ANEJO Nº 6. TELECOMUNICACIONES FIJAS.

Título del documento			
DOCUMENTO Nº 1. MEMORIA Y ANEJOS. ANEJO Nº 6. TELECOMUNICACIONES FIJAS.			
Código	Fecha	Clasificación	
	Diciembre 2014	Restringido cliente	
Edición	Realizado por	Firma	Fecha
	Marcos A. Aparisi Arenzana Cristina Concejal Heras Carlos Díez		14-12-2014
Tipo de documento	Revisado por	Firma	Fecha
ANEJO.	Javier Gutiérrez		15-12-2014
	Aprobado por	Firma	Fecha
	Rafael Gutiérrez Cantarero		16-12-2014
Nombre del fichero			
Ruta en archivo			
Estado	Borrador / documento final		

ÍNDICE

1. INTRODUCCIÓN

El presente anejo, describirá las diferentes redes y sistemas de Telecomunicación necesarios para dar soporte a todos los servicios del tramo objeto del proyecto de línea ferroviaria entre Las Palmas de Gran Canaria y Maspalomas. Se entiende por sistema al conjunto de equipamiento tanto hardware como software, con funciones específicas definidas y que sirve de soporte para uno o varios servicios y Subsistemas (Comunicaciones de voz, Señalización, Datos, Energía, etc.), siendo el medio por el cual o a través del cual se tienen que proporcionar los servicios mencionados.

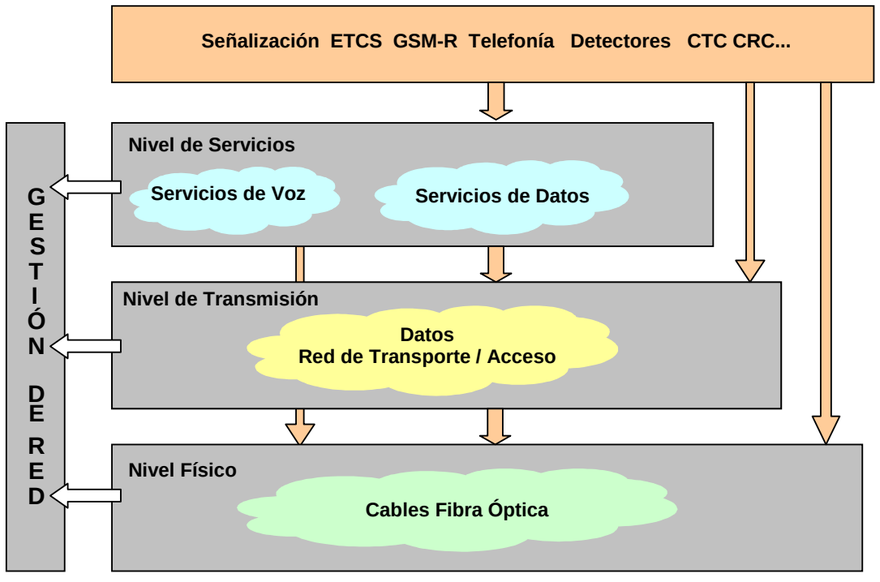
Los Sistemas de Telecomunicaciones Fijas prestarán soporte y servicios de comunicaciones a la operación, gestión, mantenimiento y administración de la línea. Darán soporte a los servicios de comunicaciones demandados por diversos usuarios externos al sistema (señalización, GSM-R, detectores, energía, etc.), por ello se instalarán equipos de comunicaciones y/o se configurarán enlaces sobre equipos existentes en todos los emplazamientos donde debe proveerse algún servicio. De forma general estos emplazamientos son los siguientes:

- Salas de Enclavamiento en estaciones.
- Salas de Telecomunicaciones ferroviarias en estaciones.
- Centro de Regulación y Control (CRC). Se ha proyectado su ubicación en el Edificio de Gerencia, uno de los edificios a construir en el complejo de Talleres, Cocheras y Área de Mantenimiento, en el término municipal de Santa Lucia de Tirajana.
- Casetas GSM-R.
- Subestaciones Eléctricas.
- Estaciones de viajeros.
- Casetas de Operadores Públicos (si procede).
- Casetas técnicas.

El diseño de la red de Telecomunicaciones planteada deberá cumplir, al menos, los siguientes aspectos:

- Tecnología: Elección de tecnologías punteras (IP/MPLS, IP, VoIP, GbE, Eth, etc.) pero a la vez totalmente probadas y, por ende, seguras y con elevadas características de gestión.
- Arquitectura: la solución debe ser multiservicio (voz, datos, etc.) y “abierta” (es decir, no propietaria), haciendo uso en la medida de lo posible de estándares.
- Topología: Diseño para dar Garantía de Seguridad (Redundantes).
- Gestión: Integrada y jerárquica (red y servicio).
- Evolución: Continuidad con las líneas existentes y extensión a futura. De tal forma que las posibles evoluciones y ampliaciones sean mínimas en la parte Hardware y se limiten en la medida de lo posible a ampliaciones de software o de configuración de los equipos.
- Interoperabilidad: Integración entre líneas, servicios y gestión. Es fundamental que las nuevas redes sean interoperables, tanto a nivel de operación como de gestión.

La infraestructura de telecomunicaciones proporcionará, en todas sus capas funcionales, caminos de transmisión extremo a extremo que garanticen el transporte de toda la información demandada por los servicios a los que prestará soporte.



Nivel Físico

Estará basado en su mayor parte en los cables de fibra óptica que transportarán la información necesaria para los niveles superiores, proporcionando conectividad extremo a extremo entre las diferentes localizaciones donde sea necesario.

Nivel de Transmisión

El Nivel de Transmisión estará integrado por las redes que soportarán las comunicaciones de interconexión entre los distintos centros de la línea y dará el soporte de transmisión para redes de conmutación de circuitos o de paquetes, tanto internas como externas a telecomunicaciones fijas con las que se interconecta.

La fiabilidad de estas redes es fundamental ya que es la espina dorsal de las comunicaciones del trayecto. Por tanto se les dotará de una arquitectura de red robusta incluyendo caminos físicos de conexión redundantes (topologías en anillo utilizando rutas de fibra no coincidentes, etc.), que permitan utilizar esquemas de protección del tráfico que cursan. Las redes que componen el nivel de transmisión son las siguientes:

- Red de Datos de Explotación (RDE): compuesta por anillos de routers IP/MPLS 1 GbE (ampliable a 10GbE) comunicados con fibra óptica, y situados en los emplazamientos oportunos para el correcto diseño de la red. Estas redes se apoyarán en la red de cables de fibra óptica para comunicar sus equipos. En la RDE se implementarán VPN N3 sobre MPLS para cada uno de los servicios de telecomunicaciones a proporcionar. La RDE se configurará para permitir obtener tiempos de restablecimiento ante fallos inferiores a 50 ms extremo a extremo para todos los servicios que lo demanden.

- Red de Acceso Datos (RAD): Representa el punto de recogida del tráfico Ethernet en los diferentes emplazamientos de la línea para transmitirlo hasta los nodos de la RDE, garantizando las comunicaciones entre todos los emplazamientos. Esta RAD será también IP/MPLS y sobre ella se implementarán VPN N3 o VPLS según conveniencia del servicio a proporcionar. La RAD se conformará en base a anillos de acceso entre nodos de la RDE en la que se implementará IP/MPLS permitiendo obtener tiempos de restablecimiento ante fallos inferiores a 50 ms extremo a extremo para todos los servicios que lo demanden. Hay que considerar que, para el servicio de CCTV, deberá soportar multicast.

Nivel de Servicios

Este nivel consumirá recursos del nivel de transmisión (GbE) o directamente del nivel físico mediante fibras dedicadas. Dentro de este nivel se distinguen fundamentalmente:

- Red de Voz: Dará servicio de Telefonía Fija (Operacional e Interfonía, Administrativa y de Gestión; de Mantenimiento y de Vigilancia) a todas las instalaciones del tramo y en los diferentes centros de control del mismo. Estará basada en VoIP.

- Servicios de Datos: Serán las diferentes redes de datos que darán conectividad IP a los diferentes servicios que lo requieran, cada una de ellas con el adecuado nivel de redundancias y protecciones, haciendo uso de la Red de Acceso Datos. Las necesidades de cada una de estas redes de datos se detallan con más profundidad (tanto en localizaciones como en requisitos de disponibilidad y redundancia) en el capítulo dedicado a ellas en este documento.

Nivel de Gestión de Red

El nivel de Gestión de Red incluye los diferentes gestores de cada una de las redes, tanto de transmisión como de datos, así como el sistema de Supervisión de Fibra Óptica, de la red de voz y del sistema de energía para los equipos de telecomunicaciones. Se deberá considerar además un Sistema de Gestión Integrada que proporcionará una plataforma de gestión global de los sistemas de Telecomunicaciones de la línea, o su integración en el actualmente en servicio.

2. RELACIÓN DE LAS OBRAS E INSTALACIONES A REALIZAR

A continuación se enumeran las actuaciones a realizar para el despliegue de la red de telecomunicaciones fijas en el tramo Las Palmas de Gran Canaria - Maspalomas. En este documento se describen de forma general las actuaciones a realizar:

- Suministro, tendido, empalme y pruebas ópticas de cables troncales de fibra óptica (96 FO).
- Suministro, tendido, empalme y pruebas ópticas de cables de 16 f.o. para repetidores del sistema GSM-R.
- Suministro, instalación, tendido, ejecución de empalmes y pruebas ópticas de cajas de empalme, cables de segregación y repartidores ópticos.
- Suministro, instalación, configuración, pruebas y puesta en servicio de nodos de la Red de Datos de Explotación IP/MPLS en el ámbito de la línea ferroviaria entre Las Palmas de Gran Canaria y Maspalomas en configuración en anillo.
- Suministro, instalación, configuración, pruebas y puesta en servicio de la Red de Acceso de Datos IP/MPLS y otras redes privadas IP que darán servicio a:
  - Servicios de Propósito General
  - Servicios de Alta Disponibilidad
  - Servicios Privados de Señalización y Detectores.
  - Servicios de Voz
  - Servicios de Protección y Seguridad Corporativa.
  - Servicios corporativos (informática, telemedida fiscal, calidad de la energía, etc.).
  - Otros
- Suministro, instalación, configuración, pruebas y puesta en servicio de nodos de la Red Unificada de Señalización y Detectores (RUSD) para los servicios privados de señalización y de detectores.
- Suministro, instalación, configuración, pruebas y puesta en servicio de nodos de la Red de acceso de los sistemas de VCA.
- Suministro, instalación, configuración, pruebas y puesta en servicio de centrales de la Red de Voz.
- Suministro, instalación, configuración, pruebas y puesta en servicio de terminales de telefonía (interfonos, terminales analógicos, digitales y VoIP).
- Suministro e instalación, configuración, pruebas y puesta en servicio de las grabadoras de voz necesarias en el CRC y en los edificios con PLO.
- Suministro, instalación, configuración, pruebas y puesta en servicio de un sistema de Supervisión de Fibra Óptica que realice pruebas de potencia y reflectometría de las fibras oscuras del cable de 96 f.o. de cada lado de vía (reflectometría y potencia).
- Suministro, instalación, configuración, pruebas y puesta en servicio del sistema de energía para alimentar a los equipos de Telecomunicaciones (rectificadores, baterías, sistema de onduladores, etc.).
- Suministro, instalación, configuración, pruebas y puesta en servicio de Firewalls redundantes en los interfaces de las redes de explotación con las redes del CRC.
- Instalación, configuración, pruebas y puesta en servicio de un sistema de control de acceso - NAC- a las redes de datos del tramo en cuestión (incluidos todos los trabajos necesarios tanto sobre el propio sistema de control de acceso a la red como sobre los dispositivos de red y finales)
- Suministro, instalación, configuración, integración de los equipos, pruebas y puesta en servicio de los gestores de los siguientes sistemas:
  - IP/MPLS – IP
  - Voz
  - Sistema de gestión integrada
  - Sistema de supervisión de fibra óptica
  - Sistema de energía para telecomunicaciones
  - Firewalls
  - Sistema de control de acceso a la red de datos (NAC)
- Ejecución de la obra civil auxiliar necesaria para la implantación de la red de fibra óptica que dará soporte a todos los equipos de comunicaciones (apertura y tapado de canaleta, arquetas, canalizaciones, canaletas, cruces de vía, perchado, etc.).
- Todos los trabajos de ingeniería, maqueta, integración, pruebas y puesta en servicio necesarios para la correcta ejecución de los trabajos definidos en este apartado, aportando todos los medios materiales y humanos necesarios.

- Será necesario establecer una maqueta preparada para esta técnica a escala 1:1, o a criterio del Director de Obra, para poder probar previo al despliegue en campo tanto los equipos de las nuevas instalaciones como las interconexiones con las redes existentes, así como las pruebas globales del sistema y sus interfaces con otras técnicas a las que da servicio.

3. NIVEL FÍSICO. REDES DE CABLES.

3.1. CABLES DE FIBRA ÓPTICA

3.1.1. Introducción

En esta sección se describen todos los aspectos relacionados con la red de cables de fibras ópticas necesaria para soportar las comunicaciones. Estos aspectos incluyen el tendido, empalme, segregación, terminación y medidas de acuerdo a normativa Adif de los diferentes cables de fibra óptica a lo largo de todo el tramo.

Todos los cables de fibra óptica a instalar cumplirán con la versión vigente de la E.T. de Adif 03.366.780.9.

3.1.2. Tendido del cable

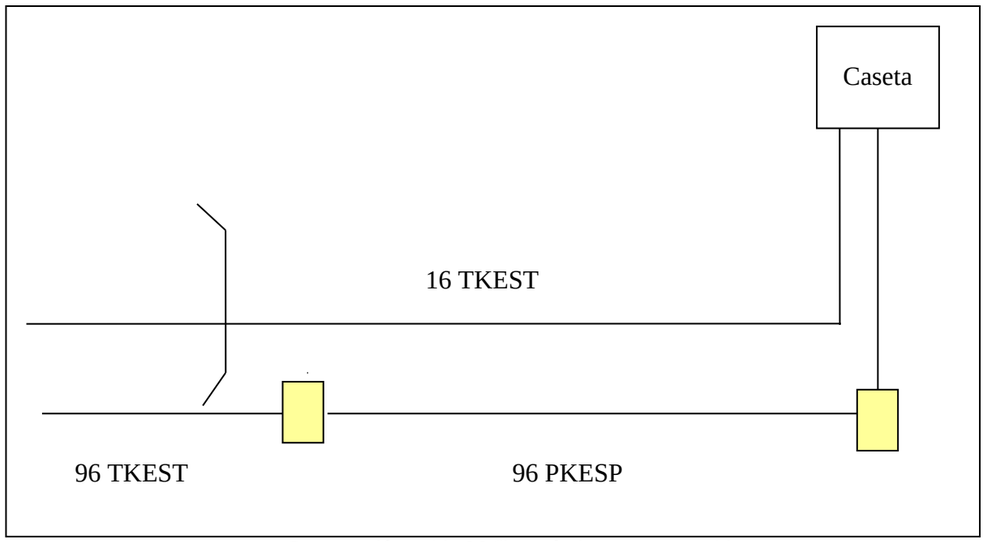
A lo largo de la línea se tenderán dos cables diferentes, distribuidos de la siguiente forma:

- Vía impar:
  - 1 cable de 96 fibras ópticas.
- Vía par:
  - 1 cable de 96 fibras ópticas

Es imprescindible garantizar caminos físicos independientes para los cables troncales de vía par e impar.

Los cables se dedicarán fundamentalmente a la interconexión de los equipos de la Red de Datos de Explotación (RDE), Red de Acceso de Datos (RAD), y como cables de servicio para otras técnicas (señalización, electrificación, telemando, detectores, sistemas de protección y seguridad, etc.). También se utilizarán para los operadores de telefonía móvil, dejando las demás fibras libres para poder ser utilizadas en el futuro. Los repartidores para estos cables estarán situados en las salas de telecomunicaciones ferroviarias de las estaciones, casetas técnicas, otros puntos singulares con necesidades de fibra óptica (viaductos, túneles, pasos superiores…) y cualquier emplazamiento con necesidades de fibra óptica.

Además se tenderá un cable adicional de 16 fibras ópticas para unir las BTS que tengan repetidores dependientes de ella. Este cable extra se utilizará únicamente para estas comunicaciones y no llevará más servicios ni se tenderá a lo largo de toda la vía. El esquema de tendido de dicho cable se presenta a continuación; una solución que aunque implica un tendido ligeramente superior de cable de 16 fibras ópticas, no necesita saber de antemano el número de fibras que se va a necesitar para dar comunicación a los repetidores.



Segregación cable 96 fibras ópticas para repetidores

Para la integración de los Detectores de Caída de Objetos (DCO) en la red de Telecomunicaciones Fijas se seguirá la instrucción de ADIF, “REQUISITOS DE INTEGRACIÓN DE LOS DETECTORES DE CAÍDA DE OBJETOS EN LA RED DE COMUNICACIONES “, que no solo se limita a la reserva de fibra necesaria, sino también a repartidores, pigtails, etc., debiendo realizar las medidas ópticas de verificación adicionales que requiere este sistema.

Todos los cables se instalarán por las perchas, canaletas de hormigón, canaletas de plástico, canalizaciones u obra civil auxiliar existente a ambos lados de la vía. El tendido de cables de segregación, desde la plataforma hasta los diferentes emplazamientos, normalmente se realizará mediante canalizaciones.

3.1.3. Asignación de servicios

Se propone a continuación una asignación provisional de fibras a los diferentes servicios, siendo idéntica para ambos lados de vía (el adjudicatario será el responsable de proponer a Ferrocarriles de Gran Canaria, para su aprobación, la asignación de fibras resultante de todos los servicios a implementar):

- Cuatro fibras (4) como medio de transmisión de los enlaces de la Red de Acceso Datos (RAD). Dos fibras estarán en uso y las otras dos en reserva.
- Cuatro fibras (4) para la supervisión del propio cable por medio del sistema de supervisión de fibra óptica. Dos fibras estarán en uso y las otras dos en reserva.
- Cuatro fibras (4) para los enlaces 1GbE de la Red de Datos de Explotación (RDE). Dos fibras estarán en uso y las otras dos en reserva.
- Ocho fibras (8) para la conexión de los equipos en caseta de los Detectores de Caída de Objetos (DCO) con las mallas situadas en los pasos superiores o bocas de túnel.
- Ocho fibras (8) para la reserva de las mallas de DCO.
- Ocho fibras (8) para los operadores públicos de Telecomunicación.
- Cuatro fibras (4) para la Red Unificada de Señalización y Detectores. Dos fibras estarán en uso y las otras dos en reserva.
- Cuatro fibras (4) como medio de transmisión para la red de switches de VCA. Dos fibras estarán en uso y las otras dos en reserva.
- Cincuenta y dos fibras (52) para enlaces de larga distancia, interconexiones con otras redes y otros servicios.

Cable 96								
Servicio	nº fibras	Tubo	Servicio	nº fibras	Tubo	Servicio	nº fibras	Tubo
Libre	4	1	Operadores	8	5	Libre	16	9
RAD	2 activas + 2 reserva							
Supervision FO	2 activas + 2 reserva	2	RUSD	2 activas + 2 reserva	6			10
RED	2 activas + 2 reserva		Libre	4				
1ª Malla DCO	8	3	VCA	2 activas + 2 reserva	7			11
			Libre	4		Libre	16	
Reserva 2ª Malla DCO	8	4	Libre	8	8			12

3.1.4. Empalmes y segregaciones

A lo largo del trayecto se realizarán dos tipos de empalmes:

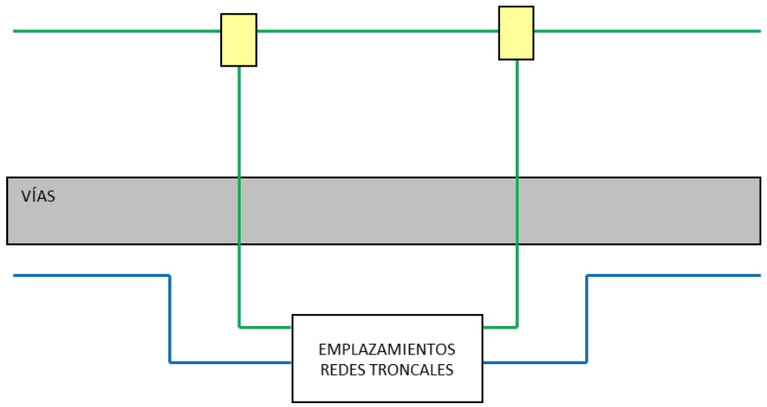
- Empalmes en recto.
- Empalmes de segregación.

Tanto los empalmes en recto como los empalmes de segregación se realizarán en bandejas de circuito individual.

Los empalmes en recto se realizarán de acuerdo a la longitud de tendido de las bobinas de fibra óptica, que en el caso de este proyecto son de 4.000 metros nominales. Las distancias de los empalmes en recto podrán reducirse o incrementarse con respecto a los 4.000 metros nominales, con el fin de hacer coincidir un empalme en recto con un empalme de segregación reduciendo el número de empalmes totales. Deberá considerarse un coca intermedia de 50 m entre dos empalmes en recto (se aprovechará la arqueta más próxima para su ubicación).

Como norma general de diseño se establece que a cada emplazamiento de la traza que tenga necesidades de fibra óptica para comunicación (subestaciones eléctricas, casetas de vía, etc.) entrarán únicamente las fibras necesarias, quedando las demás en paso en su correspondiente caja de empalme. Estos empalmes de segregación se efectuarán en arquetas situadas junto a la canaleta. En ellas entrarán los cables principales y saldrán los cables de segregación.

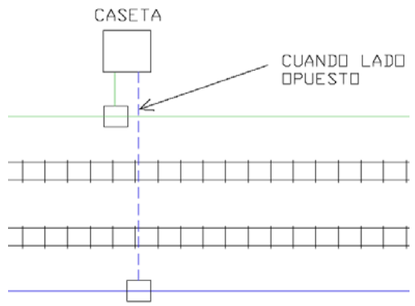
No obstante, en los emplazamientos donde existan equipos de las redes troncales entrará en punta el cable de 96 f.o. del lado de vía que corresponda según la topología de estas redes, asegurándose en todo momento que vayan por caminos separados hasta las arquetas existentes en el interior de la sala de comunicaciones (al menos 2), realizándose en el armario repartidor los empalmes necesarios para la continuidad de las fibras. Para las fibras del lado contrario, se segregarán únicamente las fibras necesarias con doble canalización independiente del cable de 96 f.o. del otro lado de vía, y se conectarán a otro repartidor de fibra óptica con el fin de independizar los lados de vía. Deberá asegurarse que los caminos de las fibras de ambos lados de vía no coincidan en ningún punto.



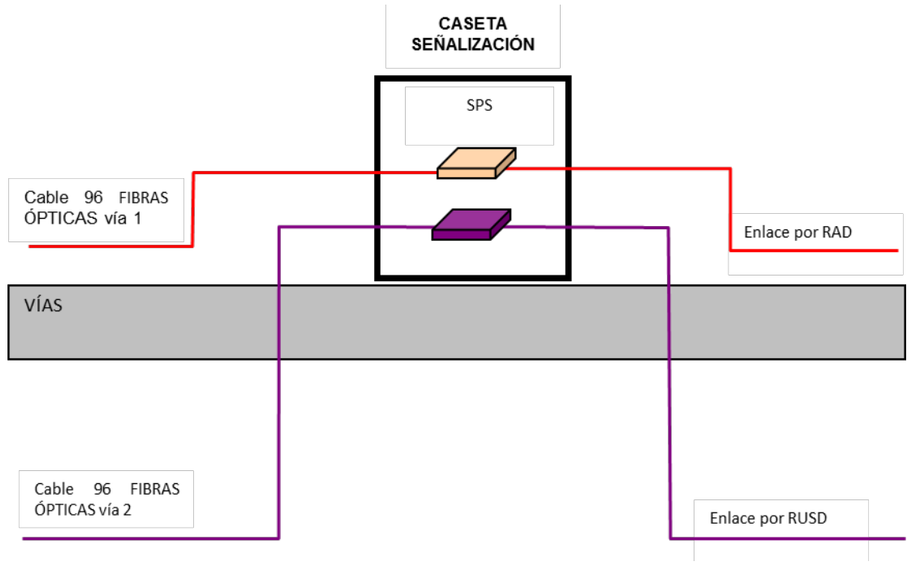
El objetivo es evitar que los cables de ambos lados de la vía, que conforman un anillo entre dos estaciones, compartan la misma canalización de acceso al edificio, y un incidente sobre dicha canalización invalide por completo la protección en anillo.

Para las casetas de GSM-R y Operadores, y otras casetas, se segregará del cable de 96 fibras el número de fibras necesarias en cada caso.

