

Con respecto al Respaldo de Información, se contemplan las siguientes actuaciones conforme a lo dispuesto en la Ley Orgánica de Protección de Datos:

Para Datos de Carácter Personal, para todos los niveles (Bajo, Medio y Alto), se debe:

- El cliente tiene la obligación de guardar los logs de acceso a esos datos durante UN (1) año.
- Particularmente, no implica que la retención de los backups deba ser de un año, si no que se debe almacenar, de aquella forma considerada adecuada por el cliente (Ej. es posible guardar los logs en un directorio de su máquina), dichos accesos.
- Telefónica guardará los accesos realizados por el Servicio de Respaldo en la plataforma de Backup.
- Y para los datos de nivel Alto:
- El cliente tiene la obligación de guardar los logs de acceso a esos datos durante DOS (2) años.
- Particularmente, no implica que la retención de los backups deba ser de dos años, si no que se debe almacenar, de aquella forma adecuada considerada por el cliente (puede ser que guarde los logs en un directorio de su máquina), dichos accesos.
- Cifrar los backups.

ALMACENAMIENTO

Cada servidor virtual tendrá por defecto 50 GB de Almacenamiento Orientado a Bloques tipo Gold (SAN – Fiber Channel (FC) en RAID 5) a modo de disco de sistema. El almacenamiento no es accesible bajo ningún concepto por ningún otro servidor virtual provisionado en la plataforma de virtualización.

Este espacio de disco podrá ampliarse contratando GB adicionales.

La contratación de GB de almacenamiento a través del servicio de Hosting Virtual tendrá las siguientes ventajas sobre el almacenamiento “tradicional”:

- Ampliación de disco de sistema en caliente.
- No se requiere la contratación de HBAs (tarjetas Host Bus Adapter) ni puertos de la red SAN
- No se requiere la contratación de SW de multipathing (Powerpath).
- Precio optimizado para el cliente al aprovechar las economías de escala.

Adicional al disco de sistema el cliente podrá contratar todas las gamas de servicio de almacenamiento disponible en el centro donde reside la plataforma de servicio (en caso de duda solicitar comprobación de disponibilidad al gestor de servicio o gestor de la capacidad). Dentro del mismo servidor no podrán utilizarse a la vez las modalidades orientadas a bloques Gold y Silver, puesto que la funcionalidad de

vMotion no distinguiría entre ambas al mover una máquina virtual de un servidor físico a otro, dándole todo el almacenamiento del mismo tipo, por lo tanto si se desea almacenamiento por bloques Silver, los 50 GB de disco iniciales de la máquina también serán de esta modalidad.

A efectos de simplificación se contemplan las gamas de almacenamiento dentro del servicio Hosting Virtual vienen reflejadas en la tabla 3:

	Almacenamiento orientado a Bloques de Datos. *Óptimo para aplicaciones con requisitos importantes de latencia y rendmiento (BBDD, ERP, data warehousing, OLTP)*			***Almacenamiento orientado a Ficheros.*** *Información no estructurada. Bajo coste optimizando rendimiento.*	
	Gold	**Silver**	**Bronze**	**Gold**	**Silver**
Requisitos	High performance	Performance	Low cost	Shared resources	Shared resources
Tecnología de Acceso	Fibre Channel	Fibre Channel	Ethernet - iSCSI	Ethernet (NFS, CIFS)	Ethernet (NFS, CIFS)
Discos	FC RAID 5	SATA RAID 5	SATA RAID 6	FC RAID 5	SATA RAID 6
Modelo de costes	Initial fee + €/GB*month	Initial fee + €/GB*month	!!0.2€/GB¡¡	€/GB + €/filesystem	!!0.2€/GB¡¡ + €/filesystem
Capacidad Mínima Recomendada	200GB	200GB	500GB	200GB	500GB

Tabla 3: Gamas de almacenamiento en servicio HV

El servicio de HV (Hosting Virtual) permitirá la conectividad de servidores virtuales con cabinas de almacenamiento alternativas a las definidas por el servicio, ya sean compartidas o dedicadas para clientes siempre y cuando éstas sean gestionadas por Telefónica.

Limitaciones de uso.

Recomendamos que no se superen los 500 GB como configuración de disco de sistema para facilitar la acción de HA (Alta Disponibilidad) - migración de máquinas entre componentes HW (Tecnología VMotion).

Una vez puesto en marcha un servidor virtual, todas las solicitudes de ampliación de disco se llevarán a cabo mediante la inserción de nuevos volúmenes de disco en el S.O. (Ej. en Windows los nuevos volúmenes de disco se añadirán en unidades de disco –D:, E:, etc.- adicionales). Por lo tanto, las ampliaciones no se llevarán a cabo sobre volúmenes operativos ya configurados.

SNAPSHOTS Y CLONADOS

El Hosting Virtual proporciona una serie de mecanismos orientados a facilitar las labores de administración de los servidores virtuales. Estas funcionalidades aportan un valor diferencial a los entornos virtualizados frente a entornos más convencionales.

El término “snapshot” o “instantánea” se utiliza de forma extendida y confusa para diversos objetivos. En el caso de Hosting Virtual se recogen los siguientes:

- **CLONES. Snapshot de servidores virtuales en vivo o clonado de servidores**. Se tratará de una o gestión que copiará un servidor virtual creando una imagen idéntica salvo por los atributos propios: hostname y direccionamiento IP. La máquina nueva estará desde el inicio en funcionamiento.

- **IMÁGENES. Snapshot o imágenes de servidores virtuales** a modo de backup, repositorio de plantillas para facilitar el crecimiento horizontal, etc. La petición del cliente creará una imagen idéntica del servidor virtual y la guardará en su área de almacenamiento de "plantillas de cliente" (almacenamiento NAS – Gama Masiva). La imagen copiada permanecerá inactiva y, bajo petición del cliente, podrá ser aplicada sobre un servidor virtual que designe.

Limitaciones de uso:

Snapshot no incluidos en el servicio:

- Snapshot de Almacenamiento: el almacenamiento se congela y se van guardando los deltas para una posible marcha atrás consistente.
- Snapshot propietario de VMWare: el servidor virtual se congela y se van guardando los deltas para una posible marcha atrás consistente.

Con utilidad en algunas soluciones puntuales: backup on-line, pruebas de test para marcha atrás,... Tanto los proveedores como las pruebas del servicio indican múltiples problemas de gestión, rendimiento e incluso completa degradación de servicio. Puede ser reemplazada por otros mecanismos menos intrusivos. El servicio no incluye y desaconseja el uso de esta funcionalidad.

SERVICIO DE BALANCEO DE CARGA

Las compañías para las que el servicio web es crítico en su negocio, tales como portales de información, tiendas on-line, distribuidores y proveedores de contenido, necesitan asegurarse de que sus servicios son rápidos, fiables, seguros y fáciles de gestionar.

Históricamente esto ha requerido del uso de balanceadores de carga propietarios basados en hardware.

Pero gracias al rápido avance de la virtualización, ahora es posible virtualizar no sólo las capas de servidores físicos, sino también las capas de aceleración y balanceo de carga [8].

El servicio de Hosting Virtual ofrecen una solución completamente integrada y virtualizada de balanceo de carga y de gestión del tráfico de las aplicaciones como una alternativa más rentable al planteamiento tradicional de utilizar dispositivos hardware propietarios. Esta solución está basada en los estándares de la industria y utiliza tecnología probada del mercado de la que disfrutan a diario millones de usuarios web.

La solución está formada por un dispositivo virtual pre-configurado que se instala en minutos basado en tecnología de Zeus, ZXTM LB [9].

Junto a los beneficios que provee la virtualización en el entorno, entre los que están la reducción de espacio, ahorro de consumo energético y de refrigeración, el dispositivo virtual de Telefónica provee además:

- Un servicio completo de Balanceo de Carga totalmente integrado en la arquitectura del servicio Hosting Virtual que complementa tanto soluciones en Hosting Virtual como en servidores físicos (figura 9).

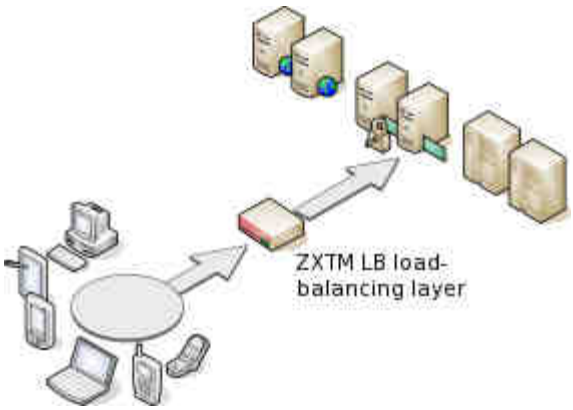


Figura 9: Balanceo de carga

- Es la alternativa natural a balanceadores físicos dedicados como F5 o Radware pero más eficiente en costes y prestaciones
- Rápido despliegue. Se trata de una VApp (ZXTM) ya preconfigurada a desplegar.
- Sin inversiones para el cliente.
- Basada en estándares de la industria que permite una gestión de la configuración simple e integrada con el servicio Hosting Virtual.
- Simplifica el mantenimiento y los tiempos de espera de reemplazo de HW en caso de avería.
- Escalado inmediato.

Funcionalidades:

- Alta disponibilidad de los servicios, incluso ante caídas de un servidor de aplicaciones/web o dispositivos de balanceo de carga.
- Escalabilidad inmediata de servidores web en el Back-End y servidores de aplicaciones.
- Mejora el rendimiento, fiabilidad y escalabilidad de las aplicaciones en red.
- Seguridad mejorada, incluyendo alta velocidad en el cifrado y descifrado de trafico SSL (Secure Socket Layer), liberando de esta carga a los servidores aplicaciones/web.
- Monitorización del rendimiento en tiempo real de los servidores del Back-End con la capacidad de priorizar el tráfico de más valor.
- Un motor de reglas y un potente algoritmo de balanceo de carga posibilita el enrutado óptimo a servidores destino. Subyacente a estos beneficios existe una potentísima maquina de generación de políticas que puede inspeccionar todo el trafico de aplicación, reescribiendo y ajustando el trafico al momento para optimizar el rendimiento y los servicios de los clientes on-line.

Los escenarios de uso que pueden desplegarse son los siguientes:

CASO 1 – MODO SIMPLE (Figura 10)

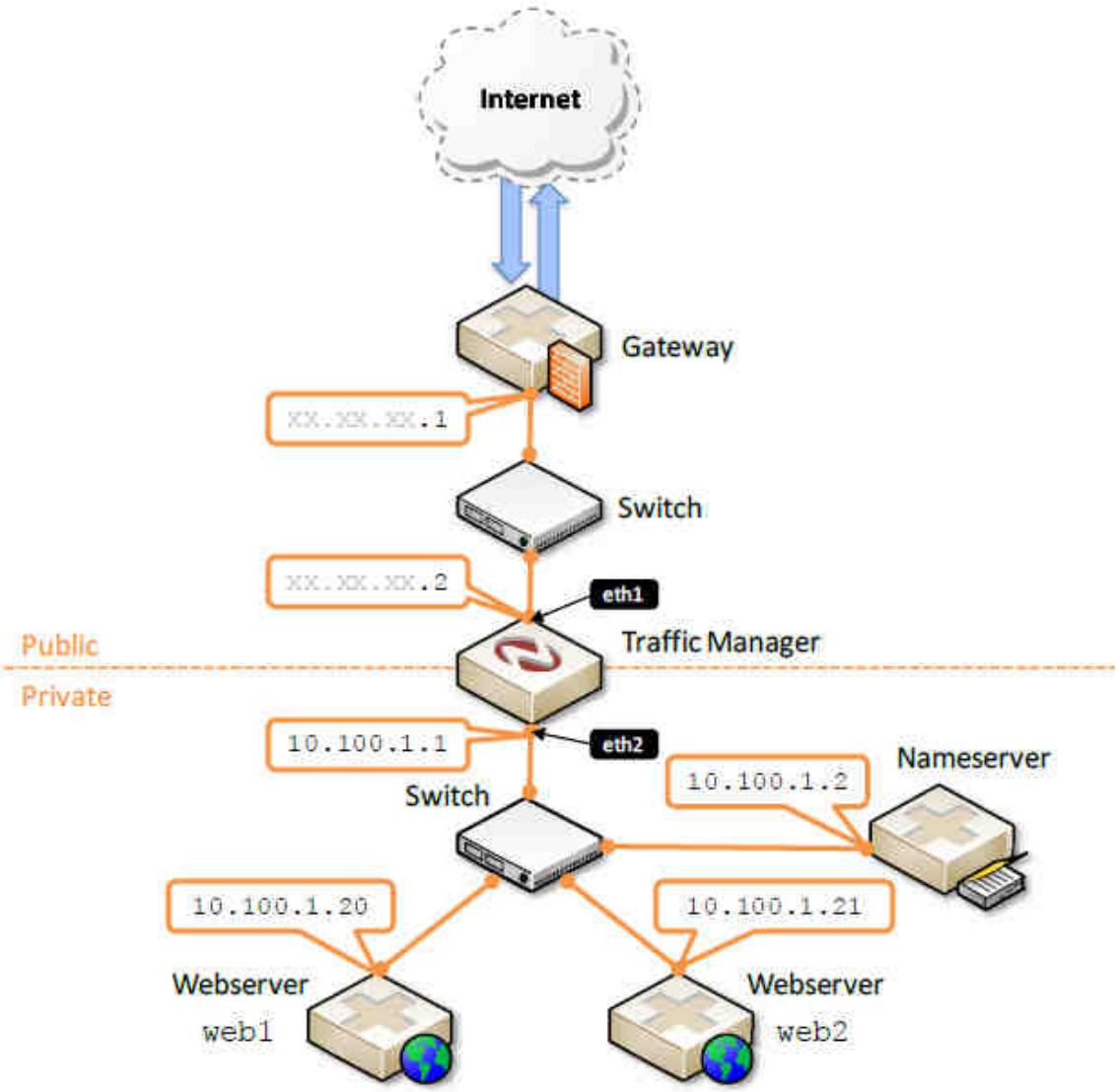


Figura 10: Balanceo de carga simple

En fase de provisión se definirán:

- Protocolos a balancear; todos sobre TCP [10] o UDP [11], salvo SSL que se describe en caso 3.
- Política de Balanceo: Round-Robin, Weighted round robin [12], Least connections, Weighted least connections [13].
- Tipos de chequeos a realizar (Health monitoring).
- Persistencia de sesiones: por cookies, por IP, transparente,…
- Protección de servicio: DoS (Denegación de Servicio) [14], DDoS (Denegación de Servicio Distribuido) [15], etc.

CASO 2 – CONFIGURACIÓN EN ALTA DISPONIBILIDAD (Figura 11)

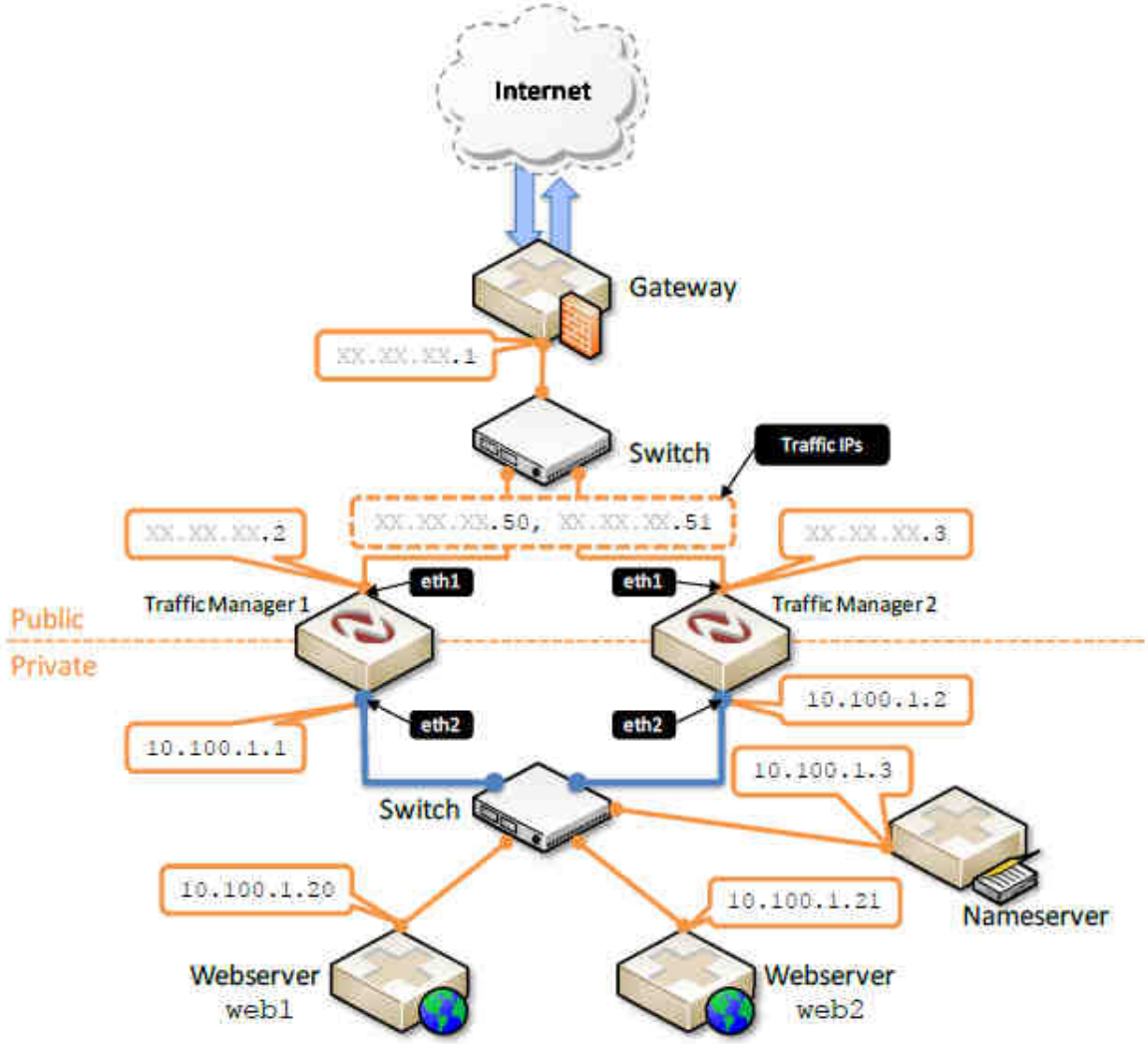


Figura 11: Balanceo de carga en Alta Disponibilidad

En este escenario se deberá contratar los nodos correspondientes de balanceo (por parejas) y contratar mediante un alta de servicio la opción de Alta Disponibilidad. El rendimiento en este tipo de solución es totalmente lineal multiplicando por 2.

CASO 3 – ACELERACIÓN SSL.

El servicio se cotiza mediante un coste de alta inicial para el despliegue y de una cuota fija mensual para la gestión completa del Balanceo de Carga en un VApp mínimo: 1 CPU, 1 GB. Para las ampliaciones de prestaciones se deberán contratar ampliaciones de vCPU y RAM.

Contratación:

Cada balanceador virtual configurado sobre una vApp de 1 VCPU y 1 GB RAM es capaz de procesar hasta el máximo de 700 Mbps o 3.000 conexiones por segundo.

La forma de contratar el servicio será mediante la composición de los siguientes componentes:

a) Calcular el número de servidores virtuales que soportarán la solución: Obtener el número de servidores reales necesario dividiendo el número máximo de conexiones por segundo deseadas entre 3.000 y sumándole uno si se desea alta disponibilidad del tipo N+1. Se conseguirá no tener degradación del servicio ante la caída de UNO de los servidores reales. La opción de SSL no tiene un cargo adicional sino simplemente instrucciones claras en la provisión del servicio.

b) Servicio Gestionado de Balanceo de Carga que incluirá los costes de licenciamiento, configuración y administración completa del servicio. Se incluirán tantas unidades como elementos indicados en el punto a).

Solicitudes:

El cliente podrá solicitar peticiones de servicio a través del portal:

- Cambio Política de Balanceo, Persistencia de sesiones o protocolo a balancear. Solicitud tipo C.
- Alta o Baja de grupos de balanceo. Solicitud tipo B
- Alta o Baja de nodos en el grupo de balanceo. Solicitud tipo B

Si la petición tiene impacto en la facturación se deberá realizar la petición vía comercial.

Informes:

El cliente tendrá acceso a la información de los grupos de balanceo definidos y los nodos incluidos, a modo de vista del inventario.

ADMINISTRACIÓN DE SERVIDORES VIRTUALES

El objetivo de esta funcionalidad es la administración, planificación, supervisión, operación y despliegue de los elementos de servicio en los entornos de preproducción/certificación y producción del cliente, bajo una garantía de calidad de servicio.

Según las necesidades del cliente, Telefónica podrá asumir toda la administración del servidor virtual o sólo parte de ella. Así, se distinguen dos modalidades de administración:

- Administración completa
- Administración compartida

Administración completa

Dicha modalidad de servicio contiene las tareas de administración, planificación, supervisión, operación y despliegue de los elementos de servicio en los entornos de preproducción/certificación y producción del cliente por parte de Telefónica, siempre bajo una garantía de calidad de servicio.

El alcance de esta modalidad de servicio se acota a las siguientes familias de productos:

- Administración de Sistemas Operativos.
- Administración de Hipervisores VMWare [16] para entornos dedicados o privados de Hosting Virtual.
- Administración de Bases de Datos.
- Administración de Middleware
    - Se entiende como Middleware la capa de productos de conectividad que ofrece un conjunto de servicios que hacen posible el funcionamiento de aplicaciones distribuidas sobre plataformas heterogéneas. Funciona como una capa de abstracción de software distribuida, que se sitúa entre las capas de aplicaciones y las capas inferiores (sistema operativo y red).

Administración Compartida

No se recomiendan (aunque son admitidos y gestionados) entornos bajo contratos de administración compartida. La responsabilidad en estos casos es difícil de delimitar y en ocasiones se diluye entre las partes.

Algunas consideraciones a tener en cuenta:

- Se admiten servidores en modalidad de administración compartida siempre y cuando Telefónica sea responsable de las capas más básicas (SO), o incluso llegando a capas intermedias (Bases de Datos (BD), Middleware).
- No se admiten entornos en los que el cliente es responsable del sistema operativo y Telefónica del resto de capas debido a los requerimientos impuestos por los sistemas de gestión (monitorización, backup,…).

- No se admiten entornos de administración compartida sobre instancias o módulos individuales. Un ejemplo, la administración de la BD deberá estar bajo la responsabilidad de un único administrador, no de forma compartida.
- Las herramientas de monitorización y backup serán las suministradas por Telefónica en este servicio.
- Existirán usuarios diferenciados para cada uno de los ámbitos de administración y activarse la correspondiente auditoría.
- El Acuerdo de Nivel de Servicio estará restringido a tiempos de atención y resolución de incidencias y solicitudes. No se aplicará objetivos de disponibilidad de servicio debido a posibles indefiniciones en la responsabilidad ante cualquier tipo de incidencia. En cualquier caso, nos comprometemos por el mejor esfuerzo para la correcta administración del servicio.
- Durante la fase de provisión y puesta en marcha del servicio, se incluirá en el Protocolo de Mantenimiento los siguientes procedimientos operativos:
    - procedimiento de atención de incidencias y problemas,
    - procedimiento de gestión de cambios;
    - procedimiento de rotación y comunicación de claves de root/administrador;
    - procedimiento de escalado;
    - procedimiento de gestión y ejecución de contratos de mantenimiento con terceros (hardware y sistema operativo).

Se entiende como Middleware la capa de productos de conectividad que ofrece un conjunto de servicios que hacen posible el funcionamiento de aplicaciones distribuidas sobre plataformas heterogéneas. Funciona como una capa de abstracción de software distribuida, que se sitúa entre las capas de aplicaciones y las capas inferiores (sistema operativo y red).

La inclusión de productos no soportados por el fabricante está totalmente desaconsejada. En caso de ser necesario su administración se llevará a cabo como una solución temporal hasta la actualización de versiones o modificación de la infraestructura de servicio. En estos casos el acuerdo de nivel de servicio se limitará al mejor esfuerzo por nuestra parte sin comprometer niveles de disponibilidad a priori.

CLOUD PORTAL

Cloud Portal es el nombre comercial de la funcionalidad de valor añadido que permitirá al servicio Hosting Virtual disponer de un portal de autoprovisión de componentes TI para todo tipo de organizaciones.

Cloud Portal posibilita la ampliación de las opciones contratables del servicio Hosting Virtual habilitando la contratación del llamado “pool de recursos”: Una organización contrata (ver apartado de Contratación) en Hosting Virtual con Cloud Portal un conjunto de recursos TI agrupados bajo el concepto de VirtualDatacenter, que se compone básicamente de:

- CPU (GHz)
- GB RAM

- GB de disco tanto para el espacio que ocuparán los servidores virtuales (vmdk), incluyendo los discos de datos y los catálogos. Podrán seleccionarse diferentes modalidades en el tipo de almacenamiento: SAN FC o SAN SATA aunque no podrán convivir diferentes modalidades de disco en un mismo VirtualDatacenter. Sin embargo el cliente podrá contratar diferentes VDC y conectarlos entre ellos para disponer de diferentes arquitecturas.

- Dispondrá de una serie de recursos preprovisionados como la VLANs, además de la configuración previa de acceso a sus servidores: firewalls, internet, etc. (figura 12)

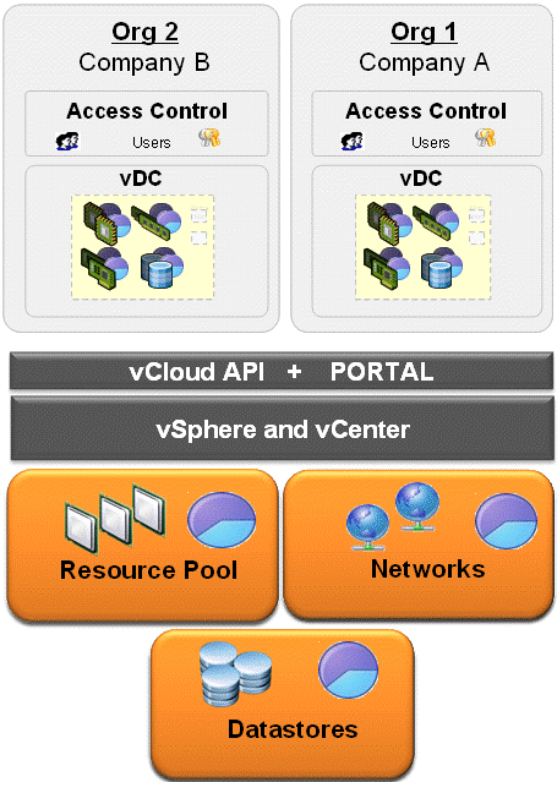


Figura 12: Pool de recursos preprovisionados en el Cloud Portal

Con esta nueva visión el cliente / organización se olvida de contratar servidores virtuales de forma unitaria y dispondrá de un conjunto de recursos para utilizarlo como requiera de forma totalmente flexible.

El servicio plantea diferentes solicitudes de servicio.A modo de resumen, se enumeran las principales funciones que los clientes de Hosting Virtual tendrán accesibles a través del panel de control:

- **Solicitud Tipo A o simple**. Solicitudes que implican tareas a realizar por Nivel 1 u operación. Sin coste:
  - Acceso a sala para conexión por consola al servidor virtual
  - Operaciones básicas: chequeo, reinicio, otras peticiones

- **Solicitud Tipo B o estándar**. Se trata de solicitudes en la que un administrador debe actuar pero el tiempo para realizar la tarea no es excesivo. Solicitudes con coste y que pueden conllevan cambios en el servicio con impacto económico en el recurrente mensual:
    - Reglas de firewall
    - Cambios DNS
    - Reglas de afinidad
    - Parada/Arranque de servidor
    - Modificaciones sobre la monitorización
    - Solicitud backup / restore puntual
    - Alta/Baja /Modificación de grupos de balanceo
    - Alta/Baja/Modificación de nodos en grupos de balanceo

- **Solicitud Tipo C o compleja**. Se trata de solicitudes en las que se requiere un conocimiento a fondo del entorno e incluso una planificación preliminar. Solicitudes con coste y que pueden conllevan cambios en el servicio con impacto económico en el recurrente mensual:

    - Clonación de servidores
    - Creación de imágenes de servidores (snapshots)
    - Importación de imágenes y vApp
    - Cambio Política de Balanceo, Persistencia de sesiones o protocolo a balancear.
    - Modificación patrón de simulación para la Monitorización Transaccional.

Estas peticiones serán gestionadas como cambios en el servicio y tramitadas a través de los mecanismos comerciales y de provisión oportunos. En el portal se incluirán estas peticiones correctamente tipificadas.

- **Solicitud Tipo D**. Se trata de solicitudes que deberán ser tratadas a nivel comercial incluyendo una valoración a medida.

    - Modificación de recursos: memoria y CPU
    - Parametrización y reinstalación de SO
    - Parada/Arranque de servidor de larga duración
    - Ampliación caudal Internet
    - Direcciones IP públicas adicionales
    - Cambio política de backup dentro de las estándar
    - Cambio política de backup a otra personalizada
    - Solicitudes de almacenamiento

Además de estas solicitudes, a través del portal se podrá solicitar las siguientes acciones, asociadas a la contratación de los servicios de monitorización o inherentes al propio servicio, como son:

- Monitorización de alarmas y rendimiento / Servicios Internet / Monitorización Transaccional. Información detallada de alarmas a través del panel de alarmas.
- Monitorización de servicio: visión agregada en el mapa de red o de servicio del estado de los distintos elementos monitorizados
- Informes de rendimiento de los recursos virtuales del servidor (CPU, memoria, swap).

- Informe de uso de Conectividad Internet.
- Documentación: manual de usuario, plantilla de mantenimiento y proyecto técnico.

2.2 SERVICIO MACROLAN

MacroLAN es una solución que permite al cliente, constituir redes privadas virtuales de banda ancha, con Equipos en Domicilio de Cliente (EDC) gestionado, de ámbito metropolitano y/o nacional, con opción de oficina del cliente en el CDG.

MacroLAN permite que las redes locales del cliente situadas en distintas ubicaciones geográficas estén conectadas con prestaciones similares a las que se obtendrían si estuvieran dentro de un mismo edificio, con elevada fiabilidad, escalabilidad y simplicidad. El cliente percibirá que todas sus dependencias están conectadas en una red con velocidades tipo LAN de modo que el acceso a los servidores remotos se produce a la misma velocidad que si tuvieran ubicación local. De este modo, todos los recursos de la empresa son accesibles con las mismas prestaciones desde cualquier ubicación del cliente.

Debido a la elevada velocidad y fiabilidad que la solución ofrece a los clientes, es posible la centralización de servidores y aplicaciones, optimizando de este modo las tareas y costes de gestión y mantenimiento de los mismos. Además, se ofrece la posibilidad de incluir a los CDG como una oficina más en la red del cliente y alojar en ellos las aplicaciones y/o servidores que el cliente considere oportunas.

La figura 13 muestra la arquitectura de la solución ofrecida al cliente en un escenario de conectividad nacional con presencia en dos capitales y además, en el CDG:

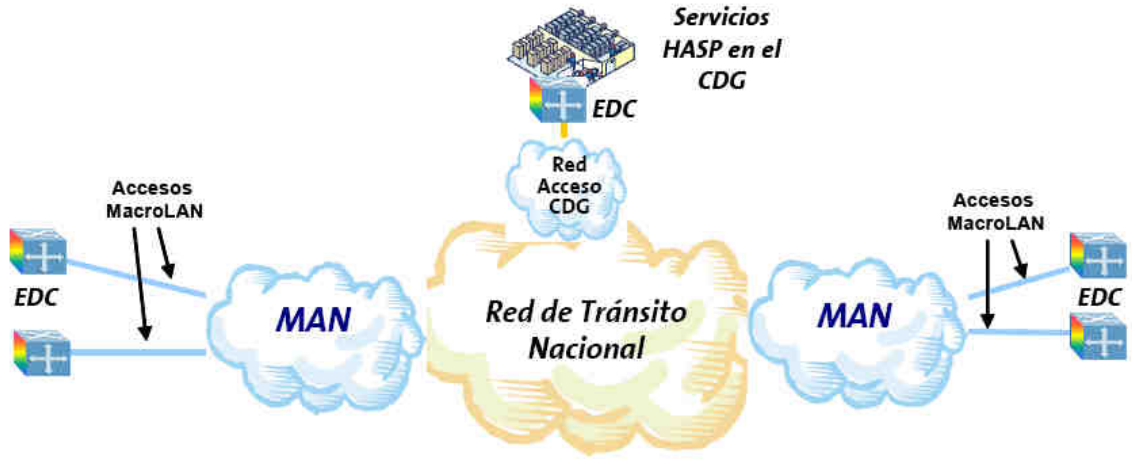


Figura 13: Arquitectura servicio macrolan

La figura 13 representa un caso general de configuración de la solución para un cliente, en donde aparecen todos los elementos de red necesarios.

Como puede observarse en la figura 13, el servicio MacroLAN incluye el acceso, el Equipo de Datos en domicilio de cliente (EDC) -tanto en las sedes del cliente como en el CDG- y todo el tráfico soportado sobre la red MAN y la red de tránsito nacional.

En el ejemplo de la figura 13, el cliente tiene cuatro sedes, repartidas en dos provincias diferentes, a las cuales quiere dar conectividad de muy alta velocidad. Además, el cliente tiene contratado servicios de Hosting y Active Server Pages (ASP) en el CDG, que deben ser accesibles desde todas las sedes.

Cada una de las sedes está equipada con un Equipo en Domicilio de Cliente (EDC). Este equipo se encarga del intercambio de tráfico entre la red local del cliente y la MAN.

La MAN ofrece al cliente comunicaciones entre las sedes situadas en la misma provincia. Sin embargo, para las comunicaciones con sedes situadas en otra capital, es necesaria la participación de una red de tránsito nacional: la red MPLS (Multi-Protocol Label Switching) (ver Anexo 6.2). Esta red se encarga del intercambio del tráfico con otras capitales y con el CDG.

2.2.1 DESCRIPCIÓN DEL SERVICIO

Los componentes que integran la oferta MacroLAN son los siguientes:

- Equipo en Domicilio del Cliente (EDC): es el equipo switch router gestionado por Telefónica. Este elemento es indispensable y obligatorio en cualquier escenario MacroLAN.
- Acceso MacroLAN: necesario para conectar el EDC a la red MAN. Tienen velocidades desde 2 Mbps hasta 1Gbps.
- Caudal metro: permite las comunicaciones con otras sedes ubicadas, exclusivamente, en el ámbito de la MAN.
- Caudal Nacional: permite al cliente las comunicaciones con sedes situadas en otras provincias. Igualmente, para las sedes situadas en capitales donde no existe un CDG, el tráfico nacional permite cursar tráfico con destino a los CDG. Existen dos tipos de Caudal Nacional: Agregado y Exclusivo.
- Gestión extremo a extremo, que permite al cliente tener un interlocutor único para la gestión de todos los aspectos relacionados con la solución completa ofrecida al cliente. Al igual que el EDC, es un elemento indispensable y obligatorio en cualquier escenario MacroLAN.
- Mantenimiento, con dos opciones Estándar y Avanzado para cubrir las distintas necesidades del cliente.
- Facilidades, de contratación opcional. Son las siguientes:

    - Facilidad de alojamiento de Oficina en el CDG. Esta facilidad permite al cliente el acceso a servicios de Hosting y ASP en el CDG. Esta facilidad, incluye varios componentes específicos: Accesos CDG, Caudal CDG (de acceso y nacional) y Alojamiento del EDC (espacio físico, alimentación eléctrica, etc.).
    - Facilidad de Redundancia, para los entornos de cliente que con requisitos de máxima disponibilidad.
    - Facilidad de soporte a otros protocolos: Ethernet, que permite el transporte transparente de tráfico Ethernet entre EDC.
    - Facilidad de Redirección Plus que permite establecer las comunicaciones con un centro secundario bajo petición expresa del cliente.

A continuación se detallan cada uno de los conceptos anteriores en más detalle.

2.2.2 EQUIPO EN DOMICILIO DEL CLIENTE

El equipo en domicilio del cliente (EDC) tiene la misión de realizar la conexión entre la LAN del cliente y la red.

Son equipos con funcionalidad de router y de switch (excepto Cisco 2621XM que es sólo router). La funcionalidad de switch se utiliza para el soporte de la facilidad de transporte de protocolo Ethernet que permite cursar tráfico Ethernet de modo transparente entre la LAN del cliente y la red. El servicio no soporta conmutación Ethernet local, es decir, tráfico Ethernet con origen y destino en la misma LAN del cliente.

Estos equipos son gestionados siempre por Telefónica y en la versión actual, no se contempla la posibilidad de gestión compartida con el cliente.

Existen tres fabricantes homologados en catálogo: RiverStone, Cisco y Teldat. Los equipos seleccionados de cada fabricante son los más adecuados para las aplicaciones en uso, los servicios del catálogo y para todo tipo de entornos empresariales.

2.2.3 ACCESO MACROLAN

La conectividad del EDC a la red MAN se establece utilizando un elemento del servicio denominado Acceso MacroLAN. Constituye el acceso a la red, que unen el domicilio del cliente con el nodo de la red MAN más próximo. Estos accesos pueden tener las siguientes velocidades: 2 Mb, 10 Mb, 100 Mb y 1 Gb.

2.2.4 CAUDAL METRO

El Caudal metro se contrata asociado al acceso de una sede y permite la comunicación de ésta con cualquier otra sede ubicada en la misma MAN. El ámbito de la comunicación que permite el Caudal metro es por lo tanto un ámbito provincial, ya que hay una MAN por cada provincia.

Tiene además las siguientes características:

- En cada una de las sedes de una MAN en las que no se contrate un Caudal Nacional Exclusivo es necesaria y obligatoria la contratación de un Caudal metro. Si alguna de las sedes con Caudal metro requiere además poder comunicarse con otras sedes del cliente situadas en otras provincias será además necesaria la contratación de un Caudal Nacional Agregado asociado a dicha MAN.
- Permite el envío de tráfico hacia un CDG situado en la misma MAN. Por ejemplo, tráfico enviado desde Getafe al CDG de Madrid.

- Existen tres clases de servicio para el transporte de tráfico sobre la MAN: Plata, Oro y Multimedia.
- En un acceso MacroLAN es incompatible la contratación de un Caudal metro con la de un Caudal Nacional Exclusivo. Como se ve en el siguiente punto, ambos son excluyentes.
- El Caudal metro limita el volumen máximo de caudal que puede cursarse a través del acceso. De este modo, un acceso de 2 Mb de velocidad, siempre puede cursar 2 Mbps de caudal, pues lleva ese caudal asociado por defecto. Sin embargo, un caudal de acceso de 5 Mbps sobre un acceso de 10 Mb, implica que el máximo caudal que puede cursarse a través de ese acceso, es siempre de 5 Mbps

Se permite la contratación de los Caudales metro reflejados en la Tabla 4, con la granularidad indicada, para cualquier clase de servicio:

Acceso	Caudal Metro
2 M	2 Mbps, asignados por defecto (e incluidos en el precio del acceso)
10 M	1 a 10 Mbps en saltos de 1 Mbps
100 M	De 10 a 100 Mbps en saltos de 10Mbps, más los valores admitidos para el acceso de 10M
1 G	De 100 a 1000 Mbps en saltos de 100 Mbps, más los valores admitidos para el acceso de 100M

Tabla 4: Caudales Metro en servicio Macrolan

A nivel lógico todo el tráfico cursado a través de un acceso se transporta asociado a una única VLAN, que es la VLAN Nacional. Esta transporta tanto el tráfico metropolitano (entre diferentes sedes pertenecientes a la misma MAN), el tráfico nacional (entre sedes ubicadas en diferentes MAN), el tráfico para comunicaciones con el CDG (si el cliente tiene una sede en el CDG) y el tráfico de gestión.

2.2.5 CAUDAL NACIONAL

El Caudal Nacional permite el intercambio del tráfico entre sedes de cliente ubicadas en provincias diferentes. Existen dos tipos de Caudal Nacional: el Caudal Nacional Exclusivo y el Caudal Nacional Agregado.

2.2.5.1 CAUDAL NACIONAL EXCLUSIVO

Tiene las siguientes características:

- Su contratación es opcional.
- Se contrata en aquellas sedes en las que se requiere un caudal de uso exclusivo y que no sea compartido con otras sedes.
- Permite la comunicación con cualquier oficina de la RPV independientemente de que esté o no a la misma MAN.

- La contratación en un acceso MacroLAN de Caudal Nacional Exclusivo es incompatible con la de Caudal metro. Ambos son mutuamente excluyentes.
- Permite el envío de tráfico hacia un CDG situado en una capital diferente. Por ejemplo, tráfico enviado desde una sede situada en Valencia al CDG de Madrid.
- Existen tres clases de servicio para el transporte de tráfico sobre la red de tránsito nacional: Plata, Oro y Multimedia.
- Transporta exclusivamente protocolo IP, esto es, no se permite el transporte de Ethernet u otros protocolos.

Para el Caudal Nacional Exclusivo se permite la contratación de los mismos valores de caudal indicados para el Caudal metro para cualquier clase de servicio (ver Tabla 4 en el apartado 3.2.4). Adicionalmente, y exclusivamente para la clase de servicio Multimedia, se permite la contratación de valores de Caudal Nacional Exclusivo de 256 Kbps y de 512 Kbps para dar cabida a las demandas de caudal de VoIP y ToIP inferiores a 1 Mbps

La contratación del Caudal Nacional Exclusivo es compatible con la contratación de Caudal CDG Exclusivo en la misma sede. Sin embargo, deberá tenerse en cuenta una limitación motivada por los EDCs en lo relativo a las clases de servicio. Para Caudal Nacional Exclusivo y Caudal CDG Exclusivo de una misma clase de servicio (Plata u Oro), no es posible garantizar cada caudal por separado. Esto se debe a que el EDC sólo dispone de una cola por clase de servicio y no por tipo de caudal.

2.2.5.2 CAUDAL NACIONAL AGREGADO

Tiene las siguientes características:

- Su contratación es opcional.
- En cada una de las sedes de una MAN en las que no se contrate un Caudal Nacional Exclusivo es necesaria y obligatoria la contratación de un Caudal metro. Si alguna de las sedes con Caudal metro requiere además poder comunicarse con otras sedes del cliente situadas en otras provincias será además necesaria la contratación de un Caudal Nacional Agregado asociado a dicha MAN.
- Es un caudal compartido por todas las sedes del cliente en una misma MAN, excepto por aquellas que tengan contratado un Caudal Nacional Exclusivo.
- Permite el envío de tráfico hacia un CDG situado en una provincia diferente. Por ejemplo, tráfico enviado desde Valencia al CDG de Madrid.
- Transporta exclusivamente protocolo IP, esto es, no se permite el transporte de Ethernet u otros protocolos.
- Existen tres clases de servicio para el transporte de tráfico sobre la red de tránsito nacional: Plata, Oro y Multimedia

2.2.6 CLASES DE SERVICIO PARA EL TRÁFICO

El servicio MacroLAN permite de contratar tres clases de servicio que permitirán al cliente dar un tratamiento diferenciado a sus aplicaciones dentro de su RPV. Todo lo descrito en este capítulo no aplica a la facilidad "transporte de otros protocolos: Ethernet". Un requerimiento de calidad de servicio aplicado sobre dicha facilidad requerirá no solamente de un proyecto especial sino también de un estudio de viabilidad técnica. Cada clase de servicio tiene asociado unos acuerdos de nivel de servicio.

Los tres grandes bloques que pueden llegar a intervenir en el servicio MacroLAN para el soporte de las clases de servicio en el tráfico son los siguientes:

- EDC: los EDC se configuran clasificando el tráfico, priorizándolo y gestionando el ancho de banda, acorde a las calidades de servicio contratadas.
- Red MAN: las calidades de servicio contratadas en el Caudal metro impactan directamente en la configuración de la MAN.
- Red de tránsito Nacional: las calidades de servicio contratadas en el Caudal Nacional Exclusivo y en el Caudal Nacional Agregado impactan directamente en la configuración de la Red de tránsito Nacional.

Cuando un cliente solicita clases de servicio en el servicio MacroLAN, es necesario especificar las siguientes variables:

- Caudal metro (obligatorio si el cliente no contrata en ese acceso Caudal Nacional Exclusivo o, en el caso de una sede CDG, no contrata un Caudal CDG Exclusivo). Habrá que indicar qué ancho de banda Ethernet de cada una de las clases de servicio contrata el cliente. En este caso esta información es necesaria no solamente para la provisión del servicio sino que afecta a la facturación del mismo.
- Caudal Nacional Exclusivo (Opcional): caudal exclusivo para la comunicación de una sede con cualquier otra independientemente de que esté o no en la misma MAN. Habrá que indicar qué ancho de banda IP de cada una de las clases de servicio contrata el cliente. En este caso esta información es necesaria no solamente para la provisión del servicio sino que afecta a la facturación del mismo.
- Caudal Nacional Agregado (Opcional): caudal agregado compartido por todas las conexiones de las sedes ubicadas en la misma MAN para la comunicación con cualquier sede que se encuentre en otra provincia. Habrá que indicar qué ancho de banda IP de cada una de las clases de servicio contrata el cliente. En este caso esta información es necesaria no solamente para la provisión del servicio sino que afecta a la facturación del mismo.
- Caudal CDG Exclusivo (Opcional): caudal exclusivo para la comunicación de una sede CDG con cualquier otra independientemente de que esté o no en la misma MAN, o de la Sede CDG virtual de otra provincia distinta de Madrid y Barcelona que envía tráfico con destino al CDG.
- Caudal CDG Agregado (Opcional): caudal agregado compartido para la comunicación de todas las sedes de un cliente ubicadas en un CDG con cualquier sede situada en otra provincia.

Habrá que indicar qué ancho de banda IP de cada una de las clases de servicio el cliente contrata.

En este caso esta información es necesaria no solamente para la provisión del servicio sino que afecta a la facturación del mismo. Además para la provisión es necesario especificar las direcciones IP de las redes del cliente que se ubican en el CDG y que hacen uso de dichas clases de servicio.

El tráfico se clasificará y marcará en el EDC origen de la comunicación para que sea tratado de la forma apropiada hasta llegar al EDC destino. Las tres clases de servicio disponibles son las siguientes:

- Clase de Servicio PLATA:
  - Prioridad normal. Es el tráfico menos prioritario de todos
  - Es la clase de servicio que se asigna por defecto.
  - Si el cliente no quiere priorizar ningún tipo de tráfico, el caudal plata será igual al caudal contratado.
  - En los escenarios de comunicaciones exclusivamente provinciales (es decir no interviene la red de tránsito nacional) la configuración de clases de servicio realizada en los EDCs permite el siguiente comportamiento: si hay excedente de tráfico PLATA y el caudal ORO no se utiliza, este excedente podrá ocupar el ancho de banda que no está usando el ORO.

- Clase de Servicio ORO:
  - Prioridad alta.
  - A nivel de recomendación, podría decirse que esta clase de servicio se aplicaría al tráfico crítico, asociado a los procesos críticos del negocio del cliente (aplicaciones financieras, aplicaciones de gestión comercial, etc.) que ante congestión quiere priorizar frente al asociado al tráfico plata.
  - El tráfico asociado a esta clase tendrá una garantía de caudal, de tal forma que las aplicaciones de cliente asociadas a esta clase, dispondrán de su caudal por muy saturada que esté la clase PLATA.
  - En los escenarios de comunicaciones exclusivamente provinciales (es decir no interviene la red de tránsito nacional) la configuración de clases de servicio realizada en los EDCs permite el siguiente comportamiento: si hay excedente de tráfico ORO y el caudal PLATA no se utiliza, este excedente podrá ocupar el ancho de banda que no está usando el PLATA.

- Clase de servicio MULTIMEDIA:
  - Prioridad muy alta.
  - Clase de servicio normalmente asociada a tráfico de voz y aplicaciones multimedia.
  - Tiene asignado un ancho de banda de forma permanente y constante (no va a utilizar el caudal vacante que pueda existir para la clase oro y plata en un momento determinado). Esta regla se aplica en el EDC.
  - En los escenarios de comunicaciones exclusivamente provinciales (es decir no interviene la red de tránsito nacional) la configuración de clases de servicio realizada en los EDCs permite el siguiente comportamiento: si el tráfico Multimedia no utiliza todo el caudal que tiene asignado éste podrá ser utilizado por las clases Oro y Plata, en este orden.

2.2.6.1 IMPLEMENTACIÓN DE CALIDAD DE SERVICIO EN EL EDC

Los mecanismos que se configuran en los EDCs para ofrecer calidades de servicio diferenciadas son los siguientes:

- Clasificación del tráfico que entra al EDC procedente de la LAN del cliente, permitiendo asociar el mismo al perfil de calidad de servicio correspondiente.
- Marcado de los paquetes según los bits DSCP (Differentiated Services Code Point) [17] para que la red IP/MPLS ejecute el tratamiento oportuno.
- Marcado de los paquetes según los bits 802.1p [18] para que la red MAN ejecute el tratamiento oportuno.
- Priorización y gestión de colas para garantizar los caudales solicitados por el cliente.
- Control agregado del caudal entregado hacia la Red de Banda Ancha de acuerdo con el Caudal de Acceso a la MAN (Metro, Nacional Exclusivo, CDG Exclusivo, Nacional Exclusivo + CDG Exclusivo) contratado.

Cuando el cliente no solicita calidad de servicio, en el EDC se clasifica y marca todo el tráfico procedente de la LAN del cliente, a excepción del tráfico de gestión, como datos pertenecientes a calidad Plata. El tráfico asociado a la gestión se sirve por una cola diferente (en aquellos EDCs en los que se pueda manipular el marcado del tráfico generado por el propio EDC, se marcará el tráfico de gestión al valor adecuado).

Clasificación del tráfico

El EDC clasifica todo el tráfico recibido desde el punto de acceso al servicio, es decir, el tráfico entrante procedente de la LAN del cliente.

Los parámetros en base a los cuales se pueden establecer los criterios de clasificación son los siguientes:

- Nivel 4 IP: se hace referencia al puerto lógico, TCP o UDP, y, por lo tanto, permite hacer referencia a las aplicaciones que los utilizan.
- Nivel 3 IP: direcciones IP origen y/o destino.
- Puerto físico.

Esta clasificación permite asociar a cada paquete un perfil de calidad de servicio que se materializa en un tratamiento diferenciado del tráfico.

Marcado de tráfico

El protocolo IP dispone desde su concepción de una facilidad que le permite indicar a una aplicación o protocolos de nivel superior cómo debe manejar un paquete. Utiliza para ello un byte definido en la cabecera IP y llamado ToS (Type of Service).