En aquellos emplazamientos que por motivo de inexistencia de espacio/camino de acceso en su lado de vía, se hayan colocado en el lado opuesto, se efectuará la segregación desde el lado contrario a dónde se ha colocado finalmente, para “virtualmente” mantenerla en el anillo en su lado de vía original. Esto sucede generalmente en BTS de una determinada capa, que han sido ubicadas en el lado opuesto, aunque es aplicable a cualquier emplazamiento que tenga esta necesidad.



En las casetas o emplazamientos de señalización se ofrecerán dos caminos de cables independientes de acceso a la sala de Telecomunicaciones, debiendo ésta disponer de dos arquetas de entrada de cables en su interior, con las correspondientes segregaciones desde ambos lados de vía del cable de 96 fibras ópticas. Con ello se consigue que la conexión del equipamiento de señalización disponga de dos accesos independientes a través de la Red de Acceso de Datos (RAD) y la Red Unificada de Señalización y Detectores (RUSD), la cual se segrega del otro lado de vía.



En cada posición de empalme se dejará una coca de cable de longitud suficiente (unos 30 metros) en cada una de los extremos de las bobinas a empalmar, así como de los cables de acometida a los diferentes emplazamientos donde se segregue (estaciones, subestaciones eléctricas, casetas técnicas, etc.) Este remanente de cable servirá para los posibles futuros trabajos que hubiera que realizar como consecuencia de una rotura del cable, degradación de los empalmes, etc.

Como norma general se tenderá cable con cubierta PKESP excepto en los túneles y las entradas a los edificios de las estaciones en los que se utilizará cable con cubierta TKEST.

3.1.4.1. Cajas de empalme y segregación

El procedimiento de realización de estos empalmes será por fusión y quedarán debidamente protegidos en cajas de empalme y segregación. Estas cajas tendrán diferentes configuraciones según el tipo de empalme o segregación que se deba realizar en ellas.

Téngase en cuenta que, en los emplazamientos con nodos de las redes troncales (IP/MPLS), el cable de 96 fibras ópticas del lado de vía que corresponda según topología de las redes, no se segregan, sino que entra en punta todo el cable directamente, por lo que no es necesario ningún tipo de caja de segregación.

El número de cables y fibras de los mismos de cada segregación será la necesaria dependiendo de las necesidades de fibra que existan en el emplazamiento, aunque siempre se utilizarán los cables definidos en este documento para ello (16 o 96 f.o.).

Las cajas de empalme serán todas del mismo tipo, si bien estarán equipadas de distinta forma según el tipo de empalmes o segregaciones que se vayan a realizar en ellas. Las cajas de empalme cumplirán con la versión vigente de la E.T. de Adif 03.366.756.9.

Las cajas estarán dotadas de elementos que aseguren la estanqueidad necesaria, de forma que el polvo y la humedad no afecten en modo alguno a los empalmes de las fibras. Estas cajas de empalme quedarán fijadas a las paredes laterales de las arquetas una vez realizados los empalmes correspondientes.

Todas las cajas estarán equipadas con las bandejas de empalme necesarias. Las fibras de cada servicio que se vayan a segregar tendrán su propia bandeja, de forma que no coincidan segregaciones de diferentes servicios en la misma bandeja. Igualmente se protegerán las fibras en paso, colocándolas en una bandeja si es necesario (fibras pertenecientes a un tubo del que se segreguen otras fibras).

Vendrán equipadas al menos con un 20% de bandejas adicionales para futuras ampliaciones.

Podrá suceder que coincidan en un mismo punto un empalme en recto con una segregación, realizándose en este caso todos los empalmes en la misma caja con objeto de facilitar las tareas de instalación así como de posteriores labores de mantenimiento.

3.1.4.2. Arquetas para empalmes

Cada caja de empalme se colocará en una arqueta independiente, siendo en este caso iguales todas las arquetas independientemente del tipo de empalme o segregación que se realice en ella.

Las arquetas que se instalarán serán las homologadas por el ADIF para la red de fibra óptica

Las arquetas serán de hormigón, con tapa también de hormigón y marco metálico y de dimensiones 1200x600x900. Estas arquetas se instalarán adosadas a la canaleta de hormigón existente de forma que los cables puedan pasar a la arqueta directamente desde la canaleta sin necesidad de ninguna protección ni canalización adicional.

En los tramos donde no sea viable la instalación de las arquetas anteriormente definidas será necesario el uso de otro tipo de arquetas adaptadas a estas circunstancias.

3.1.5. Repartidores ópticos

La terminación de los cables de fibra óptica se realizará en repartidores ópticos en todas aquellas instalaciones operativas donde deben terminar estos cables.

Se utilizarán repartidores de diferentes tipos y dimensiones, según la dependencia que se trate y el número de fibras que sean necesarias:

- Paneles de 1U para 12 fibras para instalar en armarios, ya sean de interior ya sean de intemperie (DCO).
- Paneles de 1U para 24 fibras para instalar en armarios.
- Repartidor mural 12 fibras.
- Repartidor mural 24 fibras.
- Repartidor mural 36 fibras.
- Repartidor mural 48 fibras.
- Armarios Repartidores.

Se instalarán armarios repartidores con equipamiento modular en emplazamientos donde exista una alta necesidad de fibras, típicamente salas de Telecomunicaciones en estaciones, pero no estará limitado a este tipo de emplazamientos. Estos armarios se equiparán de diferente manera según los cables que lleguen al armario. Donde sea necesario por separación de caminos habrá un armario por cada lado de vía.

Los conectores en los repartidores serán tipo SC/APC salvo en el caso de las bandejas para armarios DCO en el que los conectores serán tipo FC/PC.

3.1.6. Pruebas y documentación

Una vez finalizados todos los empalmes y con la fibra ya disponible hasta los repartidores se realizarán pruebas de reflectometría en 2ª y 3ª ventana así como medidas de potencia en los vanos entre cada dos repartidores en ambos sentidos.

Para la realización, criterios de aceptación y documentación de estas pruebas se seguirá lo definido en la norma NAT 730 de ADIF “Documentación a entregar y medidas a realizar en instalación y actuaciones sobre cables de fibras ópticas” , salvo que Ferrocarriles de Gran Canaria determine otra.

4. RED DE DATOS DE EXPLOTACIÓN

4.1. INTRODUCCIÓN

El objetivo de la Red de Datos de Explotación (RDE) proyectada es servir de red de *backbone* para las redes de datos existentes y los servicios a disponer en la línea (Servicios de Voz, Servicios de Alta Disponibilidad, Servicios de Propósito General, Servicios de Detectores, Protección y Seguridad, Corporativos, etc.).

Mediante la Red de Datos de Explotación se asegurará la conectividad de todos los servicios basados en una solución IP en una sola tecnología homogénea y fiable, que se encontrará securizada para controlar el acceso de usuarios y dispositivos mediante mecanismos de autenticación.

La RDE se estructura en un anillo 1GbE, sobre el que se cerrarán los diferentes anillos de acceso.

Estos anillos de acceso suponen un segundo nivel jerárquico para las redes IP, que se corresponde con la Red de Acceso de Datos (RAD), y que será la encargada de recoger los servicios de naturaleza Ethernet generados a lo largo de la traza en los diferentes emplazamientos. Tanto la Red de Datos de Explotación como la Red de Acceso de Datos serán IP/MPLS para mejorar los tiempos de convergencia, latencias y poder implementar VPN, QoS e Ingeniería de Tráfico.

Las principales ventajas que la RDE ofrece son las siguientes:

- Permite un uso eficiente del ancho de banda y gran granularidad. Permite concentrar el tráfico de los diferentes servicios evitando el problema de reservar ancho de banda inutilizado.
- Presenta mecanismos de Calidad de Servicio (QoS) mediante la asignación de prioridades, lo que permite que los servicios prioritarios no se vean afectados por posibles problemas de congestión.
- Es capaz de encapsular diferentes servicios de datos permitiendo mantener diferentes parámetros para cada una de ellos formando diferentes VLAN.
- Permite una gestión sencilla del ancho de banda mediante las diferentes VLAN y VPN que se configuren, asociando a cada una de ellas diferentes prioridades.

4.2. TECNOLOGÍA A UTILIZAR

La tecnología que se implementará en la RDE estará basada en el estándar IP/MPLS (*Multi-Protocol Label Switching*). MPLS permite crear VPN seguras y fiables, muy simples de gestionar, fáciles de desplegar y permitiendo diferentes Calidades de Servicio (QoS). A continuación se desarrollan las características que la RDE deberá cumplir.

4.2.1. Ingeniería de tráfico

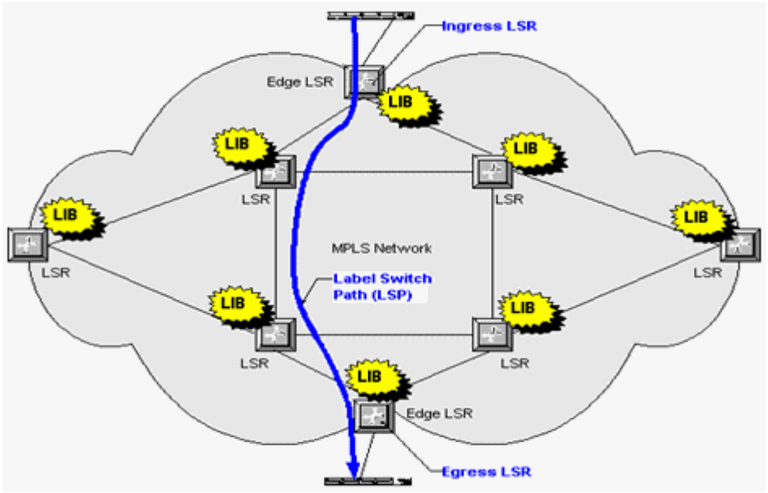
La red permitirá controlar el camino que siguen los paquetes IP y adaptar los flujos de tráfico a los recursos físicos de la red equilibrando de forma óptima los enlaces, es decir, evita que algunos enlaces y equipos de la red se saturen mientras que otros se encuentran infrautilizados, previniendo de esta manera la creación de cuellos de botella y usando de forma eficiente todos los enlaces, balanceando la carga en enlaces paralelos, con máximo rendimiento y mínimos retraso y pérdidas.

La clave de la ingeniería de tráfico en MPLS se basa en establecer LSP (*Label Switched Paths*) entre los diferentes routers, es decir rutas orientadas a conexión. LSP hace referencia por tanto, al nombre genérico de un camino MPLS.

Para conseguir este objetivo la gestión de la red permitirá:

- Que el administrador de red establezca rutas específicas.
- Obtener estadísticas de uso de cada LSP (cuanto tráfico y de qué tipo).
- Hacer encaminamiento restringido, de tal manera que se puedan seleccionar rutas específicas para transportar el tráfico de un tipo en concreto con unos requerimientos específicos. Esta posibilidad está directamente ligada a los Acuerdos de Nivel de Servicio (SLA).

La ventaja de la ingeniería de tráfico MPLS es que se puede aplicar directamente sobre una red IP, independientemente de la infraestructura que le de soporte, con un mayor nivel de detalle y de forma más sencilla y eficiente.



MPLS permitirá recalcular dinámicamente las rutas a seguir por cierto tipo de tráfico en función de parámetros variables como el nivel de utilización de un enlace o la carga de procesamiento de alguno de los nodos. De la misma manera permitirá forzar un tráfico por una ruta determinada reservada para tal efecto.

4.2.2. Calidad de Servicio (QoS)

La Red MPLS estará diseñada para poder cursar servicios diferenciados, integrándose con los modelos *IntServ* y *DiffServ* del IETF permitiendo clasificar distintos tipos de tráfico en un cierto número de clases de servicio con diferentes prioridades. Los paquetes pertenecientes a una misma clase de servicio tienen en común los mismos requerimientos de tratamiento en cuanto a ancho de banda necesario, retardo (*jitter*) y pérdida de paquetes, es decir, de calidad de servicio (QoS).

- IntServ (*Integrated Services*): apoyándose en RSVP se reservan los recursos necesarios asociándose a LSP (*Label Switched Paths*) concretos. MPLS se adapta a este modelo soslayando sus problemas de complejidad en la configuración y clasificación, ya que proporciona los servicios “extremo a extremo”.
- DiffServ (*Differenciated Services*): orientado al tráfico IP, su funcionamiento se basa en la clasificación del tráfico a la entrada de la red y en la asignación de prioridades a estos tipos de tráfico mediante los 6 bits DSCP (*DiffServ Code Point*) y el campo TOS (*Type of Service*). En función de este campo, cada nodo intermedio tratará el paquete de la forma adecuada. MPLS se adapta perfectamente a este modelo, ya que las etiquetas MPLS añaden al campo EXP (CoS) la prioridad de tráfico, de modo que cada LSR (*Label Switching Router*) conocerá las características de cada paquete.

4.2.3. Redes Privadas Virtuales (VPN)

En la RDE se establecerán VPN N3 sobre MPLS para cada uno de los servicios a soportar, siguiendo los criterios definidos en la RFC 4364 “BGP/MPLS IP VPN”. Para la interconexión de redes IP/MPLS se seguirán también los criterios definidos en la citada RFC.

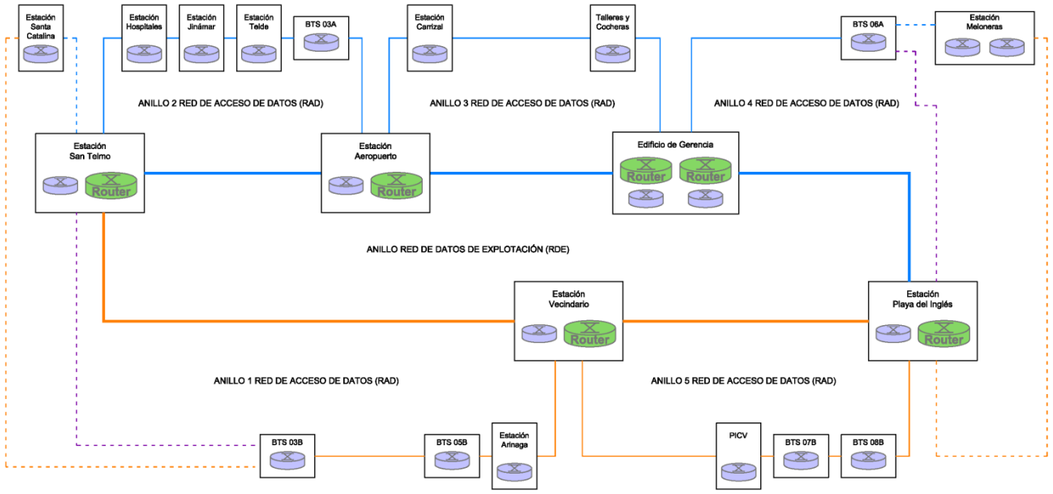
4.3. DESCRIPCIÓN DEL SISTEMA

4.3.1. Arquitectura de red

Para la configuración de los servicios de explotación deberá tenerse en cuenta que se ha proyectado que el Centro de Regulación y Control (CRC) esté ubicado en el Edificio de Gerencia, a confirmar por Ferrocarriles de Gran Canaria. Este puesto de mando controlará la nueva línea férrea a construir entre Las Palmas de Gran Canaria - Maspalomas.

Asimismo, para la comunicación con el Centro de Protección y Seguridad (CPS) deberán realizarse las conexiones y configuraciones necesarias.

Adjunto a este documento se incluye un esquema donde se representa la RDE prevista, así como las interconexiones necesarias con la red IP/MPLS.



A través de cada nodo de la RDE se conectaran las diferentes VPN de nivel 3 definidas para esta línea:

- VPN de Servicios de Propósito General
- VPN de Voz
- VPN de Servicios de Alta Disponibilidad
- VPN de VCA
- VPN para servicios corporativos
- Otras VPN que pudieran ser necesarias

Los interfaces de conexión con cada una de estas redes serán puertos 10/100/1000 Ethernet óptico o eléctrico. De esta forma la RDE se comporta de manera transparente para las diferentes redes IP a las que da soporte.

4.3.2. Descripción de los nodos LSR

Todos los nodos de la RDE serán nodos de alta capacidad con enlaces 1GbE en el lado *Backbone* y enlaces 1GbE en el lado acceso. Para mejorar los tiempos de convergencia, todos los interfaces entre nodos de la RDE, entre nodos de la RDE y de la RAD y entre nodos de la RAD serán ópticos. Solo se admitirán interfaces eléctricos para la conexión de los diferentes usuarios con la RAD. Todos los nodos de la RDE se instalaran en configuración de alta disponibilidad, con todos los elementos vitales, procesadoras, alimentación y tarjetas de línea redundadas.

4.3.3. Características de los LSR

Todos los LSR de la RDE serán GigaRouters de alta capacidad de conmutación para equipos de gran densidad de puertos y altas necesidades de fiabilidad por paquete enrutado.

4.3.3.1. Características generales

- Redundancia multifuncional.
- Enrutamiento IP/MPLS.
- Capacidad de mezclar interfaces de alta densidad, baja/alta velocidad en el mismo chasis.
- Gran escalabilidad con tablas de enrutamiento complejas.
- Fácil integración con tecnologías de otros fabricantes.
- Scripts basados en XML para facilitar la creación de APIs de terceros.
- Mecanismos de reinicio en caso de fallos.
- Reenrutamiento de tráfico en caso de fallos.
- Tecnología *FastReroute* para minimizar el tiempo de convergencia en caso de fallo del enlace.
- Rendimiento predecible para tráfico de latencia sensible (VoIP, Multicast video...).
- Separación de los niveles de control y reenvío evitando que las funciones de enrutamiento y reenvío compitan por los mismos recursos del sistema.
- Estructura modular con intercambio de tarjetas en caliente.

- Permitirá ISSU (*In Service Software Upgrade*)
- Soporte avanzado de características MPLS (VPL´s, VPN nivel 2, VPN nivel 3) y creación de paths RSVP/LDP.
- Estos nodos dispondrán de funcionalidades de emulación de E1 sobre IP (*SatOp* y *CESoPSN*) así como Ethernet Síncrono y sincronismos IEEE 1588v2.

4.3.3.2. Arquitectura de los LSR

La arquitectura hardware y software de los nodos de agregación de la RDE tendrán una separación clara entre las funciones de control (*Routing*) y las de envío (*Forwarding*) de forma que cada una de ellas se implemente y modifique de forma independiente.

- Componente de control.

Utiliza los protocolos de encaminamiento para el intercambio de información con otros routers para la construcción y mantenimiento de las tablas de encaminamiento. Contiene los procesos del software que controlan las interfaces del router, los componentes del chasis, la administración del sistema y los accesos de los usuarios al router.

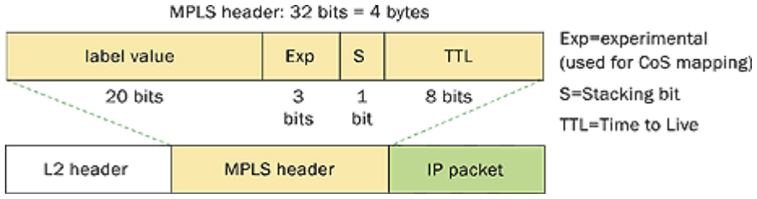
Procesa todas las actualizaciones de protocolos de rutas desde la red, de tal manera que el rendimiento de reenvío no se vea afectado.

Implementará cada protocolo de *routing* con un conjunto completo de características de Internet y proporcionará una gran flexibilidad para anunciar, filtrar y modificar rutas. Las políticas de enrutamiento se establecerán de acuerdo a parámetros de enrutamiento, como prefijos, longitud de los mismos y atributos BGP.

- Componente de envío.

Es la entidad lógica responsable del rendimiento del envío de paquetes. Físicamente está formado por el procesador de control, módulos de interfaces, y tarjetas de línea.

A continuación se presenta la estructura de un paquete MPLS:



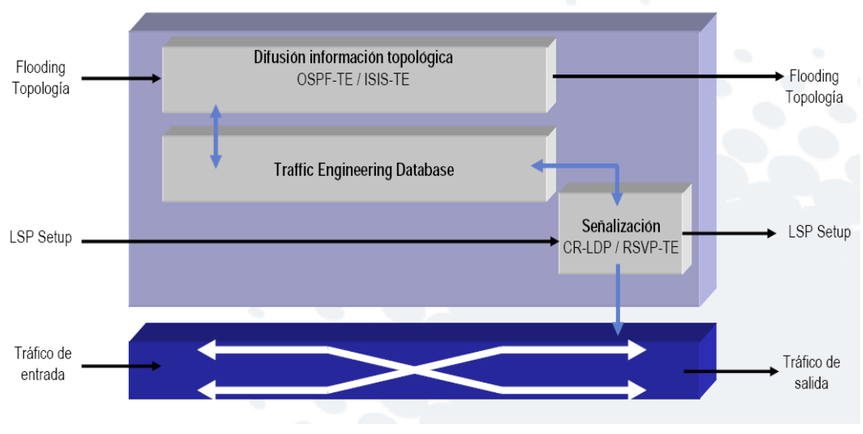
MPLS funciona anexando un encabezado a cada paquete. Dicho encabezado contiene una o más "etiquetas". Cada etiqueta consiste de cuatro campos. Estos paquetes MPLS son enviados después de una búsqueda por etiquetas en vez de una búsqueda dentro de una tabla IP. De esta manera, la búsqueda de etiquetas y el envío por etiquetas es más rápida que una búsqueda RIB (Base de información de Ruteo).

Cada uno de los campos que constituyen la cabecera tiene el siguiente significado:

- Label (20 bits): Es la identificación de la etiqueta.
- Exp (3 bits): Llamado también bits experimentales, afecta al encolado y descarte de paquetes. Prioridad de Calidad de Servicio (QoS) de 3 bits.
- S (1 bit): Stack, sirve para el apilado jerárquico de etiquetas. Cuando S=0 indica que hay más etiquetas añadidas al paquete. Cuando S=1 estamos en el fondo de la jerarquía.
- TTL (8 bits): *Time-to-Live*, con el mismo significado que en la tecnología 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.

El procesador de control realiza funciones de búsqueda de rutas y *switching* al destino, toma decisiones de encaminamiento, distribuye las células de datos a través de la memoria, procesa paquetes de excepción y de control, monitoriza los componentes del sistema y controla los reinicios de tarjetas y módulos. Al llegar los paquetes, la componente de envío busca en la tabla de envío, que mantiene la componente de control, para tomar la decisión de encaminamiento para cada paquete.

En concreto, la componente de envío examina la información de la cabecera del paquete, busca en la tabla de envío la entrada correspondiente y dirige el paquete desde el interfaz de entrada al de salida a través del correspondiente hardware de conmutación.



- Módulo de Interfaces.

  Son los encargados de conectar los interfaces al resto del router. Analizan, priorizan, y encolan los paquetes antes de enviarlos a su interfaz de destino correspondiente. Utilizarán contadores por cola así como un incremento de la memoria para permitir un gran escalado de las redes.

- Tarjetas físicas de interfaz.

  Tarjetas multiservicio que soporta interfaces WAN, LAN y servicios. Además, proporcionarán la velocidad de conexión requerida cumpliendo los estándares IEEE de aplicación, soportarán QoS, distribución de etiquetas/MPLS y velocidad de acceso garantizada (*Committed Access Rate - CAR*).

4.4. CRITERIOS DE PROTECCIÓN Y REDUNDANCIAS

Los criterios de protección se basarán en dos aspectos diferenciados: Protecciones de equipo y protecciones de enlaces. Ambos aspectos se describen a continuación.

4.4.1. Protección en los equipos

Los equipos de la RDE tendrán redundados los componentes vitales, evitando la presencia de un elemento central de fallo. De esta manera estarán duplicados todos los elementos activos que intervienen en el funcionamiento de los nodos:

- Componente de control redundada. (*Routing Engine*)
- Componente de envío redundada. (*Forwarding Engine*)
- Fuentes de alimentación redundada.
- Ventilación redundada.
- Slots de expansión para tarjetas insertables y extraíbles en caliente.
- Los interfaces del anillo estarán en tarjetas diferentes.

4.4.2. Protección en los enlaces

Estas protecciones se basan en duplicar los caminos entre dos puntos:

- Los enlaces del anillo principal (*backbone*) estarán protegidos por la disposición en anillo de la red. De esta forma existen dos caminos entre dos emplazamientos cualesquiera de la red.

4.5. SEGURIDAD DE LA RED

Algunas de las propiedades de los LSR de la RDE relativas a la seguridad de la red son:

- Utilización de filtros de Firewall de entrada y de salida. Posibilitará el filtrado de paquetes basados en contenido y la realización de una acción basada en cualquier combinación de equivalencia entre filtros. Esto permite contener ataques de denegación de servicio.
- Otras funcionalidades de seguridad: *port mirroring*, gestión de sesiones de tráfico encriptadas, funcionalidades de túneles seguros, *logins* remotos seguros, niveles de privilegios configurables etc.
- Filtros SNMP que permiten sondear un contador a través de MIB´s específicas, de manera que no tengan que chequear los routers directamente.
- Sesiones BGP IPsec para encriptar el control del tráfico. Incluirá la posibilidad de configurar manualmente claves para “abrir” la encriptación.
- Creación de logs del sistema que permitan monitorizar un sistema mediante mensajes codificados.

La Red MPLS permitirá la creación de redes VPN sobre una infraestructura compartida con topología no conectiva (nube común privada) en lugar de las conexiones VPN extremo a extremo. Las IP VPN mediante el modelo acoplado de MPLS evitan la complejidad de las VPN de IPSec de Nivel 3 y las VPN de Nivel 2 (mediante encapsulamiento de paquetes privados y conexiones punto a punto), pero tienen el inconveniente de no tener encriptación. No es problema con tal de que se configure dicha encriptación, simplemente debe observarse que MPLS no la proporciona en sus túneles VPN.

Las VPN basadas en MPLS dan un nivel de seguridad que es similar al que dan las redes L2 ATM. Debido a que toda la trayectoria de conmutación de etiqueta está predeterminada en el punto de acceso, los clientes están protegidos ya que el tráfico inyectado en un túnel MPLS no se desviará de ese túnel. El paquete en sí no se desviará de la estructura principal del proveedor. Por lo tanto, y suponiendo que el proveedor de servicios ha tomado las medidas de seguridad apropiadas, se limita la exposición a los empleados del proveedor de servicios. La índole de transferencia de etiquetas de MPLS hace que inyectar un paquete en un túnel MPLS resulte imposible a un intruso en la red.

En el borde de una red de proveedores de servicios deben entrar los paquetes de clientes por el interfaz correcto, lógico o físico. Los paquetes que entran por un interfaz para el que no hay VRF asociado se dejan caer. Finalmente, los proveedores de servicios asignan un distinguidor de rutas (RD) a cada cliente. Estos son desconocidos por los usuarios finales, lo que hace que sea imposible a un intruso entrar en la red por medio de otra puerta. El tráfico VPN sigue estando separado en la estructura principal. La comunicación entre VPN puede estar bien controlada, sea por medio de filtros de ruta, firewalls, listas de acceso, o servidores de autenticación.

En VPN de superposición IP que emplean tunelización L2TP, un tercero no autorizado podría introducir un paquete en el túnel IP, falsificando un paquete usando las direcciones apropiadas IPSA e IPDA y la encapsulación correcta. Por lo tanto, cuando el encaminador de borde de salida recibe el paquete, trata el paquete como si se hubiera originado en el encaminador de borde de acceso.

Para evitar la usurpación se autentican los paquetes destinados a los túneles L2TP usando un encabezamiento de autenticación IPsec (IPsec-AH).

En las VPN basadas en túneles IPSec, la seguridad requerida se garantiza mediante el cifrado de la información de los datos y de la cabecera de los paquetes IP, que se encapsulan con una nueva cabecera IP para su transporte por la red del proveedor. Es relativamente sencillo de implementar, bien sea en dispositivos especializados, tales como cortafuegos, como en los propios routers de acceso del NSP. Además, como es un estándar, IPSec permite crear VPN a través de redes de distintos NSP que sigan el estándar IPSec. Pero como el cifrado IPSec oculta las cabeceras de los paquetes originales, las opciones QoS son bastante limitadas, ya que la red no puede distinguir flujos por aplicaciones para asignarles diferentes niveles de servicio. Además, sólo vale para paquetes IP nativos, IPSec no admite otros protocolos.

En los túneles de nivel 2 se encapsulan paquetes multiprotocolo (no necesariamente IP), sobre los datagramas IP de la red del NSP. De este modo, la red del proveedor no pierde la visibilidad IP,

por lo que hay mayores posibilidades de QoS para priorizar el tráfico por tipo de aplicación IP. Los clientes VPN pueden mantener su esquema privado de direcciones, estableciendo grupos cerrados de usuarios, si así lo desean. (Además de encapsular los paquetes, se puede cifrar la información por mayor seguridad, pero en este caso limitando las opciones QoS). A diferencia de la opción anterior, la operación de túneles de nivel 2 está condicionada a un único proveedor.

Existen alternativas a la contención de tráfico en VLAN y el control y la securización en nivel 3, como por ejemplo la implantación de políticas en los equipos de acceso, realizando un control a niveles 2,3 y 4. Una política consta de diversos elementos, que facilitan el despliegue de distintas funcionalidades en toda la red:

- Control de acceso a la red mediante autenticación por 802.1x, por dirección MAC o a través de un portal Web.
- Contención de tráfico mediante asignación de VLAN al puerto de usuario.
- Limitación del ancho de banda de entrada y/o salida.
- Análisis de tramas a nivel 2,3 y 4 en tiempo real para:
  - Clasificación dinámica a VLAN
  - Filtrado de tramas
  - Clasificación dinámica 802.1p
  - Clasificación dinámica ToS
  - Limitación del ancho de banda de entrada y/o salida

Estas políticas pueden desplegarse en la red de forma estática (asignando de forma fija una política a un puerto) o dinámica (asignando una política a un puerto en función de la autenticación del usuario conectado a dicho puerto y mientras dure su conexión).

Se añaden ventajas de gestión de red, movilidad de usuarios, uso de los recursos, diferenciación y personalización de servicios por usuario, o integración con otros sistemas de seguridad como detectores de intrusiones.

4.6. GESTIÓN DE LA RED

Las redes de datos del presente proyecto se basan en equipos conmutadores y enrutadores, dando soporte a las comunicaciones de Ethernet/Fast Ethernet/Gigabit Ethernet y 10 GbE de la infraestructura de telecomunicaciones fijas de la línea. Los equipos a instalar incorporarán potentes capacidades de gestión proveyendo un sistema de gestión de red que aproveche dichas capacidades.

El Sistema Gestor de Red permitirá el fácil desempeño de funciones como la gestión de equipamiento, la monitorización continua de la calidad de la transmisión extremo a extremo, la supervisión de alarmas y el control de las funciones de protección de red.

La solución adoptada deberá ofrecer un único sistema de gestión que administre tanto la Red de Datos de Explotación (RDE), como la Red de Acceso de Datos (RAD), como la Red Unificada de Señalización y Detectores (RUSD), por las que circulan las diferentes redes de datos o servicios que se apoyan en ellas (Servicios de Alta Disponibilidad, Servicios de Propósito General, Red de Detectores, Red Privada de Señalización, etc.). Se incluirá dentro del suministro todo el hardware, software y licencias necesarias, que tendrán que ser válidas por un periodo indefinido, no siendo necesaria la renovación de las mismas.

Se incluirá la carga y configuración del software cliente necesario en los Puestos de Operación que defina Ferrocarriles de Gran Canaria.

Soportará, al menos los protocolos SNMP, Telnet, SSH, FTP para el intercambio de datos entre el Sistema de Gestión y los elementos de red.

Los elementos centralizados deberán suministrarse a nivel hardware y software, con la capacidad suficiente para que la red pueda crecer a medio plazo, respecto al número de informaciones que el SGR debe de manejar y procesar.

Además, debe asegurarse que en caso de una necesidad de ampliación superior a la indicada, no sea necesario sustituir los elementos fundamentales, sustituyendo únicamente elementos complementarios como puertos de conexión con la estructura de comunicaciones, de gestión, discos duros, etc., con el fin de mantener la validez del sistema, en un horizonte razonable. Se

documentará adecuadamente, en el sentido expuesto, las capacidades del sistema con el equipamiento propuesto y una estimación de necesidades para varios ejemplos de ampliaciones.

El gestor estará ubicado en el Edificio de Gerencia, a confirmar por Ferrocarril de Gran Canaria. La conexión de estos elementos se realizará a través de la red proyectada, que deberá configurarse adecuadamente para proporcionar las comunicaciones requeridas (estos trabajos son responsabilidad del adjudicatario).

Todas las aplicaciones del Sistema Gestor de datos se interconectarán con el Sistema de Gestión Integrada, exportando las alarmas y los datos de configuración de las redes IP.

Las aplicaciones de gestión incluidas en el servidor deben ser, al menos:

- **MPLS Manager:** Proporciona una visibilidad unificada sobre la infraestructura MPLS, descubriendo automáticamente los "*path*" (caminos) y asegurando la navegación topológica en tiempo real. Ante cualquier cambio en el estado de la red, el gestor correlará la información del cambio con el evento resultante y presentará una única alarma indicando el cambio de estado, su causa y su impacto.

- **Configuration Manager:** Alertará automáticamente de cualquier cambio en la configuración de dispositivos o notificación de alarmas. Descargará, almacenará, verificará y cargará archivos de configuración a intervalos predeterminados. Permite seguimiento y validación de cambios en la red y visibilidad actualizada de la infraestructura.

- **Qos Manager:** Proporciona una visión unificada y extremo a extremo de políticas QoS y clases de tráfico; correlado basado en modelos, reglas y políticas con procedimientos de resolución de problemas; priorización de cuestiones basada en clientes y servicios afectados; informes históricos y recogida de información hasta nivel de dispositivo y puerto para una determinada clase de tráfico.

- **Multicast Manager:** Análisis de causas, gestión de rendimiento y análisis de impacto, detectando la consecuencia para la red de un evento en un dispositivo concreto.

- **VPN Manager:** Vista de rendimiento detallada, estadísticas de VPN agregados y túneles individuales. Modelado preciso y rápido de conectividad VPN física y lógica. De aplicación las características del QoS Manager.

- **Report Manager:** Informes de alarmas, recursos, tendencia y disponibilidad. Creación, distribución y exportación automática de informes. Acceso remoto seguro e integración inteligente con todas las aplicaciones.

Estas aplicaciones correrán de forma integrada sobre una plataforma común que permita a los usuarios acceder a ellas con una única operación de alta, según permisos asignados por el administrador del sistema. Desde un mismo terminal de operación, un usuario podrá tener abiertas sesiones en varias aplicaciones. Las tareas de administración de usuarios y del propio sistema de gestión también se podrán realizar de forma centralizada.

Tendrá las siguientes características:

- Gestión unificada: una interfaz gráfica y una infraestructura de gestión de red comunes para realizar funciones de gestión, integrar aplicaciones y unificar la gestión de elemento de varios dispositivos.

- Visibilidad de toda la red: visión completa e informes detallados de la actividad de la red con detección y mapas de topología físicos y lógicos, gestión de eventos centralizada, gráficos e información estadística.

- Calidad de servicio basada en políticas: configuración simplificada de QoS.

- Arquitectura escalable: versiones para uno y múltiples usuarios, además de una arquitectura ampliable.

4.6.1. Funcionalidad

El sistema realizará al menos las siguientes funciones:

- Gestión de fallos. Supervisión continua de la red, mediante verificación automática del estado funcional de todos los elementos de la red, incluidos los elementos externos conectados a través de las entradas de alarmas externas.
- El sistema almacenará las alarmas que se generen en la red. Sobre la base de datos de alarmas se podrán realizar e imprimir filtros por equipo, tiempo, etc. Se valorará muy positivamente que el sistema permita calcular por servicios o por clientes el tiempo de indisponibilidad en un periodo de tiempo determinado.
- Gestión de configuración. Permitirá la instalación de nuevos equipos y modificar la programación de forma remota de los equipos de red previamente configurados. Tendrá capacidad para el almacenamiento centralizado o distribuido de todas las tablas de los equipos de la red. Todos los parámetros hasta nivel de slot, tarjeta, puerto, podrán configurarse desde el ordenador de gestión central, el cual guardará esta información en ficheros o bases de datos.

El SGR debe ser capaz de generar *backups* automáticos con periodicidad ajustable.

- Asimismo el sistema debe disponer de todos los medios y herramientas estándar para la gestión, operación y procedimientos habituales de *troubleshooting* remoto desde el centro de operación de red donde esté ubicado.
- Dispondrá de herramientas para la detección de servicios interrumpidos ante la caída de un enlace, (en caso de caída real o simulación).
- Almacenamiento y gestión de históricos de alarmas, fallos e incidencias, permitiendo análisis estadísticos y generación de informes de averías, valorándose positivamente que permita, adicionalmente, el reporte tiempo de indisponibilidad por clientes o servicios.
- Representación gráfica en color del estado de la red, con representación secuencial (filosofía *OpenView*), desde el esquema general hasta nivel de tarjeta, para una rápida localización de averías o fallos. El Sistema debe representar, también, el estado de disponibilidad de los enlaces (*links*), así como la caracterización de la incidencia que éstos pudieran soportar mediante gráficos de distintos colores y tipos de línea.
- Gestión de seguridad de acceso al sistema de Gestión, personalizando diferentes niveles de acceso, según las categorías funcionales de los diferentes posibles usuarios.
- Posibilidad de comprobar la configuración de los equipos a partir de la información de la / las base de datos (centralizadas / descentralizadas) sin necesidad de conectar directamente con el equipo.
- Generación de informes, en caso de avería o simulación, de los servicios afectados ante un fallo en un enlace o equipo.
- Las bases de datos que se generen serán gestionadas por el sistema de forma que su tamaño no ralentice el funcionamiento del sistema.

La funcionalidad se puede agrupar en diferentes elementos que se describen a continuación:

4.6.2. Interfaz gráfica de usuario

- Deberá contar con mapas topológicos de los nodos de la red con la posibilidad de crear agrupaciones y de navegar por ellas.
- Deberá de herramientas de búsqueda rápida de objetos dentro de la Base de Datos del Sistema de Gestión y la navegación cruzada.

4.6.3. Gestión de la configuración

- El Sistema de Gestión deberá descubrir los nodos de la red permitiendo establecer los filtros adecuados al operador.

- Se deberán almacenar los datos de configuración de la MIB del nodo en la Base de Datos del Sistema de Gestión garantizando su alineamiento periódico o por sincronización forzada por el Operador. Deberá proporcionar al Operador una amplia información del estado general del nodo: estado de alimentación, estado de los ventiladores y temperatura de las tarjetas y en general todos los componentes que forman parte de los equipos.
- Deberá permitir la navegación gráfica a través de la arquitectura jerárquica, al menos, del nodo.
- El sistema de gestión deberá de almacenar en su base de datos toda la estructura de servicios configurados para facilitar tareas de correlación de fallos de red / clientes afectados y servicios.

4.6.4. Gestión de fallos

- Se deberá proveer un listado de alarmas activas con clasificación por código de colores. Deben existir campos adicionales explicativos de las mismas. Deberá ser posible visualizar la información de detalle de cada alarma.
- Número máximo de alarmas almacenadas.
- La condición de alarma en los componentes de la red (nodo, tarjeta…) deberá reflejarse también en los mapas topológicos y jerárquicos.
- Posibilidad de realizar filtrado de alarmas.
- Se podrán reconocer y cesar las alarmas.
- Histórico de alarmas.
- Podrá almacenar las alarmas en una Base de Datos centralizada.
- Se deberá proveer algún tipo de correlación de alarmas para los objetos y servicios afectados.
- Monitorización se realizará en tiempo real.
- Resumen estadístico de las alarmas.
- Deberá disponer de herramientas de diagnóstico (OAM) para verificar la conectividad extremo a extremo de los servicios definidos mediante paquetes en-banda.

4.6.5. Gestión de la seguridad

- Se podrán configurar perfiles de usuario y permisos dentro del Sistema de Gestión.
- Se valorará la posibilidad de definir distintos grupos de usuarios de acuerdo a las prioridades y acciones que pueden acometer sobre la red.
- Se deberá indicar el límite de las Interfaces Gráficas de Usuario y la posibilidad de control de las mismas por parte del Administrador.

4.6.6. Gestión de MPLS

- El sistema proporcionará acceso rápido a los Servicios y Puertos usados por el Cliente.
- El sistema permitirá la configuración completa de los Túneles de Servicio.
- Realizará la configuración completa de protocolo MPLS, incluyendo interfaces lógicos, LSP y MPLS Paths.
- Realizará la configuración completa de Servicios (VLL, VPLS, HVPLS, IES, VPRN…) desde la interfaz gráfica sobre la base de Clientes, mediante formularios predefinidos de fácil uso.

4.6.6.1. Configuración mínima del sistema

El sistema de Gestión para el tramo estará configurado básicamente por al menos los siguientes elementos:

- Unidad central (Servidor de Gestión) para instalación en rack con capacidad para gestionar todas las redes de datos del presente proyecto y de las futuras ampliaciones.
- Unidades de almacenamiento. Discos de almacenamiento.

- Dos Terminal de Visualización gráfica > 17”.
- Dos terminales de operación (PC).
- Software, Sistemas Operativos
- Software específico de aplicaciones.
- Cualquier otro HW y SW que sea necesario para proporcionar la funcionalidad requerida.
- Red de comunicaciones de gestión, para transmisión de los datos entre los nodos y el ordenador central.
- Impresora

Se instalarán puestos de supervisión que dispondrán de un PC cliente el cual se conectará al sistema gestor propietario de la red de transporte a través de las Red de comunicaciones existentes. Desde estos PC se accederá gestor de la red obteniéndose un reporte de la información de estado y configuración de cada uno de los equipos que componen la red. Estos PC incluirán además el software cliente del resto de las redes de telecomunicaciones fijas de forma que desde cada puesto se tenga acceso a todos los subsistemas de la red fija.

Los elementos críticos, aquellos cuya avería pudiese dejar fuera de servicio el sistema, así como las bases de datos de configuración del sistema, estarán duplicados, de forma que en caso de avería de cualquier de estos elementos el tiempo durante el cual el sistema de gestión estuviese fuera de servicio fuese el mínimo.

La plataforma de gestión a suministrar estará de acuerdo con los últimos estándares de la UIT e ISO, debiéndose asegurar una larga vigencia según las tendencias actuales.

Se proporcionara el programa o programas auxiliares necesarios para la gestión de las bases de datos, configuración de las gráficas de representación de la red, etc., con el fin de facilitar el incremento o modificación de la misma.

4.6.7. Protección del sistema de gestión de red

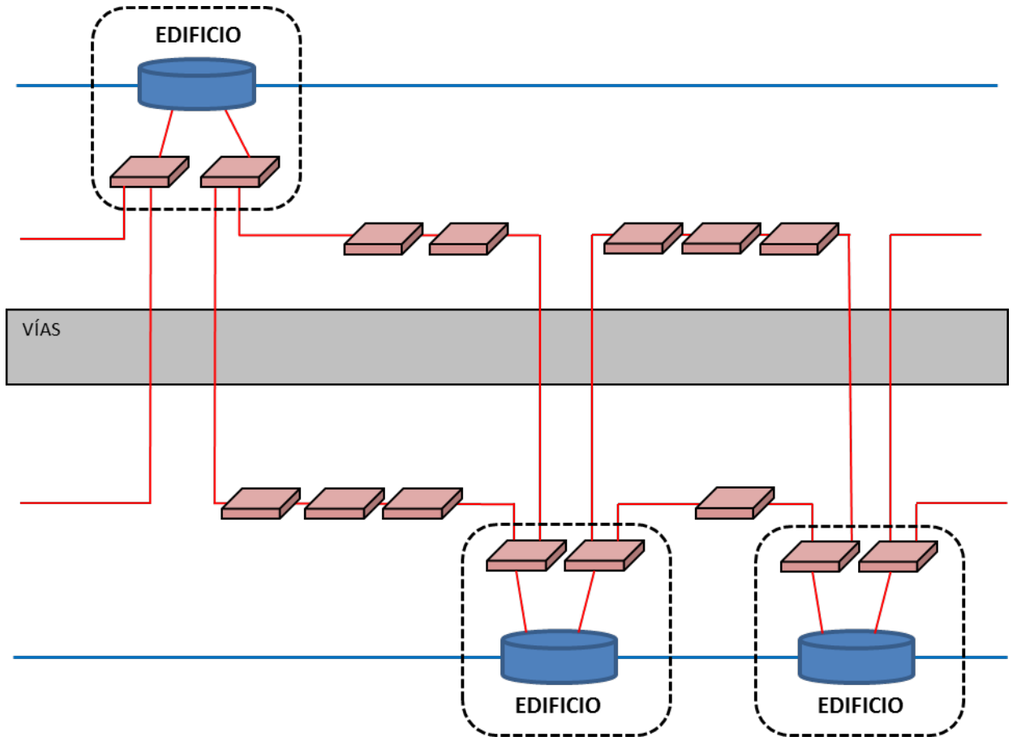
Hay que tener en cuenta que la eventual indisponibilidad del servidor no afecta al tráfico, tan solo a las funciones de gestión, lo que justifica la no duplicación del servidor completo. La pérdida de operatividad del propio sistema de gestión no implica pérdida de tráfico ni impacto en el servicio.

El sistema de gestión se basará en un servidor de última generación con altas prestaciones. El disco duro del servidor de aplicaciones estará redundado y configurado en modo espejo (*disk mirroring*).

5. RED DE ACCESO DE DATOS Y SERVICIOS DE DATOS

5.1. ARQUITECTURA DE LA RED DE ACCESO DE DATOS (RAD)

La Red de Acceso de Datos (RAD) constituye el soporte para la recogida de la información de datos de los emplazamientos que se encuentran entre emplazamientos con acceso a la RDE. Con tecnología de transmisión IP/MPLS de acceso securizado con enlaces a 1 Gigabit, el tráfico Ethernet se transmite a través de la RAD enlazando los diferentes emplazamientos de la línea de acuerdo al siguiente esquema tipo:



Los enlaces de color rojo representan anillos de acceso de la RAD entre nodos de la RDE. Los anillos de acceso podrán cerrarse directamente sobre los equipos de la RDE. Tanto la RDE como la RAD estarán configuradas para que los tiempos de convergencia ante fallos estén por debajo de 50 ms, de tal manera que los servicios no se vean afectados ante un posible corte de enlace o fallo de equipo. Cada anillo de acceso está constituido por un conjunto de nodos de acceso IP/MPLS securizados interconectados y ubicados en los distintos emplazamientos de la línea que precisan de conectividad de datos IP. Es a través de estos nodos de acceso IP/MPLS securizados donde los servicios finales tienen acceso a la red de datos.

En base a su funcionalidad, los servicios existentes y los criterios de redundancia en cada emplazamiento, el número de nodos de acceso varía. A lo largo del presente capítulo se particulariza el número requerido por servicio.

Como se ha comentado, existe una red de datos independiente y redundada a la RAD, con equipos propios y fibras dedicadas, constituyendo la Red Unificada de Señalización y Detectores (RUSD). Se tiene acceso en emplazamientos técnicos de señalización, transmitiéndose el Servicio Privado de Señalización (SPS) y Detectores con redundancia física, tanto de camino como de equipos, como se describe en el apartado dedicado al Servicio Privado de Señalización y Red Unificada de Señalización y Detectores del presente capítulo.

En aquellos emplazamientos dónde exista necesidad de servicios de alta disponibilidad se instalarán al menos dos nodos de acceso diferentes, uno de la RAD y el segundo de la RUSD.

Los anillos de acceso de la RAD disponen de conectividad a RDE a través de los Nodos IP/MPLS que cierran cada anillo. A través de esta conexión se dispone de acceso a otros emplazamientos de la línea así como a:

- CRC.
- CPS (integrado en el edificio de Gerencia).

Por criterios de redundancia, cada anillo de acceso de la RAD dispondrá de conexión a, al menos, dos Nodos IP/MPLS de la RDE distintos que aseguren que el anillo pude comunicar con el nivel principal incluso ante la caída de un equipo.

El acceso a la RAD se realiza mediante nodos de acceso IP/MPLS, cuya seguridad controlando el acceso se detalla en un capítulo posterior de este documento.

A continuación se muestra una tabla resumen con el número mínimo de equipos de transmisión de datos por emplazamiento:

EMPLAZAMIENTO	Nº DE SWITCHES IP/MPLS
Estación	1
CRC	2
CPS (actualmente está prevista su instalación en el mismo edificio que el CRC, con lo que son los mismos equipos)	2
Caseta de Señalización	1
Caseta GSM-R	1

En casetas de señalización, debido el servicio crítico privado de señalización, en realidad se instalan dos switches. Uno de ellos pertenece a la RAD y el otro es privado de la RUSD, tratándose éste de un switch n2/n3 con acceso securizado.

Esto mismo sucede en emplazamientos donde haya un concentrador de detectores se instalarán dos switches propios para este servicio. Uno de ellos pertenece a la RAD y el otro es privado de la RUSD, tratándose éste de un switch n2/n3 con acceso securizado.

Este mismo proceso se seguirá en cualquier otro emplazamiento que requiera redundancia en el acceso.

En los CRC se instalarán dos equipos de la RAD para tener redundancias en acceso.

El cable de 96 fibras ópticas deberá segregarse de su lado de vía en todos los emplazamientos de la línea donde se tenga acceso a la RAD. Se genera una estructura en anillo Gigabit entre dos nodos de la RDE consecutivos

Para el caso de emplazamientos donde existan nodos troncales, el cable de 96 fibras ópticas, entrará en punta el de su lado de vía y se segregarán las fibras necesarias del cable de la vía contraria para el cierre de los anillos de acceso. En el resto de los emplazamientos de la línea situadas entre dos nodos de la RDE, se segregarán las fibras necesarias del cable de 96 fibras ópticas de su lado de vía. La entrada de cables a estos emplazamientos deberá diseñarse adecuadamente para evitar que en ningún momento haya cruces de caminos que provoquen que un fallo simple afecte a ambos lados de los anillos de acceso y de las redes troncales.