El octeto ToS en la cabecera de un datagrama IP consta de tres campos (figura 14):

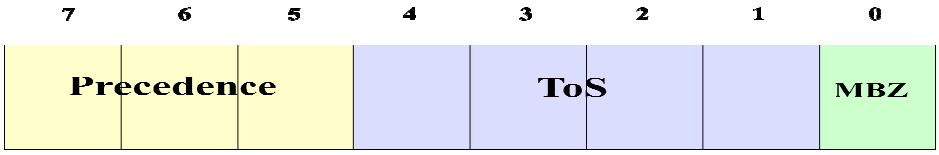


Figura 14: Datagrama IP

- Los tres bits del campo "precedence" se usan para indicar la prioridad del datagrama.
- Los cuatro bits del campo "ToS" indican información relativa al "throughput", "delay", "reliability" y "cost".
- El bit del campo "MBZ" (Must Be Zero) actualmente no se usa.

El IETF (Internet Engineering Task Force) redefinió el "ToS octet" como "DiffServ Byte" [19]. A los seis bits más significativos del ToS se les denominó DSCP. Así pues, los tres bits más significativos del DSCP coinciden con la precedencia IP señalizada en el byte ToS.

MacroLAN utiliza el marcado del DSCP y, por tanto, de la precedencia IP para diferenciar los paquetes pertenecientes a las distintas clases de tráfico.

Solamente se hace marcado del tráfico que inyecta el cliente en sentido EDC hacia la Red, es decir, no se hace un remarcado del tráfico que recibe el EDC de la Red para entregárselo al cliente.

Los EDCs marcan los seis bits de DSCP, y, por tanto, también el campo precedencia IP. Además, se marcan los bits 802.1p para que la MAN pueda hacer un tratamiento diferenciado por clase de servicio.

Los valores de DSCP y precedencia IP asignados a cada clase de servicio, así como los valores del marcado 802.1p se reflejan en la tabla 5.

Clase de Servicio (CoS)	DSCP	Precedencia IP	CoS (bits 802.1p)
Plata	8	1	1
Plata (con origen o destino en el CDG)	9	1	1
Oro	24	3	3
Oro (con origen o destino en el CDG)	25	3	3
Multimedia	40	5	5
Multimedia (con origen o destino en el CDG)	41	5	5
Gestión	56	7	7

Tabla 5: Marcado del tráfico en servicio Macrolan

El tráfico con destino el CDG solo se marca con un DSCP diferenciado en aquellos EDCs instalados en sedes para las que se haya contratado Caudal CDG Agregado o Caudal CDG Exclusivo. La contratación de este tipo de caudal estará sujeta a las limitaciones comerciales que se definan en cada momento.

En el caso de algunos de los EDCs homologados para el servicio, el tráfico generado por ellos mismos, como es el asociado a la gestión del propio EDC, no es posible marcarlo con los valores requeridos. Esta es la razón por la que será necesario que el PE marque el tráfico asociado a la gestión, con objeto de poder dotar al tráfico de gestión de QoS (Quality of Service) a lo largo backbone IP/MPLS.

Tratamiento de colas y gestión del Caudal de Acceso a la MAN

En el puerto de conexión del EDC con la MAN se utilizan cuatro colas, una por cada clase de servicio.

Para la clase Multimedia se utiliza siempre una cola de prioridad estricta o de baja latencia. El objetivo siempre es que el tráfico Multimedia se encole lo menos posible para reducir retardos y jitter.

El resto de colas se sirven con un algoritmo de WFQ (Weighted Fair Queuing) [20] o similar, en el que todas las colas se van sirviendo por turno, asignando distintas cantidades de tiempo a cada una de ellas (mediante asignación de pesos en el algoritmo). Este tipo de algoritmo permite garantizar que, en caso de congestión, ninguna clase se queda sin servicio (porque se van sirviendo todas por turno) y además permiten hacer un reparto aproximado entre las colas del caudal total (porque se asignan distintos pesos a cada cola).

Dependiendo del EDC utilizado (no sucede en todos), al cursar la clase Multimedia por una cola de prioridad estricta, se corre el riesgo de que el tráfico Multimedia pueda canibalizar el Caudal de Acceso a la MAN por completo. Para evitarlo, en estos EDCs se hace una limitación del Caudal Multimedia, descartándose el excedente.

Así pues, en cada conexión MacroLAN, el cliente debe definir un reparto aproximado del Caudal de Acceso a la MAN entre las distintas clases de servicio. Se debe tener en cuenta que:

- El reparto solo tiene efecto en caso de congestión del acceso (es decir, cuando se intente cursar tráfico por encima del Caudal de Acceso a la MAN contratado).
- En ausencia de congestión del acceso cualquiera de las clases (salvo la Multimedia) podría ocupar el total del caudal de acceso.
- El reparto que hará el EDC en caso de congestión será siempre aproximado, nunca exactamente igual, a lo que el cliente haya definido. (En la definición del algoritmo WFQ, los equipos homologados en el servicio asignan un porcentaje de tiempo de servicio a cada una de las colas para garantizar los anchos de banda contratados por cada una de las clases de servicio. Los valores de estos porcentajes tienen una granularidad que impide definir relaciones de porcentajes mayores de 1 a 100)
- La suma de los caudales que el cliente defina para cada clase en una conexión debe ser igual al Caudal de Acceso a la MAN contratado.

Implementación de la Calidad de Servicio en la MAN.

El control de Caudal Metro que hace el nodo de acceso de la MAN es el siguiente:

- En sentido EDC hacia MAN, no se hace control de caudal, la responsabilidad recae en el EDC que sí realiza el conformado correspondiente al caudal contratado.
- En sentido MAN hacia EDC será a 2 Mb, 4 Mb y 8 Mb, 10 Mb, 100 Mb, 1 Gb o 10 Gb según la velocidad del acceso contratado.

El servicio MacroLAN hace uso de las diferentes calidades de servicio disponibles en la MAN y se establece un paralelismo entre las clases de servicio definidas a nivel IP y las clases de servicio a nivel Ethernet.

Se establece un mapeo "calidad de servicio en MAN" ↔ "calidad de servicio tráfico IP". El mapeo se solicita de forma estática (se impide que existan otros tipos de combinaciones). Este mapeo debe ser transparente a los clientes. El mapeo pero podría modificarse según convenga. Por lo tanto, el cliente lo único que debe saber es que en el tramo de la MAN su tráfico recibe un tratamiento acorde a la calidad de servicio IP contratada. En estos momentos, el mapeo es el siguiente:

- Extra ↔ Multimedia IP
- Alta ↔ Oro IP
- Normal ↔ Plata IP

La percepción del servicio que tendrá el cliente es que el tráfico podrá tener, si el cliente lo contrata, un tratamiento diferenciado por calidad de servicio extremo a extremo (entre los EDCs que intervienen en la comunicación en la misma o en diferentes MAN). El EDC objeto del análisis, será capaz de cursar hacia la MAN un Caudal Multimedia de forma prioritaria y cursar una cantidad garantizada mínima de Oro y Plata en caso de congestión del acceso, pudiendo estos dos últimos utilizar vacancias de las otras clases de servicio cuando éstas se produzcan.

Para el tráfico procedente de la MAN y con destino el EDC objeto del asunto, se definirá un esquema de prioridad estricta en donde cada clase de servicio tiene prioridad estricta sobre el tráfico de clases inferiores. La priorización sigue el siguiente esquema:

- Tráfico de gestión (clase de servicio interna, no contratable por el cliente).
- Clase Multimedia. (CoS 4 y 5).
- Clase Oro (CoS 2 y 3).
- Clase Plata (CoS 0 y 1).

A continuación se indica el impacto que supone implementar el mapeo mencionado anteriormente en los siguientes elementos sobre los que se soporta el servicio MacroLAN.

- Impacto en los EDCs: En el proceso de marcado de los paquetes, además de marcarlos según los bits DSCP para que la red IP/MPLS ejecute el tratamiento oportuno, será necesario marcar el CoS según los bits 802.1p para que la red Ethernet metropolitana haga lo propio. Los valores de DSCP, precedencia IP y CoS asignados a cada clase de servicio se reflejan en la Tabla 8.

- Impacto en la MAN:

    - Control de caudal en entrada: La MAN ofrece la posibilidad de que un conjunto de VLANs dentro de un mismo acceso compartan un caudal. Además de poder contratar caudal máximo por acceso existe la posibilidad de contratar caudal por VLAN o por "conjunto de VLANs". Los valores permitidos (en Mbps) de caudal contratado por "conjunto de VLANs" y por VLAN son: de 1 en 1 hasta 10, de 5 en 5 hasta 100, de 10 en 10 hasta 1000 y de 1000 en 1000 hasta 10G, teniendo en cuenta que la suma de caudales del "conjunto de VLANs" más el de VLANs individuales debe coincidir con el caudal máximo contratado por acceso. Todas las VLANs del acceso utilizadas por MacroLAN se incluyen dentro del mismo conjunto de VLANs pero, sin embargo, el caudal de dicho conjunto no se controla en entrada, a diferencia de lo que se hacía habitualmente en los accesos de la MAN. Esto es debido a que el Caudal Metro ya es controlado por el EDC de MacroLAN.

    - En los accesos cobrelan a 2, 4 y 8 Mbps, las velocidades Ethernet efectivas se ven limitadas por la capacidad procesadora de la UTR. Es por ello que se ha realizado la parámetrización necesaria en los EDCs del Servicio Macrolan, para que en el caso de que el caudal metrolan contratado coincida con la velocidad máxima de la línea el caudal efectivo se respecte con las máximas garantías.

    - La MAN debe respetar el marcado del CoS asociado al tráfico que procede tanto de los EDCs como de los PEs (Routers de Acceso a la red MPLS).

    - Tratamiento del tráfico, según el CoS, durante el resto del tránsito hasta que el tráfico abandona la red MAN.

    - Control del caudal en salida de la MAN hacia los EDCs a 2M, 4M, 8M, 10M 100M, 1G o 10G según proceda.

    - En los puertos de acceso de la MAN, y para el tráfico que se entrega en el sentido hacia EDCs o hacia PEs, configurar esquema de prioridad estricta para las diferentes clases de servicio.

    - El hecho de que los EDCs se configuren de forma que una clase de servicio pueda utilizar las vacancias de otra, tiene la desventaja de que en un momento determinado, la cantidad de tráfico que circula por la MAN, y asociada a una clase de servicio determinada, pueda ser superior a la contratada para esa clase, en el servicio MacroLAN, dado que reutiliza la vacancia de otra y no se hace remarcado en el EDC ni control de caudal por CoS en la entrada a la MAN.

Implementación de calidad de servicio en los PEs

Hay que distinguir claramente entre el tratamiento que sufre el tráfico en entrada a la red IP/MPLS y en salida desde esta última hacia una MAN.

El tráfico entrante en la red IP/MPLS, procedente de la MAN:

- Es clasificado en la correspondiente clase de servicio.
- Es sometido a un control de caudales por clase de servicio.
- El tráfico de cada cliente se trata de un modo diferenciado.

El tráfico saliente de la red IP/MPLS, hacia la MAN:

- Es asignado a la cola de salida correspondiente en función de la clase de servicio a la que pertenezca.
- El tratamiento de colas es agregado para el tráfico de todos los clientes.
- Es marcado con el CoS apropiado para que la MAN pueda tratarlo acorde a la calidad de servicio a la que pertenece.

Clasificación del tráfico en entrada al PE

Todo el tráfico que entra al PE desde la MAN es clasificado para su correcto tratamiento en el backbone IP/MPLS. Los criterios de clasificación que se utilizan son los siguientes:

- El tráfico dirigido a las direcciones IP del centro de gestión de EDCs y con origen en los rangos de gestión de EDCs se clasifica como tráfico de gestión de EDCs (clasificación en base a dirección origen y destino).
- El tráfico marcado con precedencia IP igual a 5 se clasifica en la clase Multimedia.
- El tráfico marcado con precedencia IP igual a 3 se clasifica en la clase Oro.
- El resto del tráfico se clasifica en la clase Plata.

Marcado de tráfico en los PEs

Como norma general, en MacroLAN el tráfico viene marcado desde los EDCs y no sufre ningún remarcado en los PEs. La única excepción es el tráfico de gestión de los EDCs, puesto que algunos de ellos no son capaces de marcarlo. En este caso:

El tráfico de gestión de EDCs, hasta un caudal de 256 Kbps por cada VLAN, sufre un remarcado de la precedencia IP, que se marca al valor 7.

Entre 256 y 512 Kbps por cada VLAN, sufre un remarcado de la precedencia IP, que se marca al valor 1 (clase Plata).

Gestión de caudales en entrada al PE

A la entrada de la red IP/MPLS, en los PEs, es dónde se controlan los caudales contratados por el cliente para cada clase de servicio. Estos caudales son:

- Nacional Agregado.
- CDG Agregado.
- Nacional Exclusivo.
- CDG Exclusivo.

En el caso del tráfico de gestión de los EDCs, hasta un caudal de 512 Kbps por cada VLAN se deja pasar, marcándose la precedencia IP con distinto valor en función del caudal (ver apartado anterior), y por encima de 512 Kbps se descarta.

Control del Caudal Nacional Agregado en entrada al PE.

El control de Caudal Nacional Agregado se hace en el PE.

- En sentido de la MAN hacia el PE: Control por conexión y dentro de cada conexión por clase de servicio (Plata, Oro, Multimedia). Cada uno de estos caudales se controla individualmente y el exceso de cada uno de ellos se descarta. No se produce ningún remarcado de una clase en otra ni reaprovechamiento.

Control del Caudal CDG Agregado en entrada al PE.

El control de Caudal CDG Agregado se hace en el PE.

- En sentido de la MAN hacia el PE: control por VLAN y dentro de cada VLAN por calidad de servicio (Plata CDG, Oro CDG, Multimedia CDG). Cada uno de estos caudales se controla individualmente y el exceso de cada uno de ellos se descarta. No se produce ningún remarcado de una clase en otra.

Gestión del ancho de banda en salida en el PE

Todo el tráfico MacroLAN que sale desde la red IP/MPLS hacia la MAN sufre un tratamiento de calidad de servicio agregado, sin diferenciación entre los clientes. A grandes rasgos, el tratamiento del tráfico en este punto es el siguiente:

- La clase Multimedia se cursa por una cola de baja latencia para minimizar retardos y jitter.
- El resto de clases se cursan por colas en un algoritmo de WFQ que garantice que, en caso de congestión, ninguna clase quede sin servicio.

Control del Caudal Nacional y CDG Agregado en salida del PE.

El control de Caudal Nacional y CDG Agregado se hace en el PE.

- El tráfico saliente de la red IP/MPLS, hacia la MAN
    - El tráfico es asignado a la cola de salida correspondiente en función de la clase de servicio a la que pertenezca, y el tratamiento de colas es agregado para el tráfico de todos los clientes.

    - Los PEs, cuando entregan el tráfico hacia la MAN, deberán mapear la información de calidad de servicio IP a CoS para que la MAN pueda proporcionar un tratamiento de calidad de servicio mientras el tráfico circula por ella.

Control de Caudal Nacional Exclusivo

El control del caudal Nacional Exclusivo se hace en el EDC, MAN y PE.

- En el EDC:
    - En el EDC se limita el tráfico Multimedia y se sirve el tráfico Oro y Plata según las garantías contratadas permitiendo la reutilización de las vacancias entre ambas clases de servicio. En caso de coexistencia de tráfico "Nacional Exclusivo" y tráfico "CDG Exclusivo", hay que tener en cuenta, que en el acceso a la MAN, el tráfico Oro Nacional compite en las mismas condiciones con el tráfico Oro CDG, y el tráfico Plata Nacional compite en las mismas condiciones con el tráfico Plata CDG. En el caso del tráfico Multimedia esta competencia no existe debido a que ambos tráficos Multimedia (Multimedia Nacional, Multimedia CDG) pueden limitarse de forma independiente.

    - En el proceso de marcado de los paquetes, además de marcarlos según los bits DSCP para que la red IP/MPLS ejecute el tratamiento oportuno, será necesario marcar el CoS según los bits 802.1p para que la red Ethernet metropolitana haga lo propio.

- En el nodo de acceso a la MAN
    - Tráfico en sentido EDC hacia MAN. Las VLANs de MacroLAN se incluyen dentro de un conjunto de VLANs pero no se hace control de caudal en entrada de dicho conjunto.

    - Tráfico en sentido MAN hacia EDC. Será a 2 Mbps, 4 Mbps, 8 Mbps, 10 Mbps, 100 Mbps, 1 Gbps o 10 Gbps según lo contratado. Se aplica un esquema de prioridad estricta sobre las diferentes clases de servicio.

    - Tráfico en sentido MAN hacia PE. Se aplica un esquema de prioridad estricta sobre las diferentes clases de servicio.

    - La MAN debe respetar el marcado del CoS asociado al tráfico que procede tanto de los EDCs como de los PEs.

- Tratamiento del tráfico, según el CoS, durante el resto del tránsito hasta que el tráfico abandona la red MAN.

- El hecho de que los EDCs se configuren de forma que una clase de servicio pueda utilizar las vacancias de otra, tiene la desventaja de que en un momento determinado, la cantidad de tráfico que circula por la MAN, y asociada a una clase de servicio determinada, pueda ser superior a la contratada para esa clase, en el servicio MacroLAN, dado que reutiliza la vacancia de otra y no se hace remarcado en el EDC ni control de de caudal por CoS en la entrada a la MAN.

- En el PE:
  - En sentido de la MAN hacia el PE:
    - Se limita el tráfico Multimedia.
    - Los excesos de Oro y de Plata se dejan pasar sin sufrir alteraciones en el marcado original, teniendo en cuenta que la cantidad de tráfico Oro y Plata se limitan de forma conjunta al valor de la suma de los caudales Oro más Plata contratados.
    - Si conviven en el mismo acceso, tráfico Nacional Exclusivo y tráfico CDG Exclusivo, en el PE (a diferencia de lo que ocurría en el EDC, que ambos tráficos competían dentro de una misma clase de servicio, en el caso del Oro y la Plata) sí es posible dar un tratamiento diferenciado a cada uno de ellos y, por lo tanto, cada uno de ellos se controla independientemente en el PE y por clase de servicio:
      - Habrá un control asociado al tráfico Multimedia Nacional y otro al Multimedia CDG (esto no varía del tratamiento en los EDCs).
      - Habrá un control asociado al tráfico "Oro + Plata Nacional Exclusivo" y otro al "Oro + Plata CDG Exclusivo".
    - El tráfico saliente de la red IP/MPLS, hacia la MAN
    - El tráfico es asignado a la cola de salida correspondiente en función de la clase de servicio a la que pertenezca, y el tratamiento de colas es agregado para el tráfico de todos los clientes.
    - Los PEs, cuando entregan el tráfico hacia la MAN, deberán mapear la información de calidad de servicio IP a CoS para que la MAN pueda proporcionar un tratamiento de calidad de servicio mientras el tráfico circula por ella.

Control de Caudal CDG Exclusivo.

- **En el EDC:**
  - El EDC entrega a la MAN un total de tráfico igual al caudal total contratado. En el EDC se limita el tráfico Multimedia y se sirve el tráfico Oro y Plata según las garantías contratadas permitiendo la reutilización de las vacancias entre ambas clases de servicio. En caso de coexistencia de tráfico "Nacional Exclusivo" y tráfico "CDG Exclusivo", hay que tener en cuenta, que en el acceso a la MAN, el tráfico Oro Nacional compite en las mismas condiciones con el tráfico Oro CDG, y el tráfico Plata Nacional compite en las mismas condiciones con el tráfico Plata CDG. En el caso del tráfico Multimedia esta

competencia no existe debido a que ambos tráficos Multimedia (Multimedia Nacional, Multimedia CDG) pueden limitarse de forma independiente.

- En el proceso de marcado de los paquetes, además de marcarlos según los bits DSCP para que la red IP/MPLS ejecute el tratamiento oportuno, será necesario marcar el CoS según los bits 802.1p para que la red Ethernet metropolitana haga lo propio.

- **En el nodo de acceso a la MAN**
  - Tráfico en sentido EDC hacia MAN. Las VLANs de MacroLAN se incluyen dentro de un conjunto de VLANs pero no se hace control en entrada de dicho conjunto.
  - Tráfico en sentido MAN hacia EDC. Será a 2 Mbps, 4 Mbps, 8 Mbps, 10 Mbps, 100 Mbps, 1 Gbps o 10 Gbps según lo contratado. Se aplica un esquema de prioridad estricta sobre las diferentes clases de servicio.
  - Tráfico en sentido MAN hacia PE. Se aplica un esquema de prioridad estricta sobre las diferentes clases de servicio.
  - La MAN debe respetar el marcado del CoS asociado al tráfico que procede tanto de los EDCs como de los PEs.
  - Tratamiento del tráfico, según el CoS, durante el resto del tránsito hasta que el tráfico abandona la red MAN.
  - El hecho de que los EDCs se configuren de forma que una clase de servicio pueda utilizar las vacancias de otra, tiene la desventaja de que en un momento determinado, la cantidad de tráfico que circula por la MAN, y asociada a una clase de servicio determinada, pueda ser superior a la contratada para esa clase, en el servicio MacroLAN, dado que reutiliza la vacancia de otra y no se hace remarcado en el EDC ni control de de caudal por CoS en la entrada a la MAN.

- **En el PE:**
  - En sentido de la MAN hacia el PE:
    - Se limita el tráfico Multimedia.
    - Los excesos de Oro CDG y de Plata CDG se dejan pasar sin sufrir alteraciones en el marcado original. La cantidad de tráfico Oro CDG y Plata CDG se limitan de forma conjunta al valor de la suma de Oro CDG más Plata CDG contratados.
    - Si conviven en el mismo acceso tráfico CDG Exclusivo y tráfico Nacional Exclusivo, en el PE (a diferencia de lo que ocurría en el EDC que ambos tráficos competían dentro de una misma clase de servicio, en el caso del Oro y la Plata) sí es posible dar un tratamiento diferenciado a cada uno de ellos y, por lo tanto, cada uno de ellos se controla independientemente en el PE y por clase de servicio:
      - Habrá un control asociado al tráfico Multimedia Nacional y otro al Multimedia CDG (esto no varía del tratamiento en los EDCs).
      - Habrá un control asociado al tráfico “Oro + Plata Nacional Exclusivo” y otro al “Oro + Plata CDG Exclusivo”.

  - El tráfico saliente de la red IP/MPLS, hacia la MAN

- El tráfico es asignado a la cola de salida correspondiente en función de la clase de servicio a la que pertenezca, y el tratamiento de colas es agregado para el tráfico de todos los clientes.
- Los PEs, cuando entregan el tráfico hacia la MAN, deberán mapear la información de calidad de servicio IP a CoS para que la MAN pueda proporcionar un tratamiento de calidad de servicio mientras el tráfico circula por ella.

2.2.7 REGLAS DE INGENIERÍA

Protocolos de Routing entre EDCs y PEs

El protocolo de routing a utilizar como estándar del servicio entre EDCs y PEs, así como entre EDCs, es RIPv2 [21].

En circunstancias excepcionales se contempla la posibilidad de utilizar BGP4 [22]. Los criterios que pueden conducir a la utilización de BGP son:

- Tiempos de convergencia. Los tiempos de convergencia obtenidos con RIP son excesivamente elevados para los requisitos del cliente.
- Relación Nº de rutas/Sedes VPN. Para VPNs en las que haya un reducido número de sedes anunciando un elevado número de rutas, desde el punto de vista de consumo de recursos en los PEs, es preferible la utilización de BGP frente a RIP. El criterio general dado por Ingeniería de Red es que cuando la relación Rutas/Sedes, siendo Rutas el número total de rutas anunciadas en toda la VPN y Sedes el número total de sedes en toda la VPN, sea mayor de 25, es preferible la utilización de BGP.
- Otros criterios que se detecten durante la elaboración del proyecto para el cliente.

Lo indicado arriba es válido para el servicio MacroLAN de forma aislada, sin embargo, si se hace uso del servicio como parte integrante de RPVs (Red Privada Virtual) convergentes utilizadas por el servicio Ibercom IP, las indicaciones son diferentes. En dicho caso la única alternativa posible es BGP.

RIPv2

- 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 segundos.

- Por defecto, el EDC solo 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 cuáles son estas redes para añadirlas en el filtro anteriormente mencionado y asociado con la información que se anuncia hacia la Red.

- Asimismo, los EDCs de una sede concreta no aprenderán desde la Red de Banda Ancha los prefijos correspondientes a redes que supuestamente deban ser anunciadas desde dicha sede.

BGP

- Cada EDC mantendrá dos sesiones eBGP (una con cada uno de los dos PEs).

- Por defecto, el EDC solo anunciará hacia la Red de Banda Ancha, la red de la LAN del cliente directamente conectada. Para lograr esto habrá que aplicar el filtro correspondiente en el proceso de eBGP.

- 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 cuáles son estas redes para añadirlas en el filtro anteriormente mencionado y asociado con la información que se anuncia hacia la Red.

- Se necesitará en el PE el soporte de la funcionalidad "AS-override" con objeto de poder utilizar en todas las localizaciones de la VPN del cliente el mismo número de AS.

- A un cliente del Servicio Macrolan, se le asignará el AS privado 65000 al igual que ocurre en "VPN IP" (este número se le puede asignar a todos los clientes que necesiten de un AS privado).

- Se requiere el uso de un Site of Origin (SOO) por oficina/sede en la configuración de los PEs, para evitar bucles de routing.

- Para evitar la necesidad de mallado total con sesiones iBGP sobre la MAN entre los EDCs del cliente, los PEs no modificarán el parámetro next-hop en las rutas que aprendan por la MAN cuando anuncien estas rutas hacia el resto de EDCs en la misma MAN. De este modo, los PEs "reflejarán" sobre la MAN los prefijos aprendidos desde los EDCs.

Conexión redundante entre la red IP/MPLS y la MAN

Como ya se ha indicado, la conexión entre la red IP/MPLS y una MAN es siempre redundante, a través de dos PEs.

Se configurarán los PEs y EDCs de forma que todos los EDCs de un mismo cliente tengan un PE como destino principal y el otro de backup. Este modo de funcionamiento es necesario para garantizar que el punto de entrada del tráfico del cliente a la red IP/MPLS sea único, y así poder controlar el Caudal Nacional Agregado, el Caudal CDG Agregado, el Caudal Nacional Exclusivo y el Caudal CDG Exclusivo contratados por el cliente.

El funcionamiento deseado se consigue mediante manipulaciones en los anuncios de routing que los PEs hacen hacia los EDCs:

- Tráfico sentido EDC - PE: en el caso de RIP, un PE anunciará las redes, hacia el EDC, con una métrica diferente cuando actúa como principal que cuando actúa como backup, lo que permitirá al EDC enviar el tráfico hacia el PE deseado. En el caso de BGP se usarán atributos propios de este protocolo para alcanzar el mismo objetivo (típicamente el "MED").
- Tráfico sentido PE - EDC: se manipulará el atributo "local preference" de MBGP en la exportación hacia la VPN que los PEs hacen de las rutas recibidas de los EDCs, de manera que se prefieran las rutas exportadas desde el PE principal.

Redistribución entre protocolos en el EDC

Existen escenarios dentro del servicio en los que el EDC habla un protocolo de routing dinámico sobre la LAN del cliente (con routers del cliente) distinto del que habla sobre la MAN (con los PEs u otros EDCs). En estos casos, es necesario hacer redistribución de rutas entre ambos protocolos. Esta técnica es delicada pues puede provocar, si no se toman las medidas oportunas, bucles de routing que conduzcan a incomunicaciones del cliente. La situación es especialmente peligrosa en ubicaciones de cliente con doble EDC.

En las configuraciones estándar del servicio se aplican los mecanismos necesarios para evitar estos problemas. Típicamente:

- Si es necesario (depende del modelo de EDC) se modifican las preferencias (distancias administrativas) de los protocolos de routing en los EDCs, para conseguir que siempre se prefieran las rutas aprendidas por la MAN frente a las aprendidas por la LAN del cliente.
- En conexiones con doble EDC, se establecen filtros para evitar que un EDC aprenda rutas del otro a través de la MAN.

Conexiones entre emplazamientos del cliente paralelas a la Red de Banda Ancha

Cuando el cliente mantenga sus oficinas conectadas entre sí por otros medios alternativos a MacroLAN, será necesario hacer un estudio especial particularizado, con objeto de forzar a que el tráfico discurra por la Red adecuada.

En el caso de que el servicio contratado por el cliente sea MacroLAN con la facilidad de "Transporte Ethernet" las conexiones paralelas a la Red de Banda Ancha no están permitidas y será responsabilidad del cliente el hecho de que se formen bucles, lo cual impedirá el funcionamiento correcto de las comunicaciones del cliente. En el caso de requerirse conexiones paralelas en estos escenarios se necesitará un proyecto especial validado por Ingeniería de Servicios.

Conexión lógica "dual home" del CE a los PEs.

Para el soporte adecuado de BGP como protocolo de routing entre PEs y EDCs se requerirá en los PEs el soporte del marcado y filtrado de la comunidad extendida "Site of Origin (SOO)". Este mecanismo resulta necesario para evitar bucles de routing, debido a la conexión lógica "dual home" EDCs - PEs.

Esta funcionalidad es necesaria aplicarla porque confluyen de forma simultánea las siguientes circunstancias:

- Se configura BGP entre el EDC y el PE.
- Se hace "Override del AS" en los PEs.
- Las conexiones entre el EDC y el PE son "dual home" (La red del cliente se configura como un único Sistema Autónomo que resulta ser disjunto, pues las distintas sedes del cliente no se conectan directamente entre sí, sino a través de la red (Sistema Autónomo) del proveedor. Lo anterior implica que sea necesario activar la funcionalidad "Override AS" en las interfaces del PE con los correspondientes equipos del cliente. Si no, el propio mecanismo de prevención de bucles del BGP impediría la comunicación entre sedes del cliente.).

Es necesaria la asignación de un SOO por cada oficina/sede. Este parámetro debe ser único y distinto en cada oficina de cliente. El parámetro SOO no se asignará directamente, sino que se construirá en base al parámetro "identificador de oficina", asociado a cada sede del cliente.

Protocolos de Routing en la LAN de cliente

Sobre la LAN del cliente, el servicio contempla, de manera estándar, la utilización de los siguientes protocolos de routing:

- Sin routing dinámico. Lo único que se necesita es anunciar hacia la Red de Banda Ancha las redes directamente conectadas.

- Routing estático. El servicio permite configurar en el EDC las rutas estáticas que el cliente solicite. Para ello el cliente deberá informar de la red, máscara y "next-hop" para cada una de las rutas a configurar. Estas rutas se podrán anunciar a su vez hacia la Red de Banda Ancha. El problema de esta configuración, con routing estático, es que no permite el uso de caminos alternativos si es que existe esa posibilidad.

- RIPv2. Por defecto, el EDC solo anunciará hacia la Red de Banda Ancha, la red de la LAN del cliente directamente conectada. Si el cliente necesita anunciar otras redes además de la directamente conectada, deberá informar de cuáles son estas redes para añadirlas en el filtro correspondiente que controla los anuncios de routing desde el EDC hacia la Red de Banda Ancha. El EDC solo podrá anunciar rutas que él mismo tenga en su tabla, bien porque las haya aprendido dinámicamente o porque se le configuren de forma estática.

- OSPF [23]. En este caso, es necesario realizar una redistribución entre los protocolos sobre la LAN del cliente (OSPF) y sobre la MAN (generalmente RIP), con los riesgos de bucles de routing e incomunicaciones ya descritos en otros apartados. En los EDCs se aplican los mecanismos necesarios para evitar estos problemas.

Por defecto, el EDC solo anunciará hacia la Red de Banda Ancha, la red de la LAN del cliente directamente conectada. Si el cliente necesita anunciar otras redes además de la directamente conectada, deberá informar de cuáles son estas redes para añadirlas en el filtro correspondiente que controla los anuncios de routing desde el EDC hacia la Red de Banda Ancha. El EDC solo podrá anunciar rutas que él mismo tenga en su tabla, bien porque las haya aprendido dinámicamente o porque se le configuren de forma estática.

2.2.8 FACILIDADES

MacroLAN contempla las siguientes facilidades:

- Facilidad de traducción de direcciones (Network Adress Translation, NAT)
- Alojamiento de Oficina en el CDG
- Reserva de Caudal Plata
- Soporte de otros protocolos: Ethernet
- Redundancia
- Facilidad de Redirección Plus.
- Facilidad de Acceso a Supervisión (FAS)

A continuación se describen con mayor detalle cada una de ellas.

2.2.8.1 FACILIDAD DE TRADUCCIÓN DE DIRECCIONES NAT

La traducción de direcciones IP (NAT) [24], con o sin traducción de puertos (PAT) [25] se contempla de manera estándar en el servicio en distintas modalidades:

- **NAT estático**

Traducciones estáticas entre direcciones locales y direcciones globales. Hay una relación biunívoca entre direcciones locales y globales, de manera que cada dirección solo puede utilizarse en una traducción.

Esta es la modalidad que debe utilizarse cuando se quiere tener una relación fija entre dirección local y dirección global (p.ej. para hacer visibles servidores a través de una dirección global desde la zona exterior).

El cliente debe especificar las traducciones específicas que quiere hacer.

- **NAT dinámico**

Traducciones dinámicas entre un rango de direcciones locales y un rango de direcciones globales. En esta modalidad no existe una relación fija entre dirección local y global, siendo el propio EDC el que establece dinámicamente una traducción cuando es necesario.

El rango local tendrá siempre un número igual o mayor de direcciones que el rango global.

El número máximo de traducciones simultáneas viene dado por el número de direcciones del rango global.

El cliente debe especificar los rangos locales y globales con los que desea hacer las traducciones.

- **NAT dinámico con PAT**

Traducciones dinámicas entre un rango de direcciones locales y un rango de direcciones globales. En esta modalidad no existe una relación fija entre dirección local y global, siendo el propio EDC el que establece dinámicamente una traducción cuando es necesario.

Esta modalidad solo es aplicable a tráfico TCP o UDP, porque además de las direcciones hace una traducción de puerto. Esto permite establecer múltiples traducciones simultáneas para distintas direcciones locales usando una única dirección global.

El rango local tendrá siempre un número igual o mayor de direcciones que el rango global.

En esta modalidad el número de direcciones del rango global no limita el número máximo de traducciones simultáneas.

El cliente debe especificar los rangos locales y globales con los que desea hacer las traducciones.

En escenarios con redundancia de EDC en modo balanceo, el rango global debe tener al menos dos direcciones.

2.2.8.2 FACILIDAD DE ALOJAMIENTO DE OFICINA EN EL CDG

MacroLAN permite la contratación de los elementos de conectividad necesarios para que el cliente pueda integrar servicios de Hosting y ASP dentro de su red privada virtual. Estos elementos son los reflejados en la Tabla 6:

Elemento	Descripción
Acceso Zona CDG	- Accesos de 10, 100 y 1000 Mbps que permiten la conexión del EDC en el CDG a la red. - Contratación obligatoria cuando el cliente tiene presencia en el CDG.
Caudal metro	- Caudal de contratación obligatoria cuando el cliente tiene presencia en el CDG y no contrata un Caudal CDG Exclusivo. - Su contratación es incompatible con la del Caudal metro. - La contratación de este caudal permite cursar tráfico con destino a sedes situadas en la MAN de la misma provincia donde está ubicado el CDG. - Para comunicaciones del CDG con sedes en otras provincias es necesario contratar además el Caudal CDG o bien contratar únicamente el Caudal CDG Exclusivo.
Caudal CDG Exclusivo	- Se contrata únicamente para la sede CDG y para la Sede CDG virtual. - Es un elemento opcional y sólo se contrata cuando se requiere una comunicación de ámbito nacional con caudal exclusivo para el acceso

	de esa sede (sede CDG o Sede CDG virtual). - Su contratación es incompatible con la del Caudal metro. - Permite el intercambio de tráfico entre una sede ubicada en el CDG y cualquier otra sede del cliente que pertenezca a la misma MAN (ámbito provincial) o esté en otra provincia (ámbito nacional). - Tiene las mismas propiedades que el Caudal Nacional Exclusivo (granularidad, clases de servicio, etc.).
Caudal CDG Agregado	- Se contrata únicamente para la sede CDG. - Permite el intercambio de tráfico de ámbito nacional entre el CDG y otras sedes situadas en provincias diferentes. - Tiene las mismas propiedades que el Caudal Nacional Agregado (granularidad, clases de servicio, etc.). - Este elemento es opcional pues sólo es preciso contratarlo en los proyectos en los que existan al menos dos sedes (dos accesos) en el mismo CDG que requieran un caudal agregado y compartido para la comunicación de ámbito nacional.
Housing del EDC	- Permite dotar al EDC del espacio físico y alimentación necesarios para su correcta ubicación en el CDG

Tabla 6: Elementos contratables en alojamiento en CDG

Naturalmente, además de los elementos anteriores, es necesaria la contratación del EDC, con su correspondiente instalación, gestión y mantenimiento. Dicho elemento no está incluido dentro de esta facilidad porque no existe un EDC específico para ser alojado en el CDG.

La contratación del Caudal Nacional Exclusivo es compatible con la contratación de Caudal CDG Exclusivo en la misma sede. Sin embargo deberá tenerse en cuenta una limitación causada por los EDCs en lo relativo a las clases de servicio. Para Caudal Nacional Exclusivo y Caudal CDG de una misma clase de servicio (Plata u Oro), no es posible garantizar cada caudal por separado. Esto se debe a que el EDC sólo dispone de una cola por clase de servicio y no por tipo de Caudal. Esta limitación no aplica a la clase Multimedia. Gracias a la integración de los CDGs en las redes de Telefónica Empresas (disponiendo de nodos de red en estos centros) y a la economía de escala que proporciona la concentración de comunicaciones hacia estos centros, Telefónica Empresas proporciona al cliente las ventajas y servicios de sus CDGs con los mejores precios en sus acceso y comunicaciones.

Así, la facilidad de Alojamiento de Oficina en CDG se adapta perfectamente a escenarios de cliente en los que se dé alguna de las siguientes circunstancias:

- Las sedes del cliente se encuentran en algunas de las MANs en las que Telefónica tiene presencia de CDG (Madrid y/o Barcelona).
- Las sedes del cliente no pertenecen a MANs con presencia del CDG, pero el tráfico entre ambos elementos (CDG y dependencias de cliente) es fundamentalmente de bajada desde el CDG (servidor Web o FTP alojado en el CDG).

En estos casos los conceptos facturables y por tanto los precios que aplican para especificar el tráfico de cliente son el Caudal Acceso CDG y el Caudal Nacional CDG.

Además, el cliente tiene la posibilidad de beneficiarse de las ventajas económicas del Caudal CDG Nacional Exclusivo en una sede de una provincia en la que no haya CDG para cursar el tráfico desde una sede principal de su RPV (que llamaremos Sede CDG virtual) hacia su Oficina del CDG.

Con esta posibilidad la Sede CDG virtual elegida por el cliente puede comunicar tráfico hacia su oficina del CDG usando el Caudal CDG Nacional Exclusivo en lugar del Caudal Nacional Agregado o el Caudal Nacional Exclusivo.

Con esto facilitamos a los clientes las soluciones de redundancia servicios, redundancias de sus Centros de Redundancia de Datos o simplemente la comunicación nacional entre dos sedes de tráfico intenso siendo una la Sede ubicada en el CDG y otra la sede de la RPV identificada como Sede CDG virtual.

La figura 15 muestra un esquema de esta facilidad y los elementos que la componen.

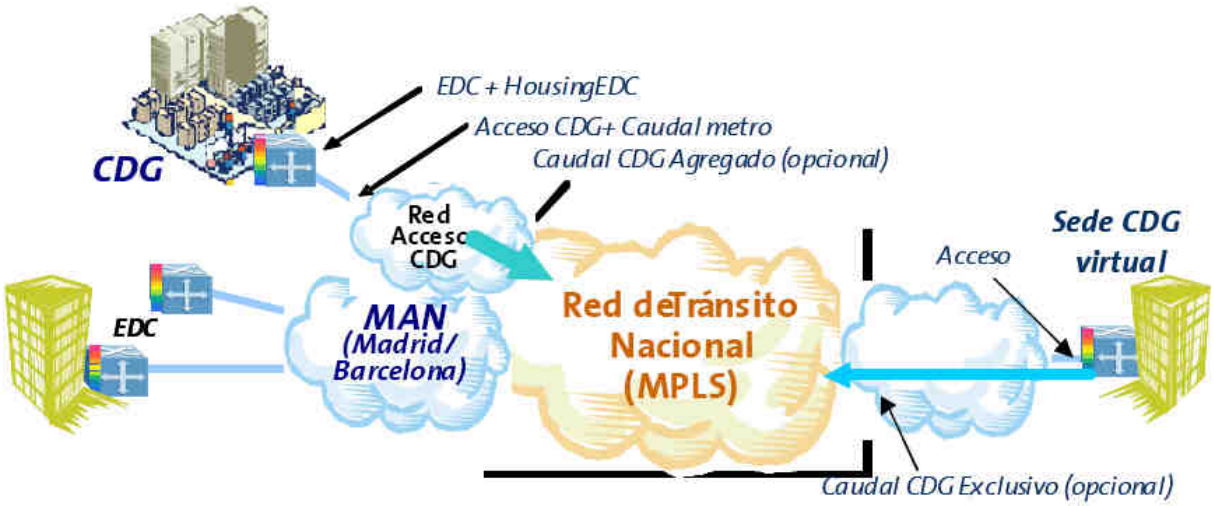


Figura 15: Macrolan con alojamiento en CDG

2.2.8.3 FACILIDAD DE RESERVA DE CUADAL PLATA

Cuando se contrate Clase Plata para los caudales de acceso a la red, se podrá diferenciar en el tráfico que se inyecta entre un tráfico "Plata reservado" (típicamente de Intranet) y un tráfico "Plata restante" (típicamente Internet) mediante el concepto de Reserva de Caudal Plata.

La Reserva de Caudal Plata añade, dentro del EDC y en sentido hacia la MAN, un nivel adicional de diferenciación del tráfico dentro de la clase Plata que permite tratarlo de forma diferenciada. Ofrece la posibilidad de que el cliente pueda hacer una reserva de caudal, dentro del caudal Plata que tenga contratada, para que la citada reserva esté disponible para cursar un determinado tipo de tráfico en caso de congestión del acceso del EDC en sentido hacia la MAN. Dicha reserva, permite al cliente un nivel más de clasificación dentro del tráfico plata tradicional que queda desglosado en dos partes: "Plata reservado" y "Plata restante". En caso de congestión, el "Plata reservado" tiene garantizado un caudal

determinado. Cuando no hay congestión los tráficos pueden reaprovechar los caudales sobrantes pudiendo cursar por encima de lo garantizado para dicha clase.

La Reserva de Caudal Plata aplica a los siguientes caudales del servicio: Caudal Nacional Exclusivo, Caudal Metro y Caudal CDG Exclusivo. Otros tipos de Caudal del servicio no disponen de la posibilidad de Reserva de Caudal Plata (no aplica para Caudal Nacional Agregado y Caudal CDG Agregado).

La reserva de caudal plata sólo se puede provisionar en los routers del servicio MacroLAN, en concreto, routers Cisco y Teldat.

El cliente debe determinar, en cada una de las sedes en las que contrate Clase de Servicio Plata (para los caudales: Caudal Nacional Exclusivo Plata, Caudal CDG Exclusivo Plata o Caudal Metro Plata) si desea o no disponer de una Reserva de Caudal Plata. Si no se indica lo contrario, por defecto se considera que no habrá diferenciación de tráficos dentro de la Clase de Servicio Plata. En caso afirmativo, el cliente debe indicar qué ancho de banda, dentro del Caudal Plata contratado, desea proporcionar a su tráfico “Plata reservado”, de forma que el resto del Caudal Plata no reservado será utilizado por el tráfico “Plata restante”.

Se supondrá por defecto que el tráfico de menor criticidad será el de Internet. Si el cliente no quisiera considerar Internet como el tráfico de menor criticidad, deberá indicar las características del tráfico Plata reservado, es decir, para qué tipo de tráfico desea hacer la Reserva de Caudal Plata.

El parámetro del ancho de banda de Reserva de Caudal Plata adopta una serie de valores discretos en Mbits iguales a los valores de los caudales del servicio, por lo que nunca podrá superar el valor de caudal asociado a la Clase Plata.

La Reserva de Caudal Plata podrá contratarse tanto en sedes nuevas como en las ya en planta, siempre y cuando se disponga del correspondiente caudal Plata. Su valor se podrá modificar en cualquier momento previa petición del cliente. Esta modificación supone el pago de un concepto facturable Si el cliente contratara Reserva de Caudal Plata abonará el importe de la activación de esa reserva y un concepto facturable mensual por la prestación de la facilidad. La posterior modificación del valor concreto de Reserva de Caudal Plata supondrá de nuevo el pago del importe de activación de la reserva.

La Reserva de Caudal Plata forma parte del esquema de calidad de servicio (QoS) del servicio MacroLAN y, por tanto, es compatible con todas las facilidades del servicio. Sin embargo, hay que tener en cuenta que la facilidad “Transporte Ethernet” sólo se puede ofrecer con los switches homologados para el servicio, mientras que la Reserva de Caudal Plata sólo se puede dar con los routers, por lo que en la práctica no es posible la convivencia de ambas facilidades.

2.2.8.4 FACILIDAD DE SOPORTE DE OTROS PROTOCOLOS: ETHERNET

Por defecto, los EDC de MacroLAN permiten cursar tráfico IP del cliente. Es decir, hacen un routing del tráfico que el cliente inyecta en el EDC a través de sus interfaces LAN.

Opcionalmente, los EDC de MacroLAN permiten transportar tráfico Ethernet. Es decir, el tráfico se encamina a una sede u otra en función de las direcciones de nivel 2, no en función de direcciones IP.

Esta facilidad debe contratarse para cada una de las sedes del cliente.

Esta facilidad tiene varios condicionantes:

- El tráfico Ethernet puede transportarse exclusivamente entre sedes del cliente que estén conectadas a una misma red MAN; es decir, su cobertura está restringida al entorno provincial.
- Esta facilidad no se soporta sobre accesos MacroLAN con Caudal Nacional Exclusivo o con Caudal CDG Exclusivo.
- No soporta clases de servicio
- No puede aplicarse sobre escenarios con EDC redundante
- El EDC Cisco2621XM, Cisco 1841, Cisco 2801, Atlas 360, Atlas 250 y Atlas 150 no soporta esta facilidad

2.2.8.5 FACILIDAD DE REDUNDANCIA

Los escenarios de redundancia se aconsejan para sedes del cliente que requieran la máxima disponibilidad.

La figura 16 muestra los escenarios de redundancia que son viables actualmente.

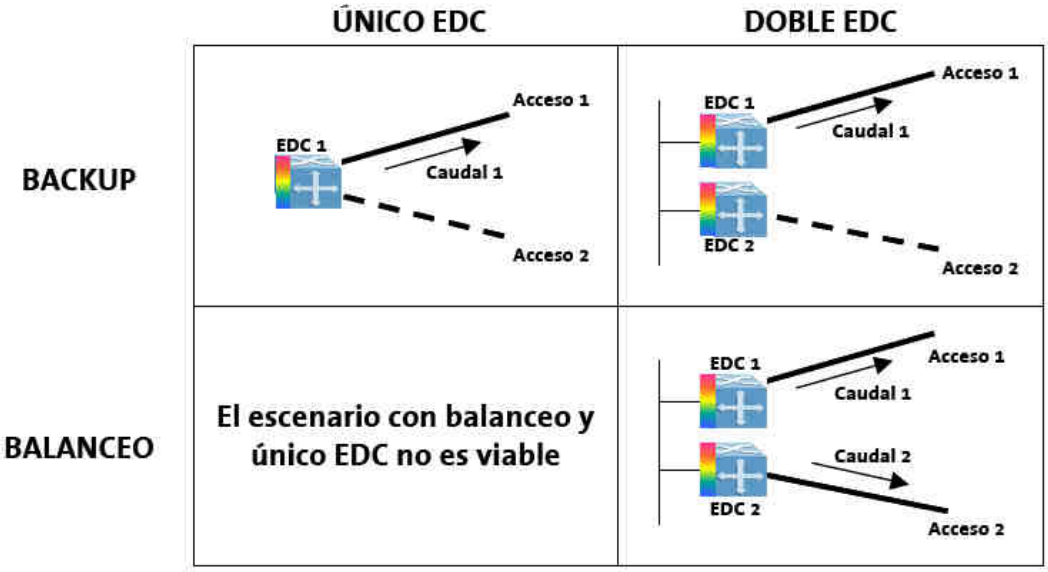


Figura 16: Redundancia en servicio macrolan

Es necesario tener en cuenta las siguientes características en los escenarios de redundancia reflejados en la tabla 7. Hay consideraciones específicas para los accesos a 2M que se indican posteriormente en este apartado:

- Siempre hay dos accesos, el principal y el diversificado. Las velocidades de estos accesos pueden ser distintas permitiéndose los escenarios de redundancia con respaldo degradado, es decir, un acceso diversificado de menor velocidad que el acceso principal.
- Existen dos modalidades de redundancia: redundancia con backup y redundancia con balanceo.
    - La redundancia con backup implica que sólo uno de los dos accesos disponibles (el "Acceso 1"), está cursando tráfico en un momento dado. El otro acceso ("Acceso 2"), se activa únicamente en caso de caída del primero. Por tanto, el cliente sólo contrata un caudal ("Caudal 1"), asociado al "Acceso 1".
    - La redundancia con balanceo implica que los EDC hacen un reparto de caudal por ambos accesos, de modo que ambos están cursando tráfico en un momento dado. En esta modalidad se contratan dos caudales "Caudal 1" y "Caudal 2" que son idénticos(Los caudales contratados son idénticos. Sin embargo, es posible que a efectos prácticos, el caudal real cursado puede no ser exactamente simétrico). El resto de elementos, EDC y acceso, también son idénticos. Si uno de los accesos cae, el otro acceso sólo podrá asumir el tráfico del acceso caído con la limitación del caudal contratado, por lo que el caudal total disponible en una caída será la mitad del que se dispone cuando los dos accesos están operativos

	Modo Backup				Modo Balanceo			
Principal	2M	10M	100M	1000M	2M	10M	100M	1000M
2M	Si				Si[2]			
10M	Si	Si				Si		
100M	Si	Si	Si				Si	
1000M	Si	Si	Si	Si				Si

Tabla 7: Redundancias en servicio Macrolan

En el caso respaldo de 2 Mbps en Modo Balanceado no existe el concepto de acceso diversificado para esta velocidad

- No se requiere la contratación de Caudales de ningún tipo en el Acceso diversificado en modo Backup.
- Si el respaldo es degradado, su capacidad de cursar tráfico será la siguiente según los caudales contratados en el acceso principal:
    - Caudal metro. Si el caudal metro contratado en el acceso principal es superior a la velocidad del acceso de respaldo, entonces el respaldo permitirá cursar caudal metro hasta fondo de línea. En caso contrario, si el caudal metro del acceso principal es inferior a la velocidad del respaldo, el caudal metro será el mismo.