En los emplazamientos donde, además, deban proporcionarse servicios de la RUSD (Red Unificada de Señalización y Detectores), para este servicio, la fibra se segregará del lado contrario de la fibra segregada para la RAD, debiendo entrar a la sala de comunicaciones por un camino completamente separado del de la RAD hasta el repartidor.

En los emplazamientos donde existan nodos troncales y, por lo tanto, se cierren anillos de acceso y donde deba proveerse el servicio de la RUSD existirán, entre la traza y la sala de comunicaciones, al menos dos caminos independientes desde ambos lados de vía, incluyendo, al menos, dos rutas de entrada a la sala de comunicaciones. En cualquier caso existirán las vías de entrada independientes que sean necesarias para cumplir con el requisito indicado anteriormente de que no haya cruces de camino para los anillos de acceso y para las redes troncales.

Tanto la RDE como la RAD estarán configuradas para que los tiempos de convergencia estén por debajo de 50 ms en caso de corte de enlace o fallo de algún equipo del anillo.

En el tramo Santa Catalina - Meloneras la RAD constará de 5 anillos de acceso de datos, distribuidos de la siguiente forma:

- Anillo 1: San Telmo – Vecindario

- Anillo 2: San Telmo – Aeropuerto
- Anillo 3: Aeropuerto – Edificio de Gerencia
- Anillo 4: Edificio de Gerencia - Playa del Inglés
- Anillo 5: Vecindario - Playa del Inglés

Los switches RAD de las Estaciones de viajeros se conectan mediante su propio anillo con el nodo de la RDE más cercano o pueden formar parte del anillo de acceso que corresponda a su ubicación.

5.2. CARACTERÍSTICAS DE LOS EQUIPOS DE LA RAD

Los equipos de la RAD consisten en equipos conmutadores / enrutadores (switch / router) de puertos 10/100/1000BASE-T y puertos ópticos 1000BASE--X SFPS, con soporte avanzado de características MPLS y creación de paths RSVP/LDP. Actuarán como nodos de acceso en la red MPLS.

Algunos de los requisitos que deben cumplir estos equipos se detallan a continuación:

Los equipos soportarán Ethernet Síncrono e IEEE 1588 v2.

Los equipos dispondrán de tarjetas de interfaces de E1 y realizarán la emulación de E1s sobre IP tanto mediante SAToP como mediante CESoPSN.

Dispondrán de dos fuentes de alimentación reemplazables en caliente. Si una fuente falla, la otra fuente asumirá toda la carga del dispositivo sin interrumpir el tráfico de la red. Incluirán un agente de gestión basado en SNMP versión 3, que proporcionará gestión en banda y fuera de banda para gestionar el switch. Los equipos serán configurables desde el sistema de gestión.

Al menos 5 puertos deben soportar tecnología PoE pudiendo suministrar hasta 15,4 W por puerto, para alimentar a los equipos conectados a ellos que permitan esta alimentación a través del propio cable Ethernet.

Soporte de VRRP y/o SEP y capacidad de actualización del firmware sin pérdida de prestaciones/ISSU.

Capacidad de conmutación multinivel (Layer 2,3,4), y funcionalidad de routing hardware por puerto.

El tipo de cableado que se soportará en los puertos RJ45 del switch será cable UTP. Si por motivos de seguridad se precisa cable apantallado, el cable será del tipo FTP/STP. Su categoría será categoría 3 o mejor para las conexiones a 10Mbps, categoría 5 o superior para conexiones a 100 Mbps y categoría 5e o 6 para conexiones a 1000Mbps.

DHCP server para que el propio equipo asigne de manera dinámica las direcciones IP, con mecanismo de seguridad como DHCP snooping para evitar DoS, Denegación de Servicio.

Soportarán conectividad con servidor AAA&Radius para mecanismo de autenticación, autorización y accounting, sobre protocolo RADIUS. El servidor Radius soportará LDAP para consulta a una base de datos externa dónde se almacenen los nombres de usuario/contraseña autorizados.

Aplicarán políticas de red por usuario conectado, y el establecimiento de una VLAN dónde se especifique los parámetros de tráfico permitidos, QoS (IEEE 802.1p), CoS, etc., siempre por puerto.

Todos los switches de acceso aplicarán una política por defecto, para el caso de que pierdan comunicación con el gestor de políticas y con el servidor RADIUS, dejando acceder a la red a los usuarios/dispositivos en unas condiciones de tráfico a determinar.

5.3. SERVICIOS DE DATOS QUE ACCEDEN A LA RDE

La Red de Datos de Explotación prestará servicios de conectividad de datos mediante la constitución de VPN de nivel 3, principalmente aunque para algún servicio determinado podrían ser necesarias VPLS entre los distintos puntos de acceso a la misma.

La Red de Acceso de Datos, por la cual se producirá la entrada de los servicios de datos, será el nivel de acceso hasta enlazar con los emplazamientos dónde exista conexión con la Red de Datos de Explotación.

Atendiendo a la disponibilidad del acceso a estos servicios, estos pueden clasificarse en:

- Servicios de Propósito General. Presentan un único punto de acceso a la red securizada. Son por ejemplo el servicio del sistema de información al viajero (SIV), gestión de alarmas y supervisión de sistemas de energía, etc.

- Servicios de Alta Disponibilidad. Dispondrán de acceso redundante a la red a través de dos equipos securizados independientes. En realidad a efectos de la RDE se comprotan igual que los servicios de propósito general ya que el segundo equipo de acceso utiliza la infraestructura de la RUSD. Incluyen los necesarios para los telemandos (energía, señalización, ERTMS, detectores, CRC, etc.) y cualquier otro que pudiera ser necesario para dotar al tramo de la funcionalidad requerida.

- Servicio de Voz. Se conectarán a un único punto de acceso a la red securizada. En caso de existir más un punto de acceso por la existencia de algún servicio crítico, la conexión de los terminales telefónicos se reparte entre los puntos de acceso. Su descripción más detallada se encuentra en el apartado dedicado al servicio de voz del presente anejo.

- Servicio de Seguridad Corporativa. Se conectarán a un único punto de acceso a la red securizado. Incluye la información de gestión de las instalaciones, videovigilancia, control de accesos y anti-intrusión, recogida en el Anejo nº 4. Este servicio recoge los servicios necesarios en los diferentes emplazamientos donde sea necesario. En aquellos casos donde exista este servicio pero no haya equipo de comunicaciones, como pueda ser un paso superior, se utilizarán fibras del cable de 96 y transceptores ópticos para transportarlo hasta el emplazamiento más cercano

- Teniendo presente la arquitectura de la Red de Acceso de Datos descrita en este mismo anejo, es importante destacar que en un emplazamiento existirán como máximo dos equipos de datos securizados para la RAD,

Adicionalmente, se añadirán otros switches en aquellos emplazamientos que necesiten el Servicio Privado de Señalización y/o el Servicio de Detectores.

5.3.1. Servicios de GSM-R

5.3.1.1. Introducción

Los servicios para GSM-R consistirán en la emulación de Enlaces E1 sobre MPLS que permitirán la conexión de las BTS de GSM-R entre ellas y con la BSC.

5.3.1.2. Arquitectura de red

Este servicio consistirá en enlaces punto a punto siguiendo la lógica de los anillos lógicos de GSM-R. Por norma general los enlaces se estructurarán en anillos que unas 4 o 5 BTS con la BSC.

5.3.1.3. Criterios de protección y redundancia

El tráfico de la los Servicios de Propósito General dispondrá de todas las prestaciones de redundancia y calidad de servicio asociado a los enlaces proporcionados por la RDE y la RAD.

La redundancia de este servicio vendrá dada por la arquitectura en a anillo de los enlaces lógicos entre BTS. Sin embargo el control de esta redundancia figura en las BTS, siendo estás las encargadas de conmutar dentro de su anillo lógico. No obstante cada enlace punto a punto configurado de esta forma gozará de las protecciones generales de la RDE/RAD.

5.3.2. Servicios de Propósito General

5.3.2.1. Introducción

Los Servicios de Propósito General (SPG) se proporcionarán mediante conectividad IP/Ethernet en los diferentes puntos de la línea. Emplearán la RAD en las diferentes casetas del trazado, y recursos de la RDE en los emplazamientos que disponen de ella, integrándose en los nodos PE de dicha red.

5.3.2.2. Arquitectura de red

La arquitectura aplicada a los Servicios de Propósito General (SPG) se planteará con el concepto de diseño que utiliza una red extendida de propósito general que proporcionará conectividad IP/Ethernet en todos los emplazamientos necesarios.

Se indican a continuación los principales, aunque no los únicos, Servicios de Propósito General:

- Gestión de equipos de las diferentes redes de comunicaciones (IP, MPLS).
- Tráfico de la red de supervisión de Fibra Óptica.
- Gestión de Control de Accesos y sistemas asociados a obra civil.
- Gestión de equipamiento del CRC fuera de banda.
- Tráfico de la Red Corporativa.
- Gestión de centrales de alarmas de las casetas.
- Sistema de Información al Viajero.
- Servicios corporativos.

Para proporcionar dichos servicios en los emplazamientos especificados, los SPG se sustentarán por la RAD con un switch MPLS de acceso securizado hasta llegar a la RDE. La seguridad con mecanismos de autenticación, generación de VLAN con políticas, etc. viene especificado en el apartado dedicado a la Seguridad en la Red de Acceso de Datos. El acceso a éste y otros servicios presentes en este capítulo seguirá el mismo mecanismo de seguridad en los equipos de datos que conforman el soporte físico de la RAD.

Los SPG consistirán en un conjunto de servicios por los cuales se proporcionará conectividad Ethernet/IP a lo largo del tramo Santa Catalina - Meloneras, y utilizarán recursos de la RDE para dar conexión con el emplazamiento que lo necesite.

El switch MPLS por el que se inicia la transmisión del SPG en los diferentes emplazamientos de la línea será compartido físicamente por otros servicios. Sin embargo la RAD se virtualizará por servicio mediante VPN de nivel 2 o 3.

5.3.2.3. Criterios de protección y redundancia

El tráfico de la los Servicios de Propósito General dispondrá de todas las prestaciones de redundancia y calidad de servicio asociado a los enlaces proporcionados por la RDE y la RAD.

5.3.3. Servicios de Alta Disponibilidad

5.3.3.1. Introducción

Bajo esta denominación se agrupan los servicios que, por su elevada criticidad, requieren una elevada disponibilidad, por lo que tendrán dos puntos de acceso (principal y redundante). Estos servicios se servirán de dos switches/MPLS en los emplazamientos donde sean necesarios, de manera que el fallo de uno de ellos no impida la correcta prestación del servicio.

No obstante, todos estos servicios compartirán equipamiento, de manera que todos aquellos que se generen en ese emplazamiento se apoyarán en los dos equipos de acceso (switches/routers) securizados, en función de la criticidad del servicio.

5.3.3.2. Redundancia de acceso

Mediante los servicios de alta disponibilidad podremos establecer la comunicación entre los Enclavamientos y el Centro de Control de Tráfico Centralizado (CTC).

También está soportado el tráfico originado en otros elementos como RBC, LEU y detectores de seguridad. Así como todos los tráficos de datos IP que sean de importancia crítica y elevada disponibilidad.

Se utilizarán recursos de la RAD y de la RDE junto con recursos de la RUSD. Puesto que estos servicios son críticos, se consideran dos equipos de datos MPLS securizados sobre los cuales accederá a la red, uno de la Rad y otro de la RUSD).

La arquitectura de la red se planteará con el concepto de diseño de red crítica y debe, por tanto, presentar una elevada disponibilidad y robustez frente a fallos. Por ello se apoyará en la red completamente redundante en enlaces y elementos que proporcionará conectividad IP/Ethernet en los siguientes puntos del trayecto:

- CTC.
- Enclavamientos en estaciones.
- Cualquier otro emplazamiento que demanda este tipo de servicio.

Esta arquitectura en esencia puede describirse como una red en la que las comunicaciones se encuentran garantizadas por el establecimiento en todos los casos de dos rutas independientes soportadas extremo a extremo por equipos y medios físicos diferentes.

Los principales servicios de alta disponibilidad serán los siguientes, aunque deberán considerarse los necesarios de acuerdo a las tecnologías de los diferentes sistemas instalados en el tramo:

- Tráfico de gestión del enclavamiento.
- Tráfico RBC ↔ CTC.
- Tráfico de la red de detectores.
- Gestión de equipamiento del CRC fuera de banda.
- Etc.

5.3.3.3. Criterios de protección y redundancia

Esta red, por su especial criticidad, se diseñará tanto con redundancia de elementos como con redundancia de enlaces.

- Como equipos de acceso a los Servicios de Alta Disponibilidad se dispondrá de dos switch-routers MPLS securizados en cada ubicación, tanto en los puntos de acceso como en aquellos en los que confluyen las comunicaciones. Estos equipos son compartidos por el resto de servicios de datos descritos en este capítulo que comparten origen con el SAD.

Ante posibles fallos de las líneas de comunicación, se han dispuesto caminos redundantes, independientes, para estos switches, de forma que un equipo dependa del equipo de la RDE de un extremo del anillo y el otro utilice el anillo de la RAD para establecer un enlace hasta el equipo de la RDE del otro extremo del anillo.

5.4. REDES DE DATOS ESPECÍFICAS PARA DETECTORES E INSTALACIONES DE CONTROL DE TRÁFICO

- **Servicios Privados de Señalización.** En aquellos emplazamientos donde exista un enclavamiento electrónico o controladores de objetos, se dispondrá de un acceso redundante con conexión a dos equipos de datos securizados privados para este servicio. Uno de ellos se conecta a la RAD y el otro da origen a la Red Unificada de Señalización y Detectores (RUSD), la cual emplea un enlace con fibras dedicadas y equipos propios, proporcionando redundancia total de equipos y medios físicos.
- **Servicios de Detectores.** En aquellos emplazamientos donde exista un concentrador de detectores que necesite redundancia, se dispondrá de un acceso redundante con conexión a dos equipos de datos securizados privados para este servicio. Uno de ellos se conecta a la RAD y el otro da origen a la Red Unificada de Señalización y Detectores (RUSD), la cual emplea un enlace con fibras dedicadas y equipos propios, proporcionando redundancia total de equipos y medios físicos.

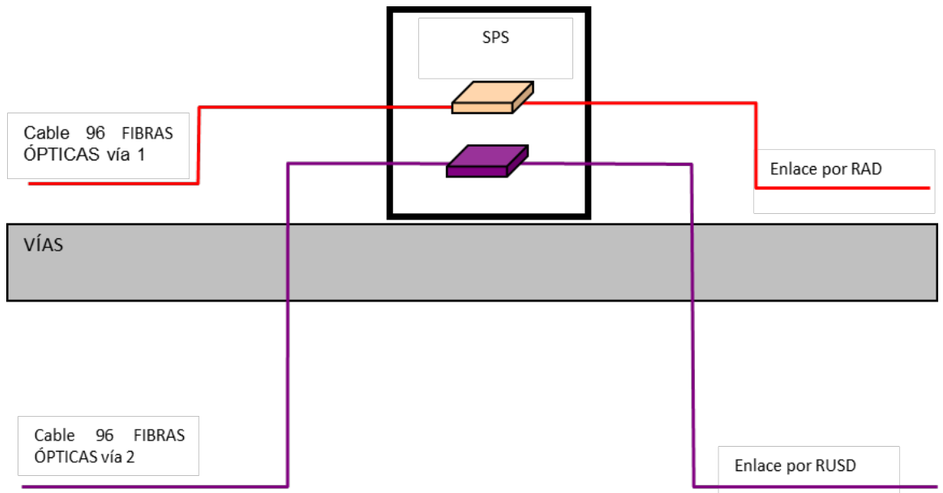
5.4.1. Servicio Privado de Señalización y Red Unificada de Señalización y Detectores

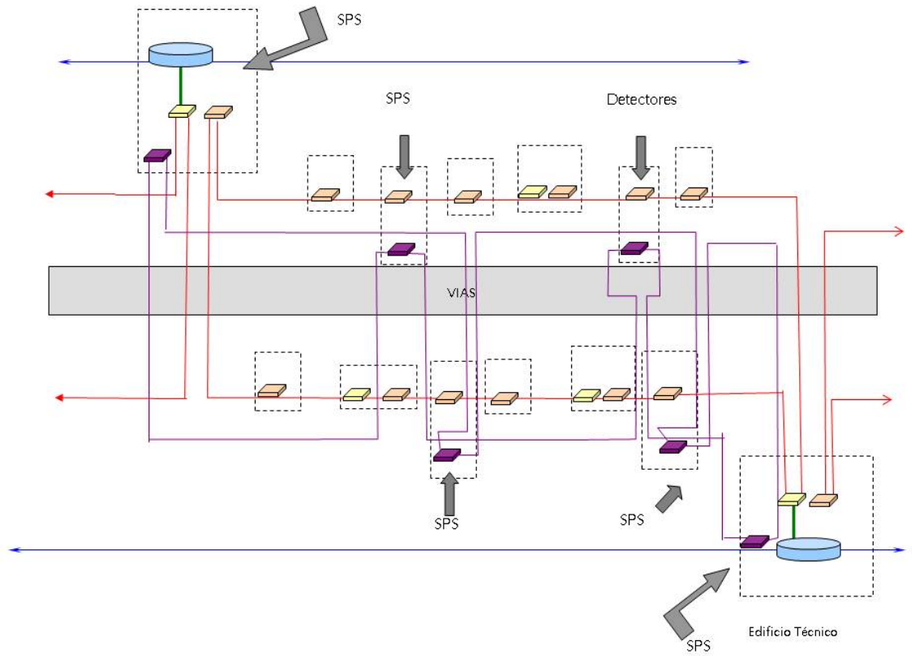
5.4.1.1. Introducción

Este servicio se encarga de unir todos los emplazamientos de señalización a lo largo de todo el trayecto. El Servicio Privado de Señalización (SPS) se utilizará para unir los enclavamientos, controladores de objetos y los sistemas ERTMS (RBC y CLC) entre sí.

Uno de los enlaces (canal B) se soporta sobre la RAD y el otro (canal A) sobre la Red Unificada de Señalización y Detectores (RUSD). En estos emplazamientos para este servicio se dispondrá de dos switches para asegurar redundancias, uno MPLS correspondiente a la RAD y el otro n2/n3 correspondiente a la RUSD. El anillo que se diseña con las fibras dedicadas va por el lado de vía

opuesto a la ruta por la RAD, estableciéndose la comunicación desde cada uno de los switches privados de un emplazamiento con los del siguiente donde exista el SPS. El SPS lleva las comunicaciones que requieren los equipos de señalización y debe, por tanto, presentar una elevada disponibilidad y robustez frente a fallos.





5.4.1.2. Arquitectura de servicio

El SPS se encarga de unir todas las salas de señalización del tramo objeto del proyecto. El acceso a este servicio se contempla los siguientes emplazamientos:

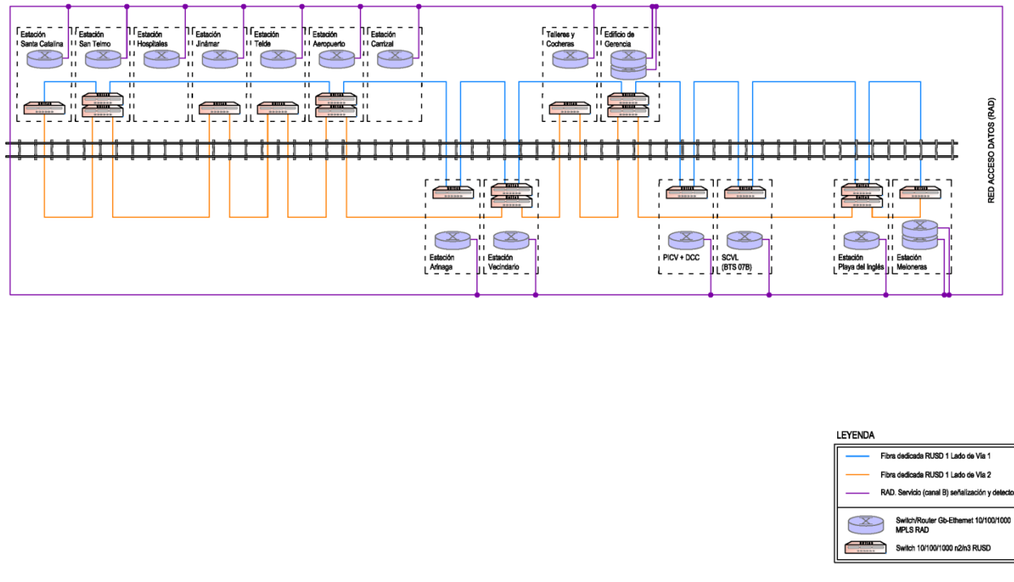
- Salas Técnicas de señalización en estaciones (enclavamiento, controlador de objetos)

5.4.1.3. Arquitectura de servicio privado de señalización (RUSD)

El Servicio Privado de Señalización, considerado un servicio crítico, es transmitido por dos rutas independientes ofreciendo redundancia de caminos y de equipos. El siguiente esquema muestra la solución diseñada para la RUSD, mostrando asimismo la existencia de la RAD como red paralela de datos que transmiten una de las rutas del SPS y otros servicios anteriormente citados:

Como se observa, para el Servicio Privado de Señalización se ofrecen dos enlaces redundados. Uno de ellos se enlaza con la RAD (color rojo) y el otro a través de un enlace con fibras dedicadas (color violeta). Esta red accede en todos los emplazamientos de la línea entre dos estaciones donde se precise este servicio de datos. El enlace es a través de medios físicos propios con fibras dedicadas (2+2) reservadas del cable de 96 fibras ópticas, enlazando directamente con los otros emplazamientos entre dos estaciones donde se ofrezca este servicio. Se reservan un total de 2+2 fibras ópticas para la configuración del canal A y 2+2 fibras ópticas para la RAD por la que se transmite el canal B. Esta asignación de fibras del cable de 96 fibras ópticas se refleja en el plano de detalle “Cable 96 fo PKESP”, siendo equivalente la asignación para el cable ignifugo 96 fibras ópticas TKEST.

La configuración de los anillos en la línea objeto del proyecto se indica en el siguiente esquema:



En cada uno de estos emplazamientos, con motivo del SPS, se instalará un Switch/Router n2/n3 de puertos securizados con enlaces Gigabit.

5.4.1.4. Criterios de protección y redundancia

El Servicio Privado de Señalización es un servicio de importancia crítica, por lo que deberá contar con una elevada protección frente a fallos. Estas protecciones son:

- Equipos. En cada emplazamiento habrá un equipo de comunicaciones Switch/Router n2/n3. Mediante mecanismos de autenticación, generación de VLAN y establecimiento de rate limit, se controla también el acceso a la RUSD y el consumo de recursos de tráfico por servicio, como sucede con la RAD. El enclavamiento, al precisar de redundancia en la transmisión, podrá conectarse al switch y transmitir la información generada en el SPS una vez superado el control de accesos a la red.
- Fuentes de alimentación redundantes. Las fuentes de alimentación estarán redundadas en cada equipo.
- Enlaces redundantes. El servicio dispondrá en cada emplazamiento de dos caminos independientes, de forma que el enlace entre uno y los adyacentes esté debidamente redundado.

5.4.2. Servicio de Detectores

5.4.2.1. Introducción

Este servicio de datos se encarga de unir los emplazamientos donde hay equipos de detectores con los concentradores de detectores localizados en los emplazamientos con enclavamiento o controlador de objetos. Estos concentradores se conectarán con el CRC a través del Servicio de Alta Disponibilidad, ya descrito anteriormente. El soporte de las comunicaciones se establece sobre la RAD y la RUSD, siendo requeridos por los equipos de detectores una elevada disponibilidad y robustez frente a fallos.

5.4.2.2. Arquitectura de servicio

La asignación de sensores a su enclavamiento se realiza a través del direccionamiento IP. Se otorga una gran flexibilidad en la organización de los sensores y su asignación a diferentes concentradores.

El servicio debe ser proporcionado entre todos aquellos emplazamientos que tengan equipamiento de detectores y/o concentradores de detectores.