- Caudal Nacional Agregado y CDG Agregado. Este caudal no depende del acceso, por lo que no aplica ninguna consideración.
- Caudal Nacional Exclusivo y Caudal CDG Exclusivo. El criterio es el mismo que para el caudal metro, ya que estos dos caudales son específicos y dedicados para un acceso concreto.
- En caso de que el cliente haya contratado clases de servicio para el tráfico en el acceso principal, se definirá un reparto de clases de servicio para el tráfico en los respaldos degradados que por defecto será proporcional al acceso principal pero se permitirá que esa asignación por defecto sea modificada a petición del cliente.

- Los escenarios con accesos diversificados de 2 Mbps aplican únicamente para los accesos a la red metropolitana (accesos desde la sede del cliente). En el CDG no se disponen de accesos de 2 Mbps
- Para cada modalidad, existe la posibilidad de utilizar uno o dos EDC ("EDC 1" y "EDC 2").

Hay una excepción: el caso de la modalidad de balanceo sólo es viable con dos EDC.

- En los escenarios con doble EDC no es posible aplicar la facilidad de Transporte de Protocolo Ethernet. Es decir, los equipos EDC funcionarán como routers y en ningún caso hará conmutación del tráfico a nivel Ethernet.

Consideraciones específicas para el uso del acceso MacroLAN de 2 Mbps con la facilidad de redundancia:

- A diferencia de lo que ocurre para los accesos de 10 Mbps, 100 Mbps y 1000 Mbps, para la redundancia en modo balanceo, deben contratarse dos accesos MacroLAN de 2 Mbps iguales puesto que en MacroLAN no existe el concepto de acceso diversificado con modalidad compartida (en el que ambos accesos pueden funcionar simultáneamente) para esta velocidad.
- Respecto al caudal metro asociado, el valor predefinido para esta velocidad de acceso es de 2 Mbps

El escenario de conexión con redundancia de EDC y acceso (un acceso por cada EDC) no plantea restricciones para la elección de EDC.

2.2.8.6 FACILIDAD DE REDIRECCIÓN PLUS

La funcionalidad "Redirección Plus" permite que un cliente con un punto central (CPD) y una serie de sedes remotas que se conectan a dicho punto central, disponga de un punto central de respaldo en el que replica todos sus servidores y aplicaciones. Bajo petición del cliente se actúa manualmente sobre la red y se redireccionan todo el tráfico de las sedes remotas hacia el punto central de respaldo. La vuelta atrás también se realiza manualmente bajo petición del cliente. El punto central de respaldo puede estar o no en la misma MAN donde se sitúa el CPD principal.

La facilidad de Redirección Plus tiene las siguientes limitaciones:

- Se utiliza para tráfico IP, es decir, no aplica al tráfico cursado mediante la facilidad de Transporte de Protocolo Ethernet. En el caso de escenarios mixtos (tráfico IP y tráfico Ethernet), la facilidad sólo aplica al tráfico IP.
- En caso de que ambos puntos centrales, principal y respaldo, tengan que intercambiar tráfico, se requiere que los servidores ubicados en ambos puntos centrales tengan doble direccionamiento.

Los escenarios típicos de aplicación de la facilidad de Redirección Plus se encuentran en aquellas empresas que manteniendo una topología en estrella de sucursales accediendo a un Centro de Cálculo de Cliente necesitan disponer de mecanismos que les faciliten desviar bajo demanda su Red de Cliente MacroLAN hacia otro Centro de Cálculo de Respaldo. Este nuevo Centro de Cálculo de Respaldo actuaría como backup en caso de desastre y podría pertenecer al cliente o bien subcontratarse a alguna empresa especializada en la explotación de este tipo de Centros de Respaldo.

La facilidad de "Redirección Plus" es compatible con todas las prestaciones definidas de MacroLAN, a excepción de la Facilidad de Transporte de protocolo Ethernet, tal y como se indicó anteriormente.

El tiempo requerido por el cliente para la activación de la facilidad de Redirección Plus no podrá ser inferior a una hora desde que se reciba toda la información necesaria por parte del cliente. Cuando el cliente requiera una prueba de funcionamiento general es preciso que toda la información del cliente necesaria para la activación de la facilidad sea recibida al menos con un día de antelación. Existe la limitación del número de pruebas de funcionamiento que puede solicitar un cliente a lo largo de un año, quedando fijado a cuatro.

2.2.8.7 FACILIDAD DE ACCESO A SUPERVISIÓN (FAS)

Mediante esta facilidad se habilitan los mecanismos necesarios en la red del cliente para que éste pueda realizar consultas en modo lectura sobre los EDCs que componen su red.

Contratarán esta opción de gestión aquellos clientes que disponiendo de su propio sistema de gestión deseen incluir como elementos a supervisar, a fin de disponer de una monitorización global del estado de su red, los propios routers del servicio.

La Facilidad de Acceso a la Supervisión está restringida al protocolo SNMP (consulta de ciertas variables MIB y envío de traps básicos SNMP con la limitación de que la dirección IP origen de esos traps será la dirección IP de gestión). Esta opción estará disponible para equipos del servicio MacroLAN y será en todo momento de solo lectura, excluyéndose por tanto la modificación de parámetros de configuración de los routers. La plataforma y el software necesario para realizar las consultas y disfrutar de esta facilidad no están incluidos en el servicio y serán responsabilidad del cliente.

Si el cliente tiene en su RPV sedes con servicio MacroLAN y sedes con servicio VPN IP, si desea contratar la facilidad FAS sólo se le aplicará un concepto facturable a toda su RPV, permitiéndole con ello tener una visión global de su red mixta, independientemente de que sus sedes sean VPN IP o MacroLAN.

2.3 SERVICIO TRÁFICO LIMPIO

Los servicios de Tráfico Limpio Internet responden a las necesidades de protección y seguridad en la navegación de los usuarios. Las amenazas y problemas más comunes en la navegación son:

- Infección por Virus/Troyanos y Malware en general
- Control de la navegación
  - Por categorías de sites
  - Por contenidos
- Gestión de diferentes flujos de tráfico
  - Video, información, multimedia
  - Experiencia de usuario
  - Navegación
- Control y gestión de las políticas de la empresa
  - Quién hizo qué
  - Adecuación a la política de uso de medios

2.3.1 ESTADO DE INTERNET

Hoy en día, no sólo hay que preocuparse de las amenazas desde Internet sino las propias debilidades de los navegadores usados en el acceso, por ejemplo las últimas vulnerabilidades [26] mostradas en la figura 17.

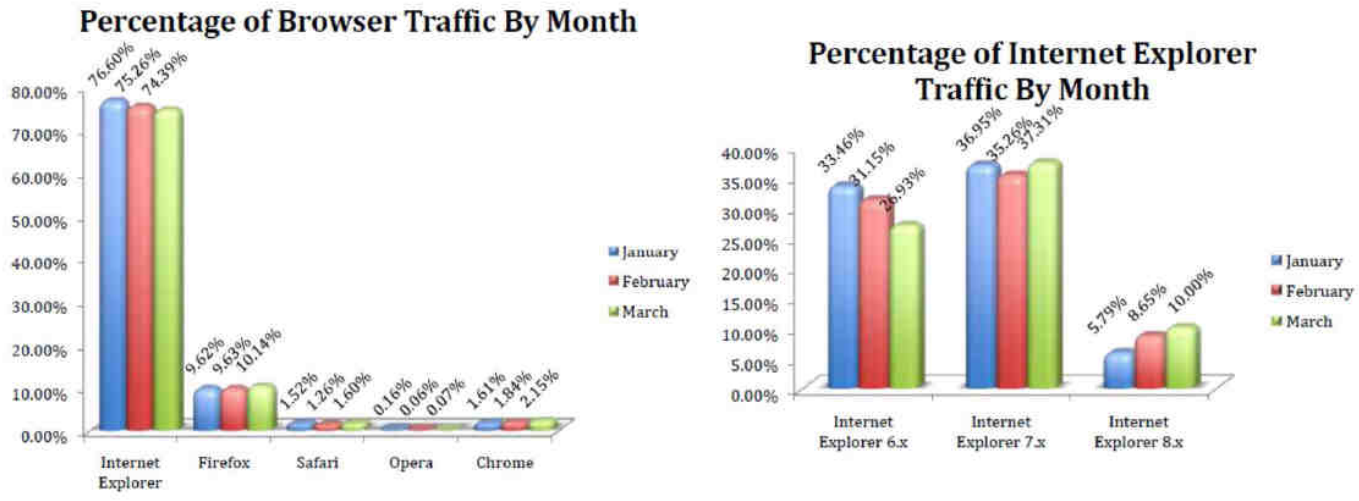


Figura 17: Tráfico internet por navegadores

En lo relativo a los contenidos, se observa que los grandes hosters (en especial EEUU) alojan por igual contenido legítimo e ilegítimo (figura 18).

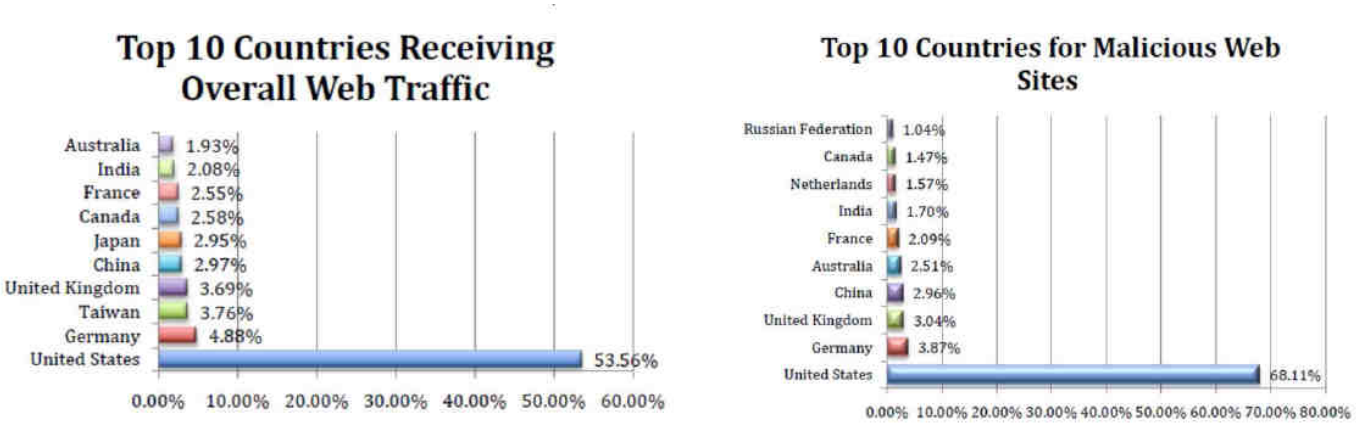


Figura 18: Origen del tráfico de internet y malware por países

La mayor amenaza a mitigar en la navegación web es actualmente la posibilidad de que los puestos de trabajo caigan en manos de redes de botnets (figura 19).

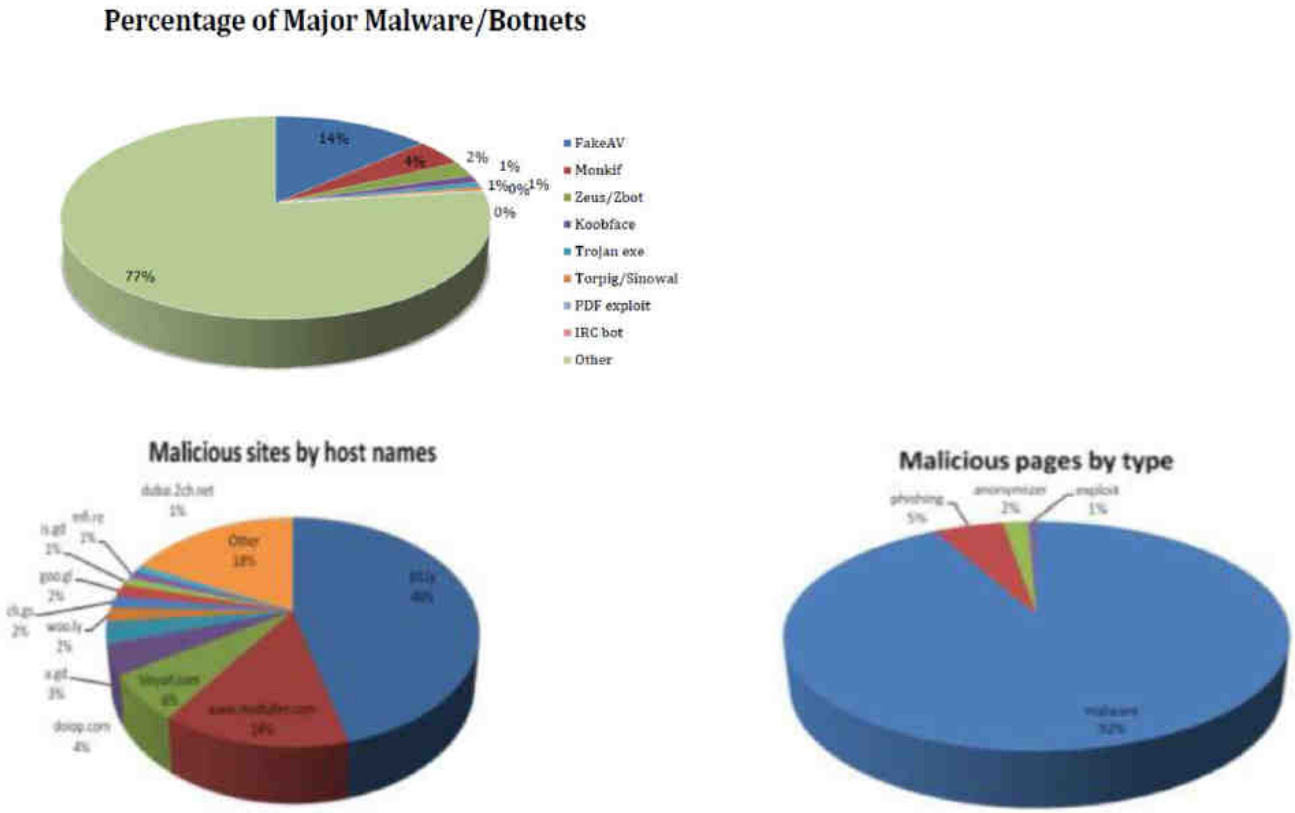


Figura 19: Orígenes del malware

2.3.2 DESCRIPCIÓN DEL SERVICIO

El servicio de Tráfico Limpio a Internet proporciona un modo de navegación seguro empleando una plataforma multicliente en alta disponibilidad con las funcionalidades fundamentales de Proxy [27], Cache [28], Antivirus y Filtrado de Contenidos, que funciona básicamente conectando la red privada virtual del cliente con la plataforma de navegación segura alojada en el CDG de Telefónica, la cual provee la salida a internet (figura 20)

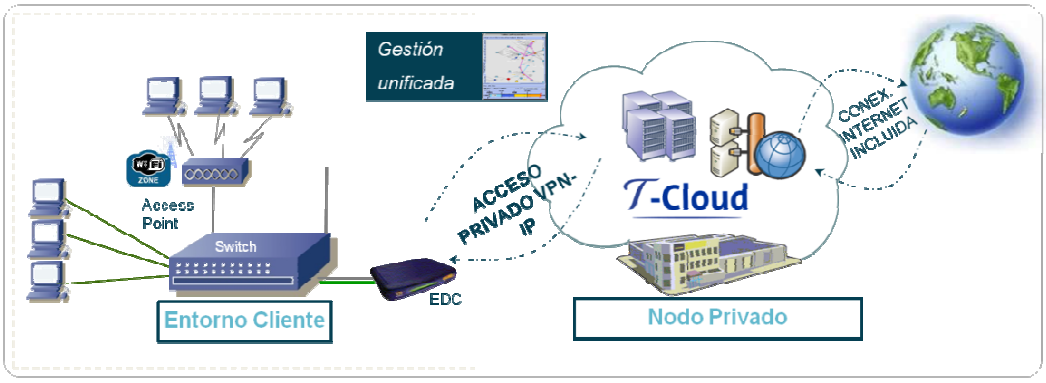


Figura 20: Esquema servicio Tráfico Limpio

En una arquitectura que proporciona un alto nivel de seguridad y rendimiento, asegurando escalabilidad y redundancia. Cada funcionalidad está construida sobre el líder de su industria en un modelo integrado (figura 21).

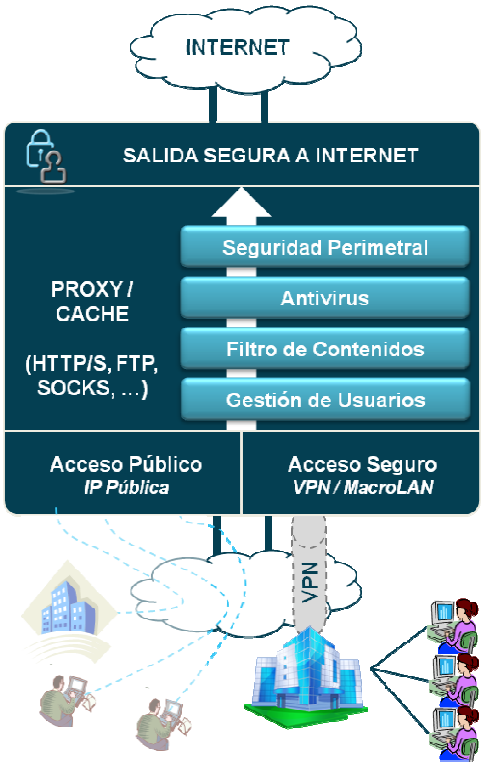


Figura 21: Niveles de seguridad en servicio Tráfico Limpio

El diseño de la solución adoptada para el despliegue en los CDGs del servicio de Tráfico Limpio Internet hace uso de dos módulos de plataforma de dichos CDGs. Estos módulos son los siguientes:

- **Módulo de Conectividad Internet (MCI):** Ofrece una plataforma de navegación que facilitará la conexión segura a Internet, independientemente del transporte utilizado hasta llegar a los CDGs
- **Módulo de Conectividad Privada (MCP):** resuelve los requerimientos que surgen de la conectividad Intranet de los clientes al CDG y de la integración con el resto de servicios del propio CDG.

La combinación de ambos módulos permite prestar el servicio de Tráfico Limpio Internet con todos los requisitos recogidos en el diseño y con parámetros de excelencia en cuanto a la disponibilidad y rendimiento de todas las plataformas desplegadas en los CDGs.

El servicio cuenta con las siguientes características principales:

- Navegación a través de proxy: HTTP, FTP
- Antivirus de navegación HTTP
- Filtrado de contenidos, que permitirá limitar las capacidades de acceso web de los usuarios mediante la clasificación de los contenidos y atendiendo siempre a las necesidades de los diferentes perfiles de navegación de cada organización.
- Informes que permitirán trazar el uso y consumos del servicio por parte de los usuarios.

El servicio proporcionará una serie de informes en el que se reflejarán datos relativos a la navegación y filtrado de contenidos accesibles por el Cliente.

La plataforma del servicio contempla los requisitos derivados de la concentración de diferentes clientes, dando solución a los siguientes problemas:

- Eficiencia de la plataforma: Mediante el uso de mecanismos de caching, definición de arquitectura escalable e implantación en una plataforma en alta disponibilidad.
- Facilidad de gestión: Empleándose un LDAP (Lightweight Directory Access Protocol) incluido en el servicio estándar, y pudiendo ser sincronizado con una base de datos del cliente (LDAP, Active Directory) permitiendo propagar las altas y bajas de los usuarios (Opcional).
- Control del caudal consumido por cada organización.
- Separación lógica de la seguridad relacionada con el acceso de cada organización.

La plataforma se ha diseñado sobre la base de una arquitectura flexible y escalable que permite la agregación de blade servers y servidores para incrementar capacidad bajo demanda para las funcionalidades de seguridad perimetral, servidor de contenidos, antivirus y filtrado de contenidos.

Tanto el módulo de conectividad privada como el módulo de conectividad Internet ya se encuentran implantados en las plataformas de los CDGs y se debe, por tanto, únicamente realizar la provisión y preparación de dichos módulos para el cliente.

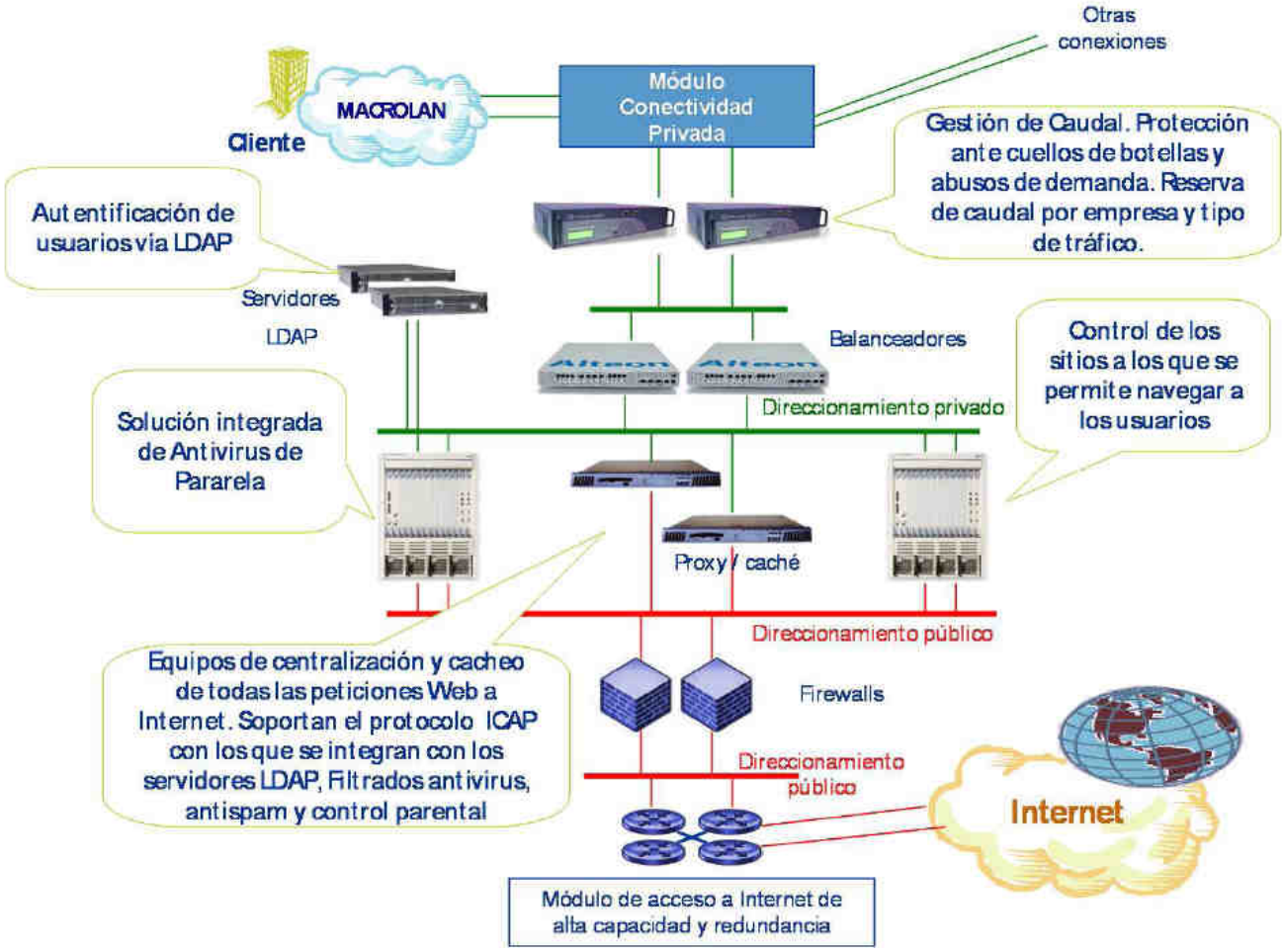


Figura 22: Esquema de red del servicio Tráfico Limpio

La figura 22 muestra un esquema de cómo viaja el flujo de datos a través de la plataforma y los diferentes niveles de seguridad y procesos que son llevados a cabo para garantizar la seguridad en la navegación.

2.3.2.1 SERVICIOS ASOCIADOS

MÓDULO DE CONECTIVIDAD A INTERNET

Solución de conectividad a Internet que soporta:

- Navegación http/s, ftp
- Caching
- Seguridad perimetral
- Balanceo de carga
- Antivirus http
- Filtrado de contenidos (control parental)
- Limitación de tráfico
- Gestión centralizada de usuarios

La administración de la solución completa estará a cargo de Telefónica.

La navegación soportará una tasa de concurrencia y anchos de banda que dependerán de la modalidad contratada por Transacciones Inmobiliarias S.A. y que se detallan en el apartado anterior.

MÓDULO DE CONECTIVIDAD PRIVADA

El servicio de Tráfico Limpio Internet requiere el uso del Módulo de Conectividad Privada (MCP), el cual resuelve los requerimientos que surgen de la conectividad Intranet de los clientes a los CDGs, y de la integración con el resto de servicios módulos de los mismos.

Todo ello, a través del compromiso de Telefónica, se deberá traducir en un servicio cuyas características principales sean:

- Solución con altos niveles de seguridad
- Solución con evolución tecnológica continua, adaptando nuevas funcionalidades y prestaciones
- Modelo de facturación del servicio con costes fijos, controlados y predecibles
- Deberá permitir el acceso universal de los empleados del cliente
- Deberá permitir acotar niveles de acceso a los recursos internos
- Proporcionará soporte flexible al teletrabajo eventual y permanente

SERVICIOS DE ADMINISTRACIÓN

Para la administración/gestión de estos equipos se reservarán interfaces de red (al margen de los interfaces de servicio) dedicados exclusivamente para tareas de gestión incluyendo gestión, monitorización, backups.

Mediante estos interfaces se procederá a la integración de dichos equipos en el módulo de gestión de los CDGs de Telefónica.

Cabe destacar que el módulo de gestión también proporcionará la conectividad entre los mencionados equipos y su correspondiente consola de seguridad. Esta consola consiste en el sistema de gestión Check Point Provider-1 [29], configurado en alta disponibilidad y gestionado/administrado desde el SOC (Security Operations Centre) ubicado en el Centro de Gestión de Aplicaciones y Servicios (CeGAS) de Julián Camarillo 6.

La administración del servicio se realizará desde el SOC (Security Operations Centre): Ubicado en el CDG y desde él se gestionarán y monitorizarán de modo centralizado los dispositivos de seguridad existentes y realizando las siguientes tareas:

- Mantiene la base de datos de los clientes.
- Recoge toda la información de los equipos de seguridad gestionada de los clientes.
- Es donde se generan las alarmas y se analizan las peticiones de cambios de configuración de los clientes.
- Lugar donde residen los analistas de seguridad.
- Los analistas analizan los resultados obtenidos por los sensores.
- Mantiene el Report Center y los webs seguros de los clientes.

Este tipo de servicio es, sin duda, el punto de más experiencia demostrada por Telefónica. Organizan su actividad de explotación de sistemas y plataformas con base en una metodología que describe los procesos relacionados con el ciclo de vida de un sistema en producción, normalizando las actividades de provisión, paso a explotación, monitorización y operación, gestión de incidencias y escalados, atención de incidentes de seguridad, planificación de infraestructuras, etc.

Los procesos relacionados con dicha actividad, bien implantados dentro de la organización en un ciclo que dura ya más de diez años, son elementos vivos y están sujetos a un proceso de mejora continua estructurado en Centros de Competencia Tecnológica (CCTs) que han sido diseñados y estructurado para cumplir las mejores prácticas de explotación de IT, es decir ITIL.

El personal de operación se distribuye en centros de competencia tecnológica que permiten un alto grado de especialización, así como establecer fronteras de responsabilidad absolutamente claras en lo relativo a la explotación, además de permitir el escalado y dimensionamiento en función de la entrada de nuevos clientes o el crecimiento de necesidades (servidores, usuarios o aplicaciones).

Entre los paradigmas de la organización, por lo que a la operación se refiere se cuentan:

- La punta tecnológica, tanto desde la perspectiva de los sistemas donde las inversiones en sistemas de soporte a la operación (OSS) son ingentes, así como desde la perspectiva del personal, contándose con los profesionales más reconocidos del sector, en atención a las principales tecnologías en operación
- Las alianzas estratégicas, donde se cuenta con un extraordinario modelo de terceros que nos permite ofrecer las tecnologías más diversas, con proveedores líderes en el mercado que se implican en el ciclo de vida completo de los servicios que se ofrecen. En este sentido y a modo de ejemplos:

- Los sistemas de soporte a la operación se basan en productos y servicios de HP
- Los sistemas de almacenamiento se basan en productos y servicios de EMC.
- Los sistemas y herramientas de backup usan productos y servicios de Veritas.
- Los sistemas de seguridad gestionada usan productos y servicios de ISS.

En definitiva, una organización que conoce qué se ha de hacer para operar un sistema, que conoce y cuenta con una descripción de cómo se hace tanto en el nivel de detalle, mediante el catálogo de procedimientos de operación de las diferentes plataformas, como desde la perspectiva del proceso, donde siempre existen un conjunto bien definido de entradas y salidas.

Nuestra propuesta para este servicio cuenta con las siguientes características:

Centro de Competencia Tecnológica de Seguridad

El CCT de Seguridad lo forman profesionales, herramientas y procedimientos (figura 23). Se conoce comúnmente como SOC (Security Operations Centre), de Telefónica. Adicionalmente se ha habilitado una zona especial dentro del edificio situado en Julián Camarillo, 6 donde se centralizan algunas de las actividades relacionadas con seguridad, concentrándose consolas, herramientas de administración y monitorización de elementos de seguridad, habiéndose habilitado una sala especial para el tratamiento de incidentes graves de seguridad que requieran de análisis y despliegue de estrategias y contramedidas con carácter especial.

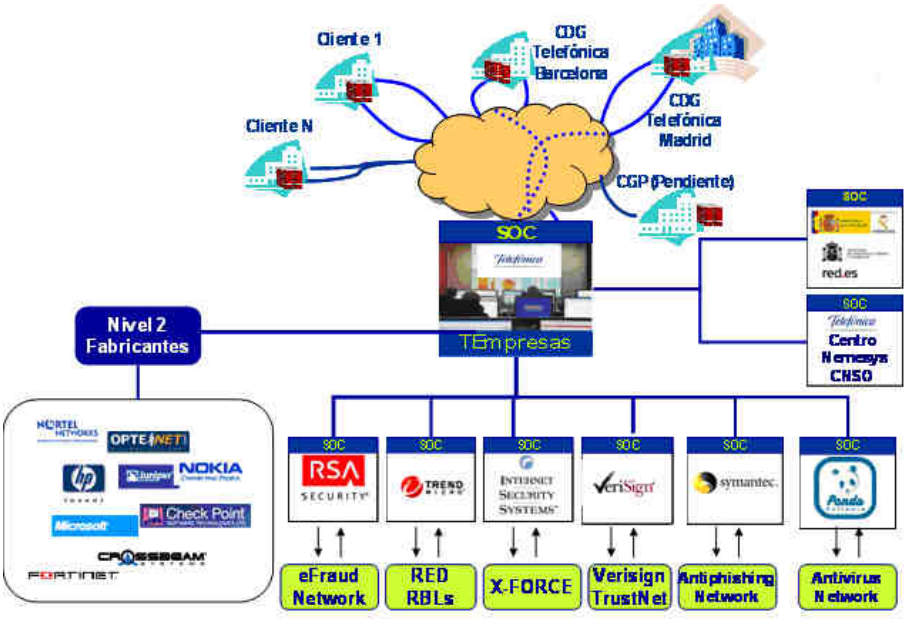


Figura 23: Centro de Competencia Tecnológica de Seguridad

Cadena de Soporte y Atención al Cliente

En las labores de operación, Telefónica estructura su CCT de seguridad según un modelo en tres capas que se describen brevemente a continuación:

- **Nivel 1:** Son el interfaz con el cliente. Tienen conocimiento básico de los servicios y plataformas del cliente. Tienen conocimiento detallado acerca del catálogo de servicios de seguridad siendo capaces de clasificar la gravedad de los problemas y articular en función, los procedimientos de escalado. Cuentan con el listado completo y contactos de las diferentes figuras participantes en la resolución de cualquier situación.

- **Nivel 2:** Lo configura el personal asociado directamente con el CCT de Seguridad. Son expertos en las tecnologías objeto del servicio. Cuentan con toda la información del cliente normalizada bajo los estándares de Telefónica lo que les permite una rápida localización en el supuesto de necesitar ejecutar alguna consulta para la resolución de una petición del cliente. Son responsables del mantenimiento de la documentación relacionada con la instalación del cliente. Se encargan de las labores de administración y operación de las plataformas. Son responsables de la validación de plataformas en el proceso de paso a explotación, verificando que éstas son conformes a los estándares definidos por los Procedimientos Operativos de Seguridad (POS) de la organización, valor que sólo una organización con el bagaje de Telefónica puede aportar. Se encarga del grueso de la actividad de operación y mantenimiento de plataformas bien directamente o bien delegando algunas facetas en centros de competencia relacionados.

- **Nivel 3:** Este nivel está determinado por un conglomerado de recursos y flujos de trabajo. Está destinado a la resolución de problemas cuyo calado exige atribuciones especiales desde el punto de vista del análisis y resolución del problema. El grueso de los recursos pertenece a los fabricantes y se articulan vía soporte técnico mediante los flujos de trabajo establecidos en relación a cada tecnología. En general el CCT de seguridad contactará en función de la gravedad de la situación, con un proveedor de servicios de soporte que permite la resolución de problemas comunes o bien con el fabricante directamente utilizando los Sistemas de Ticketing habilitados al efecto.

A grandes rasgos mencionar que los accesos son permitidos únicamente al grupo de Administradores del CDG.

Cada uno de estos accesos están securizados por una serie de firewalls de infraestructuras que se encargan de que los accesos sean única y exclusivamente los deseados.

2.4 SERVICIO BACKUP REMOTO

Este servicio ofrece la capacidad de realización de backup de datos (sistemas de ficheros, incluidos ficheros abiertos) y backup online de aplicaciones de máquinas NO alojadas en nuestros CDGs, aprovechando las excelentes infraestructuras desplegadas en dichos centros.

Las comunicaciones utilizadas para realizar dichos backups serán VPNs (Macrolan) o comunicaciones públicas vía Internet.

No está dentro del ámbito de este servicio el realizar copias de seguridad del tipo Baremetal, es decir, el poder restaurar un servidor completo como una imagen de este en un momento dado. El Backup Remoto realiza las restauraciones a nivel de fichero. Pueden restaurarse todos los ficheros de una máquina pero ello no garantiza la consistencia del sistema.

El servicio permite realizar backup en modo servicio, siguiendo las políticas estándar del servicio o adaptarse a las necesidades particulares de cada organización, permitiendo diseñar las políticas de backup deseadas.

Las políticas (Policy) se caracterízan por 3 elementos:

1. De qué información se hace backup (origen, tipo, exclusiones, inclusiones). A esto se le llama Datasets.
2. La planificación: a qué hora empieza o la ventana de duración.
3. El periodo de retención: cuándo caducan los datos (en número de días, o una fecha final o que no caduquen nunca).

3.4.1 NECESIDADES QUE CUBRE

El Servicio Backup Remoto de Información es una funcionalidad horizontal de amplio espectro. Los clientes potenciales del Servicio son organizaciones con infraestructura desplegada en ubicaciones remotas a los CDGs que requieran backup de su plataforma.

También es útil para clientes con necesidad de implementar soluciones de BRS, aunque es importante tener en cuenta que las copias del servicio Backup Remoto de Información se realizan a nivel de fichero y en ningún caso se generan imágenes de servidores para realizar restauraciones en modo Disaster Recovery [30].

3.4.2 SISTEMAS Y APLICACIONES SOPORTADAS

Los sistemas operativos y las aplicaciones de las cuales se podrá realizar backup se detallan a continuación:

SISTEMAS OPERATIVOS

Apple Macintosh OS.x
Free BSD
HP-UX
IBM AIX
Iomega
Linux
Microsoft Windows
Novell NetWare
Novell OES 2
Novell OES SP2
SCO UNIX
Sun Solaris
VMware ESX
VMware vSphere 4

APLICACIONES

IBM DB2
IBM Lotus Domino
Microsoft Exchange
Microsoft SharePoint
Microsoft SQL Server
NDMP para filers de NAS
Oracle, Oracle RAC
VMware

3.4.3 VENTAJAS DEL SERVICIO

Las principales ventajas de este servicio son:

- Posibilidad de realización de backups remotos de información sobre una plataforma alojada en el Centro de Datos.
- Acceso a recursos y niveles de especialización tecnológica, evitando problemas de obsolescencia tecnológica.
- Sistema de gestión de soportes de backup propio, alojadas en los propios centros de datos aprovechando los excelentes protocolos y medidas de seguridad, así como infraestructuras dedicadas a tal efecto.
- Permite liberar recursos para tareas más estratégicas o de mayor valor para la organización, permitiendo a ésta centrarse en su negocio core.
- El servicio de Backup asegura la calidad del servicio mediante Acuerdos de Nivel Servicio.

3.4.3.1 DEDUPLICACIÓN

La deduplicación es una funcionalidad implementada dentro del servicio que permite un uso más eficiente de la plataforma, resultando así en un ahorro de costes para el cliente, así como una reducción en los tiempos de backup y restore.

Según estudios, la información contenida en servidores pertenecientes a una misma organización suele estar duplicada en varios de los servidores [31], de manera que una vez almacenado un fichero o porte de él, es posible almacenar sólo un puntero para las sucesivas copias que de él aparezcan durante el backup, como se puede ver en la figura 24.

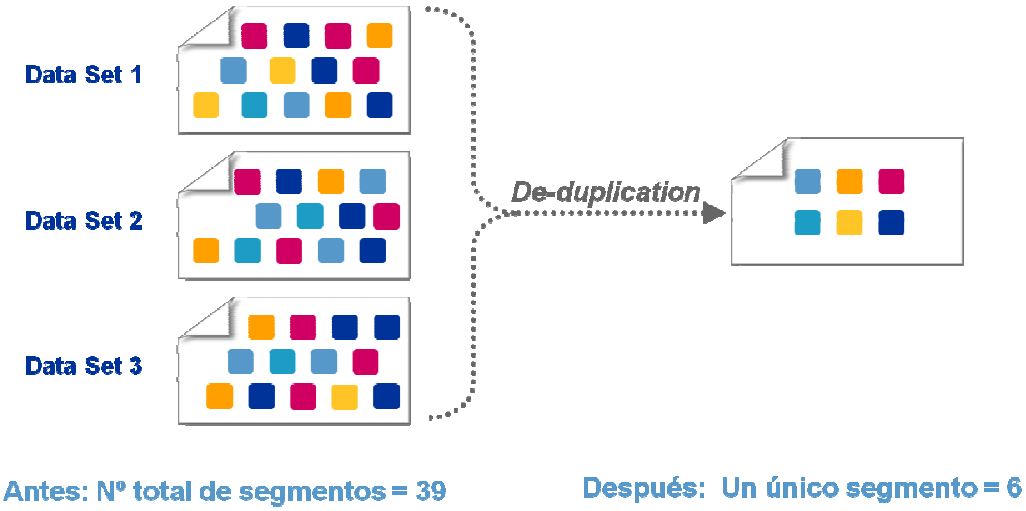


Figura 24: Deduplicación

3.4.4 CAPACIDADES DEL SERVICIO

El servicio base del Backup Remoto de Información permite las siguientes capacidades:

- Backup de directorios, ficheros abiertos vía LAN utilizando nuestra red hasta los CDGs.
- Funcionalidad de notificación de backups erróneos.
- Portal de visualización de informaciones del funcionamiento de las copias.
- Cifrado de la transmisión de los backups.
- Capacidad de auto provisión por parte del cliente en actividades como la definición de políticas, activación de backups o restores puntuales, mediante la asignación de un dominio, usuario y contraseña únicos para cada cliente.

3.4.4.1 ADMINISTRACIÓN DE ACTIVIDADES POR PARTE DEL CLIENTE

El servicio de Backup de Información permite que el cliente pueda administrarse el mismo una serie de tareas o actividades reduciendo así tiempos de espera y tramitaciones de peticiones, agilizando así el servicio y dándole al cliente total libertad para administrar ciertas tareas del servicio.

La provisión por parte del cliente se controla mediante la creación de un dominio al que el cliente accederá mediante un usuario y contraseña. Al crear el dominio, se definirán los permisos que pueden ejercer los clientes sobre ciertas acciones que describiremos a continuación.

Las actividades que el cliente podrá administrar son las siguientes:

- Provisión de las máquinas a respaldar, descarga, instalación y activación de los agentes necesarios.
- Definición de políticas de backup propias.
- Definición de las unidades/carpetas/fs que el cliente necesita respaldar de cada servidor (será posible definirlo genéricamente para que sobre un grupo de servidores se realice copia de las mismas unidades/carpetas/fs).
- Ejecución de backups según políticas definidas, y peticiones adicionales puntuales cuando el cliente lo solicite.
- Ejecución de restores puntuales cuando el cliente lo desee sobre cualquier máquina del dominio. Será factible el restaurar un fichero de un servidor a otro (si los dos están dados de alta en el dominio)
- Visualización de estado de los backups y restores lanzados. Los que están en ejecución y los históricos.
- Visualización de informes de backups (ver punto Informes de Servicio)

Debido a ello, el cliente no realizará peticiones a los grupos técnicos sólo interactuará con ellos cuando tenga una incidencia.

Los datos de espacio ocupado/respaldado por el cliente en la plataforma se presentarán siempre como valores reales de ocupación. Es decir, el cliente tendrá completa visibilidad de los ratios de deduplicación que consigue con los backups de su dominio.

3.4.4.2 RESTORES

El servicio incluye todos los restores que el cliente considere necesarios, dichos restores los lanzará el cliente desde el portal de servicio.

La administración delegada (Avamar Administrator) tiene la opción de Restore (esta opción aparecerá a los usuarios con permisos de restore), y desde esta opción puede seleccionar cualquier dato (fichero, carpeta, fecha, etc.) para hacer restore.

En la figura 25, tenemos un ejemplo donde, en amarillo, se ve los días en los que hay backup y se pueden hacer restores. En la cuadrícula de la izquierda se listan las máquinas del dominio o del cliente.

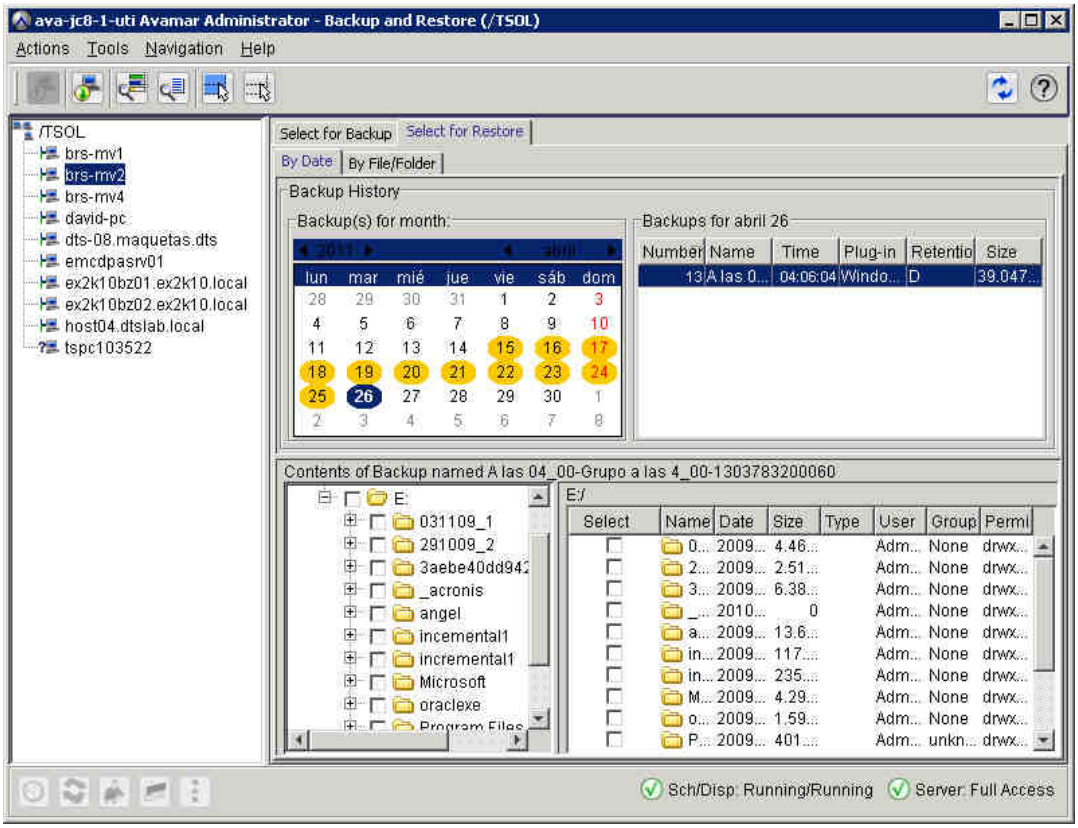


Figura 25: Herramienta de programación de backups y restores

3.4.5 ARQUITECTURA DEL SERVICIO

La tecnología utilizada para prestar el servicio se basará en sistemas de almacenamiento capaces de prestar conectividad por protocolo IP y de deduplicar la información. Hemos confiado a EMC el suministro de dichos sistemas basándose en sus productos EMC Avamar Data Store Gen3 como solución de backup y EMC Data Protection Advisor que ya se encuentran desplegados en nuestras instalaciones [32].

Avamar resuelve los desafíos asociados al Backup tradicional, habilitando un backup rápido, eficiente y recuperable a través de toda la empresa –desde los CPD hasta los CPD remotos, oficinas remotas, equipos de oficina y portátiles. Avamar utiliza la tecnología de almacenamiento patentada para la deduplicación de datos global para identificar los segmentos de datos redundantes en el origen, reduciendo el backup de datos en un factor de más de 300 (Antes de transferirlos a través de la red). Esto permite a las compañías utilizar la infraestructura existente de WAN para hacer el backup y recuperación en caso de desastre de oficinas y CPDs remotos. Los datos pueden ser cifrados al vuelo o en reposo para mayor seguridad, y la gestión centralizada hace posible la protección de cientos de oficinas remotas de manera fácil y eficiente.

EMC Data Protection Advisor es la solución para realizar la gestión centralizada de todo el reporting, análisis y alertas del backup/restore dentro de una solución Enterprise de backup/restore, el cual integra dentro de este reporting, la posibilidad de integrar cualquier elemento que esté presente en la arquitectura de Backup (Librerías, Drives, Switches FC, Switches Ethernet, HBA´s, tarjetas Ethernet, etc.) [33].

Inicialmente el servicio será soportado por una cabina Avamar Datastore de 10 TB de capacidad ubicada en el CDG de Julián Camarillo 8. Además, se dispone de una máquina virtual alojada por el Servicio de Hosting Virtual como servidor y base de datos de Data Protection Advisor.

El diagrama de comunicaciones del servicio se puede observar en la figura 26:

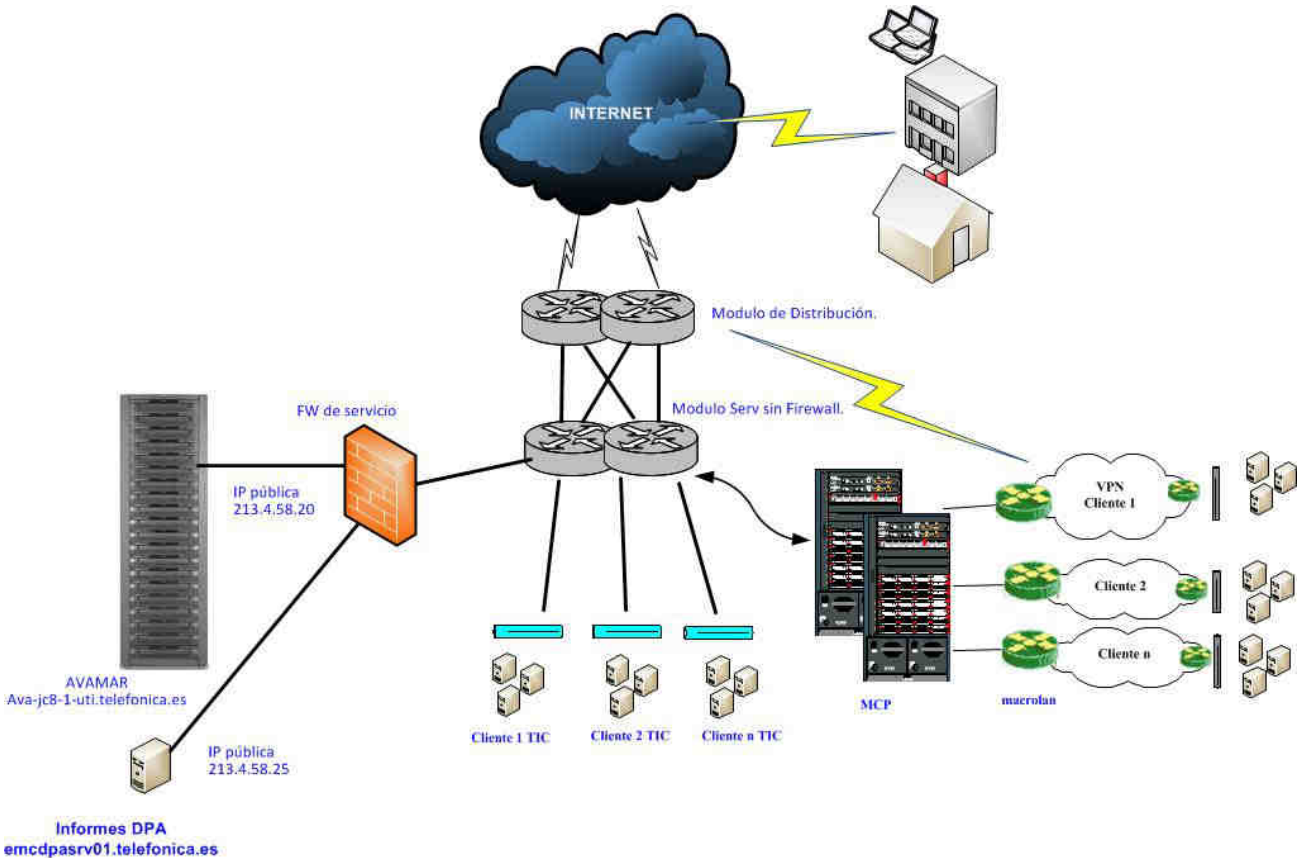


Figura 26: Arquitectura de red del servicio Backup Remoto

3.4.5.1 COMPONENTES FÍSICOS

Utility node

El primero de los componentes hardware de Avamar es un servidor de 2Us que actuará como Utility Node, encargado de programar y gestionar trabajos de Avamar. Provee servicios internos al sistema tales como consola de gestión, autenticación externa, y acceso web. El sistema operativo de este servidor es Red Hat Enterprise Linux ES release 4 (Update 8) [34]. El utility node no almacenará backups en ningún caso.