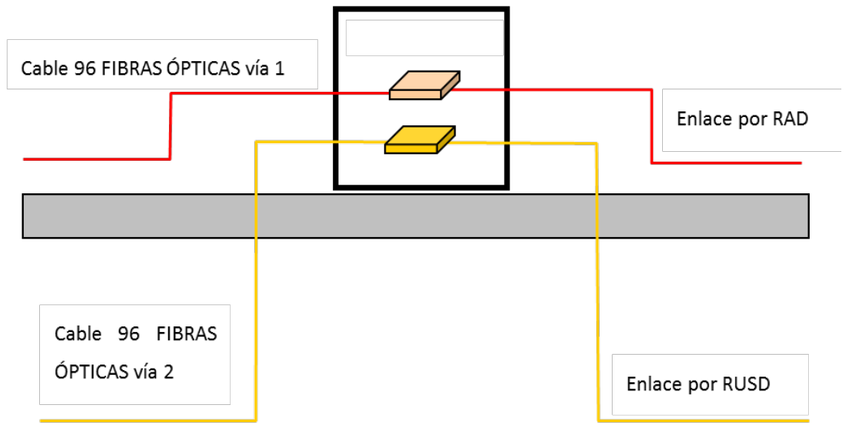
5.4.2.3. Criterios de protección y redundancia

El servicio de detectores es de importancia crítica, por lo que deberá contar con una elevada protección frente a fallos simples. Estas protecciones son:

- Duplicidad de equipos. En cada emplazamiento habrá dos equipos de comunicaciones switch securizados para este servicio, uno de ellos tipo MPLS, soportándose sobre la RAD, y el otro tipo n2/n3, sobre la RUSD.

- Enlaces redundantes. La RAD sobre la que se soporta el servicio tiene una configuración en anillo, por lo que ofrece dos caminos totalmente independientes. Además se ofrece un segundo enlace a través de un equipo RUSD.

Debido a que los concentradores de DCO se encuentran en emplazamientos con enclavamiento o controlador de objetos, el esquema de conexión del equipamiento destinado a detectores se realiza como se muestra a continuación:



6. RED DE CONMUTACIÓN DE VOZ

6.1. INTRODUCCIÓN

El objeto principal de la red de conmutación de voz será proporcionar una red de telefonía fija basada en IP con control por programación almacenada que garantice las siguientes comunicaciones:

- Comunicaciones telefónicas entre las distintas ubicaciones de la línea: estaciones, centro de control y casetas técnicas (señalización, GSM-R...).
- Comunicaciones telefónicas con la red de conmutación de voz existente en la línea (interfonía en estaciones).

La red de conmutación de voz deberá soportar la tecnología de Voz sobre IP (VoIP), mediante soporte combinado de la Red de Datos de Explotación y de la Red de Acceso de Datos, haciendo que las comunicaciones en la línea se realicen con máxima flexibilidad y rendimiento en su nivel principal.

Las características principales del sistema de conmutación de voz serán las siguientes:

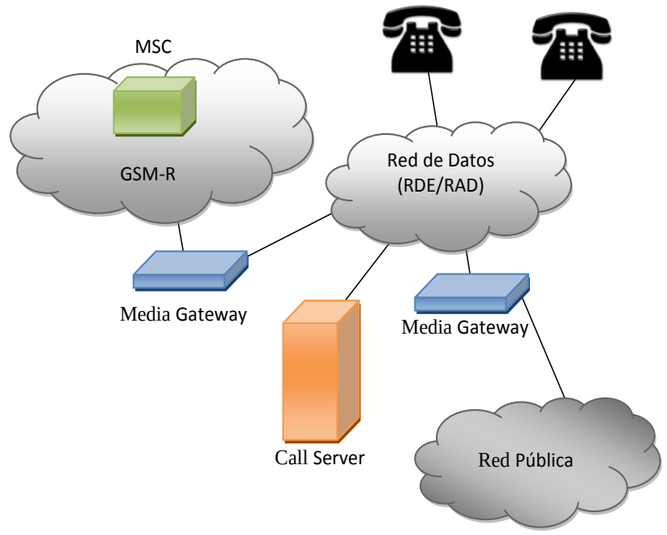
- Centrales basadas en IP.
- Control por programación almacenada.
- Hardware modular.
- Software modular y estructurado.
- Soporte de telefonía VoIP
- Redundancia total de los elementos críticos del sistema.
- Matriz de conmutación con accesibilidad total y gran capacidad de procesamiento dinámico.
- Homogeneidad de tecnologías en sus componentes: centrales, módulos, interfaces y gestión de red.
- Capacidad de ampliación y escalabilidad, previendo tanto las comunicaciones actuales como futuras, tanto en la arquitectura de la red como en el modelo de gestión.
- Soporte de protocolos QSIG, VoIP H323 y SIP.
- Prestaciones de alto nivel tales como MLPP (*Multilevel Precedence and Preemption*) y códigos de identificación privada (PIN) con derechos, prestaciones y autorizaciones asociadas al personal.
- Soporte de interfaz con los *dispatcher* DICOM tanto en RDSI (S0) como en SIP.
- Capacidad de conexión con Red Pública Conmutada.

La totalidad del sistema será gestionado por un único sistema gestor de red (supervisión Integral de Red), el cual podrá comunicarse vía SNMP con un Sistema de Gestión Superior TMN (Sistema de Gestión Integrada).

6.2. ARQUITECTURA DE RED

El diseño de la red se ha realizado teniendo en cuenta la globalidad de la red final, considerando para ello los enlaces necesarios con el Call Server y la integración con la arquitectura de red.

El esquema tipo de la red de voz es el siguiente:



6.2.1.1. Call Server

El Call Server estará a cargo del procesado y gestión de las llamadas. Este elemento debe encargarse de la gestión de usuarios y su base de datos, el control de y gestión de las llamadas y el registro de los dispositivos (teléfonos).

Al ser un elemento crítico en la infraestructura del servicio de voz este elemento debe tener las suficientes redundancias internas que le permitan operar incluso en modos degradados. Estas redundancias deben incluir al menos redundancia de procesador, tarjetas de puertos y fuente de alimentación. Se admite la posibilidad de que este elemento se encuentre totalmente redundando hasta el punto de ser físicamente dos equipos que se comporten a nivel lógico como un único elemento.

6.2.1.2. Media Gateways

Los Media Gateways serán utilizados para interconecta esta red con otras redes, como GSM-R o red pública. Se encargaran también de transmitir la señalización necesaria con las diferentes redes de voz con las que haya que conectarse.

6.2.1.2.1. Conexiones a RDSI públicas con la red de voz

La conexión con el resto de redes de voz de GSM-R y con la Red Pública se realizará a través de los media gateways.

6.3. CONECTIVIDAD DE LA RED.

La conectividad de la red proyectada se basa en IP y tendrá las siguientes características:

- Conectividad IP a través de una VLAN de Voz con mecanismo de autenticación soportada sobre una red de datos. La autenticación se realizará mediante la dirección física MAC propia e intransferible de cada teléfono, tal y como aparece descrito en el capítulo dedicado a la Seguridad en la Red de Acceso de Datos del presente anejo.

La tecnología de VoIP se basará en el estándar SIP y H323 con interfaces 10/100 Mbits. Para ello las centrales conectadas a la red IP dispondrán de módulos de pasarela, Media Gateways, adaptando la telefonía tradicional con todas sus prestaciones al entorno IP y marcando los paquetes de información con prioridad para que no se produzcan retardos y permita una calidad máxima de voz empleando la Red de Datos como soporte.

6.4. DESCRIPCIÓN DEL EQUIPAMIENTO DE LA RED DE VOZ.

6.4.1. Call Server

Características del Call Server:

- Procesado de llamadas centralizado (sobre LAN/WAN).
- Base de datos resistente.
- Soporte de Fax.
- Soporte DTMF.
- Informe de llamadas.
- Transferencia de llamadas.
- Suspender/continuar llamadas.
- Desvio de llamadas.
- Permisos de llamada basado en dispositivo de origen (bloqueo de llamadas)
- Protocolo de señalización: SIP
- Amplia gama de teléfonos soportados (software, hardware, etc.).
- Indicación del número llamante.

- Generación de reportes de actividad.

6.4.2. Media Gateways

Características de los media gateways:

- Interfaces soportados: FXO, BRI(S0), PRI (E1/T1) -ETSI/QSIG/E1 R2-, IP.
- Soporte DTMF.
- Supplementary services support: Supplementary services are typically basic telephony functions such as hold, transfer, and conferencing.
- Soporte de Fax.

6.5. PLAN DE SINCRONISMO, RETARDOS Y JITTER EN IP.

Puesto que la arquitectura de red proyectada se basa en IP con conexión a la Red de Datos de Explotación (red asíncrona) no existe necesidad de tener que sincronizar los nodos de la red de voz.

Para evitar el *jitter* se dispondrá de buffers integrados en los sistemas que eviten las variaciones en el tiempo de entrega de paquetes. En cualquier caso deberán realizarse los ajustes necesarios sobre las redes de datos para proporcionar el servicio de voz en las condiciones de retardo, *jitter* y pérdida de paquetes demandadas por el mismo.

Para evitar los retardos se marcarán los paquetes de voz como tráfico prioritario, siendo los componentes de la Red de Datos de Explotación los que interpreten esta información y asignen la prioridad adecuada.

6.6. PRESTACIONES DE LA RED

El sistema global de comunicaciones de voz deberá permitir, al menos, las siguientes prestaciones:

6.6.1. Prestaciones del Sistema Operativo

- Envío marcación multifrecuente a la red pública/privada (postmarcación).
- Servicio con/sin selección directa.
- Posibilidad de establecer restricciones de tráfico (grupo cerrado de usuarios) entre extensiones y/o entre nodos de una red.
- Discriminación de rutas.
- Posibilidad de ocupar selectivamente los haces de líneas externas.
- Selección de ruta en tráfico urbano, en función de la categoría.
- Selección de ruta en tráfico de enlace, en función de la categoría.
- Control de marcación en tráfico urbano/privado.
- Segunda llamada permitir / bloquear en teléfonos digitales.
- Desvío de llamada en caso de no contesta / ocupado.
- Preinserción de cifras.
- Repetición de cifras.
- Numeración cerrada/oculta.
- Numeración cerrada
- Numeración ampliada en red

- Llamada directa, mediante tecla de función desde teléfonos digitales.
- Llamada directa sobre línea urbana.
- Registros de tarificación.
- Llamadas entrantes.
- Llamadas salientes.
- Llamadas internas.
- Llamadas en redes.
- Conmutación a modo nocturno.
- Comprobación de líneas de extensión analógicas.

6.6.2. Prestaciones de las extensiones

- Repetición de marcación.
- Desvío de llamadas.
- Captura de llamadas.
- Marcación abreviada central/individual.
- Retrollamada (Rellamada automática).
- Transferencia llamadas externas/internas.
- Conferencia Tripartita / Múltiple hasta ocho.
- Distinción de llamadas (cadencia).
- Citas.
- Llamada alternativa.
- Restricción de tráfico interno, dentro de grupos cerrados.
- Línea colectiva (grupos de salto).
- Conmutación de categoría.
- Traslado (cambio usuario).
- Anuncios sincronizados.
- Captura de llamada maliciosa.
- Conexión de DCI o equipo terminal de datos.
- Desborde de llamadas directas entrantes hacia operadora.
- PIN / sígueme.
- No molestar.
- Aviso llamada en espera / protección contra aviso.
- Liberación de llamada en espera.
- Intercalación / protección contra intercalación (intrusión).
- Intercalación emergencia, a nivel local y en red.
- Intercalación emergencia, con corte, a nivel local y en red.
- Llamada automática sin marcación inmediata o retardada (*hotline*).
- Función interfono / protección contra interfono.

6.6.3. Prestaciones de enlaces

- Redes con líneas punto a punto o sobre la red pública.
- Redes con conexión todos con todos a través de una Red IP.
- Conexión pública digital, acoplamiento de circuitos básicos y primarios.
- Tráfico enlace privado sobre líneas punto a punto.
- Enrutamiento / reenrutamiento.
- Prestaciones de no voz.
- Presentación de información de usuario.
- Grupo de pupitres de operadora centralizado en sistemas en red.
- Ampliación de prestaciones de usuarios en toda la red.
- Uso de servidores en toda la red.
- Desvío en toda la red hacia el servicio de voz y fax.
- Indicación de buzón al nivel de red.
- Indicación de *display* al nivel de red.
- Configurar buzones de texto al nivel de red.
- Prevención de bucles de red.
- Tratamiento redes heterogéneas nivel 1 (E&M, QSIG y DSS1).
- *Break out* hacia red pública en el nodo más favorable.
- Conversiones de marcación externa.
- Optimización de la ruta.
- *Rerouting* (enrutamiento alternativo).

6.7. CAPACIDAD DE AMPLIACIÓN

En todas las configuraciones de los Call Servers se tendrá en cuenta una capacidad de ampliación de los sistemas en más del 50% mediante la instalación del software y hardware necesario para dicha ampliación.

6.8. SISTEMA DE GRABACIÓN

Se instalarán sistemas de grabación de las conversaciones telefónicas en las estaciones con Puesto Local de Operación (PLO).

Estos equipos permitirán la grabación y posterior escucha de todas las conversaciones que lleguen o salgan de las extensiones que se programen para tal efecto (jefes de estación, CTC y CRC). Para facilitar la reproducción de las conversaciones almacenadas se instalará un servidor con conexión a los equipos de grabación a través de la Red de Datos de Explotación, como Servicios de Propósito General, desde donde se podrán localizar y reproducir las conversaciones almacenadas. El sistema permitirá ofrecer más de un PC desde donde se puedan realizar las escuchas.

El equipo de grabación deberá integrarse con los equipos de telefonía especificados mediante conexión directa en paralelo en los repartidores de cableado de las centrales telefónicas. El sistema deberá incluir los interfaces necesarios para la grabación de las conversaciones realizadas desde los despachadores de la red GSM R.

El acceso a las grabaciones se realizará cumpliendo los siguientes requisitos:

- No interrumpir llamadas ni grabaciones en progreso.

- Posibilidad de almacenamiento de las conversaciones (en formato MP3 o WAV).
- Búsqueda organizada de la llamada a reproducir. El Sistema de Grabación debe proporcionar un *SW Developer's Toolkit* con capacidad de:
  - levantar un evento accesible por MOM notificando el ID asociado a cada conversación que tenga lugar, junto con su origen (del llamante) y fecha-hora
  - acceder a las llamadas grabadas por ID, para sincronizar los índices de los registros de las conversaciones con los mensajes Tibco de llamadas DICOM almacenados en la BDR.
- Posibilidad de que el Sistema de Grabación permita definir un volumen externo de almacenamiento de datos en el XP, de modo que se unifiquen las operaciones de BKP de mensajes Tibco de llamadas DICOM y las conversaciones asociadas.
- Garantizar la integración de servicios DNS, NTP, SNMP... de SRF. En particular, para la funcionalidad de SSO los usuarios del CRC dados de alta en el LDAP-SRF han de poder registrarse (preferiblemente automáticamente) en las aplicaciones de Gestión del Sistema de Grabación.

6.9. SISTEMA DE GESTIÓN

Los equipos a instalar incorporarán potentes capacidades de gestión proveyendo un sistema de gestión de red que aproveche dichas capacidades.

Los sistemas a instalar serán gestionados desde la plataforma de gestión unificada de la línea férrea, que contempla los siguientes servicios de administración:

- Gestión de Configuración.
- Gestión de Errores.
- Gestión de Rendimiento de la red y medidas de tráfico de enlaces.
- Gestión de Enrutamientos.

Utilizando todos estos servicios la misma base de datos.

De este modo, la solución planteada debe contemplar un sistema de gestión compatible e integrable con el existente, de modo que sólo exista un sistema de gestión para esta nueva línea y para las existentes, o bien una ampliación del existente.

El sistema gestor de la red de voz deberá estar equipado con un agente SNMP para poder enviar informaciones a una plataforma superior, como en este caso el Sistema de Gestión Integrada de Red.

El Sistema de Gestión ofrecerá las siguientes características:

- Acceso centralizado a todos los servicios de administración.
- Única entrada para los datos compartidos tanto en inicialización como en los cambios.
- Comunicaciones para la administración de la red a través de los enlaces de voz ya existentes.

Los puestos de operación se conectarán al servidor a través de la Red de Datos de Explotación.

6.9.1. Gestión de Accesos

El acceso a los usuarios del sistema estará controlado mediante la verificación de autorización de los usuarios pudiendo asignar aplicaciones y características particulares de acceso de forma individual.

La gestión de accesos permitirá las siguientes funciones:

- Validación de usuarios y alta en el sistema
- Verificará a qué aplicaciones puede acceder un usuario en particular.
- Verificará qué facilidades/funciones pueden utilizar los usuarios en la aplicación o aplicaciones a las que tienen acceso.

- La base de datos de autorizaciones y acceso formará parte de la base de datos central del sistema gestor.

Esta gestión del acceso está destinada al reparto de las aplicaciones incluidas en el servicio de voz; previo a este paso, el dispositivo telefónico tiene que superar un mecanismo de autenticación con su dirección física MAC para poder entrar en la red y así encontrarse autorizado a utilizar los recursos de la misma

6.9.2. Gestión de Configuración

La Administración de Configuración permitirá gestionar los datos de los abonados a nivel de red y a nivel de sistema individual.

El sistema permitirá visualizar la configuración de los distintos abonados y cambiarla si fuera necesario, validando que los parámetros introducidos son correctos y compatibles con la configuración de red.

Las tareas de administración que podrán realizarse serán como mínimo las siguientes:

- Describir las configuraciones de abonado mediante los datos adecuados.
- Visualizar la configuración de los abonados.
- Permitir el acceso a estos datos desde los demás servicios del sistema.

El servidor del Sistema Gestor de Voz se conectará directamente vía LAN a través de la Red de Datos de Explotación definida en este proyecto.

6.9.3. Gestión de Enrutamiento

Las prestaciones que aportará la administración de enrutamientos será la siguiente:

- Especificación de la clase de servicio
- Asignación de reglas de marcación de salida, rutas y clases de servicio LCR para los grupos de líneas.
- Presentación de los datos de enrutamiento y número de grupos de línea.
- Definición de los patrones de marcación para las rutas LCR.
- Especificación de las bandas de tiempo.

6.9.4. Administración de alarmas

En caso de error, falta o avería, los nodos de red enviarán el correspondiente mensaje de alarmas al servicio de Administración de alarmas del Sistema Gestor de Red.

La aplicación de Administración de alarmas proporcionará la gestión gráfica de errores y alarmas con las siguientes facilidades:

- Indicación de la situación de alarma en la red.
- Localización de las instalaciones afectadas.
- Listado de alarmas existentes.
- Listado de mensajes de error.
- Información sobre el tipo de anomalía y medidas correctivas.
- Confección e impresión de informes de anomalías.

Todos los mensajes de alarma y error podrán almacenarse en ficheros de reporte.

6.9.5. Gestión de rendimiento de red

La medición de la carga de tráfico permitirá analizar los valores de carga de los enlaces que formen parte del sistema.

La medición de tráfico en el sistema permitirá evaluar las horas punta de carga para los enlaces. El sistema permitirá configurar las horas y los enlaces del sistema donde se deben realizar las medidas de tráfico.

6.9.6. Interfaz para aplicaciones de terceros (API)

El interfaz API posibilitará la conexión de aplicaciones externas.

6.9.7. Agente SNMP

El agente SNMP del Sistema Gestor de Voz será de tipo proxy, especializado en la provisión de información sobre alarmas a un sistema externo de gestión.

El agente SNMP facilitará las siguientes tareas:

- Obtención de alarmas desde la base de datos.
- Asignación de alarmas a un componente.
- Filtrado de alarmas según patrón configurado.
- Envío de alarmas al gestor, mediante primitivas SNMP.

El agente proxy facilitará la conexión del Gestor de Red de Voz con el Sistema de Gestión Integrada existente en la línea que actuará simultáneamente como gestor SNMP.

Los aspectos de comunicaciones en la interfaz se resolverán mediante la utilización de la torre de protocolos definida por Internet para Gestión SNMP (SNMP sobre UDP/IP).

El agente SNMP tendrá organizada la información de gestión en una MIB (*Management Information Base*) siguiendo la recomendación de Internet SMI (*Structure of Management Information*).

7. SISTEMA DE SUPERVISIÓN DE FIBRA ÓPTICA

7.1. INTRODUCCIÓN

En el presente apartado se describe la instalación del Sistema de Supervisión de Fibra Óptica que se encargará de la supervisión de todas las fibras de los cables de fibra óptica de la línea férrea entre Las Palmas de Gran Canaria y Maspalomas.

El Sistema de Supervisión de Fibra Óptica supervisará cada uno de los cables de fibra (96 f.o.) mediante la realización de dos tipos de medidas sobre fibras pasivas:

- Medidas de potencia sobre una fibra de cada uno de los cables.
- Medidas reflectométricas sobre otra fibra de cada uno de los cables.

7.1.1. Descripción del sistema

A lo largo del tramo objeto del presente proyecto habrá tendidos 2 cables de fibra óptica (1 cable por cada lado de vía) que será necesario controlar mediante el Sistema de Supervisión de FO. Estos cables son:

- Vía 1: Un cable de 96 fibras ópticas
- Vía 2: Un cable de 96 fibras ópticas

Está estadísticamente demostrado que la mayoría de las averías a un cable de fibra óptica inciden sobre la totalidad de las fibras de dicho cable. Por lo que a priori se puede realizar la supervisión del cable entero, en la mayor parte de las incidencias, observando el estado de una sola fibra de cada cable. Se reservarán, por tanto, fibras en cada cable destinadas en exclusiva a este servicio.

7.1.2. Medidas sobre Fibras pasivas

Estas medidas se efectuarán sobre las fibras destinadas en exclusiva al Sistema de Supervisión de Fibra Óptica. Se realizarán dos tipos de medidas:

- Medidas reflectométricas sobre una fibra de cada cable (4 medidas)
- Medidas de potencia sobre una fibra de cada cable (4 medidas)

Por medio de estas medidas será posible realizar el mantenimiento preventivo del cable al detectar posibles pérdidas de atenuación antes de que puedan afectar a los demás sistemas. De esta forma se podrían corregir a tiempo todos aquellos defectos que afecten a la totalidad del cable.

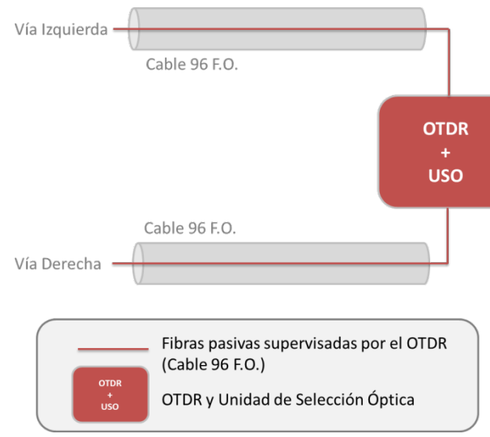
Igualmente se podrá detectar la posición exacta de una anomalía o una rotura mediante la localización a través de las medidas reflectométricas, reduciendo el tiempo medio de reparación de averías.

7.1.2.1. Medidas reflectométricas

Las medidas de los nuevos cables a supervisar se realizarán desde el OTDR.

En el caso de este proyecto, se ha proyectado instalar un OTDR en el Edificio de Gerencia con unas características que permiten realizar las medidas reflectométricas del tramo hasta Santa Catalina y del tramo hasta Meloneras, ambos de menos de 100 km de longitud.

El esquema para la realización de estas medidas se representa en la siguiente figura:



Medidas de Reflectometría

7.1.2.2. Medidas de potencia

Para efectuar las medidas de potencia será necesario iluminar las fibras con una fuente óptica. Se instalará una Unidad de Fuente Óptica (UFO) para iluminar las fibras pasivas en el tramo. Se ha proyectado instalar la UFO de la línea en el Edificio de Gerencia, salvo que Ferrocarriles de Gran Canaria determine otro lugar.