Storage node

Un storage node de Avamar (figura 27) es un nodo que almacena la información de los backups. En el caso del servicio, se han instalado inicialmente tres storage nodes con capacidad de 3.3TB cada uno que ejecutan el software de Avamar sobre Red Hat Enterprise Linux ES release 4 (Update 8).

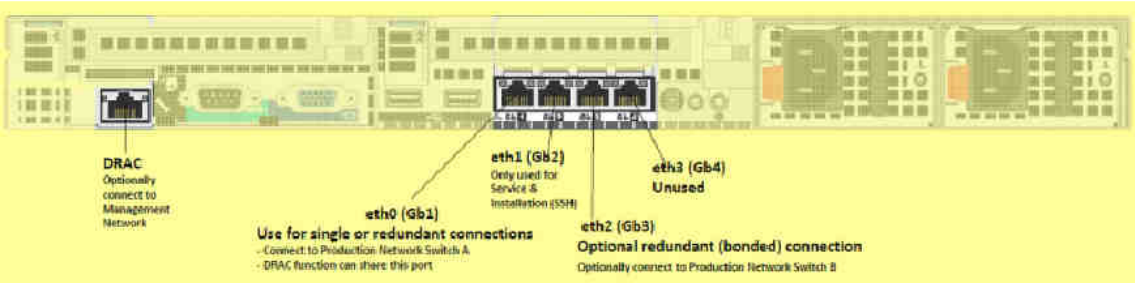


Figura 27: Storage Node

Cada uno de ellos proporciona 5 conexiones GigaEthernet de cobre identificados como DRAC (Dell Remote Access Controller), eth0, eth1, eth2, eth3. La conexión denominada DRAC provee acceso de consola al nodo, a través de la tecnología de Dell. El puerto eth0 forma un bonding con eth2 y se conectan a un switch de servicio de sala del CDG de JC8 de forma que el nodo tiene alta disponibilidad de red para hacer tanto los backups como para comunicarse con el utility node.

Además, cada storage node dispone de fuente de alimentación redundante reemplazable en caliente.

Spare storage node

Se trata de un servidor de respaldo con las mismas características que un storage node. Su estado habitual es inactivo a la espera de un fallo.

3.4.5.2 COMPONENTES LÓGICOS AVAMAR

Agente Avamar

Un agente (o cliente) Avamar es una máquina que tiene acceso al servidor Avamar a través de una conexión de red.

Telefónica proporcionará un nombre del dominio al cliente. El cliente utilizará ese nombre de dominio para activar sus máquinas. Las tareas de instalación y actualización de agentes serán responsabilidad de los clientes del servicio, en ningún caso, serán funciones de los CCTs (Centros de Competencia Tecnológica). Para ello, los clientes dispondrán tanto del manual de usuario del servicio como de la documentación técnica de producto y agentes disponibles a través del servidor web que publica la infraestructura de Avamar.

La lista de agentes soportados que ofrece Avamar es muy amplia. La matriz de compatibilidad disponible en la web muestra la lista de sistemas operativos y aplicaciones soportados [35].

Dominio

Un dominio de Avamar es una zona diferenciada dentro del servidor Avamar. Se utilizan para organizar los clientes y funcionan de forma jerárquica, pudiendo crear subdominios para facilitar una administración delegada.

Se configurará un dominio por cada cliente del servicio.

El nombre del dominio estará compuesto por una clave de 6 caracteres alfanuméricos aleatorios seguidos del nombre del cliente, de forma que el nombre sea lo suficientemente complejo como para evitar que un cliente se active por error en un dominio que no es el suyo. El nombre de dominio no debe superar los 20 caracteres.

Un ejemplo de nombre de dominio es 2AXCVNCLIENTE

Avamar sólo permite crear subdominios a usuarios superadministradores del sistema Avamar, con lo cual, si un cliente quiere utilizar subdominios, deberá solicitar vía ticketing la creación de subdominios adicionales para dar distintos permisos administrativos.

Una vez creado el subdominio, el usuario administrador del dominio del cliente puede gestionar usuarios y clientes de su dominio y subdominios jerárquicamente.

En la Consola de Administración de Avamar (figura 28), la estructura de dominios se muestra en muchas de las vistas disponibles, en el panel de la izquierda. El dominio root es siempre representado por el nombre del servidor de Avamar. Haciendo clic en el recuadro situado más a la izquierda de los dominios, se expande la estructura, mostrándose los subdominios y clientes que hayan sido asignados a dicho dominio. Hay varios dominios preconfigurados por defecto, como son MC_RETIRED y clients. El dominio clients es el dominio por defecto y no puede contener ningún cliente.

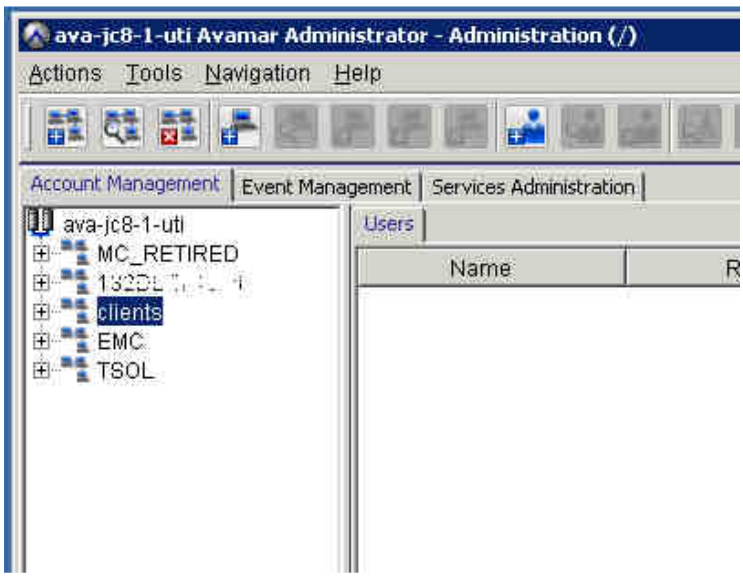


Figura 28: Consola de administración del servicio de Backup Remoto

Activaciones

Para que un cliente pueda comenzar a hacer backups, es necesario que éste se active contra el servidor de Avamar. Para realizar la activación, el cliente debe conocer el nombre de dominio que Telefónica le haya asignado.

Usuarios

Un usuario siempre tendrá asignado un rol y el usuario siempre se creará dentro del dominio de un cliente, como se representa en la figura 29.

Se creará una (y sólo una) cuenta de administrador de dominio Avamar por cada dominio de cliente. El cliente podrá crear cuentas de usuario adicionales sobre su dominio con diferentes roles (ver siguiente apartado).

Sólo se permitirá un usuario administrador del dominio de un cliente y éste se creará en tiempo de provisión de ese cliente.

El nombre de usuario administrador de un dominio siempre será "admin", independientemente del dominio.

El cliente podrá crear hasta un máximo de diez usuarios dentro de su dominio, con independencia de si tiene creados subdominios, es decir, la suma de los usuarios creados en el dominio padre de un cliente y sus subdominios no puede llegar a más de diez.

Figura 29: Consola de gestión de usuarios en servicio Backup Remoto

Roles

Los roles definen operaciones permitidas para cada cuenta de usuario. Hay tres categorías.

- Administrador

Se creará una cuenta de usuario con rol de administrador dentro del dominio de un cliente

- Operador

El rol de operador se da a ciertos usuarios para permitirles realizar backups y restores de ciertas aéreas del sistema.

El cliente podrá crear hasta un máximo de nueve usuarios con rol de operador dentro de su dominio.

Existen cuatro roles de operador:

- Restore only operator

Sólo pueden realizar restores y monitorizar esos jobs de restauración. Si el rol se da al usuario en el dominio más alto, podrá realizar restores de cualquier cliente. Si el rol se da al usuario en un dominio en concreto, podrá realizar restores dentro de ese dominio.

- Backup only operator

Sólo pueden realizar backups y monitorizar esos jobs de backups (bajo demanda de cliente o grupo). Si el rol se da al usuario en el dominio más alto, podrá realizar backups de cualquier cliente. Si el rol se da al usuario en un dominio en concreto, podrá realizar backups dentro de ese dominio.

- Backup/restore operator

Este rol es una combinación de los dos anteriores, es decir, los usuarios con este rol podrán hacer backups, restores y monitorizar como terminan esos jobs.

- Activity operator

Sólo permite monitorizar jobs de backup y restore a través de la consola de actividad y generar ciertos informes. Como siempre, dependiendo del nivel donde se asigne el permiso, se podrán monitorizar los jobs a nivel global o a nivel de dominio particular.

Grupos y políticas de grupo

Una política de grupo es un objeto lógico que une los conceptos de dataset, schedule, retention policy y cliente. Los grupos se definen a nivel de dominio, y se pueden aplicar sólo a clientes de ese dominio. Una política de grupo controla el comportamiento de un backup a menos que se defina otro comportamiento a nivel de cliente.

Todo cliente debe pertenecer al menos a un grupo. El cliente se añadirá a un grupo como parte de la provisión.

Dentro del dominio root, Avamar incluye un grupo preconfigurado: el Default Group. Este grupo incluirá automáticamente todos los nuevos clientes siempre que ningún otro grupo sea configurado. El Default Group siempre utiliza el dataset, calendario y política de retención preconfigurados. Esto no se puede modificar, sin embargo sí pueden modificarse las especificaciones del dataset, calendario y política de retención preconfiguradas

- *Dataset*

Un dataset es un objeto que define el contenido del backup de un cliente. Es una lista de directorios y ficheros de los que se hará backup. La ventaja que tienen es que es un objeto persistente aplicable a varios grupos o clientes.

Un dataset define:

- Lista de datos origen.
  - De uno o mas plugins
  - De una jerarquía de filesystem

- Lista de exclusión/inclusión
- Opciones de plugin. Dependiendo del agente de Avamar que haya instalado en el cliente habrá opciones adicionales referentes a bases de datos, filesystems, etc.

Avamar trae cinco datasets por defecto que se pueden utilizar como base para configurar los nuevos dataset, cada uno de ellos adaptado a su entorno/sistema operativo: Base dataset, Default dataset, Windows dataset, UNIX dataset, VMware dataset.

El cliente podrá crear datasets dentro de su dominio (figura 30).

La recomendación es crear el menor número de datasets posible ya que se complica la gestión para el cliente.

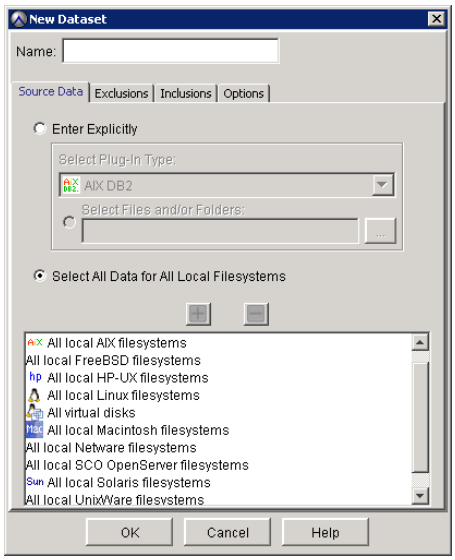


Figura 30: Creación de DataSheets en servicio Backup remoto

- *Schedule*

Un schedule es un objeto que define la planificación del backup de un cliente. En Avamar el concepto de Schedule es distinto al concepto tradicional de schedule de otras soluciones de backup. Hay que tener en cuenta los siguientes conceptos:

- Hora de inicio: define la hora inicial más temprana a la que se puede iniciar esa actividad.
- Hora de fin: define la hora de fin más tardía en la que esa actividad puede terminar.
- Duración: número de horas que puede durar esta actividad (job) antes de que el sistema la finalice, independientemente de si ha terminado o no.
- Recurrencia: número de días por día o semana que se iniciará esta actividad

En Avamar, la ventana de backup debe entenderse como el tiempo comprendido entre la hora de inicio y la duración. En la práctica, la hora de inicio se ve afectada por la carga del servidor y la hora de fin se ve afectada por la complejidad de la tarea (cantidad de datos nuevos de cliente, número de grupos a ejecutar, etc.). Existen tres opciones iniciales para definir la recurrencia en un schedule:

- Repetir diariamente: permite elegir recurrencia en base a varias horas del día
- Repetir semanalmente: permite elegir recurrencia en base a varios días de la semana
- Repetir mensualmente: permite elegir recurrencia en base criterios mensuales (primer lunes del mes por ej.)
- Repetir bajo demanda: en este caso, el schedule no se ejecutará, pero queda definido.

En activation constrains se define cuando se activará ese schedule:

- Delay until (fecha): permite dejar el schedule inactivo hasta la fecha indicada.
- No end data: se activa sin fecha de fin.
- End after (fecha): se activa hasta la fecha indicada.

Avamar viene con cinco schedules por defecto que se pueden utilizar como base para configurar nuevos schedules. El cliente podrá crear schedules dentro de su dominio (figura 31). La recomendación es crear el menor número de schedules posible ya que se complica la gestión para el cliente.

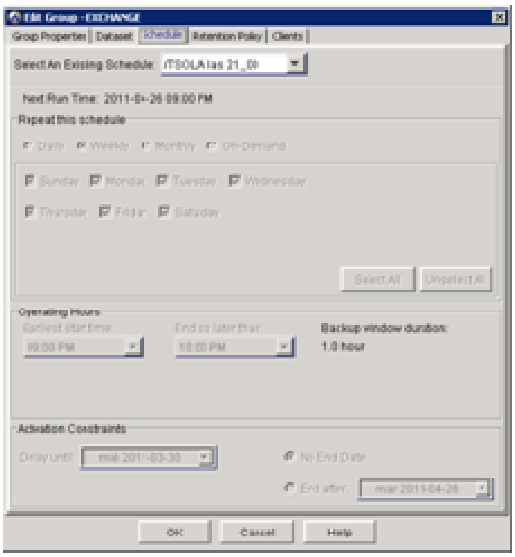


Figura 31: Creación de Schedules en servicio Backup Remoto

- *Retention policies*

Permite especificar durante cuánto tiempo se almacena un backup en el sistema. Una vez expira un backup, el sistema lo marca como para borrado, y se borrará durante las ventanas de mantenimiento.

El propósito principal de una retention policy es definir una fecha de expiración para un backup.

Los parámetros básicos que definen una retention policy son:

- Retention period: define un periodo fijo de retención en base a la fecha de inicio de un backup en particular. Puede expresarse como cualquier combinación de días, semanas, meses o años.
- End date: permite asignar una fecha concreta como fecha de expiración.
- No end date: esta opción permite guardar los backups de manera indefinida.

Los parámetros avanzados permiten definir con una granularidad mayor la fecha de expiración basándose en el número de backups diarios, semanales, mensuales y anuales que se quieran retener en el sistema. Este parámetro enlaza con la configuración de periodicidad definido en las schedules. Las

opciones avanzadas de retención están recomendadas para backups diarios en conjunción con el uso de schedules y nunca son aplicables a backups bajo demanda.

Avamar viene con cinco tipos de retención por defecto que se pueden utilizar como base. El cliente podrá crear retention policies dentro de su dominio (figura 32). La recomendación es crear el menor número de retention policies posible ya que se complica la gestión para el cliente.

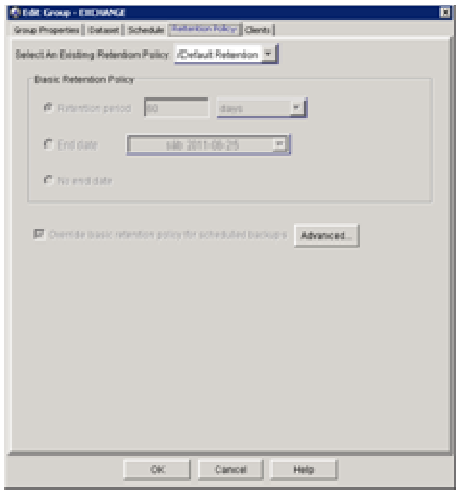


Figura 32: Retention policies en servicio de Backup Remoto

- *Ventanas de operación*

Existen tres ventanas de operación en el sistema:

- Ventana de backup: el sistema no hace tareas de mantenimiento. Se pueden hacer backups y restores hasta el límite de hilos del sistema. La tabla de la siguiente página muestra más información sobre número de hilos permitidos.

- Ventana de blackout: durante la ventana de blackout se ejecutan tareas de garbage collection (borrado de backups expirados) y se crea un checkpoint (permite restaurar el sistema a ese punto en el tiempo. El checkpoint valida los backups realizados durante el día). Durante esta ventana, el sistema se pone en modo readonly, con lo cual no se pueden realizar backups. Restores sí. La duración de la ventana de blackout será de 3 horas.

- Ventana de healthcheck: durante esta ventana el sistema valido el checkpoint creado durante la ventana de blackout. La duración de la ventana de healthcheck será de 9 horas Durante este periodo el número de hilos para backups y restores se reduce considerablemente. (Ver tabla), por lo que si el cliente necesita realizar respaldos en este periodo deberá comunicarlo previamente.

La tabla 8 muestra el número de hilos de backup/restore por nodo. Para el servicio, como se dispone de tres nodos de almacenamiento, las cifras se multiplican por tres (hasta un máximo de 250 hilos por sistema en caso de ampliación).

Un hilo se traduce en un job de backup. Si no hay hilos disponibles en algún momento, esos trabajos se encolan.

	Ventana de backup	Ventana de blackout	Ventana de healthcheck
Hilos de backup por nodo	17	0	2
Hilos de restore por nodo	1	18	1

Tabla 8: Hilos de trabajo por cada nodo en servicio Backup remoto

Las ventanas de operación se configurarán de la manera reflejada en la Tabla 9:

	Inicio	Fin
Ventana de backup	20:00	06:00
Ventana de blackout	08:00	11:00
Ventana de healthcheck	11:00	16:00

Tabla 9: Ventanas de operación en servicio Backup remoto

Es necesario destacar, que durante la ventana de backup, con la configuración inicial con la que arrancará el servicio de tres nodos de almacenamiento, el número de trabajos de backup simultáneos es de 51 y el número de trabajos de restore es de 3. A partir de esas cifras, los jobs se encolarán.

Durante la ventana de healthcheck y con la configuración inicial de tres nodos de almacenamiento, el número de trabajos de backup simultáneos es de 6 y el número de trabajos de restore es de 3. A partir de esas cifras, los jobs se encolarán.

Si se programa un backup o se lanza un backup bajo demanda durante la ventana de blackout, el sistema cancelará ese job y aparecerá como fallido en la consola de Avamar.

Si se está ejecutando un backup y entra la ventana de blackout el job quedará en pausa hasta que el sistema salga del modo solo lectura.

3.4.6 OTROS ASPECTOS DEL SERVICIO

Seguridad de la información

Por defecto, se considera que los datos a realizar backup no son datos de carácter personal. Si los datos a realizar backup son de carácter personal y de un nivel de seguridad nivel alto según la LOPD [36], deberá reflejarse y valorarse adicionalmente las medidas necesarias en la realización de los backups. La notificación de la existencia de datos de carácter personal será responsabilidad del cliente.

En caso de no cumplimiento, Telefónica se limitará a realizar su mejor esfuerzo en la prestación y calidad del servicio, quedando excluidos los Acuerdo de Nivel de Servicio que afecten al servicio.

Consideraciones LOPD

Se contemplan las siguientes actuaciones conforme a lo dispuesto en la Ley Orgánica de Protección de Datos:

Para TODOS los Datos de Carácter Personal, para todos los niveles (Bajo, Medio y Alto), se debe:

- El cliente tiene la obligación de guardar los logs de acceso a esos datos durante UN (1) año: Particularmente, no implica que la retención de los backups deba ser de un año, si no que se debe almacenar, de aquella forma considerada adecuada por el cliente (Ej. es posible guardar los logs en un directorio de su máquina), dichos accesos.

Y para los datos de nivel Alto:

- El cliente tiene la obligación de guardar los logs de acceso a esos datos durante DOS (2) años: Particularmente, no implica que la retención de los backups deba ser de dos años, si no que se debe almacenar, de aquella forma adecuada considerada por el cliente cliente (Ej. es posible guardar los logs en un directorio de su máquina) dichos accesos.
- Cifrar los backups.
- Duplicación de las copias del cliente en otra ubicación física: Por definición el Backup Remoto ya almacena los backups en otra ubicación física

3. SOLUCIÓN OFERTADA

3.1 DESCRIPCIÓN GENERAL DE LA OFERTA

Para cubrir las necesidades del cliente, se ha diseñado la siguiente solución:

Para crear la red privada que contiene a las 4 sedes recurrimos al servicio de Macrolan de Telefónica, ofreciendo para las mayores de ellas (Madrid y Barcelona) unos caudales tanto a nivel MAN, Nacional y en CDG de 4 Mb en clase plata y 2 Mb en clase Oro. Para las dos sedes nuevas, sin embargo, se ha optado, debido a su menor tamaño, por unos caudales de 4 Mb tanto a nivel MAN, como Nacional como en CDG. Los accesos utilizados para todas las sedes serán de 10 Mbps.

Los equipos finales de cliente (EDCs) instalados en cada sede serán un CISCO 2901 por sede y uno más en nuestro CDG, sin contemplar en principio la opción de redundancia por abaratar costes. La oferta incluye tanto la instalación, como el soporte y la instalación de los EDCs en oficina de cliente y en el CDG.

Para implementar la variedad de los servidores actualmente en planta, se ha optado por hacer uso del servicio de Hosting virtual de Telefónica Soluciones, levantando a través de él una serie de 5 servidores virtuales, distribuidos de la siguiente manera.

- Servidores tipo A (3 unidades): Con 4 cores de CPU cada uno, 4 Gb de memoria RAM, 500 Gb de HDD en formato RAID 5 y Sistema Operativo Windows Server 2003. Estos servidores soportarán el ERP, el servidor de correo y el repositorio compartido.

- Servidores tipo B (2 unidades): Con 2 cores de CPU cada uno, 2 Gb de memoria RAM y 300 Gb de HDD en formato RAID 5 y Sistema Operativo Linux (RedHat 5.0). En estos servidores se alojarán la página de atención al cliente y la página web de la compañía, por lo que dispondrán de una presencia en internet de 10 Mbps.

Además, estos servidores llevarán asociados los servicios de Backup para cada uno de ellos (En total, 1 Tb). En previsión de crecimientos futuros, se incluye un pool de recursos que permitirá, sin coste alguno la creación de máquinas virtuales nuevas, que se podrán solicitar a través del portal de autoprovisión (Portal Cloud) y también una bolsa de solicitudes de operaciones mensuales.

Los usuarios que se conecten a la red privada, haciendo uso del servicio de Tráfico Limpio ofrecido por Telefónica Soluciones, disfrutarán de una navegación segura que permitirá hasta un caudal de 20Kbps asegurado para una concurrencia del 50% de los usuarios. Este caudal no es limitativo, comos e describe en el correspondiente apartado.

Finalmente, y para solventar la necesidad de un backup de aquellos servidores que no se encuentran en la plataforma virtual alojada en nuestro CDG, se pondrán a disposición del cliente 2 dominios en la plataforma compartida de Backup remoto, con un espacio estimado de ocupación en la plataforma de 1,5 Tb, haciendo uso del servicio de Backup Remoto provisto por Telefónica Soluciones.

3.2 ESQUEMA DE INFRAESTRUCTURA

3.2.1 INFRAESTRUCTURA DE LA RED PRIVADA

La red privada presenta una infraestructura como la reflejada en la figura 33.

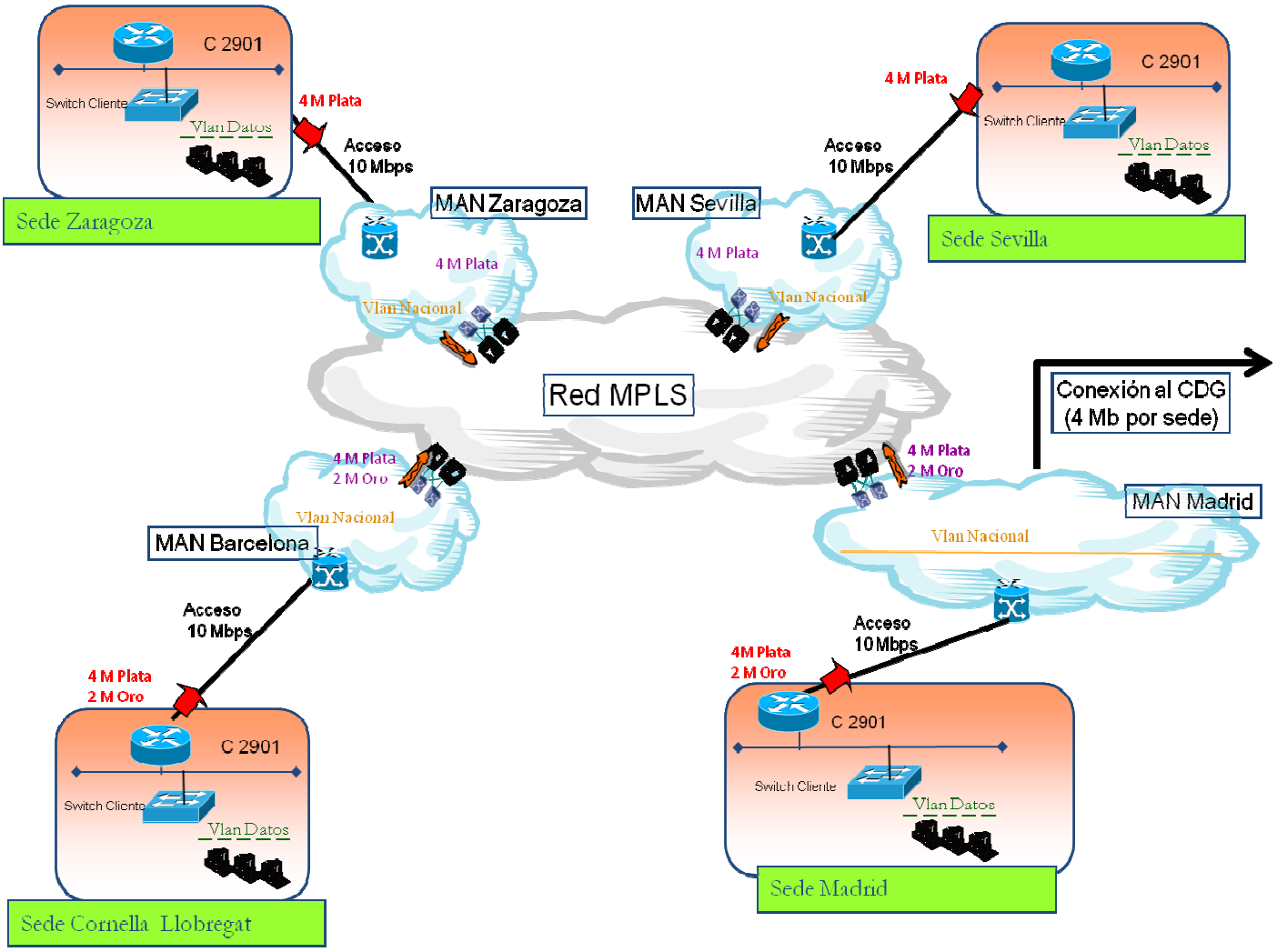


Figura 33: Infraestructura de la red privada diseñada sobre servicio macrolan

En párrafos posteriores se puede encontrar información más detallada a cerca de los accesos, caudales y equipos que conforman dicha red privada.

3.2.2 INFRAESTRUCTURA DE LOS SERVICIOS EN EL CDG

Los servicios reflejados en la oferta que serán alojados en el CDG aparecen reflejados en la figura 34.

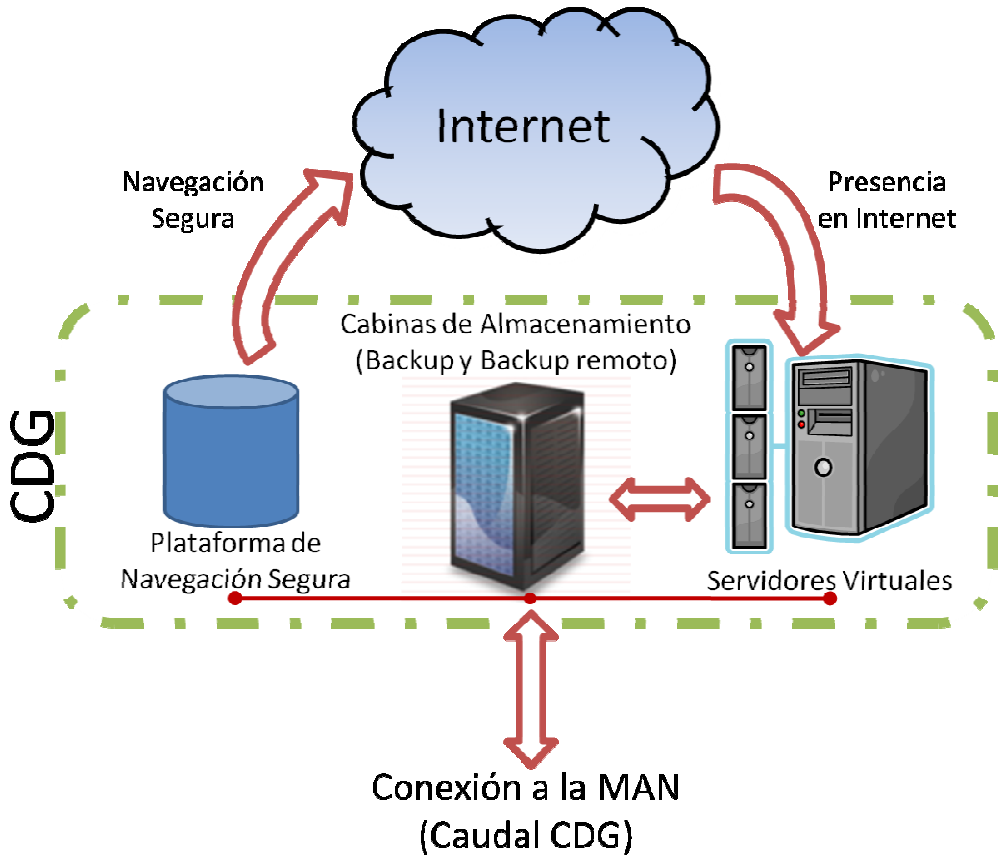


Figura 34: Esquema de los servicios desplegados desde el CDG

Todos estos servicios se encuentran alojados en los TIC de la empresa Telefónica, siendo de su completa propiedad.

La seguridad lógica que la red ofrece ya de por sí, se ve complementada además por los Firewalls y Balanceadores de carga de acceso a la sala, que permiten que se puedan cumplir unos Niveles de Servicio muy altos, asegurando una disponibilidad de casi el 100% de la plataforma.

3.3 DETALLE DE LA SOLUCIÓN

3.3.1 HOSTING VIRTUAL: DETALLE DE LA SOLUCIÓN

3.3.1.1 Componentes incluidos

La unidad básica del servicio es el servidor virtual. Para cada servidor virtual contratado, se han configurado los siguientes componentes mostrados en la tabla 10:

TIPO DE SERVIDOR	NÚMERO SERVIDORES VIRTUALES	NÚMERO VCPUS	MEMORIA RAM	DISCO	SO
Servidor 1	3	4	4 GB	500 GB	Windows Server 2003
Servidor 2	2	2	2 GB	300 GB	RedHat 5.0

Tabla 10: Servidores virtuales incluidos en la oferta

El servicio de Hosting Virtual incluye una (1) dirección pública IP **por contrato**. Se incluye en la oferta la valoración de 3 direcciones públicas adicionales sobre la ofrecida en el servicio.

Los servidores tendrán una presencia en internet a través de los firewall compartidos de 10 Mbps. No se contempla una velocidad de acceso mayor, ya que las peticiones cursadas a este tipo de servidores son satisfechas correctamente en la mayoría de los casos con esta velocidad. Un aumento de la velocidad supondría no poder recurrir a un Firewall compartido, teniendo que optar por un equipo dedicado, con el consecuente aumento de precio de la oferta, lo cual nos desposicionaría completamente.

3.3.1.2 Componentes adicionales

Los componentes o funcionalidades que se describen a continuación se contratan de forma adicional sobre los servidores virtuales básicos descritos en el apartado anterior. Dichas funcionalidades han sido específicamente adaptadas para el servicio de Hosting Virtual, mejorando así la interoperabilidad y rendimiento entre los diferentes componentes.

Funcionalidad de Monitorización

La funcionalidad de monitorización incluida en la presente oferta se detalla a continuación:

- Monitorización de Servidores Virtuales
- Monitorización de Servicios Internet y Transacciones – Monitorización de protocolos
- Monitorización de Servicios Internet y Transacciones – Monitorización de transacciones

Funcionalidad de Respaldo de la Información

La solución de backup detallada en la presente oferta se compone de los elementos presentados en la tabla 11:

CONCEPTO	MEDIDA	CANTIDAD	DESCRIPCIÓN
Licencias	Por máquina	3	Tier 1 Windows
Licencias	Por máquina	2	Tier 0 Linux

Tabla 11: Conceptos facturados en el servicio de HV. Licencias de backup

Así mismo, los agentes y número de Gb de backup ofertados aparecen en la tabla 12:

CONCEPTO	MEDIDA	CANTIDAD	DESCRIPCIÓN
Agente de Backup	Por servidor	5	Agentes necesarios para el scheduling y gestión del backup
GB ocupados política estándar	Por GB	1000 Gb	

Tabla 12: Conceptos facturados en el servicio de HV. Agentes y espacio asignado de backup

3.3.1.3 PANEL DE CONTROL (CLOUD PORTAL)

Se incluye en el precio un pool de recursos necesarios para levantar máquinas virtuales en caso de necesidad de crecimiento puntual o campañas extraordinarios, que incluye lo necesario para levantar un servidor de cada tipo.

También se incluye una bolsa de solicitudes que incluye 5 solicitudes tipo B y 3 de tipo C al mes. Todas estas acciones (solicitudes o levantamiento de máquinas) pueden ser solicitadas a través del Cloud Portal.

3.3.2 SERVICIO MACROLÁN

El servicio Macrolan ofrecido provee de una red virtual privada para el cliente, que dispondrá de los siguientes elementos de comunicaciones y caudales:

Tipología		Servicio	Acceso Principal	Ámbito Caudal
Sede de Madrid	Accesos	MacroLan	Ethernet 10 Mbps	-
	Caudales	MacroLan	4 Mbps Plata	Metro
		MacroLan	2 Mbps Oro	Metro
		MacroLan	4 Mbps Plata	Nacional
		MacroLan	2 Mbps Oro	Nacional
		MacroLan	4 Mbps Plata	CDG
		MacroLan	2 Mbps Oro	CDG
	EDC	MacroLan	Cisco **2901**	

Tabla 13: Conceptos facturados en servicio Macrolan. Sede de Madrid

Para el caso de la sede de Madrid, se ha optado por las caudales reflejados en la tabla 13. Como base, y dado que el objetivo principal es mantener una comunicación fluida con el CDG, se ha optado por caudales plata de 4 Mbps sobre accesos de 10 Mbps (es decir, existiría la posibilidad de crecimiento en el futuro) tanto en el entorno Metro, como en Nacional como CDG, para evitar congestiones.

Además, sabiendo que la comunicación puede verse afectada por tener que soportar un gran número de usuarios en la salida a internet y dado que uno de los flujos de datos que llegará al CDG es vital para la línea de negocio por ser el que porte la información al ERP, se ha añadido un caudal extra de 2 Mbps en clase Oro (con prioridad sobre los anteriores), para evitar el dropping de paquetes importantes.

Para ver una descripción de los equipos instalados en la sede de Madrid, Cisco 2901, puede acudir a la Tabla 17 y a la figura 35.

Tipología		Servicio	Acceso Principal	Ámbito Caudal
Sede de Barcelona	Accesos	MacroLan	Ethernet 10 Mbps	-
	Caudales	MacroLan	4 Mbps Plata	Metro
		MacroLan	2 Mbps Oro	Metro
		MacroLan	4 Mbps Plata	Nacional
		MacroLan	2 Mbps Oro	Nacional
		MacroLan	4 Mbps Plata	CDG
		MacroLan	2 Mbps Oro	CDG
	EDC	MacroLan	Cisco **2901**	

Tabla 14: Conceptos facturados en servicio Macrolan. Sede de Barcelona

En el caso de la sede de Barcelona, se ha optado por una solución idéntica a la adoptada para la sede de Madrid, y que se puede observar en la Tabla 14.

Dado que el número de usuarios aproximado es idéntico al de la sede de Madrid, los caudales y accesos elegidos han sido los mismos, dado que también va a ser un número importante de usuarios el que va a acceder a internet, y por ello se requiere también un marcado de paquetes importantes (todos aquellos destinados al ERP)

Tipología		Servicio	Acceso Principal	Ámbito Caudal
Sede de Zaragoza	Accesos	MacroLan	Ethernet 10 Mbps	-
	Caudales	MacroLan	4 Mbps Plata	Metro
		MacroLan	4 Mbps Plata	Nacional
		MacroLan	4 Mbps Plata	CDG
	EDC	MacroLan	Cisco **2901**	

Tabla 15: Conceptos facturados en servicio Macrolan. Sede de Zaragoza

Tipología		Servicio	Acceso Principal	Ámbito Caudal
Sede de Sevilla	Accesos	MacroLan	Ethernet 10 Mbps	-
	Caudales	MacroLan	4 Mbps Plata	Metro
		MacroLan	4 Mbps Plata	Nacional
		MacroLan	4 Mbps Plata	CDG
	EDC	MacroLan	Cisco **2901**	

Tabla 16: Conceptos facturados en servicio Macrolan. Sede de Sevilla

Para el caso de las dos sedes restantes de Sevilla y Zaragoza, por ser de nueva apertura, y por ahora en principio de menos número de empleados, se ha optado por unos caudales más limitados, los cuales se encuentran reflejados en la tabla 15 (para la sede Zaragoza) y la tabla 16 (para la sede de Sevilla) .

Para estas sedes nos hemos limitado a ofrecer caudales de 4 Mbps por segundo en clase plata, ya que se considera que son caudales suficientes para absorber todas las necesidades de navegación (tanto entre sedes, como hasta el CDG, como hacia internet), debido a su menor número de usuarios y a su, en principio, menor carga de trabajo.

No obstante, dado que son caudales soportados sobre accesos de 10 Mbps, estos caudales pueden ser incrementados o complementados con caudales de diferente clase (Oro o Multimedia) en caso de ser necesario, sin suponer un incremento del precio demasiado elevado.

Además de la red privada en sí misma y los equipos necesarios para su despliegue arriba listados, el servicio también lleva incluido el soporte, mantenimiento y administración de dichos equipos, así como el alojamiento del equipo de cliente necesario en el CDG.

3.3.2.1 CONDICIONES DE LA SALA DE EQUIPOS

El equipamiento del Servicio MacroLAN no requiere necesariamente ser instalado en dependencias especialmente climatizadas o acondicionadas, toda vez que las condiciones ambientales exigidas para su correcto funcionamiento no rebasan las habituales en dependencias de oficina o equipo. No obstante, es necesario tener en cuenta los parámetros que se dan a continuación y proveer, en su caso, los correspondientes sistemas de alimentación y acondicionamiento, sobre todo en configuraciones de múltiples equipos.

El equipo a instalar en todas las sedes es el **CISCO 2901,** del cual se anexa una tabla con sus características (tabla 17) y una figura con su rendimiento (figura 35).

Cisco 2901

VPN IP	MLAN	DINET	SILAN	Cifrado	GW ToIP	Accesos y Respaldos Móviles
OK	OK hasta 10 Mbps	OK	No Aplica	Requiere SL-29-SEC-K9	Capacidad 8 interfaces BRI / 8 interfaces E1	Con Teldat H1+/ Antena Ethernet

CISCO2901-[Cisco 2901]	
Características	**Suministro**
• 2 puertos Ethernet 10/100/1000 tipo RJ45 • 4 slots externos libres para 4 módulos EHWIC de tamaño simple o 2 módulos de doble tamaño (incluidos también los HWIC, WIC o VIC compatibles) • 2 slots internos para módulos DSP (Digital Signal Processor) • 1 slot interno para ISM (Internal Service Module) • Encriptación hardware integrada en el propio equipo sin necesitar la inclusión de módulos adicionales • Memoria DRAM por defecto (y máxima disponible) 512MB • Memoria FLASH por defecto (y máxima disponible) 256MB • 1 puerto de consola tipo USB y otro tipo RJ45 (sólo uno puede usarse para acceder al equipo) • 1 puerto asíncrono auxiliar • 2 puertos USB 2.0 • Opciones de fuente de alimentación AC y PoE • Corriente máxima fuente de alimentación: 1,5 – 0,6 Amp • Tensión de Alimentación: 100-240 VAC • Temperatura de funcionamiento: 0° to 40°C • Dimensiones : 4,45 x 43,82 x 43,94 cm • Ocupación en rack: 1RU • Peso (máximo): 7,3 Kg • Consumo de potencia: Sin módulos: 40W, Maxima sin PoE : 150W, Máxima con PoE (sólo la plataforma): 175W • Ruido: típicamente 49dBA y máximo de 61 dBA	• Cisco 2901 • Unversal SW Image • Licencia IP Base • kit de enracado de 19-pulgadas • 1 cable alimentación (elegir)  **Cisco 2901**

Tabla 17: Prestaciones del EDC ofertado

Prestaciones

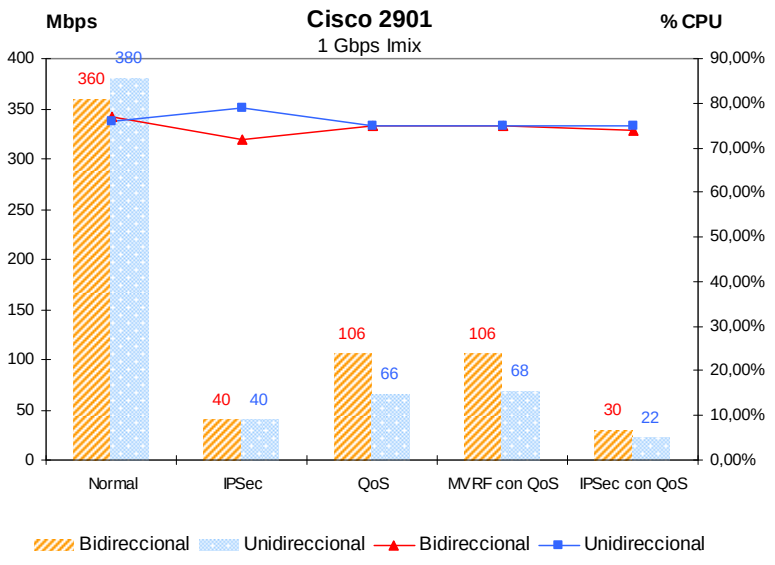


Figura 35: Prestaciones CISCO 2901

A partir de las citadas especificaciones técnicas, el Cliente deberá acondicionar su Sala de equipos ajustándose en lo posible a las siguientes recomendaciones:

- Altura mínima de techo 220 cm.
- Pared y suelo libres de obstáculos que impidan adosar rosetas/BAFOS en la pared
- Iluminación mediante lámpara fluorescente
- Temperatura entre 5º y 30º C y ventilación de la Sala
- Espacio para la operación y mantenimiento de los equipos
- Alimentación eléctrica sobre línea independiente con protección eléctrica, según el Reglamento Electrotécnico de Baja Tensión vigente
- Enchufes de alimentación de 220V. y 10/16 A. con toma de Tierra inferior a 5 Ohm De resistencia
- 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.
- Preferible suelo técnico o falso techo desmontable para facilitar la prolongación del cableado exterior

3.3.3 TRÁFICO LIMPIO: DETALLE DE LA SOLUCIÓN

La solución de navegación a Internet será provista y administrada por Telefónica en su CDG.

Se dará servicio de navegación segura a Internet para 120 usuarios (50 en la sede de Madrid, 30 en la de Barcelona y 20 en cada una de las sedes de Zaragoza y Sevilla), empleando para ello una solución con funcionalidades de antivirus perimetral y de filtrado de contenidos proporcionada a través del servicio de Tráfico Limpio Internet, cuyas características son:

- Caudal garantizado que aparece como seleccionado en la tabla 18:

Modalidad	Caudal Garantizado
Bronce	15 Kbps
Plata	20 Kbps
Oro	25 Kbps
Platino	30 Kbps

Tabla 18: Modalidad facturada en servicio Tráfico Limpio

Este caudal no es limitativo, es decir, no se producirá un "drop" de paquetes una vez alcanzado el caudal garantizado, si no que se permitirá ser superado cuando sea necesario.

A través de los informes que se generan asociados al servicio, Telefónica analiza la información correspondiente al caudal medio ocupado, y si superara el caudal contratado durante más del 50 % de tiempo de conexión, se instaría al cliente a utilizar con moderación dichos caudales.

- Concurrencia máxima de usuarios = 50 %

- Así mismo, se requieren los elementos opcionales del servicio marcados en la tabla 19:

Funcionalidad Opcional	Selección
Configuración de Single Sign On Configuración del sistema de autenticación unificada con el Directorio Activo del cliente con el objetivo de evitar la doble autenticación en dominio y en la plataforma de navegación.	☒
Navegación "sin proxy" Configuración de un grupo de navegación del cliente para que navegue directamente a Internet sin pasar por la plataforma de Navegación (Proxy). Ej. Directivos.	☐
Autenticación con LDAP del cliente Configuración de la sincronización del LDAP del cliente con la plataforma de filtrado, permitiendo la gestión unificada de los usuarios/roles.	☒
Envío de LOGS Configuración del envío periódico de logs de navegación al cliente.	☒

Tabla 19: Funcionalidad opcionales facturadas en servicio Tráfico Limpio

La solución propuesta requiere de una solución de conectividad entre las instalaciones de Transacciones Inmobiliarias S.A. hasta el correspondiente Centro de Datos Gestionado (CDG), para poder hacer uso del servicio (Como se ha mencionado en apartados anteriores, esta conectividad queda recogida en esta oferta con el nombre de Servicio Macrolan).

3.3.4 RESPALDO REMOTO DE INFORMACIÓN: DETALLE DE LA SOLUCIÓN

La opción contratada permite realizar backup adaptándose a las necesidades particulares de cada organización mediante la configuración por parte del cliente de los backups deseados.

La solución de Backup Remoto de Información detallada en la presente oferta se compone de:

- Espacio de 1.5 TB de Almacenamiento para backup. Para calcular el total de espacio (TB) y su valoración se han empleado la información facilitada por el cliente.
- 2 Dominios de backup, orientados a diferentes fines dentro de la organización

Se considera TB almacenado en la plataforma el que realmente se utiliza. Se deberán estimar los ratios de deduplicación estimados en cada cliente para realizar el cálculo del espacio a contratar. Dicha estimación afecta a la cuota del servicio por lo que será responsabilidad del cliente ajustarse a los parámetros contemplados en la provisión del servicio para que no se vea afectada la cuota por incremento de la capacidad de almacenamiento estimada.

El servicio de Backup de Información no incluye recuperación de los sistemas desde el hardware (funcionalidad “baremetal”). En caso de ser requerido por el cliente, es preciso realizar valoración específica.

3.4 SERVICE MANAGER

Se incluye en la presente oferta la dedicación de un Service Manager con una dedicación de 5 jornadas mensuales. En caso sea necesario una mayor dedicación que la contratada, bien por requisitos de cliente bien por requerimientos particulares de los servicios contratados, se deberá realizar una ampliación de las jornadas de Service Manager contratadas mediante una nueva valoración.

Recomendamos la utilización de este tipo de perfil en las siguientes situaciones:

- Entornos complejos de administración o de máxima criticidad para el negocio del cliente. (como es el presente caso)
- Entornos con disparidad de tecnología.
- Entornos de administración compartida o con diversidad de proveedores.
- Entornos de más de 20 servidores.

Dicho perfil tendrá el conocimiento global de toda la infraestructura y arquitectura técnica del cliente, servicios contratados y criticidad, siendo así el principal interlocutor entre Telefónica y el cliente. Detalladamente, las responsabilidades y tareas que asumirá esta figura para con el cliente se describen a continuación:

3.4.1 FASE DE ENTREGA Y PROVISIÓN DEL SERVICIO

- Establecer los canales de comunicación adecuados, canalizando los flujos de información entre Telefónica y el cliente.
- Si procede, y por incumplimiento por parte del cliente en obligaciones sobre requerimientos detallados en la descripción del servicio, el Service Manager será el encargado de fijar los nuevos acuerdos de nivel de servicio con el cliente. En caso contrario, se establecerán los niveles establecidos por defecto en el servicio.
- Disponibilidad de 24x7 telefónica.
- Realizar el seguimiento de la provisión del servicio, aportando la información comunicada por el cliente en dicho proceso. Igualmente, colaborando en el seguimiento y cumplimiento de los hitos establecidos en el proyecto.

3.4.2 FASE DE SOPORTE Y SEGUIMIENTO DEL SERVICIO

- Mantener informado al cliente sobre las incidencias relevantes que afecten al servicio, verificando los informes técnicos sobre incidencias/problemas de servicio.
- Verificar que la provisión realizada cumple los requisitos técnicos del cliente reflejados en la oferta, y si procede, realizar un seguimiento y plan de resolución de las carencias.

- Seguimiento y coordinación en la resolución de problemas abiertos para el cliente.
- Comprobar el correcto cumplimiento de los acuerdos de nivel, mediante informes de seguimiento, reuniones periódicas e informes de satisfacción.
- Gestionar peticiones de servicio no incluidas en el contrato específicamente.

3.5 IMPLANTACIÓN DEL SERVICIO

Una vez aceptada en firme por el Cliente la oferta recogida en el presente documento, y con el fin de establecer la fecha aproximada de provisión del servicio del objeto de la misma, Telefónica elaborará un plan de implantación al efecto, que responderá a un modelo como el reflejado en la figura 36.

Telefónica enviará al Cliente una planificación detallada de la implantación dentro de las dos semanas posteriores a la recepción del pedido. La fecha prevista de inicio del periodo de explotación, al finalizar la implantación, se fijará en la planificación detallada, aunque el compromiso inicial viene reflejado en la tabla 20:

COMPROMISOS TEMPORALES CON EL CLIENTE	FECHA
Plataforma completa en funcionamiento	T_0 + 5 semanas

Tabla 20: Compromisos en la implantación

T_0 indica la fecha de aceptación de la oferta por parte del Cliente

Se establece por defecto que los procesos de provisión y/o soporte para la implantación del servicio se realizarán en jornada/horario laboral 8x5, debiéndose valorar adicionalmente si desean otros periodos fuera de este horario (p.ej. fines de semana y/o festivos).

Así mismo, Telefónica excluye toda responsabilidad por los retrasos que se produzcan, cuando tales retrasos se deban cualesquiera causa ajena a su voluntad y, expresamente, cuando el retraso se deba a la necesaria obtención de cualquier permiso o licencia de carácter legal en el supuesto de que la provisión requiriese la ejecución de algún tipo de obra civil. Igualmente sucederá si el retraso es imputable al cliente debido a retrasos en la entrega de los datos necesarios para realizar las actividades ofertadas.

De la misma forma, en caso que el proyecto de implantación quede detenido por motivos del cliente durante más de 4 semanas, se empezarán a facturar todos los servicios provisionados o reservados en exclusiva para el cliente.

Id	Nombre de tarea
1	**Implantación del Servicio**
2	**Fase Planificación / Gestión**
3	Recepción solicitud de implantación
4	Reunión interna preventa/grupos técnicos
5	HITO 1: Documentación previa preparada
6	Reunión de Arranque con el cliente
7	Análisis, validación doc., planificación y coordinación áreas
8	HITO 2: Documentación final preparada
9	Envio al cliente de documentación (protocolos, lopd, etc)
10	HITO 3:Aceptación de la planificación
11	**Fases Instalación / Configuración / Puesta en producción**
12	**Infraestructuras**
13	Asignación Espacio/electricidad
14	Montaje equipos
15	HITO 4: Disponibilidad de las Infraestructuras
16	**Comunicaciones**
17	Asiganción de los recursos lógicos
18	Provisión comunicaciones
19	Provisión cableado de red
20	Provisión equipos EDCs
21	Instalación de los equipos EDCs
22	Configuración EDCs
23	HITO 5: Disponibilidad del Servicio Macrolan
24	**Servicios de TI**
25	**Servicio Hosting Virtual**
26	**Servidores Windows Server**
27	**Fase Administración Interna**
28	Configuración de plataforma
29	Recopilación de información
30	Generación de documentación de operación y cont
31	**Fase Inventariado**
32	Recopilación de información a Inventariar (protocol
33	**Fase Monitorización**
34	Provisión Monitorización
35	**Fase Backup**
36	Provisión Backup
37	**Servidores Linux**
38	**Fase Administración Interna**
39	Configuración de plataforma
40	Recopilación de información
41	Generación de documentación de operación y cont
42	**Fase Inventariado**
43	Recopilación de información a Inventariar (protocol
44	**Fase Monitorización**
45	Provisión Monitorización
46	**Fase Backup**
47	Provisión Backup
48	HITO 6: Disponibilidad del Servicio HV
49	**Servicio Tráfico Limpio**
50	Asignación de los recursos
51	Configuración de los nodos
52	HITO 7: Disponibilidad del Servicio TL
53	**Servicio Backup Remoto**
54	Asignación de los recursos
55	Instalación de los agentes en casa de cliente
56	HITO 8: Disponibilidad del Servicio BUR
57	HITO 9: Disponibilidad de la Plataforma Completa
58	**Fase de Paso a Explotación Plat Windows**
59	Entrega de doc.y solicitud paso a Explotación
60	**Paso a producción**
61	Validación de servicio y revisión de documentación
62	Reunión con Service Manager para entrega de la Explotación
63	HITO 9: Plataforma en Explotación

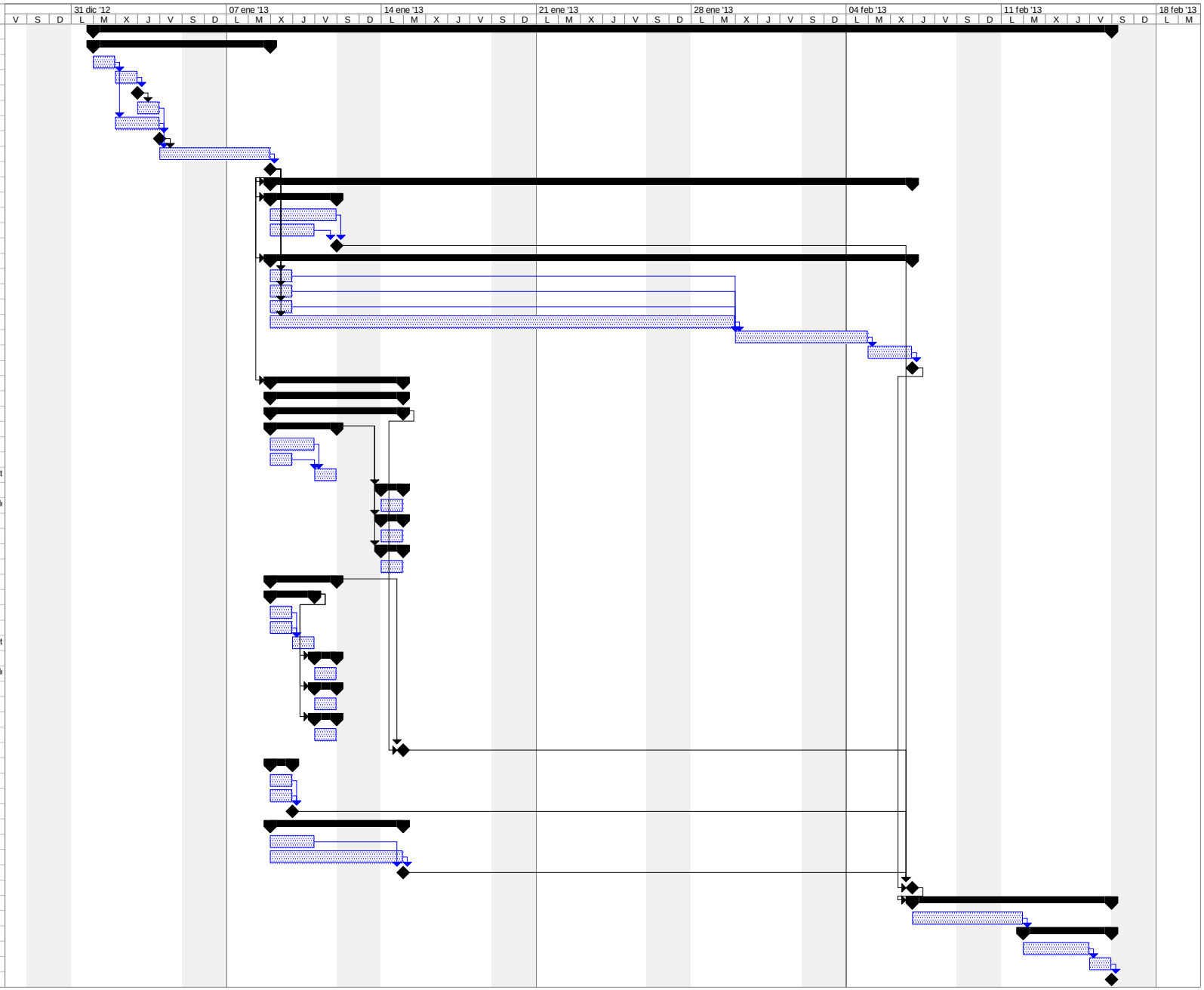


Figura 36: Diagrama de Gantt del proyecto

3.6 GESTIÓN DE INCIDENCIAS

La figura 37 muestra de forma esquemática los flujos de atención a incidencias:

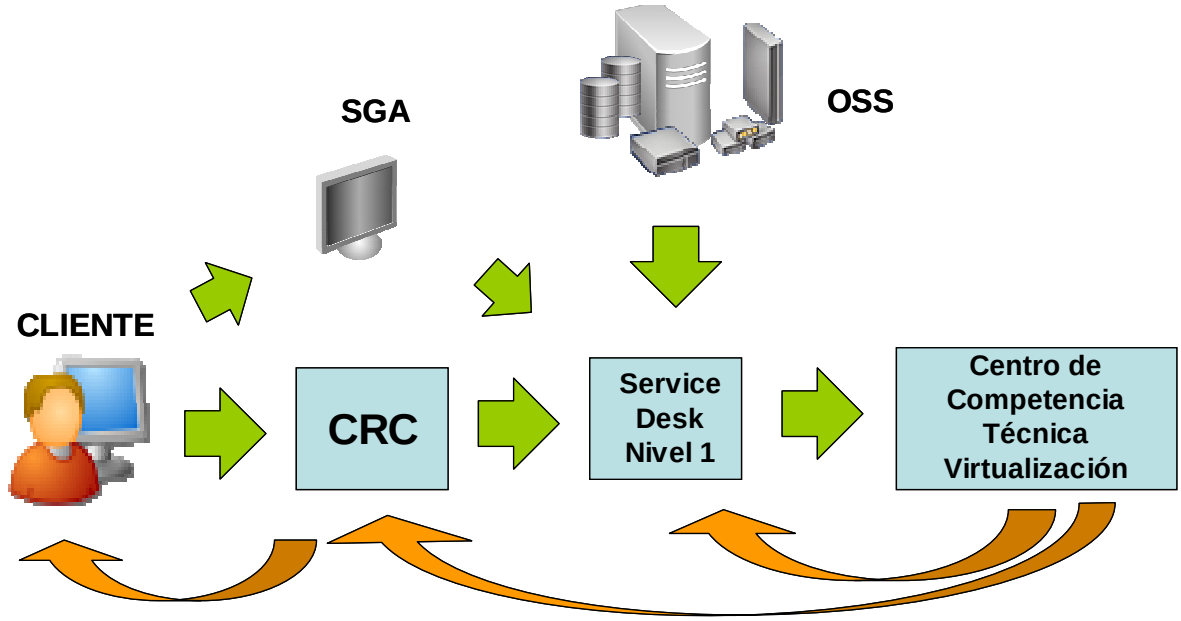


Figura 37: Gestión de incidencias

Los flujos posibles de atención a incidencias son tres:

- Incidencia detectada por los sistemas de monitorización del servicio. En este caso, la incidencia es detectada internamente, se registra en SGSD, y se comienza en su resolución aunque el cliente no haya notificado la incidencia. En este caso, el nivel 1 recibe la alarma, identifica que se trata del servicio de Hosting Virtual, y se traslada al CCT de virtualización. Una vez resuelta, es devuelta al Nivel 1 que verifica la desaparición de la alarma y resuelve la incidencia.
- Incidencia comunicada por el cliente a través del Centro de Relación de Clientes (CRC). El CRC identifica que el servicio al que se refiere el cliente es un servicio de Hosting Virtual, y se traspasa al Nivel 1, que a su vez lo transfiere al CCT de Virtualización. Una vez resuelta la incidencia, esta es devuelva al CRC que verifica con el cliente el cierre de ésta. Este es el procedimiento estándar de registro de incidencias de clientes.
- Algunos clientes disponen de acceso directo al SGSD. Estos clientes pueden introducir directamente la incidencia en este sistema. Esta incidencia le llega al Nivel 1, que verifica que se trata de un servicio de Hosting Virtual y lo propaga al CCT de virtualización. Una vez finalizada la incidencia, es devuelta al Nivel 1 que procede a su cierre.

Lógicamente, si durante el proceso de cierre se verifica que la incidencia persiste, puede devolverse al estado de abierta y es transferida de nuevo al CCT.

A continuación se describen los tipos de incidencias que se pueden producir en el servicio:

- Avería: corresponde con una incidencia notificada por un cliente. En este caso se utiliza el mismo código de que en el servicio de Hosting, y se diferencia el CCT de destino en función de la categorización de Servidor Virtual del Servidor afectado por la avería.
- Alarma del servicio. Corresponde con una alarma detectada por los sistemas de monitorización. En este caso, las posibles alarmas hacen referencia a:
    - Fallo de alguno de los servidores HW de la plataforma
    - Fallo del Virtual Center.
    - Fallo de un ESX
    - Perdida de rendimiento:
        - Disco
        - HBAs
        - Memoria
        - Máquinas virtuales

3.7 SLAs

Los SLA o ANS (Service Level Agreement o Acuerdo de Nivel de Servicio) son un acuerdo entre un proveedor de servicio y el cliente que define los términos de responsabilidad del proveedor hacia el cliente y el tipo y extensión de la penalización, si la hay, en caso de que estas responsabilidades no sean cumplidas (figura 38)

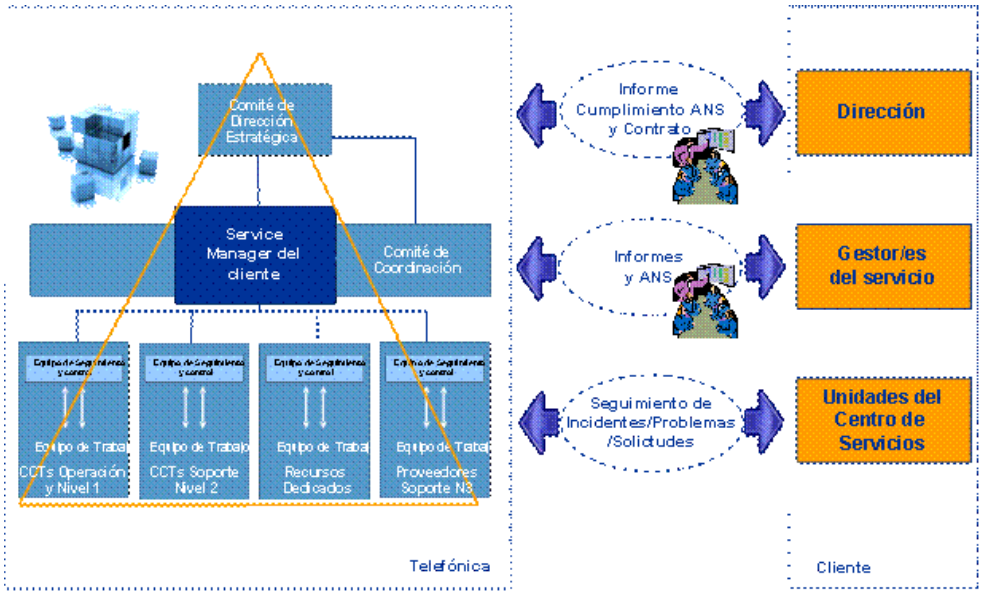


Figura 38: Gestión de los SLAs

Los SLA garantizan el correcto funcionamiento del servicio ofrecido al cliente. Este buen funcionamiento se realiza en base a unos parámetros objetivos que miden diversas características del servicio. Los SLA acotan los valores de estos parámetros, normalmente en términos de máximos, mínimos u otras operaciones estadísticas como la media. Mensualmente se informará al cliente del cumplimiento o incumplimiento de los SLA mediante los correspondientes informes. En caso de incumplimiento de los SLA se concederá al cliente una compensación económica en forma de Bonos de Servicio, a descontar de la siguiente factura del mismo.

3.7.1 DISPONIBILIDAD DE OFICINA

Definición

Se define la Disponibilidad de Oficina como el porcentaje de tiempo al mes que la comunicación de la oficina del cliente dentro de la RPV está operativa. La disponibilidad se medirá y calculará de forma individualizada por oficina. Una oficina se considera que está disponible cuando puede acceder a la RPV (bien por el escenario principal o bien por el de backup, si lo tuviera contratado)

Condiciones:

Se incluye en la oficina: el router (que debe estar gestionado y mantenido) por Telefónica, la línea de acceso, las puertas de acceso a la red, el caudal y las facilidades contratadas. Para efectos de cálculo, no se contabilizan los tiempos de indisponibilidad resultantes de:

- Una manipulación indebida por parte del cliente de los equipos gestionados por Telefónica (cambio indebido en la configuración del router o traslado de línea).
- Una línea cuya titularidad no es de Telefónica (líneas punto a punto entre oficinas del cliente y no conectadas a la red de Telefónica).
- EDC no Gestionado por Telefónica.
- Equipamiento y aplicaciones propiedad del cliente.
- Actos u omisión del cliente o cualquier usuario del servicio autorizado por el cliente.
- Razones de causa mayor

Para efectos de cálculo, no se tienen en cuenta:

- Las oficinas cuya única conexión con la red del cliente, excluidos los respaldos, se realice mediante una línea punto a punto directa entre oficinas de cliente.
- Los motivos de retención de un aviso de avería por “causa del Cliente” o “causa de Usuario” (no disponibles para la realización de pruebas conjuntas, usuario ausente, etc.)
- Las actuaciones en el domicilio del Cliente cuando se realicen con cita concertada, darán lugar a una parada de reloj hasta el instante en que se fije la cita concertada. La cita concertada es un compromiso, establecido de mutuo acuerdo con el Cliente, en el que se fija la fecha y hora de intervención en el domicilio del Cliente para la atención de un aviso de avería.
- En el caso que Telefónica no pueda acceder al lugar de ubicación de los equipos porque no se le facilite el acceso, se suspenderá del cómputo del tiempo de indisponibilidad. El cómputo se reanudará cuando el usuario declarado por el Cliente franquee el acceso a las mencionadas ubicaciones.
- En caso de que el Cliente no tenga contratado el mantenimiento del EDC y sea necesaria una intervención en dicho equipo se dará lugar a una parada de reloj hasta el instante en que se resuelva por el Cliente o su integrador.
- Las averías fuera del horario de resolución de averías (lunes a viernes de 8:00 a 20:00 y sábados de 8:00 a 15:00, domingos y festivos excluidos) relacionadas con el EDC o el acceso. El horario de admisión de solicitudes de reparación es de 24 horas al día, 7 días a la semana.

Cálculo

El tiempo de indisponibilidad se calcula sumando los tiempos de incomunicación de las averías del cliente. Con los datos de averías entregados por el Sistema de Atención a Clientes o Trouble Ticketing (SAC), se mide la disponibilidad mensual de la oficina de un cliente de la siguiente forma:

Disponibilidad de Oficina (mensual) = (Ttot - Tnodisponibilidad_oficina)/ Ttot * 100 (%)

Donde :

Ttot = tiempo total del período considerado expresado en minutos/mes, considerando número de días/mes, 24 horas/día y 60 minutos/hora.

Tnodisponibilidad = tiempo de no disponibilidad de la comunicación entre la oficina y a RPV dentro del intervalo Ttot considerado (minutos). El tiempo de no disponibilidad se contabilizará como la suma de los tiempos de no disponibilidad de todas las averías del cliente para una oficina determinada, en las condiciones expuestas en el anterior apartado de condiciones.

SLA

El compromiso de Disponibilidad de Oficina depende del tipo de oficina y sus valores están detallados en la tabla 21.

Desviación de la Disponibilidad	Compensación económica	
Hasta 0,1 %	1,5%	De la cuota mensual de la Oficina afectada
Entre 0,1 % y 0,3%	3%	
Más de 0,3%	4,5%	

Tabla 21: SLA Disponibilidad de oficina

3.7.2 DISPONIBILIDAD GLOBAL

Definición

Se define la Disponibilidad Global de la Red de Cliente como la media ponderada de las disponibilidades de todas las oficinas del cliente, según se ha definido en apartado Disponibilidad por oficina.

En caso de que el cliente haya identificado un Punto Singular/Punto Central (el cual debe tener contratado algún escenario de Redundancia), cuando se produzca una no disponibilidad del mismo, se considerarán también como no disponibles el resto de oficinas de cliente.

La Red de Cliente puede ser mixta desde el punto de vista de los servicios que la componen, así podrá tener unas oficinas con el servicios VPNIP y otras con MacroLAN. Dentro del escenario de Redirección Plus (definido sólo en MacroLAN) no se considerará como Punto Central el punto destino de la Redirección.

En los casos de VPN Multicliente (VPN formada por sedes de más de un cliente, con diferentes CIFS), por cada periodo de indisponibilidad del Punto Central/Punto Singular, se imputará el mismo periodo de indisponibilidad a toda oficina que tenga conectividad con dicho Punto Central. Independientemente del CIF que tenga esa oficina (que podría ser diferente al del Punto Central). La Disponibilidad Global se presentará para cada uno de los clientes (CIFs) referida al total de sedes que cada uno de ellos tenga contratadas; en este caso NO habrá una disponibilidad global que incluya todas las oficinas que componen la red.

Condiciones

Las mismas que en el apartado Disponibilidad por oficina.

Cálculo

Con los datos de averías entregados por el Sistema de Atención a Clientes o Trouble Ticketing (SAC), se mide la disponibilidad global (mensual) de la oficina de un cliente de la siguiente forma:

Disponibilidad Global (mensual)medida a partir del SAC =Si=1,N_Ofi (D_ Ofii)/N_Ofi * 100 (%)

Donde:

D_ Ofii = Disponibilidad de la oficina i en el período considerado, teniendo en cuenta la indisponibilidad por caídas del Punto Central (este valor es diferente al de Disponibilidad por Oficina del apartado anterior, en el cual sólo se tienen en cuenta las caídas propias de la oficina)

N_Ofi = Número total de oficinas de la red del cliente (sólo se contabilizan las oficinas con acceso pto-pto y/o ADSL que tengan backup y las oficinas TIC sin respaldo). La Red de Cliente constará de un mínimo de 10 Oficinas. En caso contrario, se considerará que la Red de Cliente consta de un número de Oficinas “ficticias” adicionales hasta completar un total de 10 Oficinas, estando estos Oficinas "ficticias" en estado disponible permanentemente

SLA

El compromiso de Disponibilidad Global depende de la distribución y número de oficinas de la red del cliente. A continuación, se muestra la tabla 22 con los coeficientes por tipo de oficina utilizados para el cálculo del valor de compromiso y la fórmula que indica como calcularlo a partir de dichos coeficientes

Tipos de Oficina	Escenario de Oficina		
	Sin Respaldo	Con Respaldo	
Oficina con Accesos Fibra	99,95%	Diversificado Fibra	Otros accesos de cobre
		99,97 %	
Oficina CDG (Fibra o dedicado)	99,95%		
Oficina dedicado red	99,50 %	99,80%	
Oficina ADSL	-	99,25%	

Tabla 22: SLA Disponibilidad Global

SLA Global = (N_Ofi_fibra_sin_respaldo*99.95+ N_Ofi_fibra_con_respaldo*99.97+ N_Ofi_pto-pto_sin_respaldo * 99,50 + N_Ofi_pto-pto_con_respaldo*99.8 N_Ofi_CDG * 99,95 + N_Ofi_ADSL_con_respaldo * 99,25) / N_Ofi (%)

Donde

N_Ofi_fibra_sin_respaldo= Número de oficinas MacroLAN con acceso principal de fibra y sin respaldo.
N_Ofi_fibra_con_respaldo= Número de oficinas MacroLAN con acceso principal y de respaldo
N_Ofi_pto-pto_sin_respaldo = Número de oficinas pto-pto sin respaldo de la red del cliente
N_Ofi_pto-pto_con_respaldo = Número de oficinas VPN cuyo acceso principal es pto-pto con respaldo (A través de Red).
N_Ofi_CDG = Número de oficinas con acceso dedicado en CDG de la red del cliente..
N_Ofi_ADSL_con_respaldo = Número de oficinas VPN IP cuyo acceso principal es ADSL con respaldo de la red del cliente. (no se contabilizan las oficinas mixtas de MacroLAN y VPNIP con ADSL).
N_Ofi = Número total de oficinas de la red del cliente sujetas a un SLA de Disponibilidad de Oficina, es decir, la suma de todos los tipos de oficina citados en los puntos anteriores de este apartado.

3.7.3 PÉRDIDA DE PAQUETES

Definición

Telefónica garantiza que el valor de pérdida de paquetes en su Red IP, se encuentra por debajo de un valor máximo para cada una de las Clases de Servicio.

La pérdida de paquetes es un concepto global para la red sobre la que se mide. Como depende de ésta y no del cliente, los valores medidos en la red son aplicables para todos los clientes. Hay un valor de pérdida de paquetes diferente por cada tipo de Clase de Servicio.

Condiciones

Al ser un parámetro de red, no se incluye en el cálculo, los tiempos correspondientes a los accesos.

También quedan excluidos los retardos relativos a los periodos programados de mantenimiento y actualización de la Red IP, así como los escenarios Provinciales del Servicio MacroLAN (sólo aplica este SLA para caudales Nacionales de MacroLAN).

Cálculo Pérdida Diaria de Paquetes

Se mide como el valor medio máximo diario de los porcentajes de paquetes perdidos entre los nodos de la Red IP. Se corresponde con el valor más alto de la pérdida de paquetes entre nodos. Se calcula como la media aritmética de todos los valores medidos (por clase de servicio) para obtener un valor único por cada CoS.

SLA

En la Tabla 23 podemos encontrar los SLAs correspondientes a cada tipo de tráfico cursado:

Pérdida Diaria de Paquetes	SLA
Clase Plata	< o igual a 0,9 %
Clase Oro	< o igual a 0,8 %
Clase Multimedia	< o igual a 0,7 %

Tabla 23: SLA Pérdida diaria de paquetes

Cálculo Pérdida de Paquetes

Se calcula el porcentaje de días que cumple el valor comprometido de Pérdida de paquetes diarios. Para calcular dicho porcentaje se obtiene, para una clase de servicio, todos los días de un mes que la Pérdida de paquetes de la Red IP en Red tenga un valor superior al Valor máximo de Paquetes perdidos Diariamente de la red IP (SLA diario). Y se aplicará la siguiente fórmula:

% Días de cumplimiento = (Número días que cumple el SLA / Número de días de un mes) * 100

El SLA asegurado apra cada tráfico cursado es el presentado en la Tabla 24:

Pérdida de Paquetes	SLA
Clase Plata	80 %
Clase Oro	80 %
Clase Multimedia	80 %

Tabla 24: SLA Pérdida de paquetes

3.7.4 RETARDO DE TRÁNSITO EN LA RED IP

Definición

El Retardo en red IP es el tiempo de transmisión medio en milisegundos entre los nodos de la red. Se considera como tiempo de transmisión, el tiempo de ida y vuelta de un paquete de prueba.

El retardo de tránsito es un concepto global para la red sobre la que se mide. Como el retardo depende de la red y no del cliente, existirá un valor único válido para todos los clientes de Telefónica. Hay valores diferenciados para cada Clase de Servicio.

Condiciones

Al ser un parámetro de red, no se incluye en el cálculo, los tiempos correspondientes a los accesos.

También quedan excluidos los retardos relativos a los periodos programados de mantenimiento y actualización de la Red IP, así como los escenarios Provinciales del Servicio MacroLAN (sólo aplica este SLA para caudales Nacionales de MacroLAN).

Cálculo Retardo de Tránsito Diario

El sistema de Gestión de Red realizará medidas periódicas de retardo entre los distintos nodos de la Red IP, generando una tabla con las sucesivas medidas. Diariamente se calculará la media aritmética de estas medidas para obtener un valor único para cada clase de servicio.

SLA

Se establece el compromiso de retardo medio diario presentado en la tabla 25:

Retardo Tránsito Diario	SLA
Clase Plata	45 mseg
Clase Oro	35 mseg
Clase Multimedia	25 mseg

Tabla 25: SLA Retardo de tránsito diario

Cálculo Retardo de Tránsito

Porcentaje de días que cumple el valor comprometido de Retardo de la Red IP.

Para calcular dicho porcentaje se obtiene todos los días de un mes y una clase de servicio que el Retardo de Tránsito de la red tenga un valor inferior o igual al Valor máximo de Retardo Diario de la red (SLA diario). Y se aplicará la siguiente fórmula:

% Días de cumplimiento = (Número de días que cumple el SLA / Número de días de un mes) * 100

SLA

El valor comprometido de días que se debe cumplir estos valores es el presentado en la tabla 26:

Retardo Tránsito	SLA
Clase Plata	80 %
Clase Oro	80 %
Clase Multimedia	80 %

Tabla 26: SLA Retardo tránsito

3.7.5 JITTER EN RED IP

Definición

El Jitter en Red IP es un parámetro que se mide únicamente en la clase multimedia del caudal. Se define como la diferencia de retardo entre un paquete y el siguiente en la transmisión de la comunicación.

Condiciones

Al ser un parámetro de red, no se incluye en el cálculo, los tiempos correspondientes a los accesos.

También quedan excluidos los retardos relativos a los periodos programados de mantenimiento y actualización de la Red IP, así como los escenarios Provinciales del Servicio MacroLAN (sólo aplica este SLA para caudales Nacionales de MacroLAN).

Cálculo Jitter Diario

Se calcula como la media aritmética de todas las medidas hechas periódicamente.

SLA Jitter Diario

Se establece el compromiso de jitter medio diario presentado en la tabla 27:

Jitter Diario	SLA
Clase Multimedia	2 mseg

Tabla 27: SLA Jitter diario

Cálculo Jitter en Red

Se calcula el porcentaje de días que cumple el valor comprometido de Jitter Diario.

Para calcular dicho porcentaje se obtiene todos los días de un mes que el Jitter Diario en Red tenga un valor inferior o igual al Valor máximo de Jitter en Red diario. Y se aplicará la siguiente fórmula:

% Días de cumplimiento = (Número de días que cumple el SLA / Número de días de un mes) * 100

SLA

El valor objetivo de días que debe cumplir estos valores es el de la tabla 28:

Jitter en Red	SLA
Clase Multimedia	80%

Tabla 28: SLA Jitter en red

3.7.6 DISPONIBILIDAD DE LA PLATAFORMA DE BACKUP REMOTO

Definición

Disponibilidad de la plataforma, medido a partir de la disponibilidad del portal para poder solicitar backups y restores.

Condiciones

La disponibilidad de servicio se medirá a partir de los tickets de avería registrados por el cliente, computando desde el momento de apertura de la incidencia hasta su resolución.

Quedan excluidos del cálculo los tiempos que coincidan con los periodos de inactividad planificados, que son ventanas programadas para la realización de actividades que tendrán como objetivo el mantenimiento de la disponibilidad acordada.

Cálculo

$$\%Disp = \frac{Tiempo\ periodo - Tiempo\ sin\ servicio}{Tiempo\ periodo} * 100$$

Donde "Tiempo sin servicio" es el sumatorio de los tiempos computados por las diversas averías registradas por el cliente en el periodo. No se computará el tiempo de aquellas averías que finalmente sean diagnosticadas como causa de cliente o debida a elementos ajenos al servicio. En el periodo de resolución de la incidencia se descontarán igualmente las paradas de reloj debidas a causa del cliente.

Los tiempos se medirán en minutos.

SLA

El SLA a cumplir es el presentado en la tabla 29:

Descripción	SLA
Disponibilidad de la plataforma de Backup Remoto	99,9%

Tabla 29: SLA Disponibilidad plataforma Backup remoto

3.7.7 ALIMENTACIÓN ELÉCTRICA EN EL CDG

Definición

Telefónica garantiza la provisión permanente (**disponibilidad 100**%) de alimentación AC a las cabinas y equipos de cliente. Si la disponibilidad mensual se viera reducida en las cifras que se detallan en la tabla 30, el cliente tendría derecho a reclamar una compensación en la cuota mensual del total de los servicios afectados.

Condiciones

Esta garantía no cubre las interrupciones motivadas por defectos o alteraciones en (1) circuitos o equipos del cliente, (2) aplicaciones o equipos del cliente, así como por (3) actos u omisiones del cliente, o debidos a cualquier uso o usuario autorizado por éste o (4) causas de fuerza mayor. La disponibilidad 100% está supeditada a la existencia en equipos de cliente con doble fuente de alimentación.

Cálculo

La periodicidad del cálculo es mensual y se tendrá en cuenta toda la planta del contrato.

La disponibilidad de la alimentación eléctrica se calculará utilizando la siguiente fórmula:

$$\%Disp = \frac{\text{Tiempo periodo} - \text{Tiempo sin servicio}}{\text{Tiempo periodo}} * 100$$

Donde:

Tiempo periodo: Total de horas de disponibilidad comprometida durante un periodo de tiempo. En este tiempo se han de restar los tiempos correspondientes a las ventanas de mantenimiento preventivo, o tiempos de indisponibilidad debidos a fallos que no sean responsabilidad de Telefónica.

Tiempo sin servicio: Total de horas de indisponibilidad durante un periodo de tiempo.

SLA

Descripción	SLA
Alimentación eléctrica en el CDG	100 %

Tabla 30: SLA Alimentación eléctrica en el CDG

3.7.8 DISPONIBILIDAD DE LA RED DE COMUNICACIONES DEL CDG.

Definición

Telefónica garantiza la disponibilidad de la Red LAN de Comunicaciones del CDG, asegurando la máxima conectividad de cliente dentro del centro de datos y la máxima privacidad entre sus circuitos y el resto de circuitos del CDG. Si la disponibilidad se viera reducida en las cifras que se detallan en la tabla 31, el cliente tendría derecho a reclamar una compensación final de su cuota mensual del total de los servicios afectados.

Condiciones

Esta garantía no cubre las interrupciones motivadas por defectos o alteraciones en (1) circuitos o equipos del cliente, (2) aplicaciones o equipos del cliente, así como por (3) actos u omisiones del cliente, o debidos a cualquier uso o usuario autorizado por éste o (4) causas de fuerza mayor. Tampoco aplica a la conectividad WAN que pudiera formar parte del proyecto.

Cálculo

La disponibilidad de la Red de Comunicaciones del CDG se calculará utilizando la siguiente fórmula:

$$\%Disp = \frac{Tiempo\ periodo - Tiempo\ sin\ servicio}{Tiempo\ periodo} * 100$$

Donde:

Tiempo periodo: Total de horas de disponibilidad comprometida durante un periodo de tiempo. En este tiempo se han de restar los tiempos correspondientes a las ventanas de mantenimiento preventivo, o tiempos de indisponibilidad debidos a fallos que no sean responsabilidad de Telefónica.

Tiempo sin servicio: Total de horas de indisponibilidad durante un periodo de tiempo.

Esta fórmula se aplicará a cada nodo del contrato mediante medidas realizadas desde una sonda instalada en la red de Comunicaciones de Servicio del CDG, de manera que se midan todos los elementos de Red.

La periodicidad del cálculo es mensual y se tendrá en cuenta toda la planta del contrato.

SLA

Descripción	SLA
Disponibilidad de la red de comunicaciones en el CDG	100 %

Tabla 31: SLA Disponibilidad de la red de comunicaciones en el CDG

3.7.9 DISPONIBILIDAD DEL SERVICIO

Definición

Se considerará que la plataforma está disponible cuando el servicio, desde el punto de vista de negocio, esté **activo y prestando servicio** en condiciones de rendimiento que no penalice los tiempos de respuesta de los servicios que soporta el/los servidores.

Condiciones

En el caso de que se configure la plataforma en alta disponibilidad si la caída de uno de los servidores provoca un rendimiento que penaliza los tiempos respuesta de los servicios ofrecidos, el cliente deberá comprometerse a una ampliación de dichos servidores para que no se produzca dicho efecto y como condición para que Telefónica pueda seguir asumiendo los niveles de servicio y penalizaciones acordadas. En el caso en que esta caída no afecte al servicio, no afectaría a las medidas de disponibilidad.

Los elementos que componen el servicio y sobre los que se aplicará este indicador serán definidos en la fase de implantación de SLAs.

Cálculo

La disponibilidad del servicio de hosting administrado se calculará utilizando la siguiente fórmula:

$$\%Disp = \frac{\text{Tiempo periodo} - \text{Tiempo sin servicio}}{\text{Tiempo periodo}} * 100$$

Donde:

Tiempo periodo: Total de horas de disponibilidad comprometida durante un periodo de tiempo. En este tiempo se han de restar los tiempos correspondientes a las ventanas de mantenimiento preventivo, o tiempos de indisponibilidad debidos a fallos que no sean responsabilidad de Telefónica.

Tiempo sin servicio: Total de horas de indisponibilidad durante un periodo de tiempo.

Esta fórmula se aplicará a cada elemento de servicio del contrato mediante medidas realizadas desde una sonda instalada en la red de Comunicaciones de Servicio del CDG, de manera que se midan todos los elementos de Red. Se realizarán tantos tipos de medidas como sean necesarias para registrar todos los elementos de servicio a través de testeos transaccionales que simulen la visión de negocio(usuario) del proyecto.

La periodicidad del cálculo es mensual y se tendrá en cuenta toda la planta del contrato.

SLA

El SLA a cumplir es el presentado en la tabla 32:

Descripción	SLA
Disponibilidad del servicio	99.90 %

Tabla 32: SLA Disponibilidad del servicio

3.7.10 TIEMPO DE RESPUESTA ANTE INCIDENCIAS

Definición

El cliente dispone de un soporte telefónico para la atención de las incidencias acaecidas en el servicio contratado. Las incidencias deben ser atendidas en el número indicado a tal efecto (soporte 24x7). En ocasiones, aplicará las incidencias notificadas por el cliente a través del Portal TI.

Condiciones

El tiempo de respuesta, se define como el tiempo transcurrido entre el momento en que el cliente notifica la avería y el momento en que un técnico del servicio empieza a trabajar en la resolución del problema y además se realiza la primera comunicación con el cliente, si fuera necesario, informándole del análisis de las causas de avería y las acciones correctivas a realizar, con los plazos en los que se llevarán a cabo.

Cada incidencia está asociada a un nivel de severidad descrito a continuación:

- Severidad Nivel 1 (Crítico): El servicio no está totalmente disponible o está seriamente afectado. No existen alternativas disponibles para que los usuarios de dicho servicio puedan acceder al mismo. La Avería tiene que resolverse lo más pronto posible.

- Severidad Nivel 2 (Grave): El servicio no es crítico, no está disponible para muchos usuarios, o no está disponible en absoluto para algunos usuarios en particular. No existen alternativas disponibles para que los usuarios de dicho cliente puedan acceder al servicio.

- Severidad Nivel 3 (Leve): Individualmente está interrumpido o no le permite usar todas las funcionalidades. Existen alternativas disponibles para la ejecución en forma precaria de las actividades. Algunas tareas pueden quedar afectadas antes hasta que la Avería sea resuelta

Esta categorización se detallará y tipificará en la fase de implantación de los SLAs de acuerdo a las características del servicio.

SLA

La tabla 33 muestra los SLAs correspondientes al tiempo de respuesta ante incidencias

Niveles de Severidad	SLA	Horario
1	30 Minutos	24x7
2	1 Hora	24x7
3	2 Horas	Primario
	4 Horas	24x7

Tabla 33: SLA Tiempo de respuesta ante incidencias

3.7.11 TIEMPO DE RESOLUCIÓN DE SOLICITUDES O PETICIONES DE SERVICIO

Definición

Se define el tiempo de resolución como el tiempo transcurrido desde el momento en que el cliente realiza una solicitud a Telefónica y el momento en que se notifica al cliente con la resolución de la solicitud. Estas solicitudes pueden realizarse por el panel de control del servicio o herramienta equivalente (Portal TI).

Condiciones

Las solicitudes que se pueden realizar dentro del servicio estándar de Housing son las siguientes:

- Reglas de FW
- Solicitudes de entrada a salas del TIC
- Configuración DNS
- Backup
- Otras a tipificar

Las solicitudes catalogadas como "Otras" se tipificarían en la fase de implantación de los SLAs acordándose un tiempo de compromiso al que aplicaría el exceso marcado en el apartado "Penalizaciones"

El nivel de atención y resolución de solicitudes se establece en horario de 9:00 a 18:00 de lunes a viernes no festivos respecto al calendario laboral de los Centros de Competencia Técnica y su valor de compromiso es de 24 h. dentro de este horario.

Cálculo

La métrica del SLA de tiempo de resolución ante solicitudes de cambio de servicio realizadas se considera la media de la diferencia entre tiempo de apertura y el de cierre de tickets dentro del Sistema de Gestión de Averías de todas las peticiones del cliente (por contrato) realizadas y tipificadas como solicitudes de cambio de servicio y pertenecientes al mes de cálculo

Se calcula la media del tiempo del cierre de dichas solicitudes registradas durante el periodo.

SLA

El SLA a cumplir aparece en la tabla 34:

Descripción	SLA
Tiempo de Resolución de Solicitudes o Peticiones de Servicio	1.5 h

Tabla 34: SLA Tiempo de Resolución de Solicitudes o Peticiones de Servicio

3.7.12 TIEMPO DE RESOLUCIÓN DE OPERACIONES BÁSICAS

Definición

Se define el tiempo de resolución de una operación básica como el tiempo trascurrido desde que en cliente solicita este tipo de operaciones a través de la herramienta correspondiente y el momento en el que dicha operación ha sido realizada.

Condiciones

Las operaciones básicas que se incluyen dentro de servicio son:

- Chequeo de equipos
- Reboot de equipos
- Backup/Restore para backup dedicado (soporte al backup dedicado)
- Operaciones que de forma general no entrañan una dificultad añadida y están recogidas en el protocolo de mantenimiento.

Cálculo

La métrica del SLA de tiempo de resolución de Operaciones básicas realizadas se considera la media de la diferencia entre tiempo de apertura y el de cierre de tickets dentro del Sistema de Gestión de Averías de todas las peticiones del cliente (por contrato) realizadas y tipificadas

SLA

El SLA a cumplir aparece reflejado en la tabla 35:

Descripción	SLA
Tiempo de Resolución de Operaciones Básicas	45 min.

Tabla 35: SLA Tiempo de resolución de operaciones básicas

3.7.13 DISPONIBILIDAD DEL SERVIDOR

Condiciones

Medido a partir de la monitorización de la máquina virtual.

No se considerará indisponibilidad dentro de este SLA la debida a fallo de cualquier aplicación SW instalada en la máquina virtual, incluido el sistema operativo, ni aquellas que sean imputables a causa de cliente.

SLA

El SLA a cumplir es el reflejado en la tabla 36

Descripción	SLA
Disponibilidad del servidor	99,4% (Mensual)

Tabla 36: SLA Disponibilidad del servidor

3.7.14 TIEMPO MÁXIMO DE RECUPERACIÓN DE UN SERVIDOR VIRTUAL

Condiciones

Medido a partir de la monitorización de la máquina virtual. Se considera exclusivamente el tiempo desde que se detecta la alarma de caída del servidor, hasta que este está de nuevo operativo sobre otra máquina física. No se considera el tiempo de arranque de ninguna aplicación SW en el servidor, ni retrasos que sean imputables a causa cliente.

SLA

El SLA a cumplir viene reflejado en la tabla 37:

Descripción	SLA
Tiempo máximo de recuperación de un servidor virtual	15 minutos

Tabla 37: SLA Tiempo máximo de recuperación de un servidor virtual

3.8 INFORMES DE CLIENTE

3.8.1 DESCRIPCIÓN

Los informes ayudan al cliente a comprobar cuál es el uso del servicio y a disponer de datos contrastables y cuantificables del mismo.

Los informes de cliente se ofrecen a través de la web corporativa de Telefónica. Cada cliente dispone de un usuario que es el único con privilegios para consultar los informes. La comunicación al cliente de dicho usuario se realizar a través de la web de Telefónica (el cliente solo debe informar del NIF de la empresa que ha contratado el servicio, así como del número administrativo asociado a su punto de acceso) y debe conservarlo con la única opción de modificación de la clave de acceso asociada. El cliente solamente puede contar con un único usuario, independientemente del número de puntos de acceso al servicio que contrate. Cuando el cliente acceda a estos informes, se le presenta un panel con el Informe de Configuración y la identificación de cada una de las oficinas. Selecciona una oficina y accede a los informes asociados a dicha oficina.

Formato de Presentación.

El formato de presentación de los informes es muy flexible. Casi todos se pueden obtener con los siguientes formatos: gráfica, tabla o fichero de datos. La excepción son los informes en los cuales no tiene sentido la representación gráfica, que pueden ser presentados como tablas o ficheros.

Los informes del servicio se estructuran de la siguiente forma:

	MACROLAN
SLA	Disponibilidad de Oficina
	Disponibilidad Global
	Pérdida de Paquetes
	Retardo de Tránsito en Red
	Jitter en Red
Configuración	Datos básicos de la configuración del cliente

Tabla 38: Informes de Servicio

3.8.2 COMPROMISOS DE CALIDAD DE SERVICIO

A continuación se detallan algunas aclaraciones comunes a todos los informes de los SLAs.

3.8.2.1 Disponibilidad de Oficina

El Informe de Disponibilidad de Oficina presenta datos sobre el cumplimiento/incumplimiento del SLA del mismo nombre. El informe consta de dos partes: la primera muestra en una tabla las oficinas cuya disponibilidad ha sido inferior al 100% en el mes seleccionado y la segunda parte muestra un detalle para cada oficina con la evolución mensual de su disponibilidad:

- Disponibilidad de las Oficinas con Disponibilidad <100%

Se presenta una tabla (figura 39) con todas las oficinas cuya disponibilidad en el mes indicado ha sido inferior al 100%, con los siguientes datos:

- Identificativo de la Oficina
- Tipo de Oficina.
- Porcentaje de Disponibilidad de la Oficina en el mes seleccionado.

Figura 39: Porcentaje de Disponibilidad de la Oficina en el mes seleccionado

- Disponibilidad de Oficina

Se presenta un buscador por código postal. Una vez seleccionada la oficina se muestran los datos de cumplimiento/incumplimiento del SLA de Disponibilidad de Oficina durante los últimos 13 meses, con la información indicada en la figura 40.

MacroLAN | ID.Oficina: [redacted] | Mayo 2007

DISPONIBILIDAD DE OFICINA

Tipo Oficina	Tráfico hacia el TIC	Redundancia	Dirección	Localidad	Provincia
No TIC	NO	Sin redundancia	[redacted]	[redacted]	MADRID

Caudales Nacionales			Caudales TIC Nacionales		
Plata (Mbps)	Oro (Mbps)	Multimedia (Mbps)	Plata (Mbps)	Oro (Mbps)	Multimedia (Mbps)
200	100	100	-	-	-

Acceso Principal	Acceso Redundante	Velocidad Acceso (Mbps)	Caudal Metropolitano (Mbps)
[redacted]		10	10

Mes - Año	% Disponibilidad Oficina	% SLA	Cumplimiento	% Desviación
MAY-2007	100.00	99.40	CUMPLE	N.A.
ABR-2007	100.00	99.50	CUMPLE	N.A.
MAR-2007	100.00	99.50	CUMPLE	N.A.
FEB-2007	100.00	99.50	CUMPLE	N.A.
ENE-2007	100.00	99.50	CUMPLE	N.A.
DIC-2006	100.00	99.50	CUMPLE	N.A.
NOV-2006	100.00	99.50	CUMPLE	N.A.

Figura 40: Disponibilidad de Oficina

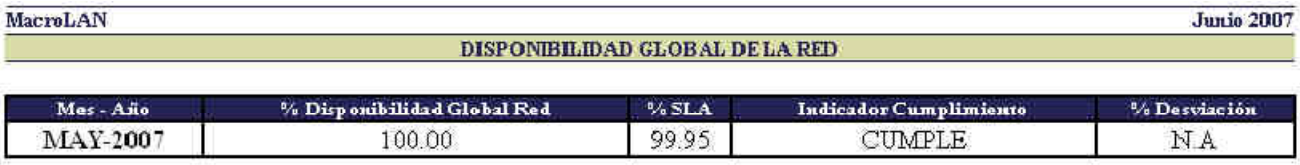
- Datos: En la parte superior de la página se muestran los datos de la oficina seleccionada:
  - ✓ Tipo de Oficina: TIC o NO TIC.
  - ✓ Redundancia: Balanceo de Carga, Backup con 1 EDC, Backup con 2 EDCs, Sin Redundancia, o Sin Definir.
  - ✓ Dirección: Provincia, Localidad, Calle y Número. Si la oficina es TIC, se mostrará la delegación TIC a la que pertenezca.
  - ✓ EDC (modelo).
  - ✓ Valores de los caudales nacionales.
  - ✓ Datos de accesos: En la parte del medio de la página se muestran los datos de los accesos conectados a la oficina.

Se presentan en cada fila los siguientes datos para cada uno de los 13 últimos meses:

- Mes-año
- Porcentaje de Disponibilidad de la Oficina en el mes indicado.
- Porcentaje de Disponibilidad de Oficina Comprometida (SLA): Aquí se indicará el valor del servicio estándar o el SLA mejorado si este últimos se ha contratado.
- Cumplimiento (SLA): CUMPLE / NO CUMPLE con respecto al SLA que aplique (SLA estándar o SLA mejorado en caso de haber contratado este último).
- Porcentaje de la desviación respecto al valor comprometido, en caso de incumplimiento

3.8.2.2 Disponibilidad Global

Se puede mostrar el dato de cumplimiento/incumplimiento del SLA de Disponibilidad Global durante los últimos 13 meses, con la información indicada en la figura 41:



MacroLAN — Junio 2007

DISPONIBILIDAD GLOBAL DE LA RED

Mes - Año	% Disponibilidad Global Red	% SLA	Indicador Cumplimiento	% Desviación
MAY-2007	100.00	99.95	CUMPLE	N.A

Figura 41: Disponibilidad Global

En la figura 40 se presentan los siguientes datos:

- Mes-año
- Porcentaje de Disponibilidad Global en el mes indicado.
- Porcentaje de Disponibilidad Global Comprometida.
- Cumplimiento (SLA): CUMPLE / NO CUMPLE+
- Porcentaje de la desviación respecto al valor comprometido, en caso de incumplimiento

3.8.2.3 Pérdida de Paquetes en Red

En este informe se presenta a nivel mensual, el porcentaje de días que no ha cumplido el SLA de Pérdidas de Paquetes de la Red IP.

Información que se presenta

Este informe presentará por cada mes los siguientes datos:

- Clase de servicio: Este campo podrá tener los siguientes valores Clase Plata, Clase Oro y Clase Multimedia.
- Mes-Año: Mes y año del que se realiza el cálculo. Si se pulsa sobre este campo, se visualizará la gráfica Pérdida Diaria de paquetes de la Red IP.
- % Días de cumplimiento: Porcentaje de días que cumple el valor comprometido.
- SLA: Porcentaje máximo de días en que se puede superar el valor de pérdida diaria de paquetes de red comprometido.
- SLO (Service Level Objectives): Porcentaje objetivo de días en que se puede superar el valor de pérdida de paquetes de red comprometido.
- Nivel de cumplimiento: Sus valores posibles son Cumple, No Cumple, N.A.
- Desviación: Número de porcentaje de desviación entre el valor de SLA y el Porcentaje de días de cumplimiento.

Este informe estará ordenado por la clase de servicio y fecha.

Parámetros del Informe

El cliente podrá visualizar los datos del mes previamente seleccionado.

La permanencia de la información será de los últimos 13 meses.