Para poder realizar las medidas de atenuación es necesaria la instalación de sondas en los extremos de los vanos que se desee medir. El siguiente esquema muestra la disposición de los equipos necesarios:

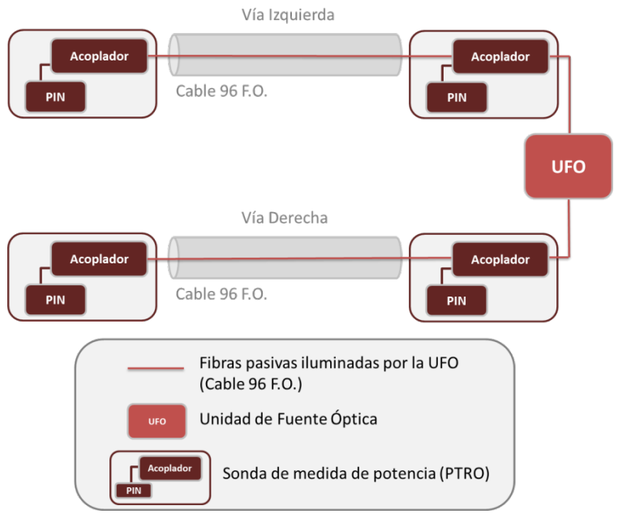


Diagrama de UFO

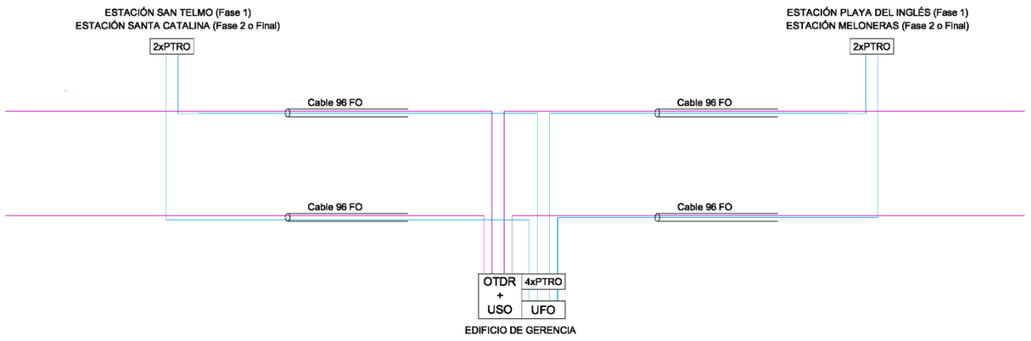
7.1.3. Arquitectura de Red

En cada punto desde el que se vayan a supervisar las fibras ópticas se colocará una Unidad Remota de Test (URT). Las funciones básicas de cada URT comprenden la medición permanente de las fibras asignadas, de acuerdo a la programación recibida, y el envío de estas medidas y los eventos necesarios al Centro de Operación y Control.

La URT puede estar compuesta por los siguientes módulos:

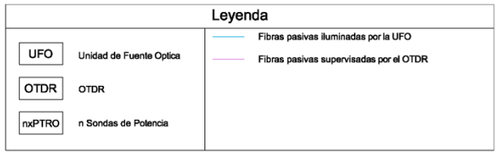
- Unidad de Control y Comunicaciones (UCC). Esta será la unidad encargada de gestionar las comunicaciones de la URT con el Centro de Control y Comunicaciones.
- Unidad de Medidas Reflectométricas (UMR). Esta unidad se compone de un OTDR por medio del cual se pueden obtener los perfiles de atenuación de la fibra a analizar, así como la localización de posibles cortes en la misma.
- Unidad de Medida de Potencia Óptica (PTRO). Estas sondas permiten la monitorización continua de la potencia óptica existente en el punto de la traza en que se sitúen, permitiendo así poder calcular la atenuación existente entre dos sondas situadas al final y al principio de cada vano.
- Unidad de Selección Óptica (USO). Esta unidad permite la selección de una fibra entre las diferentes fibras que se monitoricen en ese punto. De esta forma es posible utilizar una única UMR para monitorizar varias fibras.
- Unidad de Fuente Óptica (UFO). Por medio de ella se iluminan las fibras con una señal equivalente a la que genera un equipo de transmisión y, mediante las PTRO correspondientes, se pueden efectuar las medidas necesarias en las fibras pasivas.

La configuración específica de cada URT depende de la localización concreta de la misma.



Localización	Total Sondas Necesarias
Estación San Telmo (Fase 1)	2 (0+2)
Estación Santa Catalina (Fase 2 o Final)	2 (0+2)
Edificio de Gerencia	4 (0+4)
Estación Playa del Inglés (Fase 1)	2 (0+2)
Estación Meloneras (Fase 2 o Final)	2 (0+2)

N (n+m) -N: nº de fibras totales
-n: nº de fibras activas
-m: nº de fibras pasivas



Las unidades remotas de test de este tramo se distribuyen de la siguiente forma:

- Unidad Remota de Test para la iluminación de las fibras ópticas, las medidas reflectométricas y la medida de potencia óptica de 4 fibras pasivas en el Edificio de Gerencia. Además, en este emplazamiento se instará un OTDR y USO para iluminar fibras pasivas.

- Dos Unidades Remotas de Test para la medida de potencia óptica de 2 fibras pasivas.
  En la Fase 1, se instalará una unidad en la sala de telecomunicaciones ferroviarias de la estación de San Telmo y otra en la sala de comunicaciones de la estación de Playa del Inglés.
  En la Fase 2, o Final, se instalará una unidad en la sala de telecomunicaciones ferroviarias de la estación de Santa Catalina y otra en la sala de telecomunicaciones de la estación de Meloneras, desmontando las unidades instaladas en la respectivas salas de San Telmo y Playa del Inglés.

Todas las conexiones IP de las URT se efectuarán sobre la Red de Datos de Explotación, ya descrita en el apartado de las redes de datos.

7.2. SISTEMA DE GESTIÓN

El sistema de gestión dispone de una Unidad Central (UC) y de un Puesto de Operador (PO) desde el que se podrán supervisar, controlar y operar las URT.

La Unidad Central está basada en un servidor tipo SUN con sistema operativo Solaris (UNIX). El Puesto de Operador es un PC de tipo convencional con sistema operativo tipo Windows.

Se ha proyectado la instalación, tanto de la Unidad Central como del Puesto de Operador, en el Edificio de Gerencia, donde se instalarán la carga y configuración del software cliente necesario. El puesto de operación se conectará al servidor a través de la Red de Datos de Explotación. Será necesario obtener una licencia para este puesto.

7.2.1. Descripción funcional

Las funciones básicas del sistema de gestión son las siguientes:

7.2.1.1. Gestión de comunicaciones

Mediante esta función la UC pude comunicarse con todas URT. Parte integrada de esta función es la supervisión del latido de las unidades remotas para detectar anomalías en la red IP o en las propias URT.

7.2.1.2. Gestión de eventos

Esta función está basada en la recepción de eventos emitidos por la URT. Dichos eventos pueden ser de dos tipos:

- Eventos de fibra. Correspondientes a los elementos supervisados. A su vez estos eventos se pueden clasificar de acuerdo a su importancia de la siguiente manera:
  - Urgentes. Se producen por la superación del umbral de atenuación máxima del enlace. Indican una degradación severa o un corte con posible pérdida de servicio.
  - No urgente. Se producen por la superación del umbral que se haya establecido para detectar pequeñas degradaciones que no afecten al servicio.
- Eventos de sistema. Correspondientes a los elementos del propio sistema de supervisión. Se producen al detectar una potencia del equipo de transmisión inferior a un umbral programado, indicando una posible degradación del mismo.

La recepción de un evento implica el envío a la URT del cual procede un mensaje confirmando la recepción del mismo.

7.2.1.3. Gestión de medidas

Esta función incluye todo lo relativo al tratamiento de las medidas, tanto reflectométricas como de potencia, que realicen las URT sobre las fibras que supervisan.

Para cada fibra se mantiene un archivo con la última medida recibida de la URT. Así mismo, se dispondrá de un archivo histórico donde se almacenan, para cada fibra, las curvas reflectométricas obtenidas en diferentes instantes. A partir de estos datos se puede generar un informe con la evolución temporal y detectar degradaciones en sus características.

La presentación de las medidas reflectométricas se hará de forma gráfica, disponiendo de facilidades el usuario para calcular la atenuación entre dos puntos cualesquiera. A efectos comparativos se podrá presentar sobre la misma gráfica varias curvas de atenuación, correspondientes a una fibra, obtenidas en diferentes momentos. También se podrá utilizar el OTDR incluido en la URT como si fuera un equipo autónomo, pudiendo definir las condiciones de la medida (rango, anchura del impulso, promediado, etc.)

En el caso de medidas de potencia la representación de las mismas se hará en forma de tabla o gráfica con objeto de poder analizar la evolución temporal de los diferentes parámetros a supervisar.

7.2.1.4. Gestión de configuración

El sistema permitirá programar todos los parámetros necesarios para su operación, así como datos relevantes sobre la planta supervisada, mediante menús y formularios con objeto de facilitar al máximo las labores de los operadores.

7.2.1.5. Gestión de usuarios

El sistema permitirá establecer una estructura jerárquica de explotación basada en la asignación a cada usuario de una clave y un perfil que determine las funciones a las que pueda acceder.

En el perfil de cada usuario se definirá la funcionalidad que le está asignada así como la parte de la planta sobre la que pueda actuar dicho operador.

7.2.1.6. Gestión de tareas automáticas

El sistema podrá ser programado para realizar de forma automática, sin intervención alguna del operador, ciertas tareas de forma periódica o en determinada fecha y hora (petición de medidas, generación de informes, etc.) Como consecuencia de la ejecución de una tarea se podrán generar archivos de resultados que podrán ser consultados o borrados por los operadores.

7.2.1.7. Operación con el sistema de gestión integrada

El sistema dispondrá de un interfaz estándar de gestión que facilite su integración en sistemas TMN de jerarquía superior. Este interfaz estará basado en protocolos estándar, tales como SNMP, de forma que, a través de un agente que se ejecute en la UC, el Sistema de Gestión Integrada tenga acceso a toda la información necesaria del Sistema.

8. SISTEMA DE GESTIÓN INTEGRADA

8.1. INTRODUCCIÓN

Las redes de telecomunicaciones (fija y móvil) y los sistemas específicos asociados están constituidos por equipos de distintos proveedores y tecnologías, coincidiendo esta heterogeneidad con la mayoría de las redes privadas y públicas existentes. Los Gestores de Elementos de Red (GER) ayudan a la administración de los distintos dominios que los conforman (conmutación, transmisión, acceso, GSM-R, datos, etc.), pero únicamente en su propio ámbito tecnológico o funcional. En definitiva, cada uno de estos gestores solamente ofrece una visión parcial de la red, lo que no resuelve numerosos problemas que se plantean en la operación de una red multidominio.

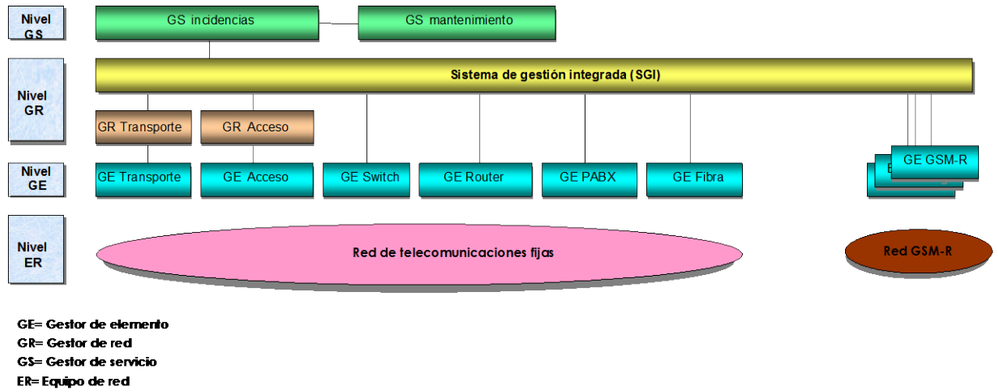
El sistema integrado ayuda a resolver estos problemas ya que permite la realización de tareas de gestión y monitorización de los diferentes sistemas de un modo centralizado y eficiente, con lo que se consigue una mayor rapidez en la detección y la solución de problemas. También permite realizar correlación de alarmas recibidas, ofreciendo al operador sólo alarmas significativas, lo que facilita el análisis del estado de la red de telecomunicaciones.

El Sistema de Gestión Integrada (SGI) es un sistema que implementa procedimientos multidominio capaces de superar la visión de las redes y sistemas como una trama de elementos individuales y de conseguir una dimensión de gestión global que permitirá un desarrollo más rápido y fiable de los procedimientos de mantenimiento que serán el soporte de los servicios.

A fecha de redacción del presente proyecto, se prevé la ubicación del CRC de línea en el Edificio de Gerencia, donde se ha proyectado la instalación de los servidores del SGI.

El Sistema de Gestión Integrada es un sistema aplicable a entornos multi-tecnología y multisuministrador, utilizándose una serie de sondas y monitores para acceder a diferentes equipos de la red y gestores. La solución es totalmente escalable y modular.

Los diferentes sistemas se integran en una arquitectura de gestión como la que se muestra en el siguiente esquema:



Arquitectura de integración general

Dentro de las actuaciones a realizar en el presente proyecto se incluye la instalación de la plataforma de Gestión Integrada de Red que permitirá gestionar todos los equipos instalados en el ámbito de la línea férrea entre Las Palmas de Gran Canaria y Maspalomas.

8.2. SOLUCIÓN PARA LA INTEGRACIÓN DE LAS ALARMAS

Se realizarán las configuraciones necesarias en la Red de Datos de Explotación y Red de Datos de Acceso para la integración del equipamiento en el Sistema de Gestión Integrada.

8.2.1. Descripción funcional

Se ha previsto la instalación del Sistema de Gestión Integrada de Red en el Edificio de Gerencia.

El sistema de fallos para la red de telecomunicaciones actual está basado en una arquitectura modular monocapa compuesta por un único núcleo central (Object Server), con clientes X11/Motif, Windows y navegadores web. Está compuesta por módulos software de la suite de productos Netcool de Micromuse perfectamente ensamblados. El sistema realiza la captura de alarmas de red, bien desde los equipos (elementos de red), bien desde los gestores de dichos equipos de la red de telecomunicaciones, procesa dicha información realizando filtrados, correlaciones y

enriquecimiento de alarmas y realiza la visualización del estado de la red en mapas, así como la redacción de informes de alarmas.

Además el sistema interacciona con sistemas externos como son el sistema Remedy de Trouble Ticketing y con la base de datos relacional asociada al módulo Reporter.

El SGI está basado en una arquitectura cliente/servidor que permite a varios usuarios acceder al sistema de manera simultánea. El gestor proporciona las siguientes funcionalidades:

- Gestión unificada. Desde una única interfaz gráfica y una única infraestructura de gestión de red se podrán realizar las tareas de gestión, posibilitando integrar aplicaciones y unificar la gestión de elementos de varios dispositivos.

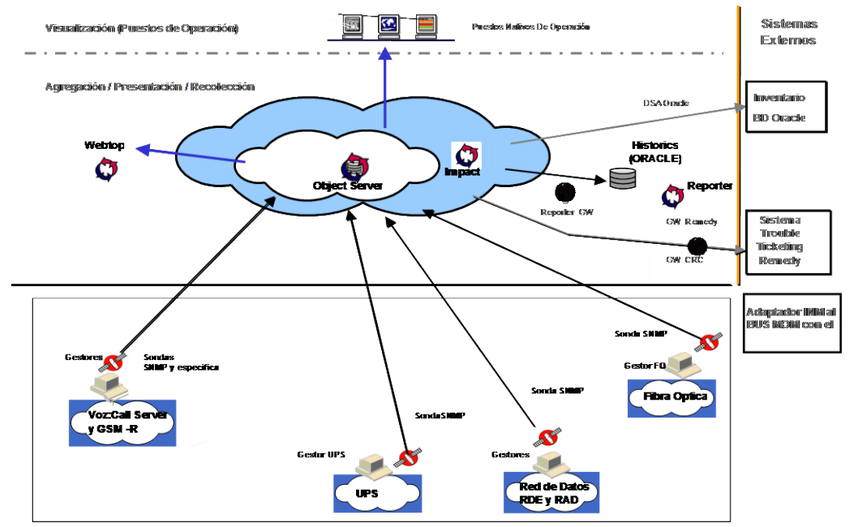
- Visibilidad de toda la red. El sistema permitirá a los administradores tener una visión completa y emitir informes detallados de la actividad de la red, con funciones como detección, mapas de topología físicos y lógicos, gestión centralizada de eventos, gráficos e información estadística.

- Gestión de elementos. Proporcionará acceso a cada uno de los dispositivos de la red a través de su gestor nativo y permitirá que todos los dispositivos de red se configuren desde una única ubicación centralizada.

- Calidad de servicio basada en políticas. Posibilitará una configuración simplificada de la calidad de servicio, lo que facilitará la gestión de las diferentes VLAN que transporte la Red de Datos de Explotación.

- Arquitectura escalable. El gestor dispondrá de una arquitectura escalable para futuras ampliaciones de la red.

En la figura siguiente se puede apreciar la arquitectura software del sistema:



Arquitectura SW del sistema de gestión integrada

Puede apreciarse que la arquitectura software es modular, con una capa funcional en la que cada módulo se encarga de realizar una función bien diferenciada. En esta capa se realiza desde la recolección, hasta la visualización y los informes, pasando por el tratamiento de las alarmas.

La recolección se realiza a través de módulos de recolección, o sondas, que recogen las alarmas de los gestores de elementos de red o de los propios elementos de red y los envían al motor del sistema para su tratamiento. Estas sondas se encargan de normalizar los eventos recolectados a un formato único común para, posteriormente, introducir los datos en el motor de la aplicación (Object Server).

Existen sondas genéricas para protocolos estándar (Generic SNMP, Syslog, TCP/IP SOCKET) o bien sondas específicas para determinados elementos (Ioo, Q3). En las sondas se puede realizar un primer filtrado de alarmas.

El motor de la aplicación está compuesto, en este caso, por un Object Server y un módulo Impact, que permiten realizar filtrado, correlación y enriquecimiento de las alarmas, así como determinar la causa-raíz de las mismas.

La visualización del estado de la red en mapas se realizará a través de un módulo WebTop de Netcool, que permitirá a los usuarios acceso web al sistema.

El sistema cuenta con un almacenamiento de datos históricos en BBDD Oracle para obtener los reports de alarmas (reports standard), utilizando el módulo *Reporter* de Netcool.

El sistema se integra con el módulo de gestión de procesos, que permite mantener el estado de los componentes de la Gestión Integrada de Red (*Objectserver*, sondas y monitores, gateways, etc.) y con el sistema de *Trouble Tickecting* (usando gateways de Netcool), para la gestión de incidencias a partir de fallos detectados en la red.

8.2.1.1. Funcionalidad del Sistema de Gestión Integrada de Fallos de Red

A continuación, se muestra una tabla con las funcionalidades que el sistema proporciona y que deberán mantenerse después de la ampliación del mismo:

FUNCIONALIDADES DEL SISTEMA		
CÓDIGO	DENOMINACIÓN	DESCRIPCIÓN
S.01	Gestión Integrada en tiempo real basado en SW de Netcool y ORACLE.	Sistema de Gestión Integrada, presenta y gestiona la información de todas las redes y servicios contemplados en tiempo real.
S.02	Multitecnología/ multisuministrador	El Sistema de Gestión Integrada propuesto permite realizar la gestión de múltiples tecnologías diferentes y con productos de distintos suministradores para cada tecnología, bajo un único Sistema.
S.03	Arquitectura modular y distribuida	Esto es posible debido a la cantidad y variedad de adaptadores o módulos software, ya desarrollados para la mayoría de suministradores y entornos, que comunican con los diferentes gestores y unifican las interfaces en un modelo único dentro del Sistema de Gestión Integrada. El Sistema permite realizar un despliegue y crecimiento funcional por módulos. Esto es posible debido a que las diferentes funcionalidades se encuentran separadas en módulos SW bien diferenciados, permitiendo adaptar el Sistema en cada caso a diferentes modelos por capas funcionales, según el modelo de Organización requerido por el Cliente. Además, esta característica permite la agrupación de los elementos de la red en dominios de operación, en función de las necesidades operativas. En cuanto a los dominios de operación se puede disponer de una división bidimensional por dominios geográficos (todo el país, región, distrito) y por dominios técnicos (red de conmutación, de transmisión,...). El Sistema corre sobre un HW distribuido, hallándose por separado el Servidor de la Base de Datos y el SW del propio Sistema de Gestión.

FUNCIONALIDADES DEL SISTEMA		
CÓDIGO	DENOMINACIÓN	DESCRIPCIÓN
S.04	Escalabilidad	El Sistema puede ir adaptándose al crecimiento paulatino de la red gestionada con la simple adición de elementos HW y SW y configurando el sistema. Permite arquitectura Multi-Capas, pudiendo organizar y redimensionar los sistemas para gestionar un mayor número de redes, sin poner en riesgo el rendimiento del sistema.
S.05	Seguridad	El Sistema ofrece: • Control del acceso al Sistema. • Control de perfiles de usuario: los usuarios se encuadran en grupos de usuarios que tienen un rol y/o un perfil de acceso determinados. • Control de acceso a la red y a su funcionalidad atendiendo al perfil del usuario del Sistema.
S.06	HW estándar	Los componentes software del sistema corren sobre plataformas basadas en hardware estándar de los principales fabricantes. Esto asegura la disponibilidad de elementos para su crecimiento, mantenimiento y la facilidad de usar sistemas operativos de mercado.

FUNCIONALIDADES DE INTERFAZ DE USUARIO		
CÓDIGO	DENOMINACIÓN	DESCRIPCIÓN
IU.01	Posibilidad de acceso y gestión del Sistema vía WEB	El acceso al sistema puede realizarse vía *web*, con el componente Netcool / Webtop. Este extiende las capacidades del Netcool nativo, permitiendo a los usuarios gestionar su Sistema Netcool desde cualquier visualizador *web* Java.
IU.02	Representación gráfica de la red en mapas	Visibilidad completa de la topología de red y de los eventos en mapas que muestran además la conectividad física y lógica de la red, siempre que el Gestor de Red específico lo ofrezca, y permiten navegar desde el más alto nivel hasta el nivel de componente de elementos mediante *clicks* de ratón.
IU.03	Presentación gráfica unificada de alarmas	A partir de la inclusión de las alarmas procedentes de los diferentes Sistemas gestionados en un único modelo y la asignación de diferentes grados de severidad de dichas alarmas, utilizando códigos coloreados, se consigue una representación gráfica de alarmas con un mismo aspecto y con información estandarizada.
IU.04	Presentación de informes	El sistema proporciona información elaborada (estadísticas, históricos,…) en forma de informes adaptándose a los requerimientos del Cliente.

FUNCIONALIDADES DE INTERFACES EXTERNOS DEL SISTEMA		
CÓDIGO	DENOMINACIÓN	DESCRIPCIÓN
IE.01	Con redes varias	El Sistema dispone de una gran variedad de interfaces o sondas que le permiten “hablar” con los diferentes dispositivos de los principales suministradores de telecomunicaciones e IT. Se trata de agentes que colectan eventos procedentes de más de 1.000 dispositivos de diferentes fabricantes y tecnologías. En concreto proporciona interfaces con: – Red IP – Red de Servidores – Servidores de servicios de Internet Sistema de Gestión del cableado……
IE.02	Con BBDD Oracle	El Sistema interacciona con la base de datos de Oracle donde residen los datos: de “Inventario” (provisión, clientes y servicios); los ficheros de “Históricos de alarmas”; y de dónde se obtienen los datos para elaborar diferentes informes y para el enriquecimiento de las alarmas.
IE.03	Trouble Ticketing	El Sistema tiene la capacidad de realizar la apertura de tickets de problemas en el Sistema de *Trouble Ticketing* (*Remedy*) a partir de la información sobre las alarmas recibidas de la red, comunicándolo inmediatamente al *Helpdesk* (personal de Mantenimiento). Soporta la integración con *Remedy* a través del

FUNCIONALIDADES DE INTERFACES EXTERNOS DEL SISTEMA		
CÓDIGO	DENOMINACIÓN	DESCRIPCIÓN
		Gateway específico ya desarrollado a tal efecto.
IE.04	Con el CRC	El sistema permite el envío tanto de las alarmas generadas por el Sistema de Gestión Integrada como de la topología de las redes gestionadas por ella. La información se envía desde el ObjectServer, mediante un adaptador INM, a través de un bus MOM (sistema de mensajería asíncrono) para su consumo por otras aplicaciones del CRC conectadas a dicho bus. Entre estas aplicaciones se encuentra la BDTR (Base de datos de tiempo real) para el almacenamiento histórico de la gestión de redes, el GIA (Gestión Integrada de Alarmas), para mostrar las alarmas de Telecomunicaciones integradas con el resto de alarmas de los sistemas, etc.

FUNCIONALIDADES DE TRATAMIENTO DE ALARMAS		
CÓDIGO	DENOMINACIÓN	DESCRIPCIÓN
A.01	Recolección de alarmas	A través de las sondas y monitores (SNMP, Ioo, Syslog) se capturan los eventos producidos en los elementos de las diferentes redes.