Formato del Informe

Este informe se presentará al cliente en una tabla como la de la figura 42:

DEMO MACROLAN

MacroLAN — Enero 2004

PERDIDA DE PAQUETES EN RED

Clase Servicio	Mes - Año	% Días Cumplimiento	% SLA	% SLO	Indicador Cumplimiento	% Desviación
Multimedia	ENE-2004	12.90	60.00	N.A	NO CUMPLE	47.10
Oro	ENE-2004	80.65	60.00	N.A	CUMPLE	N.A
Plata	ENE-2004	80.65	60.00	N.A	CUMPLE	N.A

Telefónica Data España, S.A.U. le informa de que los datos incluidos en el presente informe son meramente informativos y pueden sufrir correciones por posibles defectos en la recopilación de los datos y en los cálculos correspondientes. En este sentido, Telefónica Data España, S.A.U. pone en su conocimiento que los citados datos no son vinculantes y no constituyen prueba alguna a la hora de realizar una reclamación, en solicitud de la correspondiente penalización por incumplimiento de la calidad del servicio.

Figura 42: Ejemplo de informe servicio Macrolan

Pinchando en uno de los meses para una clase de servicio determinada, se obtiene una gráfica con las siguientes características:

- Eje X: Día
  - Leyenda: Día
  - Valor de inicio: 01.
  - Valor de fin: Último día del mes con datos de pérdida.
- Eje Y: %
  - Leyenda: Pérdida media (en porcentaje)
  - Valor de inicio: 0
  - Valor de fin: Un valor superior a la mayor pérdida que se haya producido.

Además este informe permitirá visualizar la información en formato de tabla o descargar en disco en formato csv (fichero separado por comas)

En la figura 43 se muestra un ejemplo del aspecto de la gráfica:

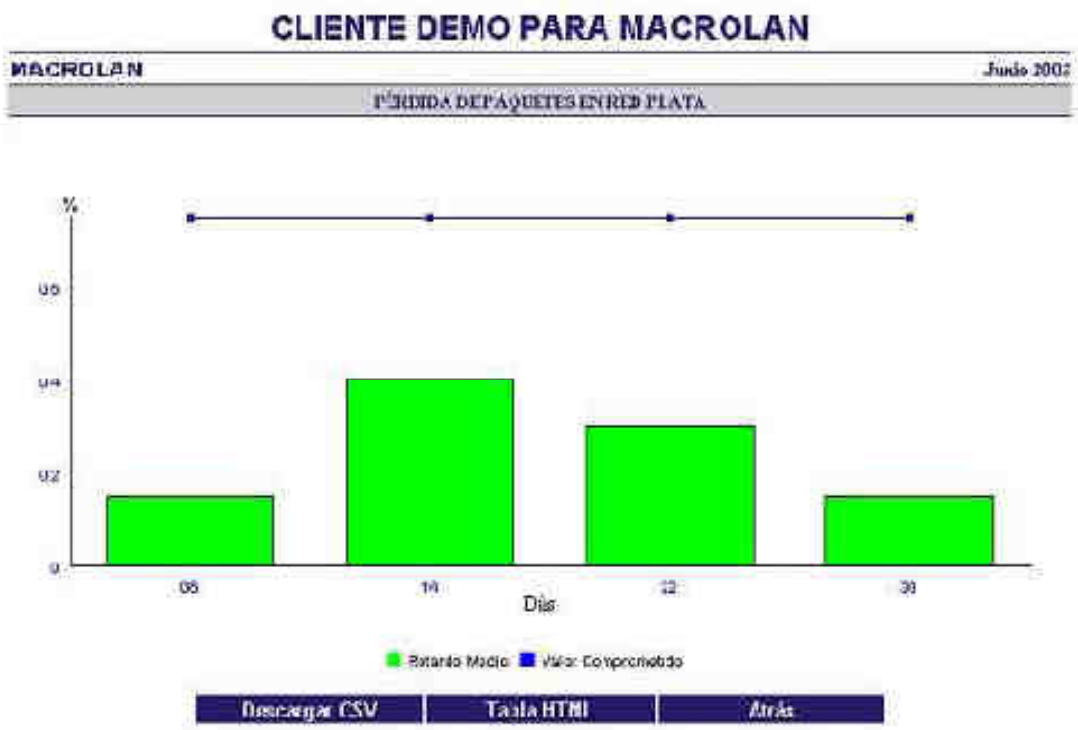


Figura 43: Gráfico informe mensual

3.8.2.4 Retardo de Tránsito en Red

En este informe se presenta a nivel mensual, el porcentaje de días que no ha cumplido el SLA de Retardo de Tránsito en la Red IP.

Información que se presenta

Este informe presentará por cada mes los siguientes datos:

- Clase de servicio: Este campo podrá tener los siguientes valores Clase Plata, Clase Oro y Clase Multimedia.
- Mes-Año: Mes y año del que se realiza el cálculo. Si se pulsa sobre este campo, se visualizará la gráfica Retardo Diario de la Red IP.
- % Días de cumplimiento: Porcentaje de días que cumple el valor comprometido.
- SLA: Porcentaje máximo de días en que se puede superar el valor de retardo diario de red comprometido.
- SLO: Porcentaje objetivo de días en que se puede superar el valor de retardo de red comprometido.
- Nivel de cumplimiento: Sus valores posibles son Cumple, No Cumple, N.A.
- Desviación: Número de porcentaje de desviación entre el Porcentaje de días de cumplimiento y el valor de SLA.

Este informe estará ordenado por la clase de servicio y fecha.

Parámetros del Informe

El cliente podrá visualizar los datos del mes previamente seleccionado.

La permanencia de la información será la de los últimos 13 meses.

Formato del Informe

Este informe se presentará al cliente en una tabla. La figura 44 muestra un ejemplo:

CLIENTE DEMO PARA MACROLAN

MACROLAN — Junio 2003

RETARDO DE TRANSITO EN RED

Clase de Servicio	Mes : Año	% Dias Cumplimiento	% SLA	% SLO	Indicador Cumplimiento	% Desviacion
Plata	JUN-2003	66.67	80.00	80.00	NO CUMPLE	13.33
Plata	MAY-2003	46.67	30.00	30.00	CUMPLE	N.A.
Oro	JUN-2003	86.67	80.00	80.00	CUMPLE	N.A.
Oro	MAY-2003	46.67	50.00	50.00	NO CUMPLE	4.33
Multimedia	JUN-2003	23.27	30.00	30.00	NO CUMPLE	7.63
Multimedia	MAY-2003	33.27	30.00	30.00	CUMPLE	N.A.

Figura 44: Informe retardo de tránsito de red

Pinchando en una clase de servicio para un mes determinado se obtiene una gráfica con las siguientes características:

- Eje X: Día
  - Leyenda: Día
  - Valor de inicio: 01.
  - Valor de fin: Último día del mes con datos de retardo.
- Eje Y: Milisegundos
  - Leyenda: Retardo medio (milisegundos)
  - Valor de inicio: 0
  - Valor de fin: Un valor superior al mayor retardo que se haya producido.

Además este informe permitirá visualizar la información en formato de tabla o descargar en disco en formato csv (fichero separado por comas).

La figura 45 muestra un ejemplo de la gráfica:

Figura 45: Gráfico mensual informe retardo de tránsito de red

3.8.2.5 Jitter en Red

Se presentarán al cliente una tabla con los datos de cumplimiento e incumplimiento del SLO de Jitter y una gráfica con los valores de jitter medio diarios obtenidos del mes seleccionado.

Información que se presenta

Este informe presentará por cada mes los siguientes datos:

- Mes-Año: Mes y año del que se realiza el cálculo. Si se pulsa sobre este campo, se visualizará la gráfica Jitter en Red Diaria.
- % Días de cumplimiento: Porcentaje de días que cumple el valor comprometido.
- SLA: Porcentaje máximo de días en que se puede superar el valor de jitter de red comprometido.
- SLO: Porcentaje objetivo de días en que se puede superar el valor de jitter de red comprometido.
- Nivel de cumplimiento: Sus valores posibles son Cumple, No Cumple, N.A.
- Desviación: Número de porcentaje de desviación entre el Porcentaje de días de cumplimiento y el valor de SLA.

Este informe se ordenará mediante la fecha.

Parámetros del Informe

El cliente podrá visualizar los datos del mes previamente seleccionado.

La permanencia de la información será la de los últimos 13 meses.

Formato del Informe

Este informe se presenta en una tabla como el ejemplo de la figura 46:

CLIENTE DEMO PARA MACROLAN

MACROLAN — Junio 2003

JITTER EN RED

Mes - Año	% Dias Cumplimiento	% SLA	% SLO	Indicador Cumplimiento	% Desviación
JUN-2003	66.67	60.00	60.00	CUMPLE	N.A.
MAY-2003	46.67	50.00	50.00	NO CUMPLE	3.33

Telefónica Data España, S.A.U. le informa de que los datos incluidos en el presente informe son meramente informativos y pueden sufrir correcciones por posibles defectos en la recopilación de los datos y en los cálculos correspondientes. En este sentido, Telefónica Data España, S.A.U. pone en su conocimiento que los citados datos no son vinculantes y no constituyen prueba alguna a la hora de realizar una reclamación, en solicitud de la correspondiente penalización por incumplimiento de la calidad del servicio.

Figura 46: Informe Jitter en red

Al pinchar sobre un mes concreto se obtiene información diaria sobre el jitter en la red IP en forma de gráfica, con las siguientes características:

- Eje X: Día
  - Leyenda: Día
  - Valor de inicio: 01.
  - Valor de fin: Último día del mes con datos de retardo.

- Eje Y: Milisegundos
  - Leyenda: Jitter medio (milisegundos)
  - Valor de inicio: 0
  - Valor de fin: Un valor superior al mayor retardo que se haya producido.

Además este informe permite visualizar la información en formato de tabla o descargar en disco en formato csv (fichero separado por comas).

En la figura 47 se muestra un ejemplo de su aspecto:

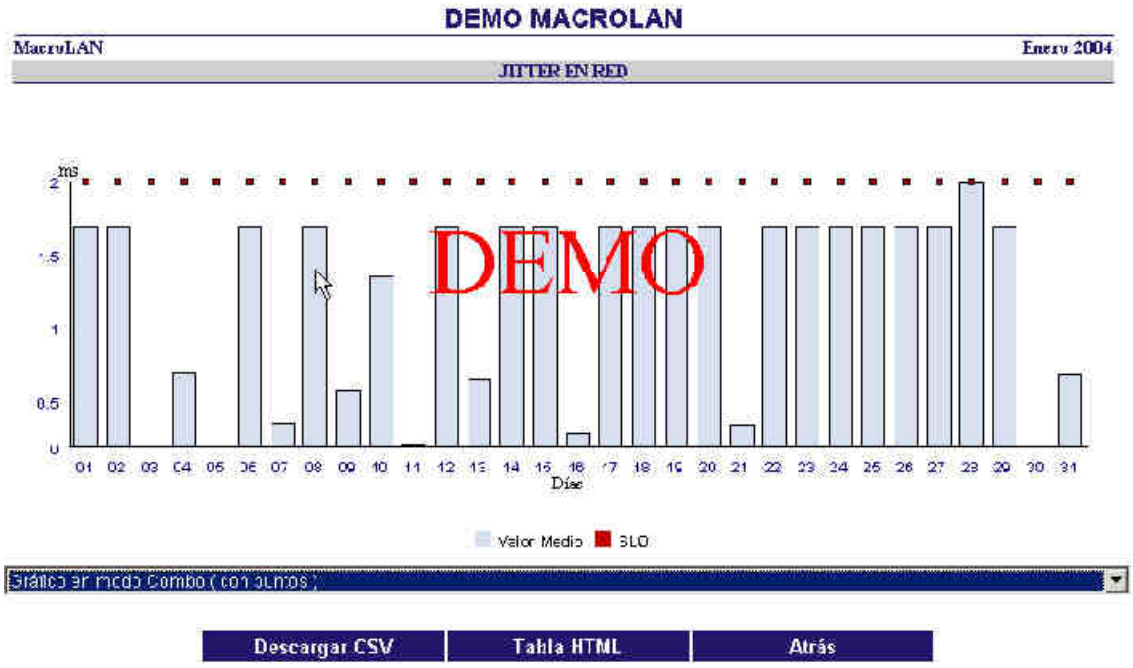


Figura 47: Informe Jitter en red formato tabla

3.8.2.6 Configuración

Recoge la información sobre la configuración de los accesos contratados por el cliente y el caudal definido sobre estos. Esta información será presentada al cliente mediante una tabla, que contendrá para cada Caudal contratado por el cliente los siguientes datos:

- Identificador de Oficina: Será el mnemónico del EDC. En los escenarios de redundancia con balanceo, se considera que son 2 oficinas. En los escenarios de redundancia con backup, se considera que es una única oficina (en el escenario con dos EDC, el id. oficina será el mnemónico del EDC principal).
- Dirección de instalación: En este orden: Calle, número, localidad, provincia. En el caso de sedes en el TIC aparecerá "TIC-Madrid", "TIC-Barcelona", etc.
- Redundancia del acceso: Balanceo de Carga, Backup con 1 EDC, Backup con 2 EDCs, No y Sin Definir.
- EDC Principal: Fabricante, modelo del EDC
- Acceso Principal: Se mostrará el acceso MetroLAN o el acceso TIC principal
- Velocidad: 10, 100, 1000 Mbps.
- Acceso redundante: Se mostrará el número de administrativo del acceso MetroLAN o el Acceso TIC redundante.
- Caudal de acceso Metropolitano: es el caudal de acceso de MetroLAN sobre el acceso principal. En Mbps. Será la suma de todos los caudales metropolitanos.
- Caudal Nacional Clase Plata: se indicará el caudal nacional Plata compartido en Mbps al que tiene acceso la oficina en cuestión. Para la oficina en el TIC, este caudal será el caudal TIC Nacional. Se mostrará la suma de los caudales nacionales plata para dicha oficina.

- Caudal Nacional Clase Oro: se indicará el caudal nacional Oro compartido en Mbps al que tiene acceso la sede en cuestión. Para la sede en el TIC, este caudal será el caudal TIC Nacional. Se mostrará la suma de los caudales nacionales oro para dicha oficina.
- Caudal Nacional Clase Multimedia: se indicará el caudal nacional Multimedia compartido en Mbps al que tiene acceso la sede en cuestión. Para la sede en el TIC, este caudal será el caudal TIC Nacional. Se mostrará la suma de los caudales nacionales multimedia para dicha oficina.

En la figura 48 puede observarse, a modo de ejemplo, como aparecen los datos anteriores de configuración para un cliente cuya RPV está constituida por tres sedes MacroLAN.

MacroLAN Junio 2007

CONFIGURACIÓN

Administrativo: Código Postal: Buscar

ID. Oficina	Dirección Instalación	EDC Principal	Redundancia	Acceso Principal	Velocidad Acceso (Mbps)	Acceso Redundante	Tráfico hacia el TIC	Caudal Metro politano (Mbps)	Caudal Nacional (Mbps)			Caudal TIC Nacional (Mbps)		
									Plata	Oro	Multi media	Plata	Oro	Multi media
	BARCELONA	Catalyst 3550-24 EMI	Sin Redundancia	FO_ 0	100	-	NO	100	60 -	- 3	- 3	- -	- -	- -
	VIZCAYA	Catalyst 3550-24 EMI	Sin Redundancia	FO_ 6	100	-	NO	100	60	-	-	-	-	-
	VIZCAYA	Catalyst 3550-24 EMI	Sin Redundancia	FO_ 7	100	-	NO	100	60	-	-	-	-	-

Figura 48: Informe de configuración

3.8.2.7 Informes específicos para el servicio Hosting Virtual

En el caso del servicio de Hosting Virtual, los informes se generan como resultado de la monitorización de rendimiento de los servidores.

Todas las gráficas mostrarán las métricas de referencia, los niveles de rendimiento e intervalos de tiempo, como se puede ver en la figura 49.

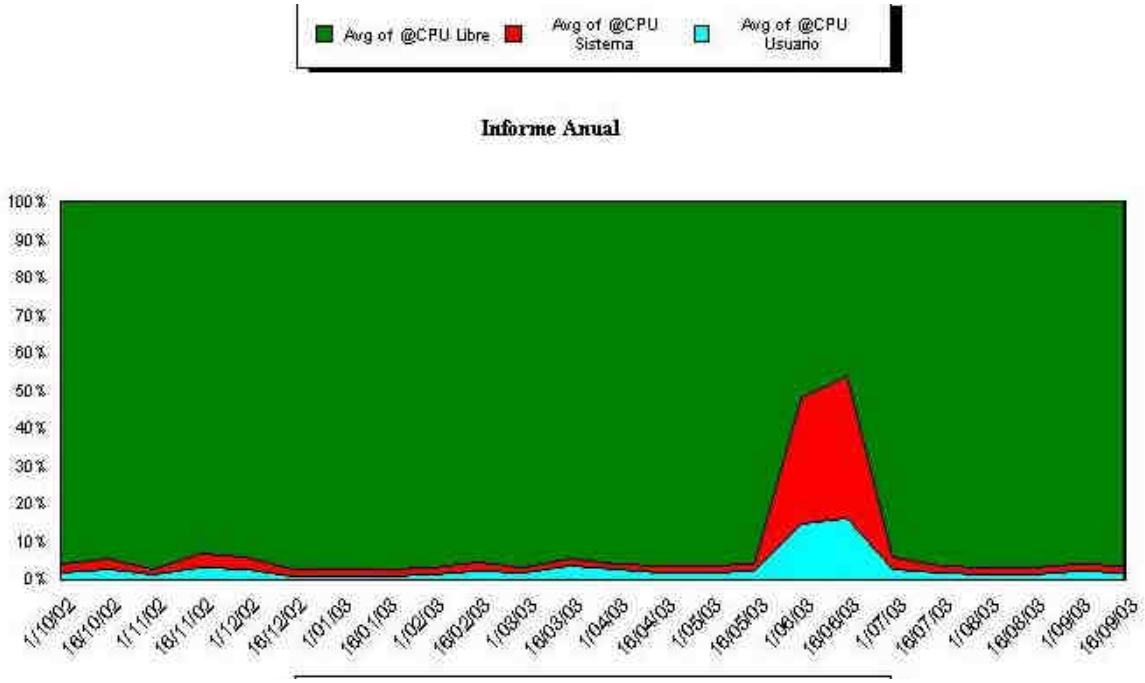


Figura 49: Ejemplo de informe anual

Los informes se agrupan en dos modalidades:

- Informes agregados por grupo de servidores.
- Informes por servidor.

En el caso de informes por grupo de servidores se mostrará un "top 10" de los servidores con mayor consumo de CPU y memoria. Los informes se mostrarán por agrupaciones lógicas de máquinas, no pudiendo mezclarse máquinas de diferentes entornos operativos (Unix o Windows).

Cada informe se presentará mediante 4 gráficas mostrando las mediciones obtenidas en diferentes intervalos de tiempo:

- Diaria
- Semanal (últimos 7 días)
- Mensual (últimos 30 días)
- Anual

Los parámetros de rendimiento estándar monitorizados, tanto en equipos Windows como Unix, son:

- Informes por grupos de servidores

    - Consumo de CPU.

    Detalla la utilización de CPU durante el intervalo de tiempo definido, comparando el comportamiento respecto a máquinas de su misma categoría (Windows, Unix) y agrupación lógica. Es un valor en tanto por ciento de ocupación. La métrica es recolectada cada 5 minutos y se promedian todas las medidas recogidas en el día, para ofrecer el valor medio de utilización de CPU.

- Consumo de Memoria RAM.

Este informe muestra los sistemas que más paginación de memoria han realizado durante la semana. El gráfico muestra el número total de páginas transferidas por cada sistema. Se trata de un informe para comparar el comportamiento de los diferentes sistemas. Un informe de ejemplo se presenta en la figura 50.

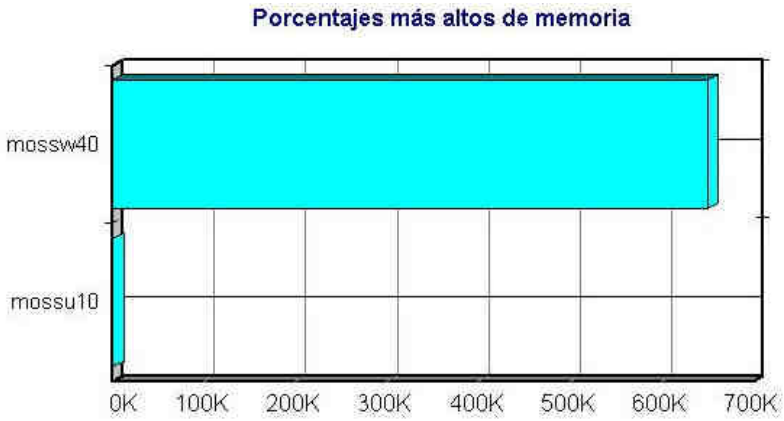


Figura 50: Informe consumo memoria RAM

- Informes por servidor

  - Consumo de CPU.

Este informe muestra el consumo de CPU de Sistema y libre de la máquina dentro del intervalo indicado en cada gráfica. Se trata de un valor porcentual.

  - Uso de Memoria por sistema

Este informe muestra el porcentaje de memoria ocupado y libre de la máquina, en intervalos diarios, semanales, mensuales y anuales (figura 51).

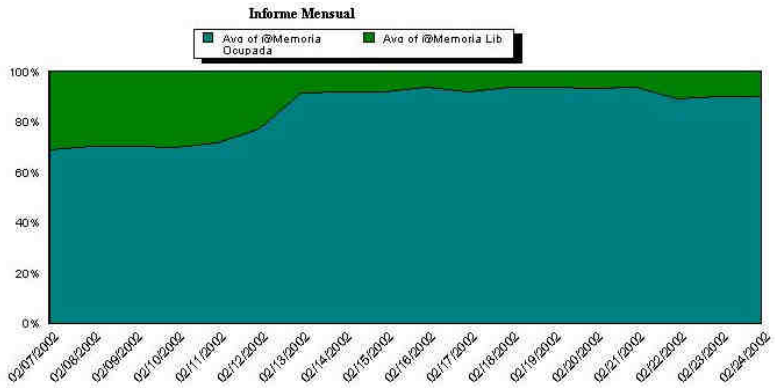


Figura 51: Uso de la memoria por cada sistema

- Paginación y Swapping.

  Este informe muestra el tamaño del fichero de swap de la máquina, en intervalos diarios, semanales, mensuales y anuales.

3.8.2.8 Informes específicos para el servicio Backup Remoto

El servicio proporcionará al cliente un sistema de notificación y envío de diferentes informes a visualizar. El cliente seleccionará en fase de provisión los informes por Dominio deseados de:

- Espacio protegido en Gb por nodo
- Informe de jobs diario
- Informe de jobs Semanal
- Informe Espacio total ocupado por Contrato
- Informe Espacio total ocupado por nodo
- Informe Mensual de Jobs por nodo
- Informe Mensual del total de espacio ocupado por máquina y el total contratado.
- Listado de Nodos y filesystem respaldados
- Listado de planificaciones activas

3.8.2.9 Informes específicos para el Servicio Tráfico Limpio

El servicio de Tráfico Limpio de Internet incluye informes de navegación y de filtrado de contenidos que serán remitidos a los interlocutores seleccionados por el cliente según la periodicidad que se desee.

- **Informes de navegación**
  Los informes de navegación a los que tendrá acceso el cliente son los siguientes:

  - Actividad por día de la semana (figura 52)
  - Actividad por día del mes
  - Actividad por hora del día
  - Direcciones IP más activas
  - Sitios web más visitados
  - Usuarios más activos

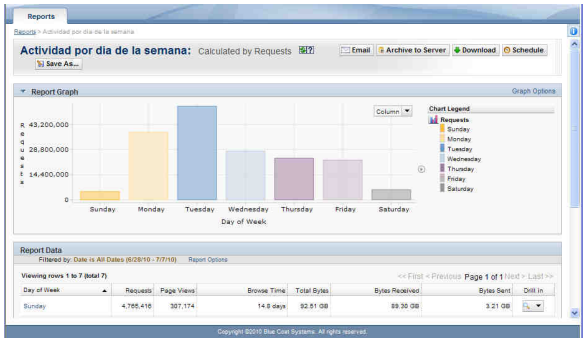


Figura 52: Informes de navegación

- **Informes de filtrado de contenidos**

  Los informes de filtrado de contenidos a los que tendrá acceso el cliente son los siguientes:

  - Actividad mensual de bloqueos por categoría (top 20)
  - Actividad mensual de accesos por categoría (top 20) (figura 53).

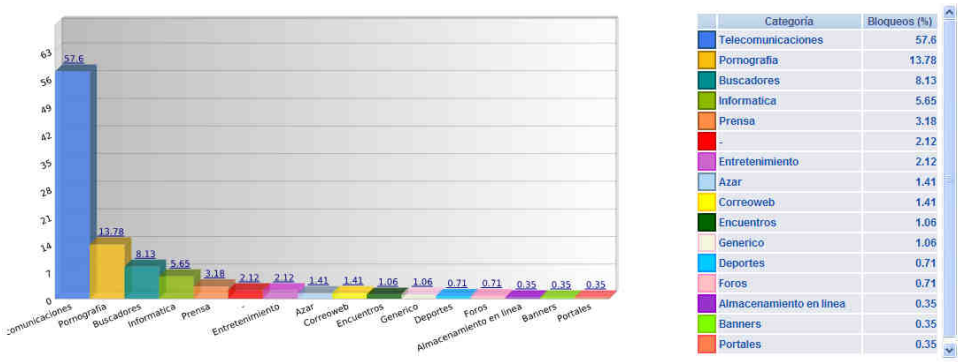


Figura 53: Informe de filtrado de contenidos

3.9 VALORACIÓN ECONÓMICA

Concepto	PVP	
Housing Básico	**Cuota de Alta €**	**Cuota Mensual €**
Puertos de red	- €	550,69 €
Operación Básica		
Alojamiento 1 Equipos CISCO Catalyst 2901		
Hosting Virtual	**Alta €**	**Mensual €**
5 Servidores virtuales • 3 Serv. Windows Server (8 Gb RAM, 4 núcleos, 500Gb HDD) • 2 Serv. Linux Red Hat (4 Gb RAM, 2 núcleos, 300Gb HDD)	1.533,88 €	4.351,12 €
Interfaces		
Monitorización		
Solicitudes • Bolsa de 5 solicitudes tipo B y 3 Tipo C al mes.		
Backup	**Alta €**	**Mensual €**
Backup Remoto • 2 dominios • 1.5 Tb de almacenamiento	3.755,48 €	334,06 €
Backup asociado a HV • 1 Tb de almacenamiento	- €	565,52 €
Nueva Plataforma hardware para el Proyecto	**Alta €**	**Mensual €**
Materiales	6.849,93 €	619,77 €
Software		
Viajes		
Otros		
Tráfico Limpio Internet (MCI)	**Alta €**	**Mensual €**
120 usuarios PLATA	1.533,42 €	301,15 €
Servicio Macrolan	**Alta €**	**Mensual €**
Incluyendo los siguientes conceptos: • Accesos • Caudales • Equipos EDC • Instalación y mantenimiento Para todas las sedes	- €	3575,26 €
Total	**13.672,70 €**	**10.297,57 €**

Total del contrato	**137.243,54 €**
Primera Cuota	**23.970,27 €**
Cuota Mensual	**10.297,57 €**

También existe la posibilidad de anualizar la cuota de alta a un año sin intereses, con lo que la facturación quedaría de la siguiente manera:

Total del contrato	**137.243,54 €**
Cuota Mensual	**11.436,97 €**

3.10 SERVICIOS CONTRATABLES COMPLEMENTARIOS

3.10.1 SERVICIO DE CIFRADO

En caso de ser necesario un nivel extra de seguridad que dote de una confidencialidad adicional a los datos que se intercambian en la red del cliente, existe la Facilidad de Cifrado extremo a extremo, que hace uso del protocolo de seguridad IPSec (Ver Anexo 6.3) y de la utilización de claves para la recuperación de la información cifrada (secreto compartido).

El Cliente puede determinar qué tráfico desea cifrar dentro de las Clases de Servicio Oro y Plata (debe tenerse en cuenta que NO se cifra el tráfico de la Clase Multimedia ni el tráfico de Internet). El cliente debe especificar para la opción de cifrado lo siguiente:

- Sedes entre las que se requiere cifrar el tráfico.
- Clase de servicio (si requiere cifrar todo el tráfico de una misma clase) o bien dirección IP origen y destino/puerto origen y destino para especificar tráfico perteneciente a una aplicación concreta.

La facilidad de cifrado es aplicable a cualquier tipo de acceso del servicio (2/10/100/1000 Mbps) y para cualquier escenario, ya que sobre una RPV de cliente totalmente mallada, se puede superponer cualquier topología de cifrado.

Se implementa utilizando los mismos EDCs del servicio, mediante software IPSec y, cuando sea necesario por requerimientos del cliente, tarjetas cifradoras. La facilidad de cifrado sólo está disponible para los Routers Cisco y Teldat homologados en el servicio para esta facilidad [37] y configurados siempre como EDCs de 1º nivel de gestión. La capacidad de cifrado de estos equipos está limitada, pudiéndose cifrar cierta cantidad de tráfico según el modelo.

Como limitación destacar que la facilidad de cifrado no se puede dar sobre el tráfico de nivel 2 asociado a la facilidad de soporte de otros protocolos: Ethernet, pero sí puede convivir en la misma sede.

Con este objetivo surge la Gestión de Funcionalidad Avanzada en el servicio MacroLAN que es obligatoria su contratación junto con el equipamiento que acompaña a la Facilidad de Cifrado.

3.10.2 SERVICIO DE CONECTIVIDAD DE USUARIOS MÓVILES

La facilidad de Conectividad de usuarios móviles a la RPV corporativa de cliente MacroLAN requiere la contratación del servicio Movistar Intranet de Telefónica Móviles (TME). Este servicio permite al cliente proporcionar acceso remoto a su RPV MacroLAN/VPN IP a los usuarios móviles que éste determine.

Con esta facilidad el cliente rentabiliza su infraestructura de comunicaciones que no requiere modificaciones para la activación de Movistar Intranet. En figura 54 se presenta un esquema general de la solución que denominaremos Movistar Intranet - Conectividad Red Corporativa Cliente/TME:

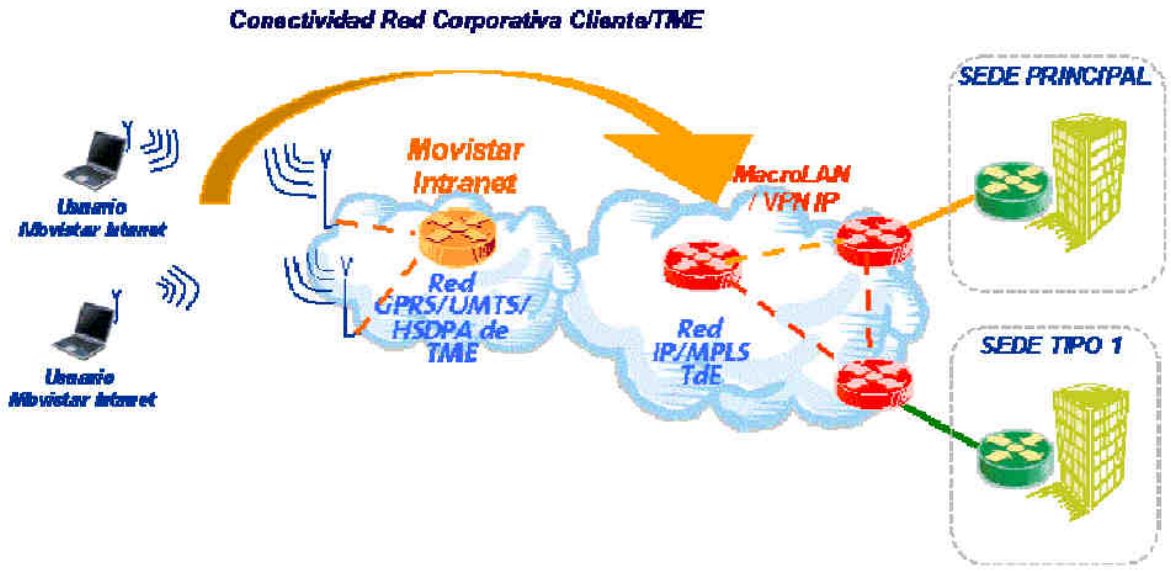


Figura 54: Conectividad de usuarios móviles

La comercialización y puesta en servicio de Movistar Intranet de TME sobre la RPV MacroLAN/VPN IP se realizará de manera integrada desde TME mediante la venta conjunta de dicho servicio y la facilidad de "Conectividad de Usuarios Móviles" incluida en las RPVs de TdE.

Esta facilidad no requiere de la instalación de elementos adicionales en la RPV, realizándose la activación en red de manera transparente al propio cliente. En caso de que el cliente o el proyecto requiriera actuaciones adicionales en la RPV MacroLAN/VPN IP (aumento ancho de banda de los accesos, cambio de EDC, etc.) se deberán realizar mediante oferta específica de el/los servicios MacroLAN/VPN IP.

3.10.3 SERVICIO DE TELEFONÍA SOBRE IP. CONVIVENCIA CON EL SERVICIO IBERCOM

Sobre la misma infraestructura utilizada por el cliente para la transmisión de datos, se puede realizar la transmisión de voz, gracias a la convivencia del servicio MacroLAN con el servicio Ibercom IP (figura 55). Por medio de esta convivencia se garantizan los niveles máximos de convergencia entre voz y datos, proporcionando una integración de funcionalidades en los EDC's, así como una adecuada Calidad de Servicio por medio de los SLAs ofrecidos en la Clase Multimedia utilizada para el transporte de las aplicaciones de voz.

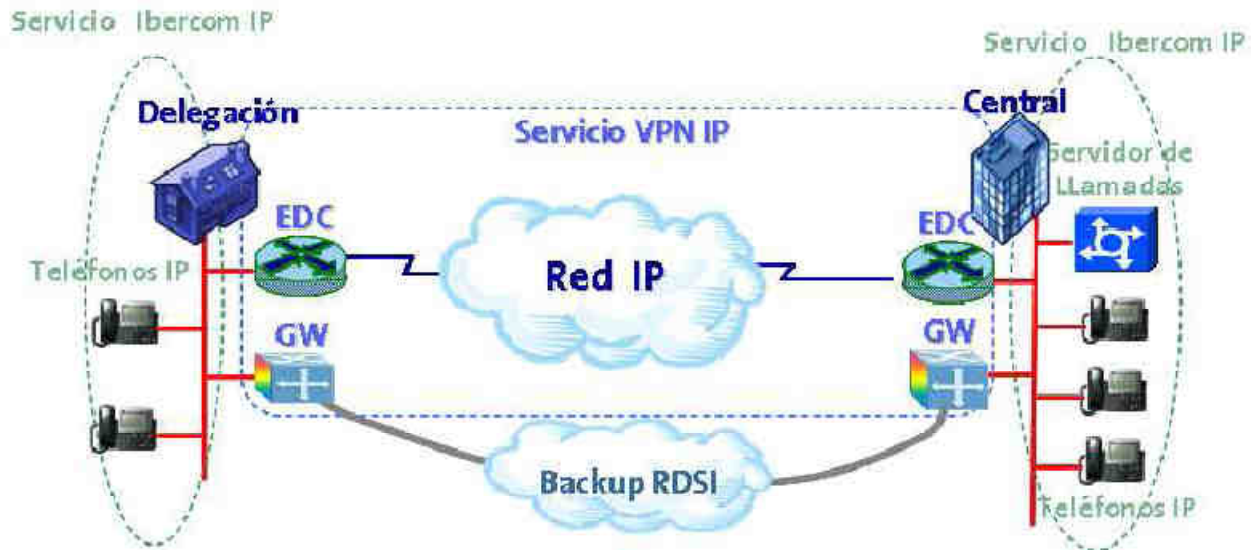


Figura 55: Integración con servicio Ibercom IP

Los elementos que están dentro del ámbito de gestión del servicio MacroLAN son el EDC, y el Gateway, los cuales son gestionados desde el Centro Nacional de Control (CNC):

- EDC (equipo en domicilio de cliente), elemento que realiza la interconexión entre la red local del cliente y la línea de acceso al servicio.
- Gateway, es el elemento que proporciona la interconexión la interconexión entre el entorno de telefonía IP y el entorno de telefonía tradicional, bien con las centralitas tradicionales en domicilio de cliente (PBX) como con la red pública (RTC/RDSI), pudiendo asumir la función de centralita local en caso de situaciones de aislamiento. Este elemento puede estar integrado en el EDC o ser un elemento independiente dentro de la LAN del cliente

Los Teléfonos IP así como el Gestor de Llamadas (encargado de gestionar la conmutación de llamadas, entre otras funciones) quedan fuera del ámbito del servicio MacroLAN, quedando dentro del servicio Ibercom IP. El backup por RDSI es utilizado para proporcionar una red alternativa al tráfico de voz; su contratación queda fuera del ámbito del servicio MacroLAN.

Dependiendo de lo elementos que formen parte del escenario de ToIP en cada sede, se distinguen los siguientes tipos de oficina:

- Oficina IP Básica, es aquella que sólo dispone de teléfonos IP para proporcionar la conectividad de voz entre las sedes que componen la RPV (sin ningún tipo de conectividad exterior por medio de RTB/RDSI). Sólo es necesario disponer del caudal multimedia necesario en la RPV
- Oficina Estándar, es aquella en la que hay comunicaciones de voz fuera de la RPV (por medio de RTB/RDSI). Para permitir las llamadas entrantes como salientes de la RPV, se hace necesaria la función de un Gateway para encaminar las llamadas con el exterior. Este Gateway puede tratarse de un elemento integrado dentro del EDC, o independiente de éste (como se muestra en la figura 56):

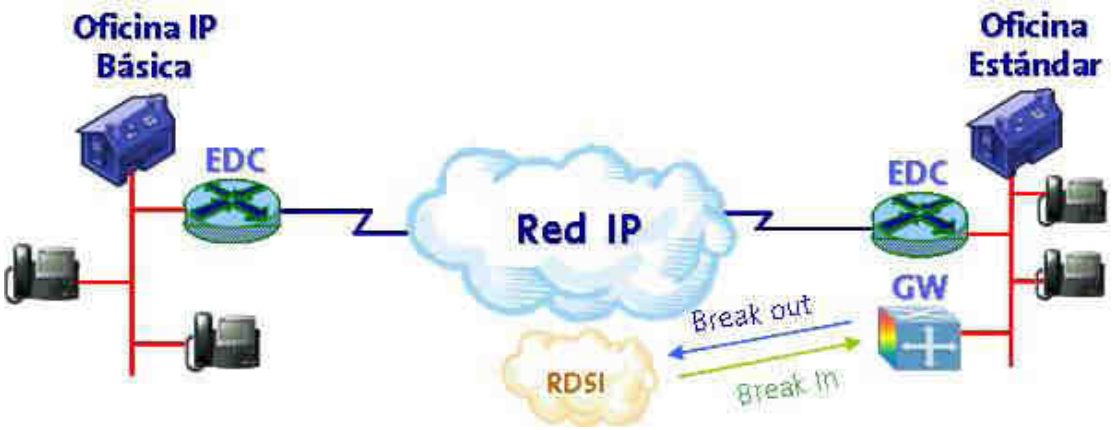


Figura 56: Gateway con integración Ibercom IP

Ambos tipos de oficina presentan opciones de redundancia para todos los elementos que componen la solución en cada caso: accesos, EDCs, y Gateway.

Esta facilidad tiene una cuota mensual, que está asociada a la existencia de la funcionalidad de Gateway (Oficina Estándar), bien sea como equipo independiente o integrado dentro del EDC. Además de este concepto, si el Gateway no está integrado en el EDC, se cobrará la Gestión de este equipo así como la cuota correspondiente al Mantenimiento si así lo contratara el cliente.

4. CONCLUSIONES

A partir de todo lo expuesto en los apartados anteriores, e intentando separarnos del carácter típicamente comercial que una oferta suele presentar, podemos observar que en las nuevas tecnologías TIC aplicadas al mundo empresarial destaca sobre todo la búsqueda del equilibrio calidad-precio.

Como se ha podido comprobar, el avance en los últimos años ha sido dirigido sobre todo a poder aplicar economías de escala que permiten conseguir equipos cada vez más potentes a precios más ajustados.

Todo ello acaba repercutiendo en una facilidad a la hora de innovar para los empresarios, ya que se cambia el modelo de negocio, desde un suministro y un servicio asociado, como venía siendo el modelo tradicional, a un IaaS (Infraestructure as a Service), que permite diluir lo que en principio sería una gran inversión inicial hacia un pago mensualizado por uso, al igual que hace con las inversiones consecutivas en caso de necesidades temporales o crecimientos futuros. Esto evita además la obsolescencia tecnológica que se venía produciendo de manera cada vez más temprana, con las consecuencias negativas que esto supone.

También es importante reseñar la cantidad de costes ocultos que se evitan con este cambio de negocio, como son:

- Evitar la subcontratación de personal que se encargue de administrar los servidores de la empresa, si esta no dispone del know how necesario para hacerlo.
- Disponer de un espacio tecnológicamente acondicionado y con unos SLAs de alto nivel, que la empresa, por no estar orientada al sector TIC, no tiene por qué poseer.
- Capacidad de crecimiento prácticamente ilimitado, o de poder dar de alta o baja servicios con muy bajo tiempo de provisión, ante necesidades puntuales del negocio.
- Evitar gastos extraordinarios en soportes, reparaciones o mantenimientos, que por ser plataformas compartidas, sí están repercutidos en los precios finales mensuales ofrecidos.

Todo esto permite a las empresas contratantes hacer foco permanente en su verdadero núcleo de negocio y no desperdiciar recursos en las tecnologías que los sustentan, así como en los problemas que de estas tecnologías pudieran derivarse.

Además, y a pesar de estar sustentadas en plataformas compartidas, todas las tecnologías empleadas aseguran una estanqueidad y un nivel estandarizado de protección de datos, que acaba repercutiendo en una satisfacción y tranquilidad del cliente en lo relativo a la seguridad de la información de carácter confidencial.

5. ANEXOS

5.1 CPDs DE TELEFÓNICA SOLUCIONES

Los Centros de Datos Gestionados de Telefónica son instalaciones altamente redundadas que garantizan altos niveles de disponibilidad y calidad de servicio, siendo la base de los servicios de TI para cliente. De forma general, las características más notables son:

- Infraestructura TI bajo demanda, que permite ajustarse a las necesidades del negocio de los clientes.
- Calidad de servicio garantizada mediante Acuerdos de Nivel de Servicio, por contrato.
- Con las mayores condiciones de seguridad física y lógica.
- Alta disponibilidad eléctrica y de comunicaciones.
- Experiencia y mejores prácticas (ISO 20000 [38] e ITIL [39]).
- Políticas Green TI [40].

5.1.1 INFRAESTRUCTIRAS EN LOS CPDs

Los Centros de Datos de Telefónica están diseñados para albergar y administrar los sistemas y aplicaciones de negocio de clientes en las mejores condiciones de seguridad, fiabilidad y flexibilidad. La figura 57 muestra el esquema general de funcionamiento de un Centro de Datos Gestionado:

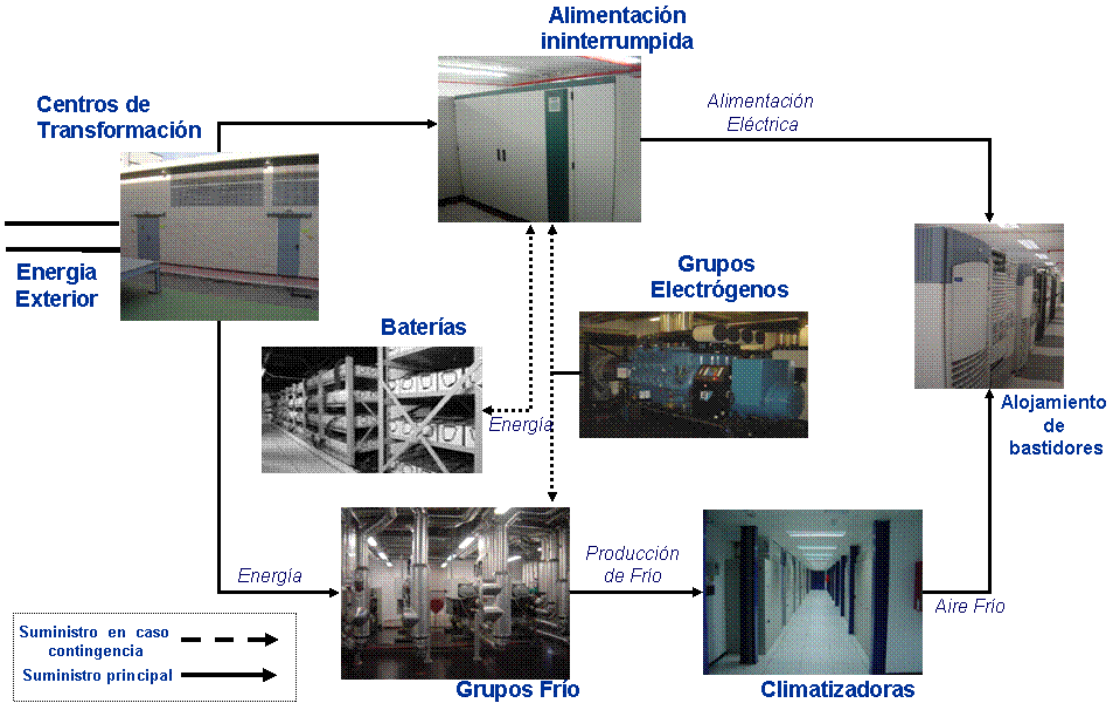


Figura 57: Infraestructuras de los CPDs

A continuación se explica cada apartado que lo compone:

Sistemas Energéticos

Centros de Transformación

La energía recibida en media o alta tensión de la red eléctrica exterior se transforma a baja tensión (230/380V) al resto de instalaciones del CDG mediante el uso de transformadores. Por seguridad en el suministro, hay dos puntos de alimentación configurados en anillo con dos subestaciones independientes. En todos los centros existe un nivel de redundancia de N+1 que garantiza el funcionamiento en caso de fallo en algún sistema.

Sistema de Alimentación Independiente (SAI)

Permite el suministro ininterrumpido de energía a todas las máquinas del CDG mientras el sistema electrógeno alcanza el rendimiento óptimo necesario para proporcionar el suministro eléctrico a las máquinas del centro. Las SAI están formadas por baterías que son revisadas y testadas por personal especializado en el centro de forma parcial mensualmente, y con una parada total anualmente. La autonomía de estos sistemas es de 10-15 minutos, tiempo suficiente para que el grupo electrógeno funcione a pleno rendimiento (2-3 minutos). Una vez que el grupo electrógeno asume la tarea de alimentación, las baterías vuelven a recargarse automáticamente. Existe un nivel de redundancia de N+1 en todos los centros y de 2(N+1) en CDG de Logroño y en el centro de Julián Camarillo, Módulo 3 Planta 5.

Grupos Electrógenos

El grupo electrógeno se encarga de suplir el suministro eléctrico a las máquinas y sistemas del CDG en caso de un fallo exterior en dicho suministro. Cada grupo electrógeno cuenta con depósitos de combustible que permiten una autonomía de varios días mientras se restablece el suministro exterior al centro. Para mayor fiabilidad, los centros cuentan con varios depósitos de gasoil a los que la compañía proveedora tiene la obligación de reabastecer, por especificación directa en el contrato, en un periodo inferior a 24h. El tiempo de arranque de los grupos electrógenos es menor de 15 segundos, debido a que se mantienen precalentados (todo el circuito de aceite), para que el arranque sea inmediato y alcancen un rendimiento óptimo y estable en 2-3 minutos.

Los grupos electrógenos son revisados y probados mensualmente de forma rotatoria (para que ninguno quede en inactividad un largo periodo) por personal de conducción con los que cuenta cada centro con disponibilidad 24x7. Como en los sistemas anteriores, el nivel de redundancia es N+1 para todos los CDGs.

Sistemas Refrigeración

Sistemas de producción de frío

Son los encargados de proporcionar el aire frío necesario a las climatizadoras en la ventilación de las máquinas de las salas técnicas. Todos los centros cuentan con sistemas autónomos que forman un circuito cerrado de agua, basado en grupos de frío en configuración de tornillo que hacen bajar la temperatura del agua de 12º/13º C a 6º, permitiendo así el enfriamiento del aire. A su vez, la redundancia de N+1 en estos equipos garantiza el suministro de frío a las máquinas climatizadoras situadas en los pasillos exteriores a salas técnicas, para mayores medidas de seguridad.

Mantenimiento y soporte de infraestructuras

Todo el personal de mantenimiento y supervisión del centro realiza turnos que permiten un servicio de atención 24x7 en todos los centros Telefónica. Además, para cada sección del CDG existe un equipo especializado encargado únicamente de revisar y mantener los equipos de su área en las mejores condiciones funcionales. Adicionalmente, se cuenta con un centro de seguimiento y monitorización de los sistemas eléctricos. De esta forma, se pueden distinguir tres equipos y un centro de competencia técnico dedicados a la supervisión de nuestros centros de datos:

Personal en Conducción

Un grupo especializado (frigorista/electricista) revisan y mantienen los sistemas de alimentación y frío del CDG, con disponibilidad de 24x7.

Cableadores

Un equipo especializado es el encargado de realizar el cableado eléctrico y de datos en las salas técnicas en cada CDG, con disponibilidad de 24x7.

Operadores

Personal especializado en el manejo y supervisión de los equipos en las salas técnicas. Disponibilidad del personal: 24x7, In-situ; en todos los centros de datos Telefónica. Ver apartado Operación Básica “Servicio Manos Remotas“.

Seguridad del Centro de Datos

Seguridad Física

Todos los centros cuentan con doble control perimetral en el que es necesaria una acreditación, quedando registrado en el sistema cada acceso al CDG. La rigurosa política de seguridad en los centros

no permite el acceso con teléfonos móviles o cámaras, estando inclusive custodiada la lista de personas con acceso al centro por los guardias armados en el centro de vigilancia del CDG. En caso de necesitar acceso al centro se irá siempre acompañado por personal cualificado perteneciente a Telefónica que facilitará las tareas y trabajos que el cliente especifique. Como medida adicional de seguridad, es obligatorio el registro de paquetes mediante un control de Rayos-X, así como pasar satisfactoriamente el arco detector de metales en la entrada al centro de datos. Los guardias de seguridad cumplen una vigilancia de 24x7. El acceso de personal y equipos del cliente será de acuerdo al Protocolo de Seguridad Física de Telefónica y siguiendo las indicaciones del cliente contempladas en el Protocolo de Mantenimiento del Servicio.

Sistemas de Seguridad

En los CDG se dispone de un sistema de televisión cerrado 24h (CCTV) con cámaras situadas tanto en el perímetro del centro como en las salas y pasillos en el interior, estando todos los sistemas conectados con el centro de seguridad del centro. Además, los equipos de seguridad del centro cuentan con sistemas de infrarrojos, sensores volumétricos, equipos de iluminación sorpresiva y red de interfonos distribuidos por el centro estratégicamente. Para mayor seguridad, se dispone de tarjetas de proximidad y en algunos casos de sensores biométricos que registran y limitan la entrada a cada zona del edificio según el nivel de acceso del que se disponga.

Sistemas Antiincendios

Sistemas de Detección

Todos los centros cuentan con sistemas de detección basados en detectores de tipo óptico y de detección precoz mediante sistemas de aspiración ubicados por todo el edificio. Todos los detectores están unidos con la central de control y cuentan con doble alimentación independiente garantizando el perfecto funcionamiento en todo momento Cada sala del centro está aislada del resto mediante paredes RF-180 y RF-120, y puertas ignífugas RF-60 [41] que convierten cada sala en una zona independiente de incendio.

Sistemas de Extinción

En los centros existen extintores de polvo, CO2 y BIEs (Bocas de Incendio Equipadas) con la correspondiente señalización en cada sala. Estos mecanismos se consideran manuales, existiendo además sistemas automáticos de extinción como son:

- Agua nebulizada, micro partículas de agua a alta presión (en algunos centros se dispone de Gas FE-13 [42]), inocuo para personas y equipos. Las botellas contenedoras de gas son independientes para cada sala.
- Sistemas de detección y recogida de humos.

Salas dentro del CDG

Dentro de los Centros de Datos Telefónica se distinguen distintos tipos de salas especialmente acondicionadas para cada funcionalidad. Entre otras, se identifican:

- Salas Técnicas – Permite el alojamiento de los equipos de TI.
- Sala Blanca – Sala de seguimiento del CDG
- Sala de Armarios ignífugos – Sala especialmente diseñada que contiene las cajas fuertes con las cintas de almacenamiento y otra información adicional.
- Sala Galvánica – Sala especialmente diseñada que contiene información confidencial. (Emisión de Certificados de Seguridad)
- Salas de Puestos de Administradores
- Salas de Reuniones y juntas – Salas habilitadas para reuniones y otro tipo de eventos.
- Centro de Seguridad – ubicación que concentra los sistemas de seguridad para vigilancia y supervisión.

5.1.2 POLÍTICAS "GREEN TI"

Telefónica participa proactivamente en las mejores prácticas de Green TI, destacando en la implementación en los CDGs de las siguientes iniciativas.

- Normativa ISO 14001 [43]. Para tratar el reciclado de residuos (aceites, luminarias, tóners, cartones, baterías, soportes magnéticos,…).
- Seguimiento PUE (power usage efectiveness). Relación entre la energía total consumida y la realmente suministrada para servidores.
- Pasillo Frío – Pasillo Caliente para mejorar la eficiencia de los sistemas de refrigeración, limitación de la disponibilidad eléctrica por rack. Un ejemplo viene reflejado en la figura 58.

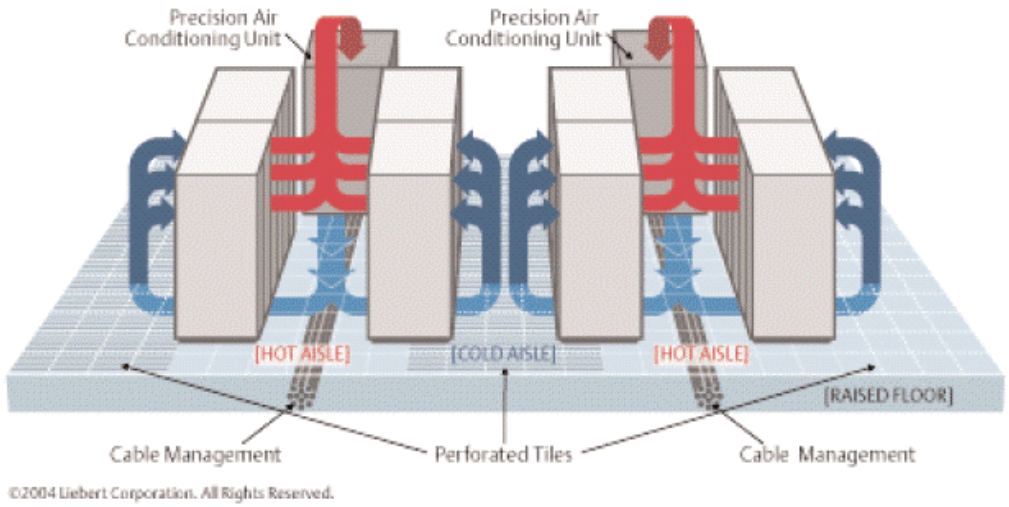


Figura 58: Pasillos fríos

- Eco-Extinción. Eliminación de gases con efecto invernadero.
- Eficiencia en Servicios de Hosting: almacenamiento bajo demanda, hosting virtual,... Hasta un 80% de ahorro energético. Plan comercial de sustitución de servidores físicos por virtuales.
- Free Cooling. Aprovechar las bajas temperaturas del exterior para compensar la diferencia de temperatura con las salas internas al enfriar el agua de los Grupos de Frío.
- Cogeneración. Las unidades enfriadoras cuentan con recuperador de calor para un dar confort a las salas de operaciones, oficinas y salas de reuniones.
- Depósitos de Inercia (aljibes isotérmicos) para retener agua fría y maximiza la eficiencia energética de los compresores de los grupos de frío.

5.1.3 CERTIFICACIONES

Certificación ISO 20.000

Telefónica Soluciones ha sido la primera empresa española en obtener la certificación ISO20000 para la prestación de servicios TI a clientes externos (figura 59). Este sello garantiza la calidad de los servicios, la correcta adaptación de procesos de gobierno y la implantación de buenas prácticas en la prestación de servicios TI.

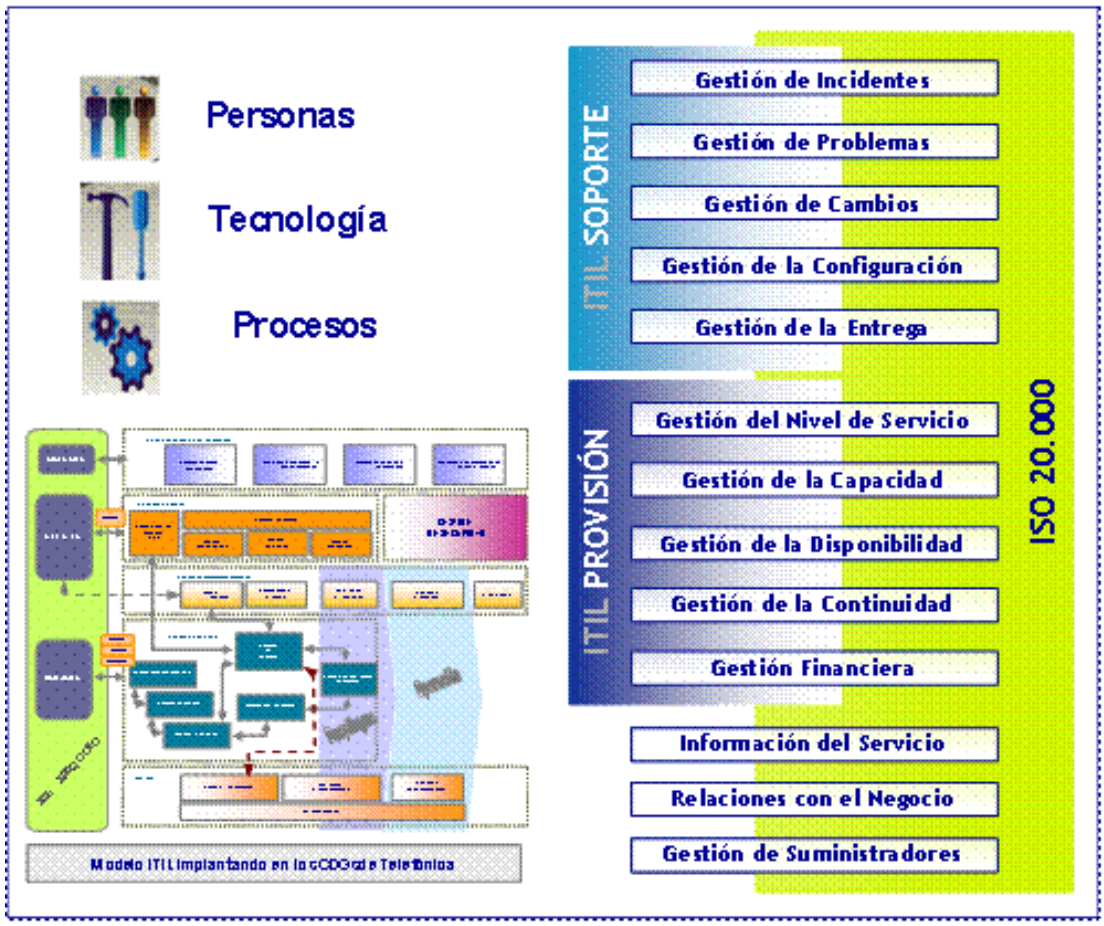


Figura 59: Certificaciones ISO 20.000

Certificaciones CDG

Los centros de datos gestionados de Telefónica disponen de numerosos certificados que corroboran la calidad y buenas prácticas llevadas en las distintas tareas (figura 60):

Figura 60: Certificaciones de los CDGs

5.2 RED MPLS

5.2.1 INTRODUCCIÓN

El enorme crecimiento de la red Internet ha convertido al protocolo IP (Internet Protocol) en la base de las actuales redes de telecomunicaciones, contando con más del 80% del tráfico cursado. La versión actual de IP, conocida por IPv4 [44], lleva operativa desde 1980. Este protocolo de capa de red (Nivel 3 OSI, Open System Interconnections [45]), define los mecanismos de la distribución o encaminamiento de paquetes, de una manera no fiable y sin conexión, en redes heterogéneas; es decir, únicamente está orientado a servicios no orientados a conexión y a la transferencia de datos, por lo que se suele utilizar junto con TCP (Transmission Control Protocol) (Nivel 4 de OSI) para garantizar la entrega de los paquetes.

A mediados de la década de los 90, la demanda por parte de los clientes de los ISP (Internet Service Providers) de aplicaciones multimedia con altas necesidades de ancho de banda y una calidad de servicio o QoS (Quality of Service) garantizada, propiciaron la introducción de ATM (Asyncronous Transfer Mode) [46] en la capa de enlace (Nivel 2 de OSI) de sus redes. En esos momentos, el modelo de IP sobre ATM satisfacía los requisitos de las nuevas aplicaciones, utilizando el encaminamiento inteligente de nivel 3 de los routers IP en la red de acceso, e incrementando el ancho de banda y rendimiento basándose en la alta velocidad de los conmutadores de nivel 2 y los circuitos permanentes virtuales de los switches ATM en la red troncal. Esta arquitectura, no obstante, presenta ciertas limitaciones, debido a: la dificultad de operar e integrar una red basándose en dos tecnologías muy distintas, la aparición de switches ATM e IP de alto rendimiento en las redes troncales, y la mayor capacidad de transmisión ofrecida por SDH/SONET [47] (Synchronous Digital Hierarchy / Syncronous Optical NETwork) y DWDM [48] (Dense Wavelength Division Multiplexing) respecto a ATM.

Durante 1996, empezaron a aparecer soluciones de conmutación de nivel 2 propietarias diseñadas para el núcleo de Internet que integraban la conmutación ATM con el encaminamiento IP; como por ejemplo, Tag Switching de Cisco o Aggregate Route-Based IP Switching de IBM. La base común de todas estas tecnologías, era tomar el software de control de un router IP, integrarlo con el rendimiento de reenvío con cambio de etiqueta de un switch ATM y crear un router extremadamente rápido y eficiente en cuanto a coste. La integración en esta arquitectura era mayor, porque se utilizaban protocolos IP propietarios para distribuir y asignar los identificadores de conexión de ATM como etiquetas; pero los protocolos no eran compatibles entre sí y requerían aún de infraestructura ATM.

Finalmente en 1997, el IETF (Internet Engineering Task Force) establece el grupo de trabajo MPLS (MultiProtocol Label Switching) para producir un estándar que unificase las soluciones propietarias de conmutación de nivel 2. El resultado fue la definición en 1998 del estándar conocido por MPLS [49]. MPLS proporciona los beneficios de la ingeniería de tráfico del modelo de IP sobre ATM, pero además, otras ventajas; como una operación y diseño de red más sencillo y una mayor escalabilidad. Por otro lado, a diferencia de las soluciones de conmutación de nivel 2 propietarias, está diseñado para operar sobre cualquier tecnología en el nivel de enlace, no únicamente ATM, facilitando así la migración a las redes ópticas de próxima generación, basadas en infraestructuras SDH/SONET y DWDM.

5.2.2 CONCEPTO DE MPLS

MPLS es un estándar IP de conmutación de paquetes del IETF, que trata de proporcionar algunas de las características de las redes orientadas a conexión a las redes no orientadas a conexión. En el encaminamiento IP sin conexión tradicional, la dirección de destino junto a otros parámetros de la cabecera, es examinada cada vez que el paquete atraviesa un router. La ruta del paquete se adapta en función del estado de las tablas de encaminamiento de cada nodo, pero, como la ruta no puede predecirse, es difícil reservar recursos que garanticen la QoS; además, las búsquedas en tablas de encaminamiento hacen que cada nodo pierda cierto tiempo, que se incrementa en función de la longitud de la tabla.

Sin embargo, MPLS permite a cada nodo, ya sea un switch o un router, asignar una etiqueta a cada uno de los elementos de la tabla y comunicarla a sus nodos vecinos. Esta etiqueta es un valor corto y de tamaño fijo transportado en la cabecera del paquete para identificar un FEC (Forward Equivalence Class), que es un conjunto de paquetes que son reenviados sobre el mismo camino a través de la red, incluso si sus destinos finales son diferentes. La etiqueta es un identificador de conexión que sólo tiene significado local y que establece una correspondencia entre el tráfico y un FEC específico. Dicha etiqueta se asigna al paquete basándose en su dirección de destino, los parámetros de tipo de servicio, la pertenencia a una VPN, o siguiendo otro criterio. Cuando MPLS está implementado como una solución IP pura o de nivel 3, que es la más habitual, la etiqueta es un segmento de información añadido al comienzo del paquete. Los campos de la cabecera MPLS de 4 bytes, son los siguientes:

- Label (20 bits). Es el valor actual, con sentido únicamente local, de la etiqueta MPLS. Esta etiqueta es la que determinará el próximo salto del paquete.
- CoS (3 bits). Este campo afecta a los algoritmos de descarte de paquetes y de mantenimiento de colas en los nodos intermedios, es decir, indica la QoS del paquete. Mediante este campo es posible diferenciar distintos tipos de tráficos y mejorar el rendimiento de un tipo de tráfico respecto a otros.
- Stack (1 bit). Mediante este bit se soporta una pila de etiquetas jerárquicas, es decir, indica si existen más etiquetas MPLS. Las cabeceras MPLS se comportan como si estuvieran apiladas una sobre otra, de modo que el nodo MPLS tratará siempre la que esté más alto en la pila. La posibilidad de encapsular una cabecera MPLS en otras, tiene sentido, por ejemplo, cuando se tiene una red MPLS que tiene que atravesar otra red MPLS perteneciente a un ISP u organismo administrativo externo distinto; de modo que al terminar de atravesar esa red, se continúe trabajando con MPLS como si no existiera dicha red externa.

5.2.3 ELEMENTOS DE UNA RED MPLS

En MPLS un concepto muy importante es el de LSP (Label Switch Path), que es un camino de tráfico específico a través de la red MPLS, el cual se crea utilizando los LDPs (Label Distribution Protocols), tales como RSVP-TE (ReSerVation Protocol – Traffic Engineering) o CR-LDP (Constraint-based Routing – Label Distribution Protocol); siendo el primero el más común. El LDP posibilita a los nodos MPLS descubrirse y establecer comunicación entre sí con el propósito de informarse del valor y significado de las etiquetas que serán utilizadas en sus enlaces contiguos. Es decir, mediante el LDP se establecerá un camino a través de la red MPLS y se reservarán los recursos físicos necesarios para satisfacer los requerimientos del servicio previamente definidos para el camino de datos.

Una red MPLS está compuesta por dos tipos principales de nodos, los LER (Label Edge Routers) y los LSR (Label Switching Routers), tal y como se muestra en el ejemplo de la Figura 1. Los dos son físicamente el mismo dispositivo, un router o switch de red troncal que incorpora el software MPLS; siendo su administrador, el que lo configura para uno u otro modo de trabajo. Los nodos MPLS al igual que los routers IP normales, intercambian información sobre la topología de la red mediante los protocolos de encaminamiento estándar, tales como OSPF (Open Shortest Path First), RIP (Routing Information Protocol) y BGP (Border Gateway Protocol), a partir de los cuales construyen tablas de encaminamiento basándose principalmente en la alcanzabilidad a las redes IP destinatarias. Teniendo en cuenta dichas tablas de encaminamiento, que indican la dirección IP del siguiente nodo al que le será enviado el paquete para que pueda alcanzar su destino final, se establecerán las etiquetas MPLS y, por lo tanto, los LSP que seguirán los paquetes. No obstante, también pueden establecerse LSP que no se correspondan con el camino mínimo calculado por el protocolo de encaminamiento.

Los LERs están ubicados en el borde de la red MPLS para desempeñar las funciones tradicionales de encaminamiento y proporcionar conectividad a sus usuarios, generalmente routers IP convencionales. El LER analiza y clasifica el paquete IP entrante considerando hasta el nivel 3, es decir, considerando la dirección IP de destino y la QoS demandada; añadiendo la etiqueta MPLS que identifica en qué LSP está el paquete. Es decir, el LER en vez de decidir el siguiente salto, como haría un router IP normal, decide el camino entero a lo largo de la red que el paquete debe seguir. Una vez asignada la cabecera MPLS, el LER enviará el paquete a un LSR. Los LSR están ubicados en el núcleo de la red MPLS para efectuar encaminamiento de alto rendimiento basado en la conmutación por etiqueta, considerando únicamente hasta el nivel 2. Cuando le llega un paquete a una interfaz del LSR, éste lee el valor de la etiqueta de entrada de la cabecera MPLS, busca en la tabla de conmutación la etiqueta e interfaz de salida, y reenvía el paquete por el camino predefinido escribiendo la nueva cabecera MPLS. Si un LSR detecta que debe enviar un paquete a un LER, extrae la cabecera MPLS; como el último LER no conmuta el paquete, se reducen así cabeceras innecesarias.

Un ejemplo de esquema de las redes MPLS y sus elementos podría ser el representado en la figura 61:

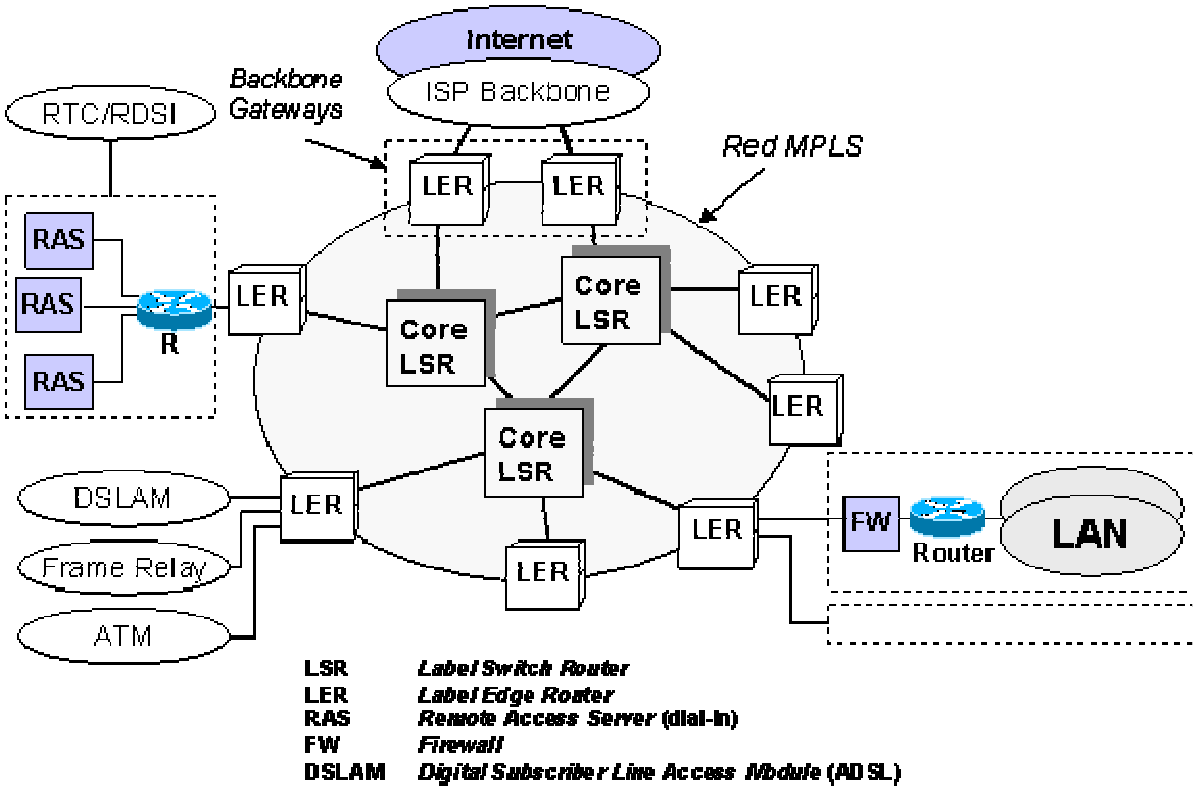


Figura 61: Esquema red MPLS

5.2.3.1 Características básicas y funcionamiento

La tecnología MPLS ofrece un servicio orientado a conexión:

- Mantiene un «estado» de la comunicación entre dos nodos.
- Mantiene circuitos virtuales

5.2.3.2 Arquitectura MPLS

Elementos

- LER (Label Edge Router): elemento que inicia o termina el túnel (pone y quita cabeceras). Es decir, el elemento de entrada/salida a la red MPLS. Un router de entrada se conoce como Ingress Router y uno de salida como Egress Router. Ambos se suelen denominar Edge Label Switch Router ya que se encuentran en los extremos de la red MPLS.
- LSR (Label Switching Router): elemento que conmuta etiquetas.
- LSP (Label Switched Path): nombre genérico de un camino MPLS (para cierto tráfico o FEC), es decir, del túnel MPLS establecido entre los extremos. A tener en cuenta que un LSP es unidireccional.

- LDP (Label Distribution Protocol): un protocolo para la distribución de etiquetas MPLS entre los equipos de la red.
- FEC (Forwarding Equivalence Class): nombre que se le da al tráfico que se encamina bajo una etiqueta. Subconjunto de paquetes tratados del mismo modo por el conmutador.

Cabecera MPLS (figura 62)

Figura 62: Cabecera MPLS

Donde:

- Label (20 bits): Es la identificación de la etiqueta.
- Exp (3 bits): Llamado también bits experimentales, también aparece como QoS en otros textos, afecta al encolado y descarte de paquetes.
- S (1 bit): Del inglés stack, sirve para el apilado jerárquico de etiquetas. Cuando S=0 indica que hay mas etiquetas añadidas al paquete. Cuando S=1 estamos en el fondo de la jerarquía.
- TTL (8 bits): Time-to-Live, misma funcionalidad que en IP, se decrementa en cada enrutador y al llegar al valor de 0, el paquete es descartado. Generalmente sustituye el campo TTL de la cabecera IP.

Pila de Etiquetas MPLS (figura 63)

Figura 63: Etiquetas MPLS

MPLS funciona anexando un encabezado a cada paquete. Dicho encabezado contiene una o más "etiquetas", y al conjunto de etiquetas se le llama pila o "stack". Cada etiqueta consiste en cuatro campos:

- Valor de la etiqueta de 20 bits.
- Prioridad de Calidad de Servicio (QoS) de 3 bits. También llamados bits experimentales.
- Bandera de "fondo" de la pila de 1 bit.
- Tiempo de Vida (TTL) de 8 bits.

Estos paquetes MPLS son enviados después de una búsqueda por etiquetas en vez de una búsqueda dentro de una tabla IP. De esta manera, cuando MPLS fue concebido, la búsqueda de etiquetas y el

envío por etiquetas eran más rápido que una búsqueda RIB (Base de información de Ruteo), porque las búsquedas eran realizadas en el switch fabric y no en la CPU.

Creación de la Red

Los puntos de entrada en la red MPLS son llamados Enrutadores de Etiqueta de borde (LER), es decir enrutadores que son interfaces entre la red MPLS y otras redes. Los enrutadores que efectúan la conmutación basados únicamente en etiquetas se llaman Enrutadores Conmutadores de Etiqueta (LSR). Cabe notar que un LER es simplemente un LSR que cuenta con la habilidad de rutear paquetes en redes externas a MPLS.

Las etiquetas son distribuidas usando el Protocolo de Distribución de Etiquetas (LDP). Es precisamente mediante el protocolo LDP que los enrutadores de etiquetas intercambian información acerca de la posibilidad de alcanzar otros enrutadores, y las etiquetas que son necesarias para ello. También es posible hacer la distribución de etiquetas usando el protocolo RSVP-TE.

El operador de una red MPLS puede establecer Caminos Conmutados mediante Etiquetas (LSP), es decir, el operador establece caminos para transportar Redes Privadas Virtuales de tipo IP (IP VPN), pero estos caminos pueden tener otros usos. En muchos aspectos las redes MPLS se parecen a las redes ATM y Frame Relay (FR) [50], con la diferencia de que la red MPLS es independiente del transporte en capa 2 (en el modelo OSI).

En el contexto de las Redes Privadas Virtuales, los enrutadores que funcionan como ingreso o regreso a la red son frecuentemente llamados enrutadores a la Orilla del Proveedor (enrutadores PE), los dispositivos que sirven solo de tránsito son llamados similarmente enrutadores de Proveedor (enrutadores P).

En MPLS el camino que se sigue está prefijado desde el origen (se conocen todos los saltos de antemano): se pueden utilizar etiquetas para identificar cada comunicación y en cada salto se puede cambiar de etiqueta (mismo principio de funcionamiento que VPI/VCI (Virtual Path Identifier/Virtual Channel Identifier) en ATM, o que DLCI (Data Link Control Identifier) en Frame Relay).

Paquetes destinados a diferentes IPs pueden usar el mismo camino LSP (pertenecer al mismo FEC).

Las etiquetas con el mismo destino y tratamiento se agrupan en una misma etiqueta: los nodos mantienen mucha menos información de estado que por ejemplo ATM. Las etiquetas se pueden apilar, de modo que se puede encaminar de manera jerárquica.

Paso de un paquete por la red

Cuando un paquete no etiquetado entra a un enrutador de ingreso y necesita utilizar un túnel MPLS, el enrutador primero determinará la Clase Equivalente de Envío (FEC), luego inserta una o más etiquetas en el encabezado MPLS recién creado. Acto seguido el paquete salta al enrutador siguiente según lo indica el túnel.

Cuando un paquete etiquetado es recibido por un enrutador MPLS, la etiqueta que se encuentra en el tope de la pila será examinada. Basado en el contenido de la etiqueta el enrutador efectuará una operación apilar (PUSH), desapilar (POP) o intercambiar (SWAP).

En una operación SWAP la etiqueta es cambiada por otra y el paquete es enviado en el camino asociado a esta nueva etiqueta.

En una operación PUSH una nueva etiqueta es empujada encima de otra (si existe). Si en efecto había otra etiqueta antes de efectuar esta operación, la nueva etiqueta «encapsula» la anterior.

En una operación POP la etiqueta es retirada del paquete lo cual puede revelar una etiqueta interior (si existe). A este proceso se lo llama «desencapsulado» y es usualmente efectuada por el enrutador de egreso con la excepción de PHP (Hypertext Preprocessor) [51].

Durante estas operaciones el contenido del paquete por debajo de la etiqueta MPLS no es examinado, de hecho los enrutadores de tránsito usualmente no necesitan examinar ninguna información por debajo de la mencionada etiqueta. El paquete es enviado basándose en el contenido de su etiqueta, lo cual permite «rutado independiente del protocolo».

En el enrutador de egreso donde la última etiqueta es retirada, sólo queda la «carga transportada», que puede ser un paquete IP o cualquier otro protocolo. Por tanto, el enrutador de egreso debe forzosamente tener información de ruteo para dicho paquete debido a que la información para el envío de la carga no se encuentra en la tabla de etiquetas MPLS.

En algunas aplicaciones es posible que el paquete presentado al LER ya contenga una etiqueta MPLS, en cuyo caso simplemente se anexará otra etiqueta encima. Un aspecto relacionado que resulta importante es PHP.

En ciertos casos, es posible que la última etiqueta sea retirada en el penúltimo salto (anterior al último enrutador que pertenece a la red MPLS); este procedimiento es llamado «remoción en el penúltimo salto» (PHP). Esto es útil, por ejemplo, cuando la red MPLS transporta mucho tráfico. En estas condiciones los penúltimos nodos auxiliarán al último en el procesamiento de la última etiqueta de manera que este no se vea excesivamente forzado al cumplir con sus tareas de procesamiento.

5.2.4 IMPLEMENTACIONES DE MPLS

Una vez visto el concepto de MPLS, veamos los distintos tipos de implementaciones actuales, en concreto: MPLS como una solución IP sobre Ethernet, IP sobre ATM, e IP sobre Frame Relay. No se contempla la aplicación de MPLS a las redes ópticas de próxima generación, conocida como GMPLS (Generalized MPLS) [52], por encontrarse aún en proceso de estudio y estandarización por parte del IETF. GMPLS es una extensión natural de MPLS para ampliar el uso de MPLS como un mecanismo de control y provisión, no únicamente de caminos en dispositivos basados en paquetes, sino también de caminos en dispositivos no basados en paquetes; como los conmutadores ópticos de señales multiplexadas por división en longitud de onda, los conmutadores de fibras ópticas, y los conmutadores de señales digitales multiplexadas por división en el tiempo. Es decir, GMPLS busca una integración total

en la parte de control de las redes de conmutación de paquetes IP y las redes ópticas SONET/SDH y DWDM; dando lugar a las redes ópticas inteligentes de próxima generación, cuya evolución final será la integración de IP directamente sobre DWDM utilizando algún mecanismo de encapsulamiento como los "digital wrappers".

La implementación de MPLS como una solución IP sobre Ethernet, Fast Ethernet o Gigabit Ethernet, es la conocida como IP pura. Puesto que IPv4 es un protocolo diseñado mucho antes que MPLS, en este caso, la etiqueta MPLS está ubicada después de la cabecera de nivel 2 y antes de la cabecera IP. Los LSR saben cómo conmutar utilizando la etiqueta MPLS en vez de utilizar la cabecera IP. El funcionamiento de IPv4 ha sido totalmente satisfactorio, no obstante, el sorprendente crecimiento de Internet evidenció importantes carencias, como: la escasez de direcciones IP, la imposibilidad de transmitir aplicaciones en tiempo real y los escasos mecanismos de seguridad. Estas limitaciones propiciaron el desarrollo de la siguiente generación del protocolo Internet o IPv6 [53]. La versión IPv6 puede ser instalada como una actualización del software en los dispositivos de red de Internet e interoperar con la versión actual IPv4, produciéndose esta migración progresivamente durante los próximos años. En este caso, la etiqueta MPLS forma parte de la propia cabecera IPv6, estando su uso descrito en la RFC 1809.

La implementación de MPLS como una solución IP sobre ATM también está muy extendida. Primeramente indicar, que MPLS no fue desarrollado para reemplazar ATM, sino para complementarlo. De hecho, la aparición de switches ATM e IP con soporte de MPLS, ha integrado las ventajas de los routers IP y los switches ATM y ha supuesto una mejora de la relación precio/rendimiento de estos dispositivos. La diferencia principal entre MPLS y otras soluciones de IP sobre ATM, es que las conexiones MPLS se establecen utilizando LDP, y no por los protocolos de señalización ATM tradicionales, tales como PNNI (Private Network to Network Interface). Por otro lado, MPLS elimina la complejidad de hacer corresponder el direccionamiento IP y la información de encaminamiento directamente en las tablas de conmutación de ATM, puesto que LDP entiende y utiliza direcciones IP y los protocolos de encaminamiento utilizados en las redes MPLS son los mismos que los utilizados en las redes IP. En este caso, descrito en la RFC 3035, la etiqueta es el valor del VPI/VCI de la cabecera de la celda ATM.

Finalmente, MPLS también se ha desarrollado como una solución IP sobre Frame Relay [54]. En este caso, la etiqueta es el DLCI (Data Link Control Identifier) de la cabecera Frame Relay.

5.2.5 BENEFICIOS DE MPLS

La migración a IP está provocando profundos cambios en el sector de las telecomunicaciones y configura uno de los retos más importantes para los ISP, inmersos actualmente en un proceso de transformación de sus infraestructuras de cara a incorporar los beneficios de esta tecnología. MPLS nació con el fin de incorporar la velocidad de conmutación del nivel 2 al nivel 3; a través de la conmutación por etiqueta; pero actualmente esta ventaja no es percibida como el principal beneficio, ya que los gigarouters son capaces de realizar búsquedas de rutas en las tablas IP a suficiente velocidad como para soportar todo tipo de interfaces. Los beneficios que MPLS proporciona a las redes IP son: realizar ingeniería del tráfico o TE (Traffic Engineering) [55], cursar tráfico con diferentes calidades de clases de servicio o CoS (Class

of Service) o grados de calidad de servicio o QoS (Quality of Service), y crear redes privadas virtuales o VPN (Virtual Private Networks) basadas en IP.

La TE permite a los ISP mover parte del tráfico de datos, desde el camino más corto calculado por los protocolos de encaminamiento, a otros caminos físicos menos congestionados o menos susceptibles a sufrir fallos. Es decir, se refiere al proceso de seleccionar los caminos que seguirá el flujo de datos con el fin de balancear la carga de tráfico entre todos los enlaces, routers y switches en la red; de modo que ninguno de estos recursos se encuentre infrautilizado o sobrecargado. La TE, se ha convertido en la principal aplicación de MPLS debido al crecimiento impredecible en la demanda de recursos de red.

Mediante MPLS, los ISP pueden soportar servicios diferenciados o DiffServ [56]. El modelo DiffServ define varios mecanismos para clasificar el tráfico en un pequeño número de CoS. Los usuarios de Internet demandan continuamente nuevas aplicaciones, teniendo los servicios actualmente soportados unos requerimientos de ancho de banda y de tolerancia a retrasos en la transmisión muy distintos y para satisfacer estas necesidades óptimamente, los ISP necesitan adoptar no sólo técnicas de ingeniería de tráfico, sino también de clasificación de dicho tráfico. De nuevo, MPLS ofrece a los ISP una gran flexibilidad en cuanto a los diferentes tipos de servicios que puede proporcionar a sus clientes.

Finalmente, MPLS ofrece también un mecanismo sencillo y flexible para crear VPN. Una VPN simula la operación de una WAN (Wide Area Network) privada sobre la Internet pública. Para ofrecer un servicio de VPN viable a sus clientes, un ISP debe solventar los problemas de seguridad de los datos y soportar el uso de direcciones IP privadas no únicas dentro de la VPN. Puesto que MPLS permite la creación de circuitos virtuales o túneles a lo largo de una red IP, es lógico que los ISP utilicen MPLS como una forma de aislar el tráfico. No obstante, MPLS no tiene en estos momentos ningún mecanismo para proteger la seguridad en las comunicaciones, por lo que el ISP deberá conseguirla mediante cortafuegos y algún protocolo de encriptación tipo IPsec. Existen varias alternativas para implementar VPNs mediante MPLS, pero la mayoría se basan en la RFC 2547.

5.2.6 FORO MPLS

El Foro MPLS es una organización internacional constituida a primeros del 2000, cuyo objetivo es acelerar la adopción y desarrollo de MPLS y sus tecnologías asociadas. El Foro MPLS sirve como un punto de encuentro y discusión para los proveedores de servicios, fabricantes de equipos, vendedores de componentes y compañías de integración y verificación de soluciones, con el fin de establecer las necesidades de la industria MPLS. Esto incluye la creación de servicios empresariales sobre redes MPLS y el desarrollo de productos que incorporan tecnologías MPLS. El Foro consigue estos objetivos a través de iniciativas de interoperabilidad, acuerdos de desarrollo y cooperación, y programas educativos.

Este organismo está abierto a cualquier organización, persona, o agencia gubernamental dedicada al progreso de Internet y de las redes IP en general, a través de la pronta adopción de la tecnología MPLS. Los miembros fundadores fueron: Data Connection Ltd., Integral Access, Lucent Technologies, Marconi, NetPlane, Qwest, Telcordia Technologies, Tenor Networks y Vivace Networks; y en la actualidad, se han integrado empresas como: Alcatel, Ericsson, Equant, Huawei America Inc., Intel, NEC, Siemens AG, etc.

El papel del Foro MPLS es totalmente complementario al de otros organismos de estandarización existentes previamente, tales como el IETF (Internet Engineering Task Force), el ITU (International Telecommunications Union), u otros foros de la industria como el Foro ATM. Únicamente tiene la intención de desarrollar acuerdos de implementación en aquellas áreas de MPLS donde no desempeñan actividad otros organismos de estandarización y, después, trabajar con total colaboración con ellos.

La mayor parte de los routers y switches actuales destinados a redes troncales están preparados para utilizar MPLS, y muchos de los antiguos podrían soportarlo actualizando su software. No obstante, aunque varios ISP han realizado experiencias pilotos o han implantado MPLS en la parte troncal de sus redes, no se espera una introducción masiva hasta el 2003 o 2004, cuando los fabricantes alcancen una compatibilidad total en sus equipos. Del mismo modo que ocurrió con la actualización de las infraestructuras X.25 [57] y Frame Relay (FR) a ATM, la migración a MPLS como núcleo de las redes multiservicio con soporte de voz, vídeo y datos, se realizará de forma gradual durante varios años; máxime dada la crisis mundial del sector de las telecomunicaciones, que está repercutiendo muy negativamente en las inversiones de los operadores de red y fabricantes de equipos.

5.3 IPSEC

5.3.1 DESCRIPCIÓN DEL PROTOCOLO

IPsec (abreviatura de Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

Los protocolos de IPsec actúan en la capa de red, la capa 3 del modelo OSI. Otros protocolos de seguridad para Internet de uso extendido, como SSL, TLS [58] y SSH [59] operan de la capa de transporte (capas OSI 4 a 7) hacia arriba. Esto hace que IPsec sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP, los protocolos de capa de transporte más usados. IPsec tiene una ventaja sobre SSL y otros métodos que operan en capas superiores. Para que una aplicación pueda usar IPsec no hay que hacer ningún cambio, mientras que para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar su código.

IPsec está implementado por un conjunto de protocolos criptográficos para:

- Asegurar el flujo de paquetes
- Garantizar la autenticación mutua
- Establecer parámetros criptográficos.

La arquitectura de seguridad IP utiliza el concepto de asociación de seguridad (SA) como base para construir funciones de seguridad en IP. Una asociación de seguridad es simplemente el paquete de algoritmos y parámetros (tales como las claves) que se está usando para cifrar y autenticar un flujo particular en una dirección. Por lo tanto, en el tráfico normal bidireccional, los flujos son asegurados por un par de asociaciones de seguridad. La decisión final de los algoritmos de cifrado y autenticación (de una lista definida) le corresponde al administrador de IPsec.

Para decidir qué protección se va a proporcionar a un paquete saliente, IPsec utiliza el índice de parámetro de seguridad (SPI), un índice a la base de datos de asociaciones de seguridad (SADB), junto con la dirección de destino de la cabecera del paquete, que juntos identifican de forma única una asociación de seguridad para dicho paquete. Para un paquete entrante se realiza un procedimiento similar; en este caso IPsec coge las claves de verificación y descifrado de la base de datos de asociaciones de seguridad.

En el caso de multicast, se proporciona una asociación de seguridad al grupo, y se duplica para todos los receptores autorizados del grupo. Puede haber más de una asociación de seguridad para un grupo, utilizando diferentes SPIs, y por ello permitiendo múltiples niveles y conjuntos de seguridad dentro de un grupo. De hecho, cada remitente puede tener múltiples asociaciones de seguridad, permitiendo autenticación, ya que un receptor sólo puede saber que alguien que conoce las claves ha enviado los datos. Hay que observar que el estándar pertinente no describe cómo se elige y duplica la asociación a través del grupo; se asume que un interesado responsable habrá hecho la elección.

5.3.2 MODOS DE FUNCIONAMIENTO

5.3.2.1 MODO TRANSPORTE

En modo transporte, sólo la carga útil (los datos que se transfieren) del paquete IP es cifrada y/o autenticada. El enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP; sin embargo, cuando se utiliza la cabecera de autenticación (AH), las direcciones IP no pueden ser traducidas, ya que eso invalidaría el hash. Las capas de transporte y aplicación están siempre aseguradas por un hash, de forma que no pueden ser modificadas de ninguna manera (por ejemplo traduciendo los números de puerto TCP y UDP). El modo transporte se utiliza para comunicaciones ordenador a ordenador.

Una forma de encapsular mensajes IPsec para atravesar NAT ha sido definida por RFCs que describen el mecanismo de NAT-T

El propósito de este modo es establecer una comunicación segura punto a punto, entre dos hosts y sobre un canal inseguro. Este ejemplo queda ilustrado en la figura 64:

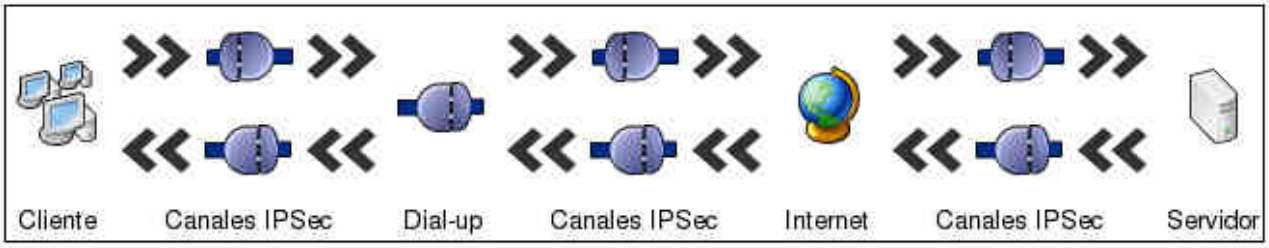


Figura 64: Conexión IPSec

5.3.2.2 MODO TUNEL

En el modo túnel, todo el paquete IP (datos más cabeceras del mensaje) es cifrado y/o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento. El modo túnel se utiliza para comunicaciones red a red (túneles seguros entre routers, Ej. para VPNs) o comunicaciones ordenador a red u ordenador a ordenador sobre Internet. El propósito de este modo es establecer una comunicación segura entre dos redes remotas sobre un canal inseguro. El ejemplo queda ilustrado en la figura 65:

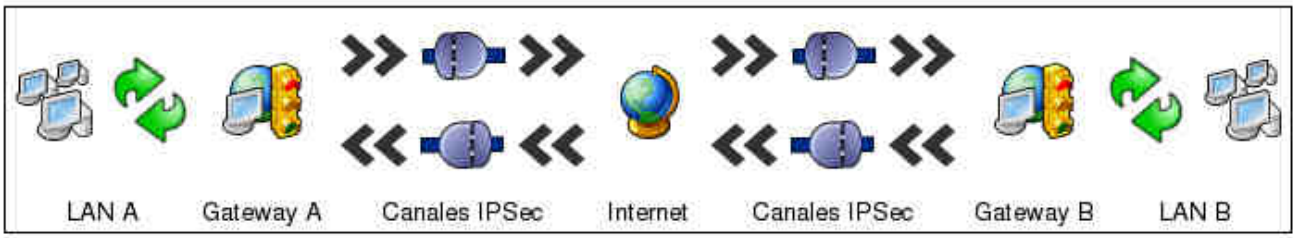


Figura 65: IPSec Modo túnel

5.3.3 CABECERAS

5.3.3.1 CABECERA IP

La cabecera del paquete IP es la mostrada en la figura 66:

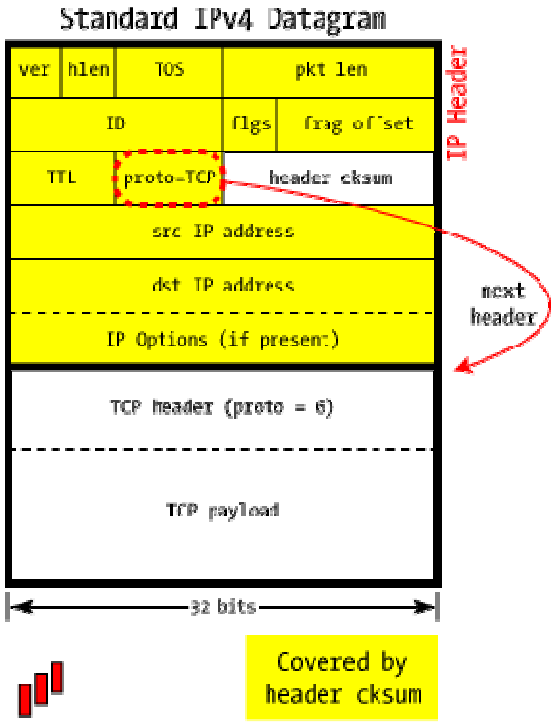


Figura 66: Cabeceras IPSec

Donde:

- **ver** Es la versión del protocolo IP. IPsec se monta sobre IPv4.
- **hlen** Longitud de la cabecera, en palabras de 32 bits. Su valor mínimo es de 5 para una cabecera correcta, y el máximo de 15. El tamaño de la cabecera **nunca** incluye el tamaño del payload o de la cabecera siguiente.
- **TOS** Indica una serie de parámetros sobre la calidad de servicio deseada durante el tránsito por una red. Algunas redes ofrecen prioridades de servicios, considerando determinado tipo de paquetes "más importantes" que otros (en particular estas redes solo admiten los paquetes con prioridad alta en momentos de sobrecarga).
- **pkt len** Es el tamaño total, en octetos, del datagrama, incluyendo el tamaño de la cabecera y el de los datos. El tamaño máximo de los datagramas usados normalmente es de 576 octetos (64 de cabeceras y 512 de datos). Una máquina no debería enviar datagramas mayores a no ser que tenga la certeza de que van a ser aceptados por la máquina destino. En caso de fragmentación este campo contendrá el tamaño del fragmento, no el del datagrama original.
- **ID** Indica el identificador del fragmento actual en caso de que el paquete estuviera fragmentado
- **fgls** Actualmente utilizado sólo para especificar valores relativos a la fragmentación de paquetes:

bit 0: Reservado; debe ser 0

bit 1: 0 = Divisible, 1 = No Divisible (DF)

bit 2: 0 = Último Fragmento, 1 = Fragmento Intermedio (le siguen más fragmentos) (MF)

La indicación de que un paquete es indivisible debe ser tenida en cuenta bajo cualquier circunstancia. Si el paquete necesitara ser fragmentado, no se enviará.

- **frag offset** En paquetes fragmentados indica la posición, en unidades de 64 bits, que ocupa el paquete actual dentro del datagrama original. El primer paquete de una serie de fragmentos contendrá en este campo el valor 0.
- **TTL** Indica el máximo número de enrutadores que un paquete puede atravesar. Cada vez que algún nodo procesa este paquete disminuye su valor en uno por cada router que pase. Cuando llegue a ser 0, el paquete no será reenviado.
- **proto** Indica el protocolo de siguiente nivel utilizado en la parte de datos del datagrama. Los más utilizados son:

Código	Descripción
1	ICMP [60] — Internet Control Message Protocol
2	IGMP [61] — Internet Group Management Protocol
4	IP en IP (una encapsulación IP)
6	TCP — Transmission Control Protocol
17	UDP — User Datagram Protocol
41	IPv6 — next-generation TCP/IP
47	GRE [62]— Generic Router Encapsulation (usado por PPTP)
50	IPsec: ESP — Encapsulating Security Payload
51	IPsec: AH — Authentication Header

Tabla 39: Campo proto en IPSec

5.3.3.2 CABECERA IPSEC AH (authentication only)

AH está dirigido a garantizar integridad sin conexión y autenticación de los datos de origen de los datagramas IP. Para ello, calcula un Hash Message Authentication Code (HMAC) a través de algún algoritmo hash operando sobre una clave secreta, el contenido del paquete IP y las partes inmutables del datagrama. Este proceso restringe la posibilidad de emplear NAT, que puede ser implementada con NAT transversal. Por otro lado, AH puede proteger opcionalmente contra ataques de repetición utilizando la técnica de ventana deslizante y descartando paquetes viejos. AH protege la carga útil IP y todos los campos de la cabecera de un datagrama IP excepto los campos mutantes, es decir, aquellos que pueden ser alterados en el tránsito. En IPv4, los campos de la cabecera IP mutantes (y por lo tanto no autenticados) incluyen TOS, Flags, Offset de fragmentos, TTL y suma de verificación de la cabecera. AH opera directamente por encima de IP, utilizando el protocolo IP número 51. Una cabecera AH mide 32 bits. Un diagrama de cómo se organizan queda reflejado en la figura 67:

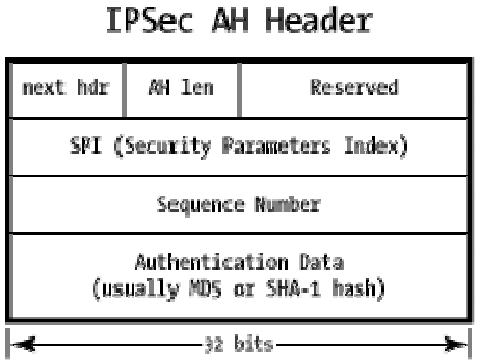


Figura 67: Cabecera IPSec AH

- **next hdr** Identifica cuál es el siguiente protocolo, es decir, cual es el protocolo que será autentificado, cuál es el payload.
- **AH len** El tamaño del paquete AH.
- **RESERVED** Reservado para futuras aplicaciones. Debe estar a 0
- **Security parameters index (SPI)** Indica los parámetros de seguridad, que en combinación con los parámetros IP, identifican la asociación de seguridad del paquete
- **Sequence Number** Es un número creciente usado para prevenir ataques por repetición. El número está incluido en los datos encriptados, así que cualquier alteración será detectada
- **Authentication Data** Contiene el valor de identificación de integridad. Puede contener relleno. Se calcula sobre el paquete entero, incluidas la mayoría de las cabeceras. El que recibe calcula otra vez el hash, y si este no coincide, el paquete se tira.