FUNCIONALIDADES DE TRATAMIENTO DE ALARMAS		
CÓDIGO	DENOMINACIÓN	DESCRIPCIÓN
A.02	Modelo único	A pesar de la variedad de tipos de red a supervisar, el Sistema proporciona un modelo único de tratamiento así como de almacenamiento en la base de datos en la que se recogen las alarmas históricas. Y proporciona las funciones básicas de manipulación de todas las alarmas de las diferentes redes. Se contemplan tanto alarmas de red como alarmas en Servicios.
A.03	Enriquecimiento de alarmas	Bien en los datos almacenados en la base de datos, o bien a partir de ficheros importados, el Sistema proporciona, en algunos casos, información adicional aclaratoria de los eventos producidos, o bien información de acciones a realizar ante determinados eventos como ayuda a la operación.
A.04	Filtrado de alarmas	Las sondas proporcionan módulos de filtrado de alarmas que reducen el número de las mismas a gestionar, facilitando así la labor de operación. Entre otros, se pueden destacar los siguientes filtros de alarmas de red: – Filtro de avalancha – Filtro de duplicación – Filtro de tiempo de activación/ desactivación
A.05	Correlaciones y análisis causa-raíz	A partir de un modelo de datos de la red y de los servicios (las relaciones entre los elementos que conforman la red y las relaciones con los servicios y clientes), el Sistema realiza correlaciones de alarmas previamente programadas en reglas de correlación y además realiza análisis de la causa raíz de las alarmas.
A.06	Alarmas históricas	Existe un almacenamiento histórico de las alarmas producidas en el Sistema, a fin de realizar consultas sobre las mismas, obtener informes de estadísticas y comportamiento de la red.
A.07	Gestión de alarmas por operador	El Sistema permite la asignación de las alarmas a un determinado Operador, atendiendo a una serie de criterios definidos de acuerdo a las necesidades del Cliente. El Sistema permite el reconocimiento de las alarmas, el cambio de criticidad de las mismas, la asignación por parte del operador.

FUNCIONALIDADES DE MAPAS DE RED		
CÓDIGO	DENOMINACIÓN	DESCRIPCIÓN
MR.01	Fondos	El Sistema permite importar fondos sobre los cuáles se plasman las diferentes arquitecturas de red, según los requerimientos del cliente (mapas

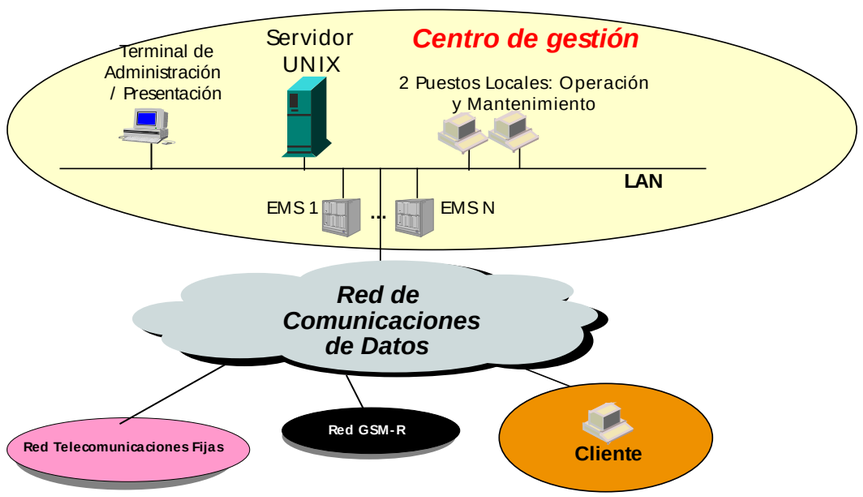
FUNCIONALIDADES DE MAPAS DE RED		
CÓDIGO	DENOMINACIÓN	DESCRIPCIÓN
		geográficos, plantas de edificios,....)
MR.02	Varios niveles y navegación	El Sistema permite representar las redes en varios niveles de modo que mediante clicks sucesivos se van desplegando los diferentes niveles de elementos, desde las redes backbone hasta los componentes de un determinado equipo.
MR.03	Representación de nodos y enlaces animados	Se pueden asignar colores a los nodos de la red de modo que, según el estado de alarma o no alarma en que se encuentren, cambien de color. Asignación de colores según criticidad.
MR.04	Navegación de gestores	Desde el Sistema de Gestión Integrada se puede navegar hasta los gestores de red y de elementos de las diferentes redes gestionadas.

FUNCIONALIDADES DE INFORMES		
CÓDIGO	DENOMINACIÓN	DESCRIPCIÓN
I.01	Estadísticas de alarmas	El SW básico del Sistema permite la obtención de informes de alarmas a partir de la información recibida. El sistema captura, almacena y analiza los datos de los eventos mostrándolos en distintos informes al operador, y ayudándole a interpretar los

FUNCIONALIDADES DE INFORMES		
CÓDIGO	DENOMINACIÓN	DESCRIPCIÓN
		fallos ocurridos en la red. Permite un vistazo rápido de las alarmas, agrupadas según características (por nodo, por gestor, por nodo y severidad, etc.)
I.02	Informes de Servicios	Permiten centrarse en el comportamiento de áreas de rendimiento operativo claves que pueden interesar a los responsables de red. Además les permiten profundizar en el comportamiento de áreas conflictivas de la red.
I.03	Informes de Histórico de Alarmas	El módulo de gestión de informes realiza la función de gestor de alarmas históricas del sistema, al tener almacenadas en la base de datos todas las alarmas.
I.04	Informes complejos a medida	El Sistema permite diseñar y obtener informes adicionales con más complejidad que los básicos, a la medida de las necesidades del Cliente, y además accesibles vía Web. Por ejemplo informes estadísticos orientados a la operación.
I.05	Exportado de Informes	Se van a poder exportar los informes activándolos en diferentes formatos (Excel, PDF, HTML)

8.2.2. Arquitectura del Centro de Control

En la figura siguiente, se muestra una vista general del centro de gestión integrada, donde puede observarse que se trata de un sistema abierto cliente/servidor:



Visión General del Centro de Gestión Integrada

En el servidor se encuentran instalados, tanto la base de datos, como los módulos funcionales de la aplicación. Existen puestos locales de operación o bien puestos remotos, que acceden vía web a través de la Red de Datos.

Tanto el servidor como los puestos locales se encuentran conectados a una misma LAN del centro de control.

El sistema cuenta, asimismo, con un puesto de administración para realizar labores de administración.

8.2.3. Situación Definitiva

Los sistemas y redes a integrar en el SGI son los siguientes:

- Red de Datos de Explotación (RDE)
- Red de Acceso de Datos (RAD)
- Red Unificada de Señalización y Detectores (RUSD)
- Red de acceso VCA
- Red de Telefonía Fija
- Red de GSM-R
- Red de Fibra Óptica
- Energía (UPS)
- Firewalls (tanto en lo referente a alarmas de los propios equipos como a alarmas generadas por eventos producidos en la aplicación de las políticas definidas)
- Sistema de Control de Acceso a las Redes de Datos (tanto en lo referente a alarmas de los propios equipos como a alarmas generadas por eventos producidos en el control de accesos a la red)

La integración permitirá ver la nueva red en un entorno común, pero con dominios separados si así se requiriese. La funcionalidad del sistema, para esta nueva red, será la misma que para la red gestionada actualmente.

Las tareas a realizar en el entorno Netcool serán las siguientes:

- Suministro y configuración de las sondas de recolección de alarmas necesarias

- Parametrización de las sondas de recolección de alarmas o eventos de las nuevas tecnologías, bien desde los gestores de las mismas, o bien desde los propios elementos de red (mediante sondas genéricas).
- Los trabajos en el motor del Sistema de Gestión Integrada serán:
  - Implementación de reglas de filtrado.
  - Implementación de reglas de correlación, enriquecimiento de alarmas y causa-raíz (Impact).
  - Mapas de alarmas y parametrización de las sondas (Object Server).
  - Generación de históricos de alarmas.
  - Generación de informes históricos de alarmas.
- El interfaz con Remedy.
- El interfaz con Inventario.
- El interfaz con CRC.

9. SEGURIDAD Y CONTROL DEL ACCESO A LA RED

9.1. ALCANCE

Con el objeto de dotar a las redes de datos IP de un sistema de control de acceso a dichas redes, se incluye dentro del alcance de este proyecto el sistema de control de acceso a la red y la puesta en servicio de toda la solución de control de acceso a las redes de datos de la línea ferroviaria entre Las Palmas de Gran Canaria y Maspalomas.

El sistema de control de acceso deberá venir con todas las licencias necesarias para proporcionar las siguientes funcionalidades, que deberán implementarse para todas las redes de datos de la línea:

- Detectar e identificar nuevos usuarios y dispositivos en la red de forma automática.
- Autenticar los sistemas finales.
- Analizar los sistemas finales para determinar el cumplimiento de las políticas de seguridad de la empresa (sistema operativo, anti-virus, etc.)
- Autorizar el uso de la red a los sistemas finales que cumplan las políticas específicas de seguridad definidas, asignándoles una VLAN, una QoS y hasta un conjunto de ACL de acuerdo a su perfil.
- Aplicar políticas de cuarentena y remediación para aquellos dispositivos que no hayan superado las políticas de seguridad.
- Monitorizar el tráfico y realizar un análisis post-conexión para auditar si los criterios y las políticas de uso de la red se cumplen una vez autorizado el acceso y revocar la autorización si no se mantienen. Permitirá controlar en tiempo real cualquier evento de seguridad que se genere en las redes.

9.1.1. Introducción

La importancia de establecer mecanismos de seguridad en cuanto al acceso de los equipos se ha convertido en una necesidad primordial. Los mecanismos de protección existentes en las redes de transmisión para asegurar las comunicaciones entre emplazamientos, como son las configuraciones en anillo, generando rutas de backup en redes de conmutación de paquetes, etc., debe ser complementado con un control de quien se conecta a la red, si se puede conectar a la misma y que perfiles de usuario se les va a conceder para establecer su comunicación.

Se debe desarrollar un procedimiento operativo que permita establecer una conexión segura y eficaz. A lo largo de este capítulo se describen las diferentes fases que deben implementarse en este procedimiento de actuación, resumiéndose a continuación:

- IDENTIFICACIÓN DE USUARIOS Y DISPOSITIVOS

  Para ello el usuario o equipo que quiera acceder a la red debe iniciar un proceso de autenticación a través de:

  – IEEE 802.1x: "*Port Based Network Access Control*". El usuario que disponga de este protocolo se puede autenticar mediante nombre de usuario y contraseña. Todos los PC´s de la línea tanto fijos como portátiles deben soportar 802.1x. Se debe realizar un registro previo en el servidor AAA (*Authentication, Authorization, Accounting*) basado en un servidor estándar RADIUS.

  – MAC Address: Este mecanismo está basado en un proceso de autenticación a través de la dirección MAC del equipo. Va dirigido hacia aquellos dispositivos que no disponen de usuario para autenticarse, como puede ser una cámara de videovigilancia o un enclavamiento. Es necesario un gestor de MAC paralelo al servidor RADIUS dónde las direcciones sean previamente registradas para que puedan ser validadas.

  – Acceso Web: Para usuarios que no tengan acceso directo a la red y necesitan realizar tareas de gestión desde un puesto remoto, existe la posibilidad de ser autenticado mediante un nombre usuario y contraseña utilizando el navegador Web y un acceso a Internet.

Igualmente que en los casos anteriores, se necesita un registro previo de los usuarios potenciales.

- Otro sistema a indicar por el licitador en su oferta.

- ACTIVACIÓN O DENEGACIÓN DEL ACCESO

  El usuario o dispositivo, mediante protocolo EAP (*Extensible Authentication Protocol*), envía sus credenciales encriptadas al dispositivo de acceso a la red, el cual redirige la petición al servidor RADIUS mediante protocolo RADIUS. Este servidor comprueba que la información es correcta mediante esquema de autenticación. Para ello comprueba un archivo de texto propio (base de datos local) o consulta una base de datos externa mediante protocolo LDAP (*Lightweigth Directory Access Protocol*). Es recomendable hacer coincidir las credenciales de acceso al sistema operativo con el nombre de usuario y contraseña solicitado en suplicantes 802.1x. Para ello el servidor RADIUS usa LDAP para consultar la autenticación. En este archivo de texto o base de datos deben estar almacenados todos los nombres de usuarios y contraseñas, y debe tener asociado un gestor MAC de dispositivos que tengan permiso de acceder a la red, para el caso de autenticación basada en MAC.

  En base a estas comprobaciones se envía un mensaje al equipo de acceso para permitir o denegar el acceso, constituyendo el mecanismo de autorización.

  Por último se debe realizar un proceso de *accounting* con el fin de registrar en un archivo quién, dónde y a qué hora cada usuario ha accedido a la red.

- LIMITACIÓN DE CAPACIDADES A USUARIOS PERMITIDOS

  Tan importante resulta que un usuario no permitido no acceda a la red, como que aquellos que si lo son no colapsen los recursos de tráfico. Para ello se define un sistema basado en políticas y perfiles de usuario de manera dinámica, lo cual nos permite asignar diferentes calidades de servicio en función de las características del usuario o dispositivo que quiere acceder.

  Estas políticas podrán residir en los equipos de acceso a la red y se deberán actualizar de manera periódica, o bien se producirá una consulta al gestor de políticas cada vez que se autentique el usuario, con el fin de descargarse la política particularizada. En función de las indicaciones de validación y perfil realizadas desde el servidor RADIUS, se asignan unas limitaciones de capacidad de los usuarios autorizados mediante mecanismos como:

  - Asignación de VLAN. Así las cámaras pertenecerán a un grupo de usuarios, los equipos de enclavamiento a otro, etc.

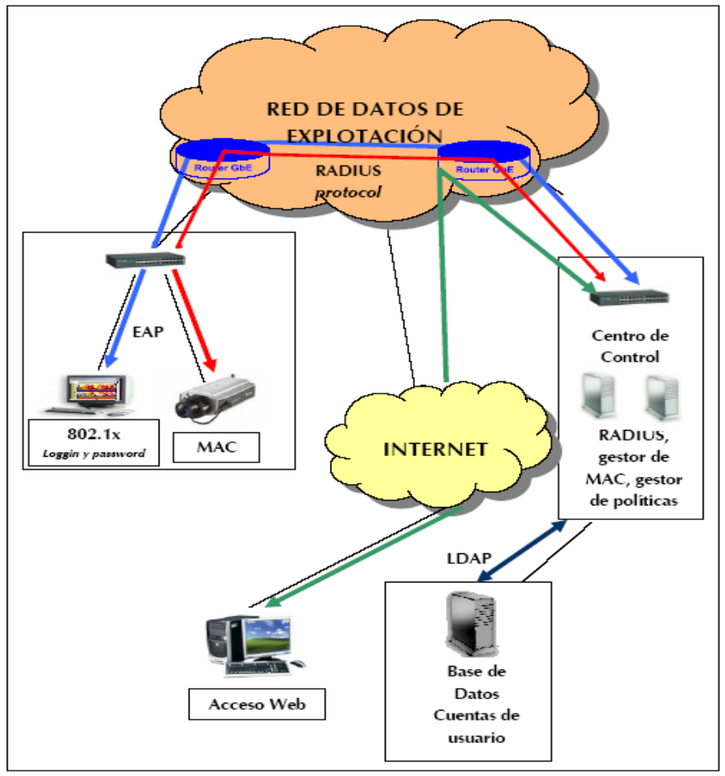
  - *Rate Limit* por VLAN. La limitación del ancho de banda a la que determinados usuarios pueden transmitir resulta clave para evitar un consumo excesivo de los recursos de la red. Por ejemplo, esto resulta muy útil para la VLAN de cámaras, de tal manera que limitemos el ancho de banda del grupo y así se vean obligadas a adaptar su transmisión a los recursos de los que disponen.

Los usuarios denegados en su intento de acceso a la red deberán registrarse previamente en la base de datos de usuarios. Esto exige una importante labor de formación hacia todos los usuarios de la red, haciéndoles conocedores que sus equipos no funcionarán si no realizan esa labor previa de registro. Un caso muy importante y crítico aparece con los dispositivos de repuesto y mantenimiento; si un equipo no funciona y se decide sustituir por uno nuevo, no funcionará simplemente con conectarlo al equipo de acceso a la red. Será preciso que la dirección MAC del dispositivo se registre en la base de datos del gestor, con el fin de que supere el proceso de autenticación.

9.1.2. Procedimiento operativo de acceso a la red

El proceso de acceso a la red de debe seguir unas fases bien definidas que se describen a continuación. Son secuenciales e imperativas, de tal manera que no superar alguna de ellas implica no tener permiso de acceso a la red.

La figura siguiente refleja los flujos de información con los cuales opera este procedimiento.



Procedimiento operativo de Control de Accesos

El procedimiento operativo consta de tres fases bien diferenciadas denominadas AAA:

- Autenticación: Proceso de intento de verificación de la identidad del remitente de una comunicación con una petición para conectarse. El remitente puede ser un usuario con un dispositivo o el propio dispositivo. (Ver punto 2.1 Identificación de usuarios y dispositivos).

- Autorización: Proceso por el cual la red de comunicaciones de datos autoriza al usuario identificado a acceder a determinados recursos de la misma. Es importante que los recursos de tráfico estén bien definidos y delimitados para que no existan interferencias entre servicios. (Ver puntos 2.2 Validación o denegación del servicio y 2.3 Limitaciones de capacidades y perfiles de usuario).

- Auditoría o *Accounting*: Mediante la cual la red registra todos y cada uno de los accesos a los recursos que realizan los usuarios autorizados o no. Así se puede realizar una trazabilidad de la actividad del usuario. (Ver punto 2.2 Validación o denegación del servicio).

Todos los elementos del procedimiento operativo de autenticación deben ser gestionados mediante SNMP versión 3.

9.1.2.1. Identificación de usuarios y dispositivos

Los switches n3 distribuidos a lo largo de la línea constituyendo el nivel de acceso de la red de comunicaciones, deben tener la capacidad por puerto de poder realizar peticiones de autenticación mediante:

- IEEE 802.1x: Permite la autenticación de dispositivos conectados a un puerto del equipo de datos que soporte la red LAN del emplazamiento, estableciendo una conexión punto a punto. 802.1x también es conocido como EAPOL (EAP sobre LAN).

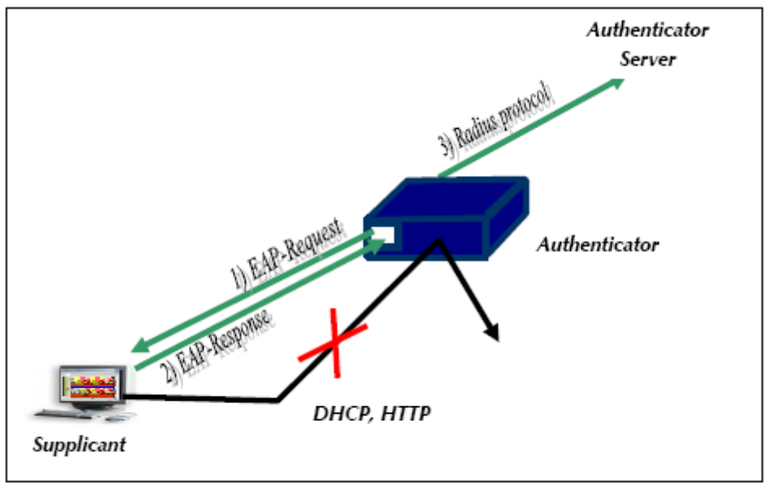
En este proceso de autenticación participan:

- Supplicant: es el dispositivo usuario que quiere acceder a la red, el cual inserta mediante un EAP-Response su nombre de usuario y contraseña para poder acceder a los recursos de la red.

- Authenticator: el equipo de datos que supone la barrera de entrada para el dispositivo y que no permite su acceso a la red hasta que la identidad del dispositivo sea autorizada. Para ello solicita los credenciales al dispositivo mediante un EAP-Request y se los reenvía al servidor.

Es importante determinar que los puertos del switch, mientras se esté realizando el proceso de autenticación, deben bloquear todo el tráfico excepto el proveniente de 802.1x.

Esta operativa queda plasmada en la siguiente ilustración:



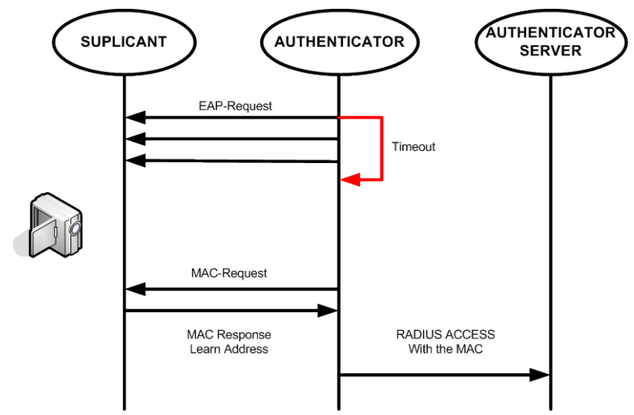
Identificación de usuario

Cuando el usuario se desconecte, envía un mensaje *EAP-loggoff* al equipo de datos y el puerto queda no autorizado, de tal forma que el nuevo equipo que se conecte en el mismo deba realizar de nuevo el procedimiento. Se aplica lo descrito en la RFC 3576 "*Dynamic Authorization Extensions to RADIUS*" para el procedimiento de autenticación de usuarios.

- Filtrado de direcciones MAC: aquellos dispositivos que no dispongan de usuario, como son las cámaras, enclavamientos, etc., deberán identificarse mediante su dirección física MAC, la cual debe estar previamente registrada en el servidor. Esto implica un mantenimiento de la base de datos del gestor de MAC con todas las direcciones actualizadas. Esta dirección está representada por 12 dígitos en formato hexadecimal dividida en grupos de dos dígitos separados por guiones.

- Acceso mediante Portal WEB: existen usuarios remotos los cuales no tienen acceso directo a la red de comunicaciones, y mediante navegador WEB, introducen su nombre de usuario y contraseña. Una vez que alcanzan el *authenticator*, el proceso es igual al descrito anteriormente

Los mecanismos de autenticación citados deben estar implementados en todos los puertos del equipo de datos. Si es un usuario quien intenta acceder a la red, se le solicitará su nombre de usuario y contraseña; si es un dispositivo, su dirección física MAC.



Autenticación por MAC

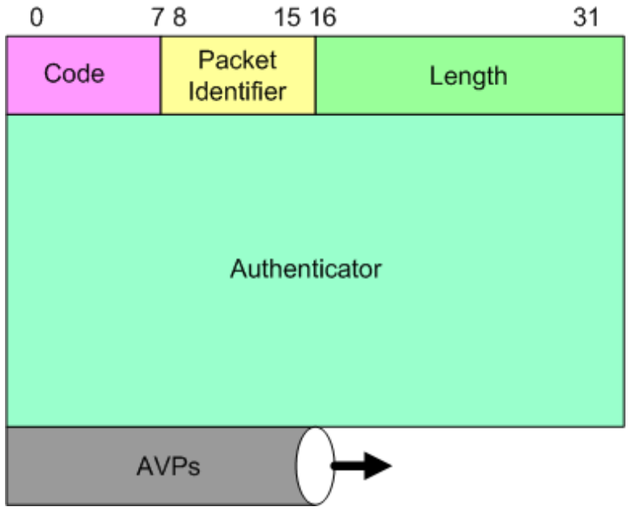
9.1.2.2. Validación o denegación del acceso

Para completar el proceso de autenticación, existe un tercer elemento que se encarga del proceso de autorización:

- *Authenticator Server*: servidor RADIUS que realiza la comprobación de la validez de la identidad, y le envía un mensaje al authenticator para habilitar o no el puerto. Para establecer esta comunicación se establece el protocolo RADIUS (definido por la RFC 2865 "*Remote Authentication Dial-in User Service* (RADIUS)" y la RFC 2866 "*RADIUS Accounting*").

El proceso de autenticación de usuarios IEEE 802.1x sobre protocolo RADIUS, se soporta sobre la RFC 3580.

Los mensajes RADIUS son enviados como mensajes UDP (*User Datagram Protocol*). Estos mensajes UDP tienen encapsulados paquetes RADIUS con la siguiente estructura:



Paquete RADIUS

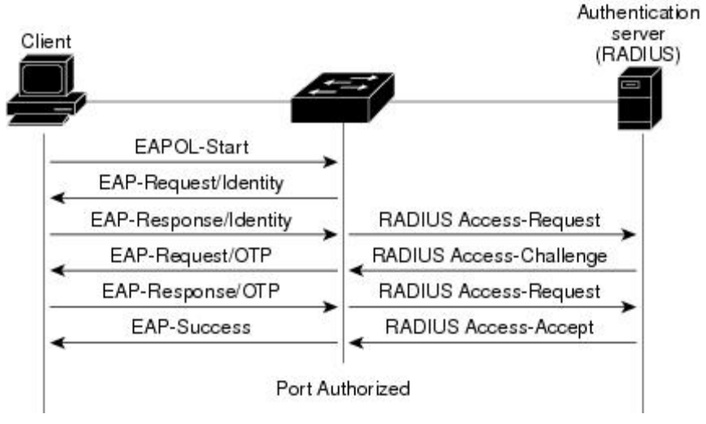
Los campos del paquete RADIUS son:

- *Code*: Octeto que contiene el tipo de paquete.
- *Packet Identifier*: Octeto que permite al cliente RADIUS relacionar una respuesta RADIUS con la solicitud adecuada.
- *Length*: Longitud del paquete (2 octetos).
- *Authenticator*: Valor usado para autenticar la respuesta del servidor RADIUS. Es usado en el algoritmo de encubrimiento de la contraseña.
- AVP: Aquí se almacenan un número arbitrario de atributos. Los únicos atributos obligatorios son el *User name* y el *user password*.