AH en Modo Transporte

La manera más fácil de entender el modo transporte es que protege el intercambio de información entre dos usuarios finales. La protección puede ser autentificación o encriptación (o las dos), pero no se hace usando un túnel (para eso está el modo túnel). No es una vpn, es una simple conexión segura entre dos usuarios finales.

En AH en Modo Transporte, el paquete IP es modificado ligeramente para incluir una nueva cabecera **AH** entre la cabecera IP y la información transmitida (TCP, UDP, etc.) y después se requiere un proceso "de arrastre" que interconecta las distintas cabeceras entre ellas.
Este proceso "de arrastre" se necesita para que el paquete original IP sea reconstituido cuando llegue a su destino; cuando las cabeceras IPsec han sido validadas en el receptor, se despojan las cabeceras IPsec y la carga a transmitir (TCP, UDP, etc.) es guardada nuevamente en la cabecera IP.

Cuando el paquete llega a su siguiente destino y pasa el test de autenticidad, la cabecera AH es quitada y el campo **proto=AH** es reemplazado con el siguiente protocolo de la carga transmitida (TCP, UDP, etc.). Esto pone al datagrama es su estado original, y puede ser enviado al proceso original.

Las cabeceras Cabecera IPSec AH en modo transporte pueden verse en la figura 68:

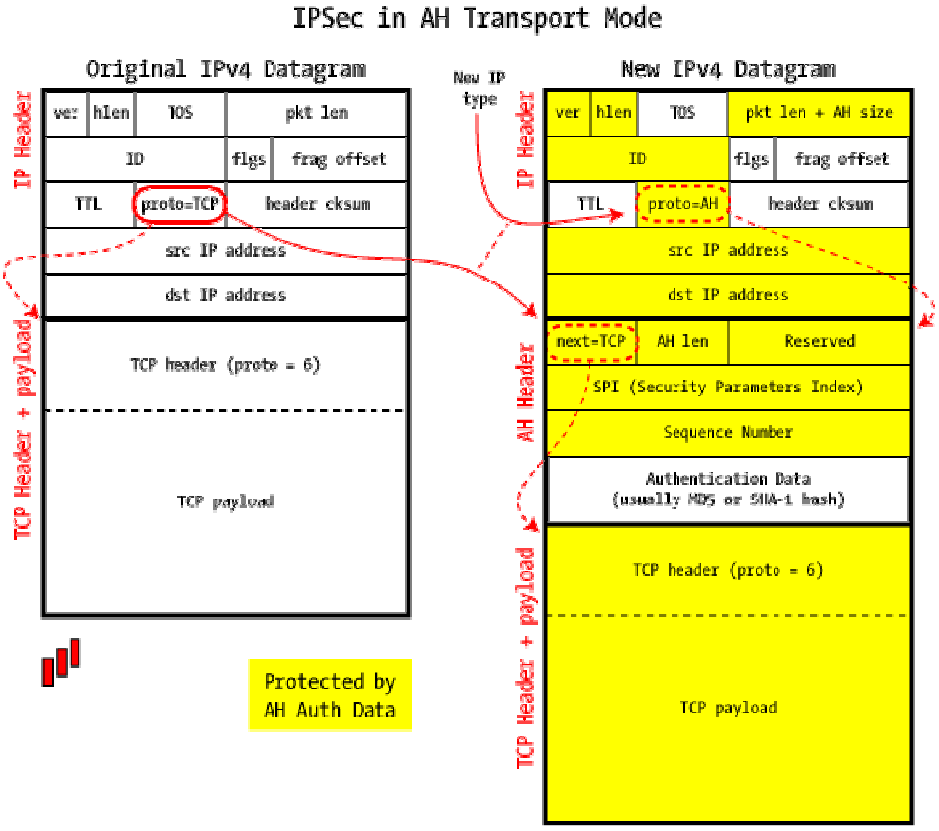


Figura 68: Cabecera IPSec AH en modo transporte

AH en Modo Túnel

El modo túnel es el más común para dar una funcionalidad de VPN, donde un paquete IP es encapsulado dentro de otro y enviado a su destino.

Igual que en el modo transporte, el paquete es "sellado" con un ICV para autentificar al que envía la información para prevenir modificaciones durante el tránsito. Pero a diferencia del modo de transporte, el modo túnel encapsula todo el paquete IP, no sólo la carga útil (TCP, UDP, etc.). Esto hace que el destinatario del paquete sea uno diferente al destinatario original. Esto ayuda a la formación de un túnel.

Cuando un paquete en modo túnel llega a su destino, pasa el mismo proceso de autentificación igual que cualquier paquete AH-IPsec. Este proceso hace que se despoje de sus cabeceras IP y AH, luego nos queda el datagrama original, que es enrutado mediante un proceso normal.

La mayoría de las implementaciones tratan el final del túnel como una interfaz de red virtual - exactamente igual que una Ethernet o localhost - y el tráfico entrante y saliente de él está sujeto a todas las decisiones normales de enrutamiento.

El paquete reconstituido puede ser entregado a la máquina local o enrutado donde sea (dependiendo de la dirección IP encontrada en el paquete encapsulado), pero de ninguna manera vuelve a estar sujeto a las protección de IPsec. Esta finaliza al final del túnel. A partir de allí es tratado como un datagrama IP normal.

Tal como el modo de transporte es usado estrictamente para asegurar conexiones de extremo a extremo entre dos ordenadores, el modo túnel es usado normalmente entre pasarelas (routers, firewalls o dispositivos VPN) para proveer una Red Privada Virtual (VPN).

Las cabeceras Cabecera IPSec AH en modo túnel pueden verse en la figura 69:

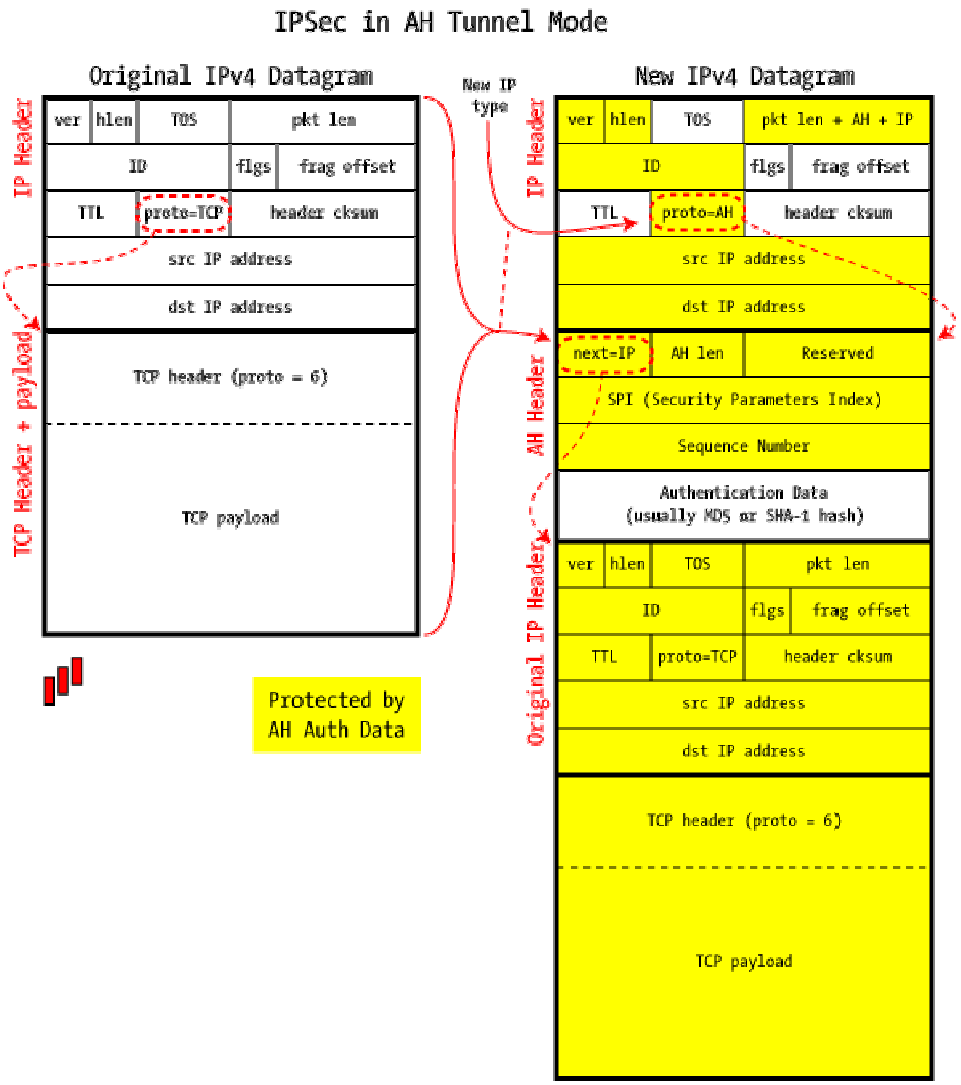


Figura 69: Cabecera IPSec AH en modo túnel

¿Transporte o Túnel?

Curiosamente, no hay un campo explícito "Modo" en IPsec que distinga entre el modo de transporte y el modo túnel. Lo que los distingue es el campo *siguiente cabecera (next head)* en la cabecera AH.

Cuando el valor de "siguiente cabecera" es IP, significa que este paquete encapsula un datagrama IP entero (incluyendo los campos de destino y origen IP que nos permiten saber dónde va el paquete que va encapsulado después de la desencapsulación. Así se comporta el modo túnel. Otro valor cualquiera (TCP, UDP, ICMP, etc.) significa que estamos usando el modo transporte y se trata de una conexión segura extremo a extremo.

El nivel superior de un datagrama IP es estructurado de la misma manera, sin tener en cuenta el modo, y los routers inmediatos tratan todo tipo de tráfico IPsec/AH de la misma manera que el tráfico normal, sin una inspección más profunda.

Hay que darse cuenta que un host - en contraposición a una pasarela - es necesario que soporte los dos modos, de transporte y túnel, pero en una conexión host-to-host parece superfluo usar el modo túnel.

Además, una pasarela (router, firewall, etc.) tiene que tener soporte únicamente para modo túnel, sin embargo tener soporte para el modo transporte es útil sólo cuando la pasarela se considera como destino ella misma, como en caso de funciones de administración de red.

Algoritmos de autentificación

AH lleva un campo ICV (Integrity Check Value) para comprobar la integridad del paquete y que nadie lo ha manipulado durante el trayecto. El valor de ese campo está dado por algoritmos de encriptación tales como MD5 o SHA-1.

Más que usar un checksum convencional, el cual podría no proveer una seguridad real contra una manipulación intencional, este usa una Hashed Message Authentication Code (HMAC) [63], que incorpora una clave secreta mientras se crea el hash. Aunque un atacante puede recalcular un hash fácilmente, sin la clave secreta no sería capaz de crear el ICV apropiado. HMAC se ilustra en la figura 70:

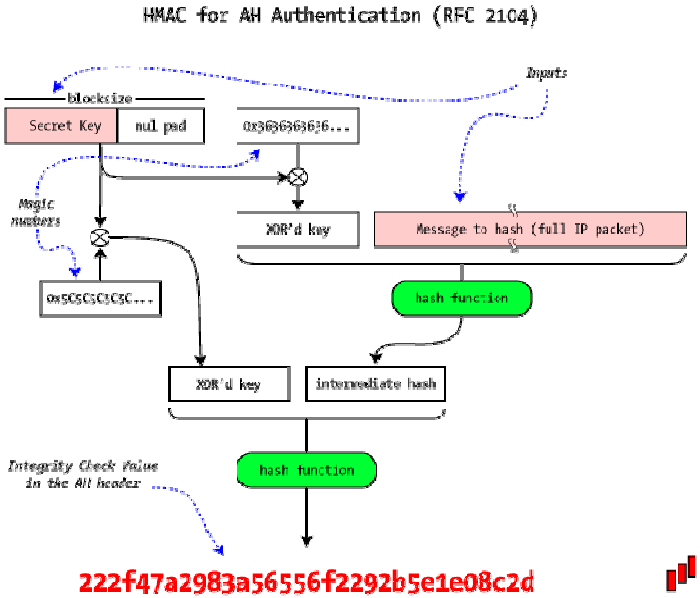


Figura 70. IPSec: Algoritmo de identificación

Huelga decir que IPsec no define ni obliga como debe hacerse la autentificación, simplemente ofrece un marco de seguridad en la que los dos hosts que realizan la comunicación se ponen de acuerdo sobre qué sistema usar. Pueden usarse firmas digitales o funciones de encriptación, pero es obligatorio que ambos los conozcan y sepan cómo usarlos

NAT y AH

AH da una protección muy fuerte a los paquetes porque cubre todas las partes que se consideran inmutables. Pero esta protección tiene un coste: AH es incompatible con NAT (Network Address Translation).

NAT se usa para trazar un rango de direcciones privadas (192.168.1.X) de un conjunto (normalmente más pequeño) de direcciones públicas, para reducir la demanda de direcciones IP públicas. En este proceso, la cabecera IP se modifica "al vuelo" por el dispositivo NAT para cambiar las direcciones IP de origen y destino.

Cuando es cambiada la dirección de origen de la cabecera IP, se fuerza a recalcular el checksum de la cabecera. Esto se tiene que hacer a parte, porque el dispositivo NAT es como un "agujero" en el camino del origen al destino, y esta situación requiere decrementar el campo TTL(Time to Live).

Dado que el campo TTL y el checksum de la cabecera siempre son modificados "al vuelo", AH sabe que tiene que excluirlos de su protección, pero no tiene que excluir a las direcciones IP. Estas están incluidas en el control de integridad, y cualquier cambio en las direcciones ip de origen y destino va a hacer que el control de integridad falle cuando llegue al destinatario. Dado que el valor del control de integridad contiene una llave secreta que sólo la saben el host origen y el host destino, el dispositivo NAT no puede recalcular el ICV.

Las mismas se aplican también al PAT(Port Address Translation), el cual traza múltiples direcciones IP en una en una sola dirección IP externa. No solo se modifican las direcciones IP "al vuelo", sino además los números de los puertos UDP y TCP (a veces hasta la carga útil que se transfiere. Esto requiere un sistema más sofisticado por parte del dispositivo NAT, y unas modificaciones más extensas en todo el datagrama IP.

Por esta razón, AH - en el modo Túnel o Transporte - es totalmente incompatible con NAT y sólo se puede emplear AH cuando las redes de origen y destino son alcanzables sin traducción.
Hay que decir que esta dificultad no se aplica al ESP, ya que su autentificación y encriptación no incorpora la cabecera IP modificada por NAT. Aún así, NAT también impone algunos desafíos incluso en ESP (explicado más adelante).

NAT traduce las direcciones IP al vuelo, pero también guarda un registro de que conexiones siguen el camino traducido y así poder enviar las respuestas al origen de manera correcta. Cuando se usa TCP o UDP, esto se hace mediante los números de los puertos (que pueden ser reescritos al vuelo o no), pero IPsec no da ninguna interfaz para hacer esto.

En la figura 71 podemos ver por qué son incompatibles NAT y AH:

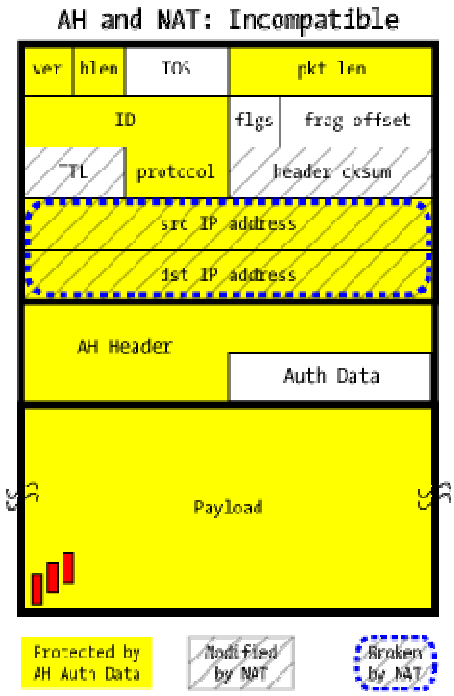


Figura 71: Incompatibilidad entre NAT y AH

5.3.4 ESP (Encapsulating Security Payload)

Añadir encriptación hace que ESP sea un poco más complicado, ya que la encapsulación rodea a la carga útil es algo más que precederla con AH: ESP incluye cabecera y campos para dar soporte a la encriptación y a una autentificación opcional. Además, provee los modos de transporte y túnel, los cuales nos son ya familiares.

Las RFCs de IPsec no insisten demasiado en un sistema particular de encriptación, pero normalmente se utiliza DES [64], triple-DES o AES [65] para asegurar la carga útil de “ojos indiscretos”. El algoritmo usado para una conexión en particular es definido por la Security Association (SA), y esta SA incluye no sólo el algoritmo, también la llave usada.

A diferencia de AH, que da una pequeña cabecera antes de la carga útil, ESP rodea la carga útil con su protección. Los parámetros de seguridad Index y Sequence Number tienen el mismo propósito que en AH, pero nos encontramos como relleno en la cola del paquete el campo “siguiente campo” y el opcional “Authentication data”.

Es posible usar ESP sin ninguna encriptación (usar el algoritmo NULL), sin embargo estructura el paquete de la misma forma. No nos da ninguna confidencialidad a los datos que estamos transmitiendo, y sólo tiene sentido usarlo con una la autentificación ESP. No tiene sentido usar ESP sin encriptación o autentificación (a no ser que estemos simplemente probando el protocolo).

El relleno sirve para poder usar algoritmos de encriptación orientados a bloques, dado que tenemos que crear una carga a encriptar que tenga un tamaño múltiplo de su tamaño de bloque. El tamaño del relleno viene dado por el campo pad len. El campo next hdr nos da el tipo (IP, TCP, UDP, etc.) de la carga útil, aunque esto sea usado como un punto para volver hacia atrás en el paquete para ver que hay en el AH.

Además de la encriptación, ESP puede proveer autentificación con la misma HMAC de AH. A diferencia de AH, esta autentifica sólo la cabecera ESP y la carga útil encriptada, no todo el paquete IP. Sorprendentemente, esto no hace que la seguridad de la autentificación más débil, pero nos da algunos beneficios importantes.

Cuando un extraño examina un paquete IP que contiene datos ESP, es prácticamente imposible adivinar que es lo que tiene dentro, excepto por los datos encontrados en la cabecera IP (siendo interesantes las direcciones IP de origen y destino). El atacante va a saber casi seguro que son datos ESP (está en la cabecera que son datos ESP), pero no va a saber de qué tipo es la carga útil.

Incluso la presencia de Authentication Data no puede ser determina solamente con mirar al paquete. Esta resolución está hecha por la Security Parameters Index, que hace referencia al conjunto de parámetros precompartidos para esta conexión.

En la figura 72, se muestran los campos de las cabeceras IPSec con ESP, tanto en el caso de llevar Autentificación como cuando no la llevan.

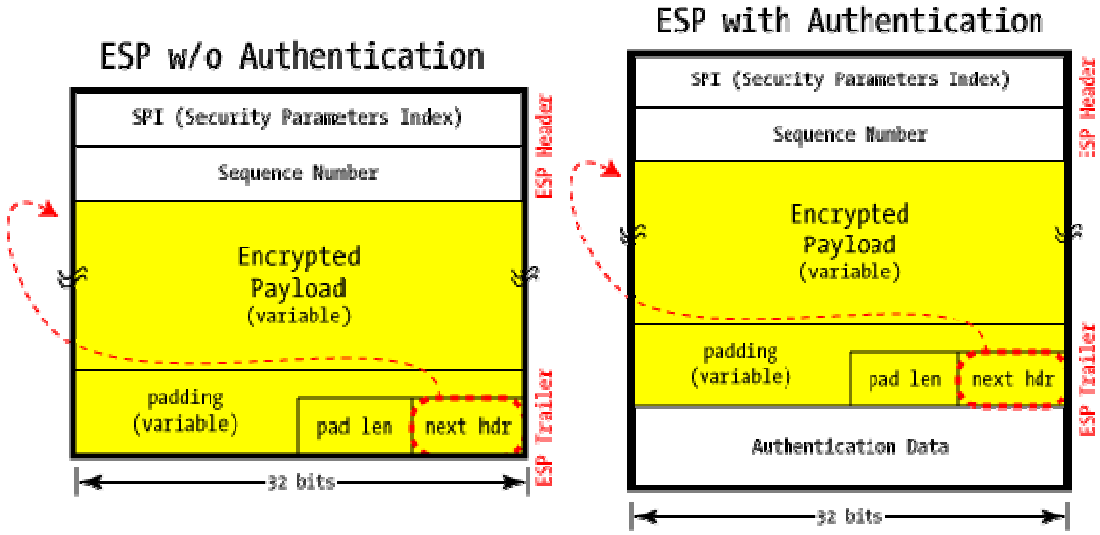


Figura 72: IPSec con ESP

ESP en Modo Transporte

Al igual que en AH, el modo transporte encapsula justamente la carga la carga útil del datagrama y está diseñado justamente para comunicaciones extremo-a-extremo. La cabecera IP original se deja (excepto por el campo cambiado Protocol), y esto hace - además de otras cosas - que las direcciones IP de origen y destino se quedan como están.

En la figura 73 se muestran las cabeceras de IPSec con ESP en modo transporte.

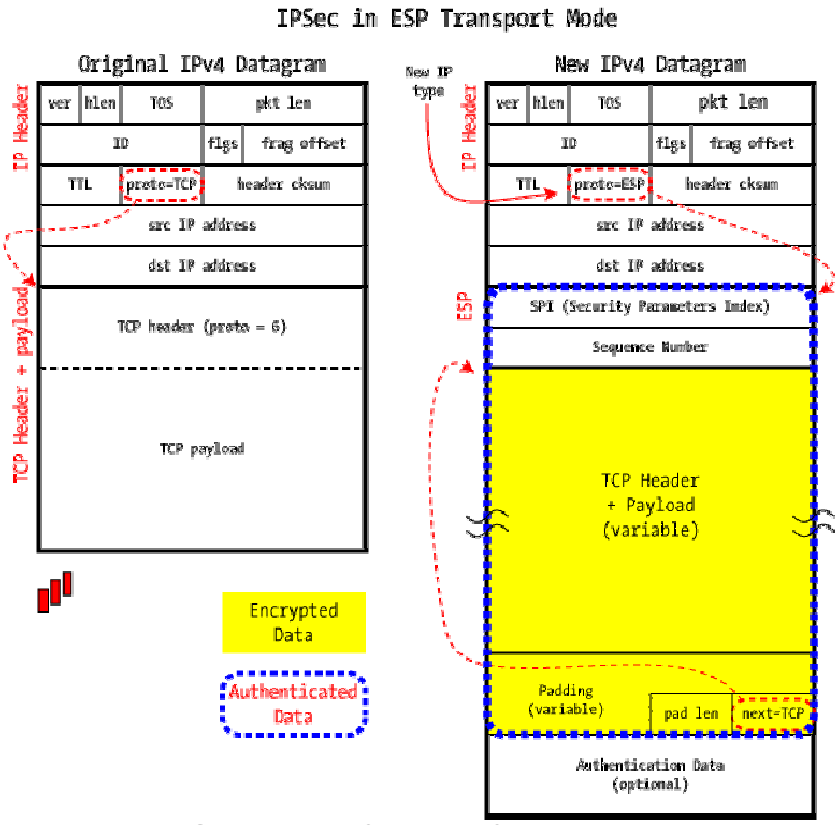


Figura 73: Cabeceras IPSec con ESP en modo transporte

ESP en Modo Túnel

El ESP en modo Túnel encapsula el datagrama IP entero y lo encripta, como se muestra en la figura 74:

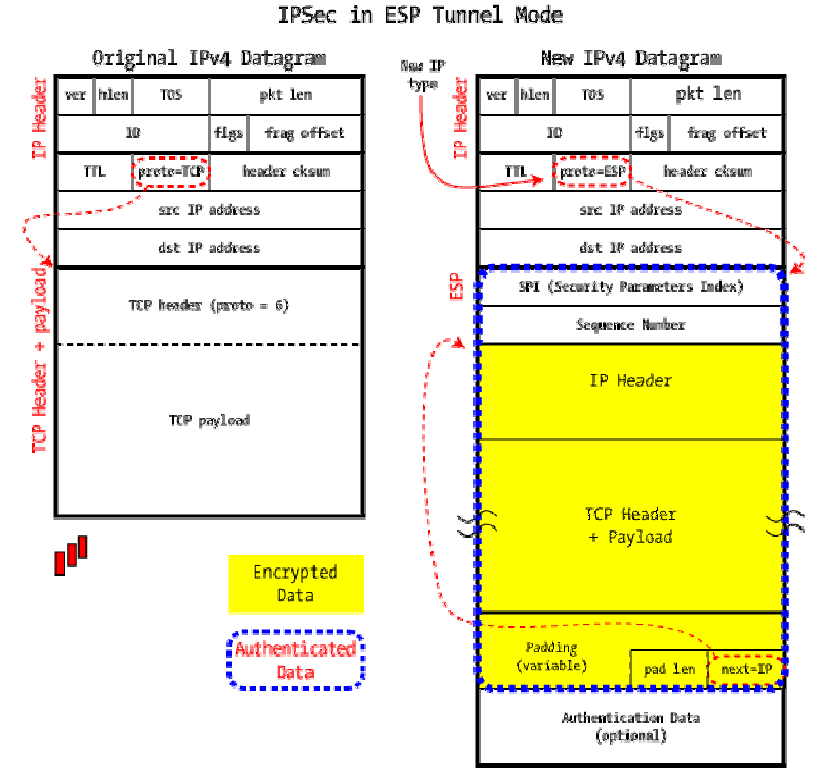


Figura 74: Cabeceras IPSec con ESP en modo túnel

Proveer una conexión encriptada en modo túnel es dar una forma muy cercana a como se crea una VPN, y es lo que se nos viene a la cabeza a la mayoría cuando pensamos acerca de IPsec. Además de esto, tenemos que añadir autentificación. Esta parte se trata en la siguiente sección.

A diferencia de AH, donde un forastero puede ver fácilmente que es lo que se transmite en modo Túnel o Transporte, usando ESP eso no ocurre; esa información no está disponible para el forastero. El caso es que en el modo túnel (poniendo next=IP), el datagrama IP entero original es parte de la carga útil encriptada, y no será visible para nadie que no pueda desencriptar el paquete.

Construyendo una VPN real

Con la explicación de AH y ESP ahora somos capaces de habilitar la encriptación y la autentificación para construir una VPN real. El objetivo de la VPN es juntar dos redes seguras a través de una red insegura, tal como sería tirar un cable Ethernet muy grande entre las dos redes seguras. Es una tecnología muy usada para juntar por ejemplo filiales de compañías con la sede central de la compañía, dando a los usuarios acceso a recursos que no pueden caer en manos indebidas, tales como documentos secretos.

La figura 75 muestra un ejemplo de VPN:

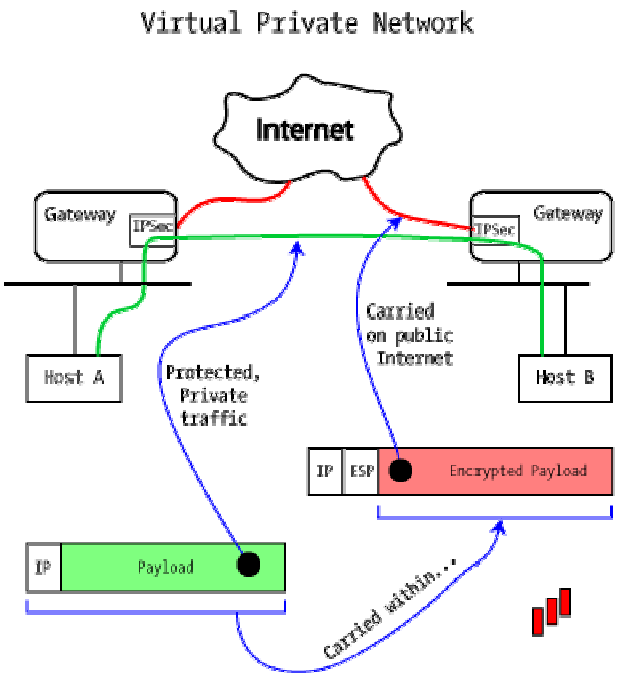


Figura 75: Red VPN

Claramente, una red VPN segura requiere las dos cosas: autentificación y encriptación. Sabemos que la única manera de conseguir encriptación es ESP, pero ESP y AH pueden proveer autentificación: ¿cuál de las dos usar?

La solución obvia de envolver ESP dentro de AH es técnicamente posible, pero en la práctica no es muy usada por las limitaciones de AH respecto al NAT. Usar AH+ESP puede hacer que no podamos atravesar el dispositivo NAT.

En cambio, ESP+Auth es usado en modo Túnel para encapsular completamente el tráfico a través de una red no segura, protegiendo este tráfico con encriptación y autentificación.

El tráfico protegido de esta manera produce información inútil para un intruso, ya que los dos hosts que se comunican están conectados a través de una VPN. Esta información puede ayudar al atacante a entender que los dos hosts se comunican por un canal seguro, pero nunca revela el contenido del tráfico. Incluso el tipo de tráfico encapsulado en el protocolo (TCP, UDP o ICMP) está oculto para las personas de fuera.

Lo particularmente bonito de este modo de operación es que los usuarios finales no saben nada de la VPN o las medidas de seguridad tomadas. Desde que una VPN está implementada por una pasarela, este trata la VPN como otra interfaz, y enruta el tráfico que va a otra parte como normalmente lo haría.

Este paquete-en-paquete puede ser anidado a más niveles: Host A y Host B pueden establecer su propia conexión autenticada (vía AH) y comunicarse sobre una VPN. Esto pondría un paquete AH dentro de un paquete con una cobertura ESP+Auth.

La figura 76 muestra los campos de un paquete IPSec, utilizando ESP con autentificación en modo túnel, sobre una red VPN tradicional.

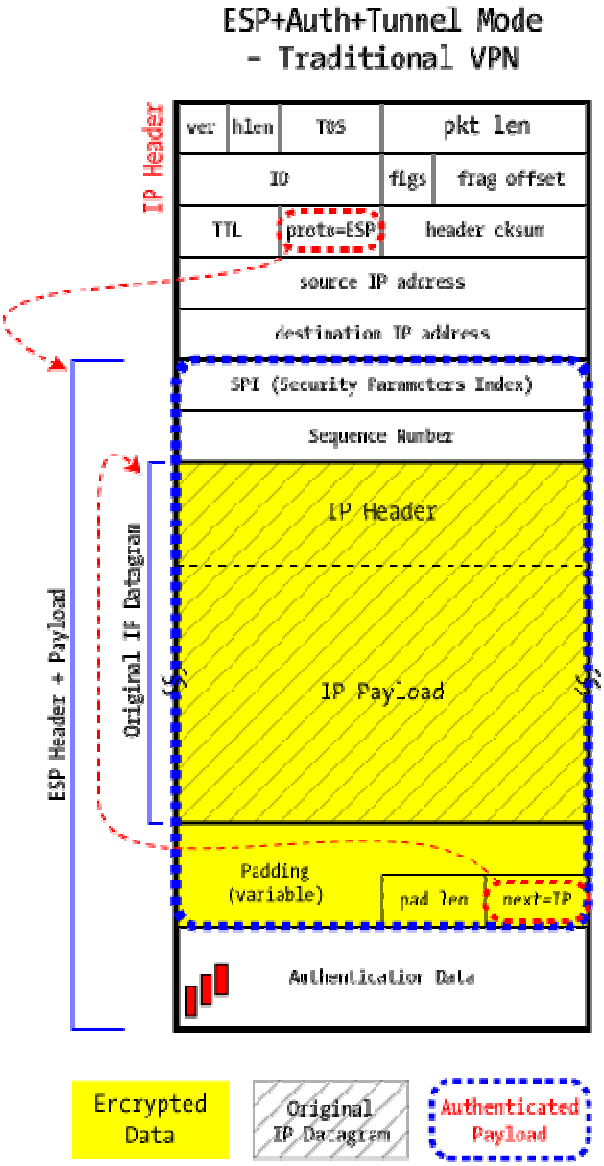


Figura 76: Cabeceras IPSec con ESP y autentificación en modo túnel en una VPN

5.3.5 Security Association y SPI

Es obvio que si los dos hosts o pasarelas van a establecer una conexión segura, se requiere algún tipo de clave secreta compartida para llevar a cabo la función de autentificación o la y/o la clave del algoritmo de encriptación. La cuestión es como esos "secretos" son establecidos a para poder ser dirigidos desde cualquier sitio, y para los propósitos de esta guía vamos a suponer que han llegado "mágicamente" a su lugar.

Cuando un datagrama IPsec - AH o ESP - llega a una interfaz, ¿cómo sabe la interfaz que conjunto de parámetros usar (clave, algoritmo y políticas)? Un host puede tener varias conversaciones simultáneas, cada una con un diferente conjunto de claves y algoritmos, y tenemos que tener un gobernador que lleve todo este proceso.

Estos parámetros son especificados por la Security Association (SA), una colección de parametros específicos de conexión, y cada pareja pueden tener uno o más colecciones de parámetros específicos de conexión. Cuando llega el datagrama son usadas tres piezas de los datos para localizar dentro de la base de datos o Security Associations Database (SADB) la SA correcta.

- Dirección IP de la pareja (el usuario con el que nos estamos comunicando)
- Protocolo IPsec (AH o ESP)
- Security Parameter Index

Hay muchas maneras para asociar este triplete a un socket IP, el cual está denotado de forma única por la dirección IP, protocolo y el número del puerto

Una SA es de sentido único, así que una conexión en los dos sentidos (el caso típico) requiere al menos dos. Además, cada protocolo (ESP/AH) tiene su propia SA en cada dirección, por tanto una conexión completa AH+ESP VPN requiere 4 SAs. Todas ellas están en la Security Associations Database.

En la SADB tenemos una cantidad ingente de información, pero sólo podemos tocar una parte de esta:

- AH: algoritmo de autenticación
- AH: secreto de autenticación
- ESP: algoritmo de encriptación
- ESP: clave secreta de encriptación
- ESP: autenticación activada si/no
- Algunos parámetros de intercambio de llaves
- Restricciones de enrutamiento
- Política de filtración de IPs

Algunas implementaciones mantienen la SPD (Security Policy Database) con herramientas de tipo consola, otras con GUIs y otras proveen una interfaz basada en web sobre la red. El grado de detalle mantenido por cualquier implementación en particular depende de las facilidades ofrecidas, así como si está en modo Host o modo Pasarela (Gateway).

Glosario

Acrónimo	Significado
AES	Advanced Encryption Standard
AH	Cabecera de Autentificación
ANS	Acuerdo de Nivel de Servicio
ASP	Active Server Pages
ATM	Asynchronous Transfer Mode
BD	Base de Datos
BGP	Border Gateway Protocol
BIES	Boca de Incendios Equipada
CCT	Centro de Competencia Tecnológica
CCTV	Circuito Cerrado de Televisión
CDG	Centro de Datos gestionado
CeGAS	Centro de Gestión de Aplicaciones y Servicios
CoS	Clase de Servicio (Class of Service)
CPD	Centro de Procesado de Datos
CRC	Centro de Relación de Clientes
CR-LDP	Constraint-based Routing – Label Distribution Protocol
DDoS	Denegación de Servicio Distribuido (Distributed Denial of Service)
DES	Data Encryption Standard
DLCI	Data Link Control Identifier
DNS	Domain Name Server
DoS	Denegación de Servicio (Denial of Service)
DWDM	Dense Wavelength Division Multiplexing
EDC	Equipo en Domicilio de Cliente
ERP	Enterprise Resource Planning
ESP	Encapsulating Security Payload
FC	Fiber Channel
FEC	Forward Equivalent Class
GMPLS	Generalized MPLS
HA	Alta Disponibilidad (High Avaliability)
HBA	Host Bus Adapter
HMAC	Hash Message Authentication Code
HV	Hosting Virtual
IaaS	Infrastructure as a Service
ICMP	Internet Control Message Protocol
ICV	valor de verificación de integridad
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
ISO	Organización Internacional de Estandarización (International Organization for Standardization)
ISP	Internet Service Provider
ITIL	Biblioteca de Infraestructura de Tecnologías de Información (Information Technology Infrastructure Library)
ITU	Unión Internacional de Telecomunicaciones (International Telecommunications Union)
LAN	Large Area Network
LDAP	Lightweight Directory Access Protocol
LDP	Label Distribution protocol

LER	Label Edge Routers
LOPD	Ley Orgánica de Protección de Datos
LSP	Label Switch Path
LSP	Label Switched Path
LSR	Label Switching Routers
MAN	Metropolitan Area Network
MCI	Módulo de Conectividad a Internet
MCP	Módulo de Conectividad Privada
MPLS	Multi-Protocol Label Switching
NAT	Network Address Translation
NAT	Network Address Translation
OSI	Open System Interconnections
OSPF	Open Shortest Path First
OSS	Sistemas de Soporte a la Operación
PAT	Port address translation
PBX	Centralita Telefónica Tradicional
PE	Router de entrada a la red MPLS
PHP	Hypertext Preprocessor
PNNI	Private Network-to-Network Interface
POS	Procedimientos Operativos de Seguridad
PPTP	Point-to-Point Tunneling Protocol
PUE	Power Usage Effectiveness
QoS	Calidad de Servicio (Quality of Service)
RFP	Request for Proposal
RIB	Base de información de Ruteo
RIP	Routing Information Protocol
RPV	Red Privada Virtual
RSVP-TE	ReSerVation Protocol – Traffic Engineering
RTB/RDSI	Redes conmutadas tradicionales
SA	Asociación de Seguridad
SADB	Base de Datos de Asociaciones de Seguridad
SAI	Sistema de Alimentación Ininterrumpida
SAN	Storage Area Network
SDH/SONET	Synchronous Digital Hierarchy / Synchronous Optical NETwork
SLA	Service Level Agreement
SLO	Service Level Objectives
SNMP	Simple Network Management Protocol
SOC	Centro de Operaciones de Seguridad
SOO	Site Of Origin
SPD	Security Policy Database
SPI	Índice de parámetro de seguridad
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TdE	Telefónica de España
TE	Traffic Engineering
TI	Tecnologías de la Información
TI+C	Tecnologías de la Información + Comunicaciones
TLS	Transport Layer Security
TME	Telefónica Móviles España
ToIP	Texto sobre IP (Texto ver IP)
ToS	Tipo de servicio (Type of Service)
TTL	Tiempo de Vida (Time To Live)

UDP	User Datagram Protocol
VCI	Virtual Channel Identifier
VLAN	Virtual LAN
VM	Máquina virtual (Virtual Machine)
VoIP	Voz Sobre IP (Voice over IP)
VPI	Virtual Path Identifier
VPN	Virtual Private Network
VPN	Virtual Private Network
WAN	Wide Area network
WFQ	Weighted Fair Queuing

Referencias

[1] Martín, Isabel – "Ventajas y desventajas de la virtualización", Mayo de 2008. Última vez accedido en Mayo de 2012 en http://www.techweek.es/virtualizacion/tech-labs/1003109005901/ventajas-desventajas-virtualizacion.1.html.

[2] "Consolidación de Servidores" de VMWare. Última vez accedido en abril de 2012 en http://www.vmware.com/es/solutions/datacenter/consolidation/index.html

[3] Network World – "La virtualización de los servidores ofrece ahorros de hasta un 50%", Febrero de 2009. Última vez accedido en Mayo de 2012 a través de http://www.networkworld.es/La-virtualizacion-de-los-servidores-ofrece-ahorros/seccion-networking/noticia-76673

[4] Ideas Múltiples Log – "Las ventajas de un servidor dedicado virtual VPS frente a uno estándar", Noviembre de 2007. Última vez accedido en Mayo de 2012 a través de http://blog.ideasmultiples.com/2007/11/29/las-ventajas-de-un-servidor-dedicado-virtual-vps-frente-a-uno-estandar/

[5] "VMWare Compatibility Guide" de VMWare. Última vez accedido en Mayo de 2012 a través de http://www.vmware.com/resources/compatibility/search.php.

[6] "VMWare Virtual Appliances" de VMWare. Última vez accedido en Abril de 2012 a través de http://www.vmware.com/appliances/

[7] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal de España

[8] ITNews - "Tipos de Virtualización – Virtualización de Red". Última vez accedido en Abril de 2012 a través de http://www.itnews.ec/marco/000039.aspx

[9] "ZXTM LB – Balanceador de carga de alto rendimiento" de Zycko. Última vez accedido en Abril de 2012 a través de http://es.zycko.com/fabricantes/zeus/zxtm-lb/

[10] Information Sciences Institute. University of Southern California - RFC 793 – "TRANSMISSION CONTROL PROTOCOL. DARPA INTERNET PROGRAM. PROTOCOL SPECIFICATION", Septiembre de 1981

[11] Postel, J. - RFC 768 – "User Datagram Protocol", Agosto de 1980.

[12] Rai, Idris A. y Alanyali, Murat - "Uniform Weighted Round Robin Scheduling Algorithms for Input Queued Switches", 2001

[13] Handley, M.RFC 4732 – "Internet Denial-of-Service Considerations", Noviembre de 2006.

[14] United States Computer Emergency Readiness Team – "Security Tip (ST04-015), Understanding Denial-of-Service Attacks**".** Última vez accedido en Abril de 2012 a través de http://www.us-cert.gov/cas/tips/ST04-015.html

[15] "Distributed Denial of Service (DDoS) Attacks/tools" – Marzo de 2012. Última vez accedido en Mayo de 2012 a través de http://staff.washington.edu/dittrich/misc/ddos/

[16] "VMware vSphere Hypervisor", de VMWare. Última vez accedido en Marzo de 2012 a través de http://www.vmware.com/products/vsphere-hypervisor/overview.html

[17] Haskin, D. y Allen, E. - RFC 2474 – "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", Diciembre de 1998

[18]American National Standard Institute - IEEE 802.1D – "Standard for Local and Metropolitan Area Networks:Media Access Control (MAC) Bridges", Junio de 2004

[19] Rosen, E. - RFC 2547 - "BGP/MPLS VPNs", Marzo de 1999

[20] Stiliadis, D. y Varma, A. - "Latency-rate servers: a general model for analysis of traffic scheduling algorithms", 1998.

[21] Malkin, G. - RFC 1723 – "Carrying Additional Information", Noviembre de 1994

[22] Meyer, D. y Patel, K. - RFC 4274 – "BGP-4 Protocol Analysis", Enero de 2006.

[23] Moy, J. - RFC 2328 – "OSPF Versión 2", Abril de 1998

[24] Egevang, K. - RFC 1631 – "The IP Network Address Translator (NAT)", Mayo de 1994

[25] Ocón Carreras, A. – "Tutorial y descripción técnica de TCP/IP". Capítulo 6.2 "La tecnología NAT", Enero de 2011.

[26] National Institute of Standards and Technology – "National Vulnerability database". Última vez accedido en Mayo de 2012, a través de http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0806

[27] "Use a Web Proxy for Cross-Domain" – Yahoo Developer Network. Última vez accedido en Mayo de 2012 a través de http://developer.yahoo.com/javascript/howto-proxy.html

[28] Alegsa – "Diccionario de Informática. Definición de Caché Web". Última vez accedido en Junio de 2012 a través de http://www.alegsa.com.ar/Dic/cache%20web.php

[29] “Multi-Domain Security Management” de CheckPoint. Última vez accedido en abril de 2012, a través de: http://www.checkpoint.com/products/multi-domain-security-management/

[30] International Organization for Standardization - ISO/IEC 27001:2005 (formerly BS 7799-2:2002) - “Information Security Management System”, Octubre de 2005

[31] “EMC NETWORKER Y LA DEDUPLICACIÓN”, de EMC. Última vez accedido en Marzo de 2012, a través de http://mexico.emc.com/collateral/software/data-sheet/h3979-nw-dedup-ds.pdf

[32] “AVAMAR, SISTEMA Y SOFTWARE DE RESPALDO CON DEDUPLICACIÓN”. Última vez accedido en Marzo de 2012, a través de http://spain.emc.com/backup-and-recovery/avamar/avamar.htm

[33] Telefónica Soluciones - “Proyecto Técnico Infraestructura Backup Remoto de la Información v1.0”, Octubre de 2011

[34] “Red Hat Enterprise” de RedHat. http://www.redhat.com/products/enterprise-linux/

[35]“EMC PowerLink Portal”, de EMC. Última vez accedido en Marzo de 2012, a través de http://powerlink.emc.com/km/live1/en_US/Offering_Technical/Interoperability_Matrix/300-008-867.pdf

[36] Boletin Oficial del Estado - “REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL”, 1999. Última vez accedido en Abril de 2012. A través de: https://boe.gob.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf

[37] Telefónica de España – “Manual Técnico de MacroLAN”, Enero de 2012

[38] International Organization for Standardization - ISO/IEC 20000-1 – “Information technology - Service management - Part 1: Specification.”, Diciembre de 2005

[39] ITIL Official Website. Última vez accedido en Mayo de 2012, a través de http://www.itil-officialsite.com/

[40] Green IT, sustainable Information Technology. Última vez accedido en Mayo de 2012, a través de http://www.greenit.net/

[41] EmergeMAP - “El fuego y los medios de protección contra incendios. Las medidas pasivas”. Última vez accedido en Mayo de 2012, a través de http://www.conectapyme.com/gabinete/emergemap/guia/nivel2apartado3.html

[42] DuPONT – “Freon 23, Material Data Sheet”, Noviembre de 2002. Última vez accedido en Mayo de 2012, a través de http://msds.dupont.com/msds/pdfs/EN/PEN_09004a2f8000630b.pdf

[43] International Organization for Standardization – “ISO 14000 essentials”, 1996. Última vez accedido en Marzo de 2012, a través de http://www.iso.org/iso/iso_14000_essentials

[44] Information Sciences Institute, University of Southern California - RFC 791 – “Internet Protocol”, Septiembre de 1981

[45] Lores Jacinto, J. - “Configuración y pruebas de funcionamiento de la interconexión de redes heterogéneas con troncal MPLS”. Capítulo “1.1.1 – Modelo OSI”. Junio de 2011.

[46] TelecomSpace – “Asynchronous Transfer Mode”, diciembre de 2012. Última vez accedido en Marzo de 2012, a través de http://www.telecomspace.com/vop-atm.html

[47] International Telecommunication Union - ITUG.803 – “Architecture of transport networks based on the synchronous digital hierarchy (SDH)”, Marzo del 2000.

[48] International Telecommunication Union - ITUG.694.2 - “WDM applications: CWDM wavelength grid“, Diciembre de 2003

[49] Rosen, E. y Viswanathan, A. - RFC 3031 – “Multiprotocol Label Switching Architecture”, Enero de 2001

[50] International Telecommunication Union -T I.122. – “Multipoint communication service - Service definition “, Febrero de 1998

[51] Hypertext PreProcessor. Última vez accedido en Febrero de 2012, a través de http://www.php.net/

[52] Mannie, E. - RFC 3945 – “Generalized Multi-Protocol Label Switching (GMPLS) Architecture”, Octubre de 2004

[53] Deering, S. y Hinden, R. - RFC 1883 – “Internet Protocol Version 6”, Diciembre de 1995.

[54] Conta, A. y v Doolan P. - RFC 3034 – “Use of Label Switching on Frame Relay Networks”, Enero de 2001

[55] Awduche, D., Malcolm, J., Agogbua, J. y McManus, J. - RFC 2702 – “Requirements for Traffic Engineering Over MPLS”, Septiembre de 1999.

[56] Le Faucher, F., Wu, L. y Davie, B. - RFC 3270 – “Multi-Protocol Label Switching (MPLS). Support of Differentiated Services.” Mayo de 2002

[57] International Telecommunication Union –X.25 – “Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit “, Octubre de 1996

[58] Rescorla, E. - RFC 5746 - “Transport Layer Security (TLS) Renegotiation Indication Extension”.

[59] Lehtinen, S. - RFC 4250 – “The Secure Shell (SSH) Protocol Assigned Numbers”, Enero de 2006

[60] Postel, J. - RFC 792 – “INTERNET CONTROL MESSAGE PROTOCOL. DARPA INTERNET PROGRAM. PROTOCOL SPECIFICATION”, Septiembre 1981.

[61] Cain, B. y Deering, S. - RFC 3376 – “Internet Group Management Protocol, Version 3”, Octubre de 2002.

[62] Hanks, S. y Li, T. - RFC 1701 – “Generic Routing Encapsulation”, Octubre de 2004

[63] Touch, J. - RFC 2104 – “HMAC: Keyed-Hashing for Message Authentication”, Febrero de 1994.

[64] National Institute of Standards and Technology - FIPS PUB 46-3- “Data Encryption Standard”, Octubre de 1999

[65] National Institute of Standards and Technology - FIPS PUB 197 – “Advanced Encryption Standard”, Noviembre de 2001,

Bibliografía

Libros

- "Hosting Virtual, Manual de marketing" – Telefónica Soluciones, Febrero de 2011
- "Hosting Virtual, Manual Comercial" – Telefónica Soluciones, Febrero de 2011
- "Tráfico Limpio, Manual de marketing" – Telefónica Soluciones, Septiembre de 2010
- "Tráfico Limpio, Manual Comercial" – Telefónica Soluciones, Septiembre de 2010
- "Backup remoto, Manual de marketing" – Telefónica Soluciones, Octubre de 2011
- "Backup remoto, Manual Comercial" – Telefónica Soluciones, Octubre de 2011
- "Manual Técnico Servicio Macrolan" – Telefónica de España, Junio de 2011
- "Servicio Macrolan. Manual Comercial" – Telefónica de España, Junio de 2011
- "Definición y Gestión del ANS" - Telefónica Soluciones, Marzo de 2010
- "Libro Blanco" - VMware, Junio 2010.
- Guasch Murillo, D. - "Diseño de una infraestructura de telecomunicaciones municipal". Proyecto Fin de Carrera. Junio de 2009
- Lores Jacinto, J. - "Configuración y pruebas de funcionamiento de la interconexión de redes heterogéneas con troncal MPLS".
  Proyecto Fin de Carrera. Junio de 2011.

Medios Electrónicos:

- Wikipedia. En concreto los artículos:
  - Red MPLS
  - IPSec

http:// es.wikipedia.org

- Página web Ramón Millán, apartado Tutoriales:
  http://www.ramonmillan.com/tutoriales/

- Proyecto TelDatsi, de la Universidad Politécnica de Madrid:
  http://laurel.datsi.fi.upm.es/proyectos/teldatsi/

- Página Web IETF Tools
  http://tools.ietf.org/

- Ocón Carreras, A. – "Tutorial y descripción técnica de TCP/IP". Enero de 2011.
  http://www.cicei.com/ocon/gsi/tut_tcpip/