En los documentos RFC 2865 y 2866 se definen los siguientes tipos de mensajes RADIUS:

- *Access-Request* (solicitud de acceso): Enviado por un cliente RADIUS (*Authenticator*) para solicitar autenticación y autorización de un intento de conexión (*Supplicant*).
- *Access-Accept* (aceptación de acceso): Enviado por un servidor RADIUS (*Authenticator Server*) como respuesta a un mensaje *Access-Request*. En él se informa al cliente RADIUS de que se ha autenticado y autorizado el intento de conexión.
- *Access-Reject* (rechazo de acceso): Enviado por un servidor RADIUS como respuesta a un mensaje *Access-Request*. En él se informa al cliente RADIUS de que se ha rechazado el intento de conexión. Un servidor RADIUS envía este mensaje si las credenciales no son auténticas o si no se ha autorizado el intento de conexión.
- *Access-Challenge* (desafío de acceso): Enviado por un servidor RADIUS como respuesta a un mensaje *Access-Request*. Este mensaje es un desafío al cliente RADIUS que exige una respuesta.
- *Accounting-Request* (solicitud de administración de cuentas): Enviado por un cliente RADIUS para especificar información de administración de cuentas de una conexión que se ha aceptado.
- *Accounting-Response* (respuesta de administración de cuentas): Enviado por el servidor RADIUS como respuesta a un mensaje de Solicitud de administración de cuentas. En este mensaje se confirman la recepción y el procesamiento correctos del mensaje de Solicitud de administración de cuentas.

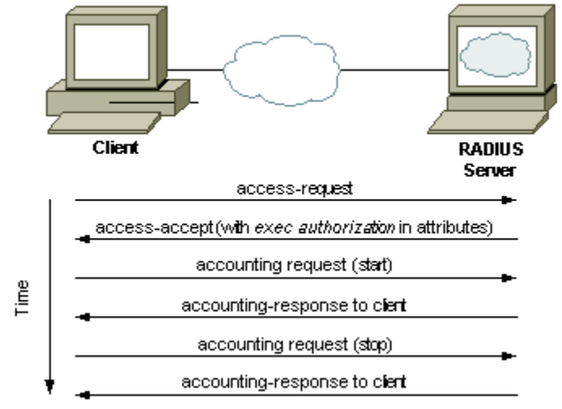
A continuación se muestra un esquema de cómo se lleva a cabo el proceso de validación de un puerto. Una vez que se haya validado, se permitirá el tráfico DHCP para asignar una dirección IP al dispositivo.



Para el caso en el cual el usuario no sea autorizado, el mecanismo es el mismo, con la diferencia que el servidor enviará un mensaje *RADIUS-access-reject* al equipo de datos, y éste inhabilitará el puerto denegando el acceso.

El sistema debe ser capaz de forma paralela de realizar tareas de *accounting* para registrar todas las entradas al sistema y poder conocer quién, dónde y cuándo se producen los accesos a la red.

El siguiente diagrama muestra la secuencia seguida cuando un cliente accede a la red y es autorizado (fase 1 y 2, ya descrito anteriormente), cuando inicia el proceso de *accounting* (fase 3 y 4), y finalmente cuando finaliza su acceso.



La secuencia de comandos es la siguiente:

1. El cliente envía su nombre de usuario y contraseña, esta información es encriptada con una clave secreta y enviada en un *Access-Request* al servidor RADIUS (Fase de Autenticación)

2. Cuando la relación Usuario/Contraseña es correcta, el servidor envía un mensaje de aceptación, *Access-Accept* con información extra (por ejemplo: dirección IP, máscara de Red, tiempo de sesión permitido, etc…, valores de perfil de usuario) (Fase de Autorización). Para comprobar si los datos son correctos consulta una base de datos local o un directorio de usuarios LDAP.

3. El cliente a continuación envía un mensaje de *Accounting-Request* (Start) con la información correspondiente a su cuenta y para indicar que el usuario está reconocido en la red (Fase de *Accounting*).

4. El servidor RADIUS responde a un mensaje *Accounting-Response*, cuando la información de la cuenta es almacenada.

5. Cuando el usuario ha sido identificado, éste puede acceder a los servicios proporcionados. Finalmente, cuando desee desconectarse, enviará un mensaje de *Accounting-Request* (Stop) con la siguiente información:
    - Delay time. Tiempo que el cliente lleva tratando de enviar el mensaje.
    - Input Octets. Número de octetos recibidos por el usuario.
    - Ouput Octets. Número de octetos enviados por el usuario.
    - Session time. Número de segundos que el usuario ha estado conectado.
    - Input Packets. Cantidad de paquetes recibidos por el usuario.
    - Output Packets. Cantidad de paquetes enviados por el usuario.
    - Reason. Razón por la que el usuario se desconecta de la red.
6. El servidor RADIUS responde con un mensaje de *Accounting-Response* cuando la información de cuenta es almacenada.

9.1.2.3. Limitación de capacidades y perfiles de usuario

Limitar los recursos de red que un usuario y/o dispositivo puede utilizar, una vez superado el proceso de autenticación y estando autorizado por parte del *Authenticator Server*, es una tarea imprescindible para satisfacer el óptimo rendimiento de la red. Así evitaremos circunstancias indeseables como el abuso de ancho de banda por parte de un tipo de usuario, que pueda denegar o empobrecer otros servicios simultáneos más críticos para la explotación ferroviaria.

El mecanismo que se implementa es la aplicación de políticas en los switches n3 de acceso basándose en la asignación de VLAN por perfil de usuario. Cuando el servidor RADIUS compruebe que los datos enviados son correctos, enviará un mensaje al switch para habilitar el puerto, y además le indicará la VLAN a la que pertenece el usuario y/o dispositivo. Estos datos deben estar previamente registrados en la base de datos a la cual consulta el servidor, con una relación entre nombre de usuario/contraseña o MAC y VLAN asignada. El switch debe soportar protocolo IEEE 802.1q (Virtual VLANs) para el desarrollo de las redes privadas virtuales.

Por dirección MAC

La base de datos consultada por el *Authenticator Server RADIUS* o por el gestor de MAC, tendrá una relación entre las direcciones MAC autorizadas y la VLAN a la que pertenecen.

Las ventajas que presenta este mecanismo de asignación de recursos de tráfico son:

- Facilidad de movimientos: No es necesario en caso de que una terminal de trabajo cambie de lugar la reconfiguración del switch.
- Multiprotocolo.
- Se pueden tener miembros en varias VLANs.

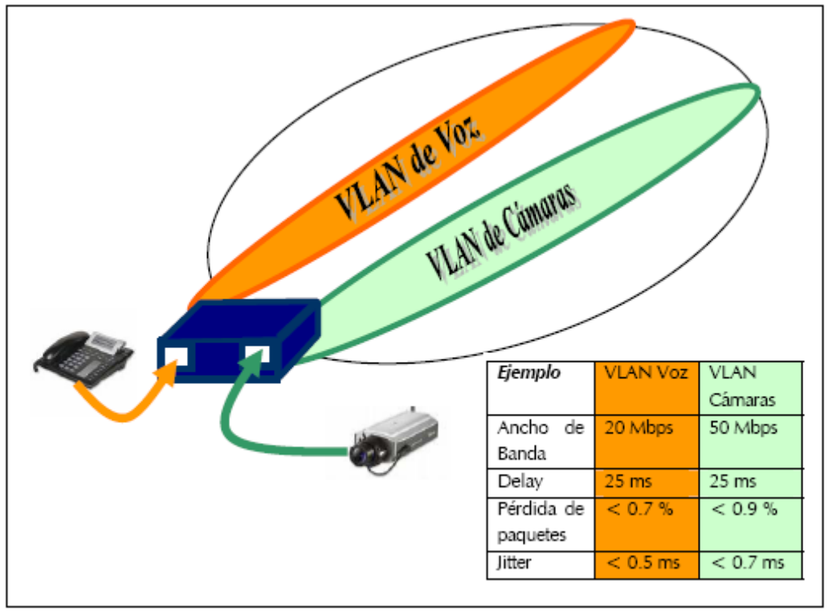
Por nombre de usuario

Se basan en la autenticación del usuario y no por las direcciones MAC de los dispositivos. VLAN 1 pertenece a personal de gestión y VLAN 2 a personal de mantenimiento.

Las ventajas que presenta este método son:

- Facilidad de movimiento de los integrantes de la VLAN.
- Multiprotocolo.

Una vez que el switch ha asignado una VLAN al equipo que quiere acceder a la red, debe ofrecer un ancho de banda límite (*Rate Limit*), que no impida o dificulte la transmisión de otros dispositivos pertenecientes a otras VLAN.



Asignación de VLAN

Las ventajas que nos ofrece en general la creación de VLAN son:

- Reducción en el tráfico de la red ya que solo se transmiten los paquetes a los dispositivos que estén incluidos dentro del dominio de cada VLAN.
- Mejor utilización del ancho de banda.
- Confidencialidad respecto a personas ajenas a la VLAN.
- Alta performance en servicios.
- Reducción de latencia.
- Facilidad para armar grupos y aislar tráfico.

9.1.3. Gestor de seguridad y control de accesos

El Gestor de Seguridad representa una solución centralizada en el CRC del Edificio de Gerencia.

Se encargará de gestionar y desplegar las políticas en la red, previo proceso de autenticación de los usuarios y/o dispositivos. Será necesario definir estas políticas de acuerdo a los perfiles de usuario que vayan a utilizar los recursos de la red.

El Gestor de Seguridad tendrá que trabajar coordinadamente con el gestor de los equipos de datos, en plataformas independientes o de manera integrada. El objetivo es definir estados de puertos, configuraciones, etc. sobre un switch, en función del proceso de autenticación que un usuario haya realizado sobre ese equipo.

9.1.3.1. Servidor Radius

Debe ser capaz de trabajar con los equipos de acceso proyectados para la línea y futuros, soportando una arquitectura multifabricante. Este servidor Radius podrá estar integrado con el gestor de políticas.

El servidor Radius es el encargado de procesar los mensajes de autenticación que se establecen entre el *Suplicant* (usuario que quiere entrar en la red), el *Authenticator* (switch n2/n3 que representa el punto de acceso) y el *Authenticator Server* (servidor encargado de gestionar y validar los accesos).

Para ello debe tener capacidad de manejar protocolos como RADIUS y EAP en sus diferentes versiones, EAP- MD5 (RFC 3748), EAP-TLS (RFC2716), EAP-TTLS, etc. Las peticiones de acceso y las credenciales enviadas deben ir encriptadas para evitar usos fraudulentos con mecanismos de sniffing.

Asimismo establecerá los procesos de *accounting* para llevar un control de la actividad realizada por los diferentes usuarios y dispositivos.

El servidor recibirá peticiones con credenciales 802.1x, las cuales almacenará en una base de datos de los usuarios con acceso al sistema. Contendrá información sobre *logins* y contraseñas, métodos de autenticación, perfiles y VLAN por tipo de usuario, etc. Se podrá integrar la base de

datos de las direcciones MACs en el mismo servidor, no necesitando de esta manera la presencia de un gestor de MACs independiente. El objetivo de definirlos con independencia física pero trabajando coordinadamente, es evitar sobrecargar la capacidad de proceso del servidor Radius.

Cuenta con un repositorio de datos que almacena las sesiones activas en toda la red, con datos que recibe de los equipos de accesos en los mensajes de autenticación y *accounting*. Son datos del tipo *User-Name*, dirección MAC, dirección IP asignada, puerto conectado, autenticación realizada mediante 802.1x, MAC o WEB, etc.

El servidor debe soportar de forma completa autenticación contra credenciales almacenadas en directorios LDAP, dominios de Windows y *Active Directory*.

Asimismo estará diseñado y configurado para soportar arquitecturas jerárquicas, redundantes y con balanceo de carga, permitiendo distribuir las peticiones de autenticación entre varios servidores.

9.1.3.2. Gestor de políticas

El gestor de políticas es la herramienta encargada de definir y distribuir los perfiles de usuario que van a determinar el reparto óptimo de los recursos de tráfico de la red. Para ello existe tanto la posibilidad de enviar la política al switch de acceso (Authenticator) cada vez que se autentique un usuario, como descargar previamente las políticas definidas en los propios switches de datos, y ya sean éstos quienes al recibir por parte del servidor RADIUS la confirmación que el usuario que se ha autenticado está autorizado para acceder a la red, le aplique la política que le corresponde y la cual tiene almacenada.

Deberá permitir realizar todas las funcionalidades descritas en el apartado 11.1 de este documento.

El gestor debe poder integrarse en un entorno multifabricante, teniendo la capacidad de modificar de manera automática una política de usuario determinada, en función de una alerta o evento que se haya producido en la red.

Deberá mantener un enlace configurado con el servidor RADIUS, si no se encuentra integrado en el propio sistema. Ésta coordinación es necesaria para que el servidor informe al gestor de políticas del perfil de usuario que se debe aplicar si el usuario autenticado está autorizado para entrar en la red.

9.1.3.3. Gestor de MAC

El gestor de direcciones MAC tiene como objetivo manejar el tráfico de autenticación por MAC, sin necesidad de intervenir el servidor RADIUS. Debe encontrarse integrado con el gestor de políticas para poder aplicar el perfil de usuario determinado, con la VLAN definida previamente.

Su comunicación con los Authenticator se soporta sobre el protocolo RADIUS.

Es capaz de aplicar un Control de Acceso y funcionalidades de seguridad a múltiples usuarios o dispositivos conectados a un único puerto.

Como el resto de los gestores y servidores citados en este capítulo, debe tener una elevada capacidad de registro de dispositivos, ofreciendo escalabilidad para ampliaciones futuras.

Se puede ofrecer una solución en la que el gestor de MAC este integrado en el servidor RADIUS. Todo el sistema de gestión debe soportarse con estándares y permitir la integración de los dispositivos de red multifabricante desplegados en las líneas existentes y futuras de Alta Velocidad.

9.1.3.4. Módulos adicionales a considerar

El sistema propuesto deberá incluir funcionalidades no solo para la autenticación, sino también para asegurarse que las condiciones actuales del usuario y/o dispositivo, en cuanto a lo instalado en el equipo y a lo que está transmitiendo, son las adecuadas para poder usar los recursos de red.

Los módulos complementarios que completan este proceso de securización de la conexión a la red, se dividen en una etapa de chequeo antes de permitir la conexión, y otra posterior para asegurarse que no se está transmitiendo fuera de unos patrones normales de comportamiento de tráfico.

- Antes de la conexión

  Se debe realizar un chequeo del software instalado en el dispositivo que quiere conectarse a la red, debiendo estar actualizado en torno a las últimas versiones de sistema operativo, antivirus, firewall, etc. Si el dispositivo no cumple con los requerimientos exigidos, se le comunica al servidor RADIUS para que envíe un mensaje de rechazo de la solicitud de acceso, por lo que se convierte en una condición necesaria que junto con las credenciales del usuario o dispositivo determinan el permiso de conexión a la red.

- Posterior a la conexión

  Una vez se ha habilitado el puerto permitiendo la conexión a la red, se realiza un control continuo del tráfico enviado por el equipo, sin necesidad de agente instalado en el equipo. Esto se traduce en la comparación con unos patrones de tráfico normalizados en función del tipo de usuario; si no resulta dentro de los límites establecidos, se envía un mensaje al servidor RADIUS para iniciar un proceso de EAP-logoff.

9.1.3.5. Ventajas mecanismos de seguridad y control de accesos

- Seguridad en la conexión mediante la gestión de la identidad del dispositivo y/o usuario.
- Control del tráfico que circula por la red.
- Monitorización de los flujos de datos y posibilidad de respuesta automática ante ataques.
- Movilidad, permitiendo a los usuarios y dispositivos poder variar su ubicación. Debido a que sus credenciales o bien su dirección MAC están registrados en el servidor RADIUS, únicamente tendrán que realizar el proceso de autenticación y autorización en el nuevo emplazamiento, y así poder tener permiso a los recursos de red que le sean autorizados.
- Gestión centralizada.

10. ALIMENTACIÓN DE EQUIPOS DE TELECOMUNICACIONES FIJAS

Los equipos de suministro de energía proyectados se encargan de alimentar los equipos de la red de comunicaciones fijas con la energía eléctrica necesaria para su correcto funcionamiento y de la protección frente a elevaciones bruscas de tensión y perturbaciones que puedan proceder de la acometida eléctrica.

10.1. CONSUMIDORES DE CORRIENTE CONTINUA

Los distintos equipos de la red de comunicaciones fijas, según sus características de alimentación, se engloban como consumidores de corriente continua. Para la alimentación de los equipos de comunicaciones fijas se procede a instalar un sistema de alimentación ininterrumpida monofásico independiente, compuesto por:

- Módulo rectificador/cargador de baterías.
- Baterías estacionarias sin mantenimiento.
- Módulo de control del sistema.

10.2. COMPONENTES DEL SISTEMA DE ENERGÍA

Para el funcionamiento de los equipos de la red de telecomunicaciones fijas instalados en los diversos emplazamientos a lo largo de la vía, es necesario disponer de una alimentación de corriente continua. Ésta es suministrada por unos rectificadores y unas baterías estacionarias libres de mantenimiento. Los rectificadores son convertidores de energía que, a partir de una alimentación de corriente alterna, generan corriente continua, filtrada y estable, con capacidad para cargar y mantener en flotación bancos de baterías (asegurando, ante caídas de la red eléctrica, el suministro a los equipos que deben estar en funcionamiento de manera continuada) y que disponen de una derivación para alimentar equipamientos que requieran corriente continua.

Entre los consumidores de corriente continua están los siguientes equipos:

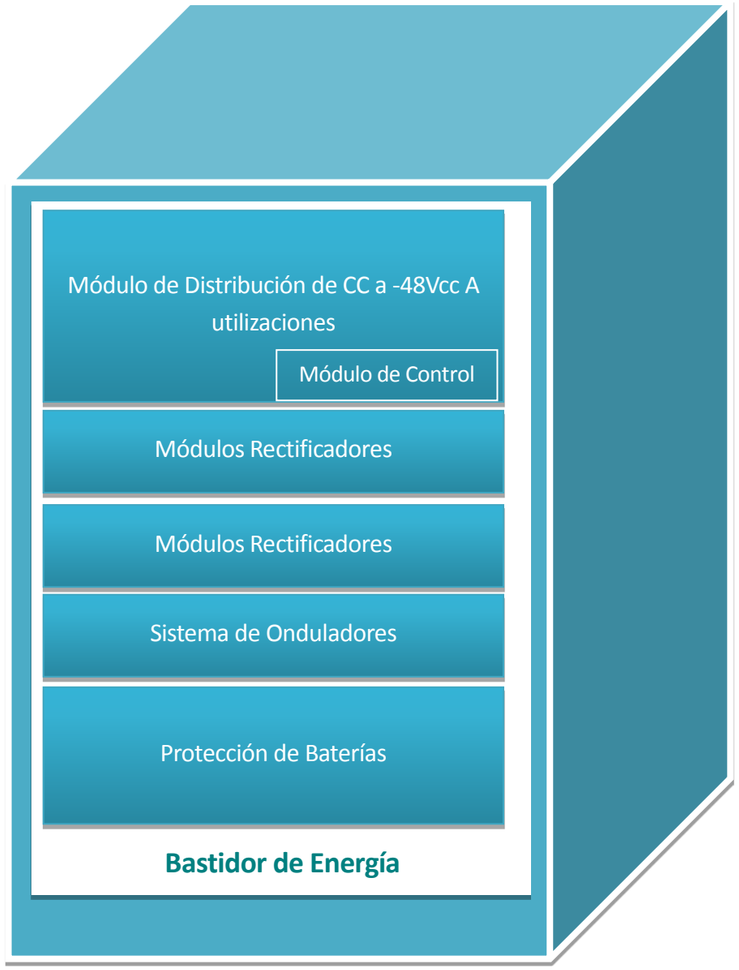
- Switch MPLS y switch n2/n3 con el nº de puertos necesarios.
- Router IP/MPLS de la RDE.
- Sistema de supervisión de fibra óptica.
- Otros

Los switches MPLS de la RAD se alimentarán preferentemente en corriente continua, aunque habida cuenta que deben proporcionar POE también se admite que se alimenten en corriente alterna. Se admitirá que se proponga un sistema de alimentación de dispositivos finales mediante inyectores de POE siempre que estos sean gestionables y dispongan de alimentación en continua a –48 Vcc.

Para garantizar la alimentación a estos equipos se instalará un sistema de energía compacto, modular, ampliable, tolerante a fallos y de muy alta fiabilidad. Se integrará en un armario bastidor que alojará los siguientes componentes:

- Módulos rectificadores.
- Módulo de control.
- Protección de baterías.
- Módulo de distribución de corriente continua -48 Vcc a utilizaciones.
- Sistema de Onduladores (solo serán necesarios si existen equipos que se alimenten en corriente alterna).

En la siguiente figura se muestra de forma esquemática la disposición de estos componentes en el armario de energía:



En todos los emplazamientos donde se alojen equipos de comunicaciones fijas con necesidades de alimentación se instalarán baterías de hasta 190 Ah en un rack de energía. La capacidad máxima de estos armarios será de como máximo cuatro (4) secciones de baterías. En todos los casos se presupuestará un armario de energía, sin embargo, en emplazamientos con altas necesidades de energía y fuera necesaria la instalación de un número mayor de cuatro (4) secciones de baterías se presupuestará otro rack para alojar baterías.

La disposición de estos equipos se realizará en el armario modular y las características generales del sistema son las siguientes:

- Alta fiabilidad.
- Tensión de entrada para dos redes, monofásicas o trifásicas.
- Amplio margen de temperatura de funcionamiento (-40ºC a 75ºC).
- Factor de potencia unidad.
- Simplificación extrema en tareas de mantenimiento.
- Refrigeración forzada, con velocidad controlada y con alarma de funcionamiento.
- Alto rendimiento.
- Módulos rectificadores y módulo de control enchufables y desenchufables en marcha.
- Muy alta flexibilidad y simplicidad para el crecimiento futuro en potencia.
- Bandejas para alojar hasta 4 secciones de baterías de 190 Ah cada una.
- Acceso totalmente frontal.
- Configuración y Supervisión locales (LED, display y PC).
- Parámetros de control y supervisión configurables por el usuario.
- Supervisión y configuración remota punto a punto y punto – multipunto (contactos libres de potencial, interfaz RS232 y USB, protocolo SNMP, conexión a redes TCP/IP y supervisión WEB).
- Gestión inteligente de baterías.
- Cumplimiento de estándares internacionales.

El sistema de energía se integrará en un sistema para la gestión de los equipos de energía de la línea.

El sistema de energía dispondrá de gestión remota vía TCP/IP, pudiendo supervisar desde el puesto central las alarmas y el estado, tanto de los rectificadores como de las baterías, además de ser capaz de realizar test remoto de baterías.

El bastidor dispondrá de salidas y protecciones diferenciadas para atender los diferentes consumos.

El sistema de energía se diseñará para proporcionar la potencia necesaria para el funcionamiento de los equipos de telecomunicaciones y cumplirá con los siguientes requisitos:

- Autonomía de las baterías 6h

A continuación, se detallan por separado las distintas partes que componen el sistema de energía, aunque el licitador deberá incluir todos los necesarios para el correcto funcionamiento del mismo.

10.2.1. Módulos rectificadores

Los módulos rectificadores serán enchufables/desenchufables con el sistema de energía en marcha y estarán dotados de la más alta tecnología para alimentación de los equipos de telecomunicaciones fijas. Estarán instalados en un subbastidor de rectificadores de 1 U de altura, que puede contener hasta 8 módulos rectificadores.

El armario de rectificadores suministrará inicialmente una potencia total de al menos 2.500 W, con una configuración de rectificadores en redundancia n+1 para asegurar la operatividad del conjunto en caso de fallo de uno de ellos; igualmente permitirá la ampliación de módulos rectificadores hasta al menos 20.000 W de potencia total, en dos bastidores de rectificadores de 10.000 W cada uno. Se podrán proponer módulos rectificadores de otra potencia siempre que se cumplan el resto de requisitos del apartado.

Para emplazamientos donde se requieren pequeños consumos de potencia, se instalarán módulos rectificadores de potencia mucho mayor que la que se consume, por homogeneidad con el resto de emplazamientos, debido a que por razones de explotación, repuestos y mantenimiento, es conveniente utilizar, el mismo tipo de sistema de energía en todos los emplazamientos.

El módulo rectificador incorporará un microprocesador que proporcionará la más alta capacidad en monitorización y control de funcionamiento mediante encendido-apagado controlado por el usuario a través del módulo de control del sistema.

Las características y prestaciones de los rectificadores se desglosan a continuación:

- Amplio margen de tensión alterna de entrada (85 Vca a 300 Vca).
- Amplio margen de temperatura de funcionamiento (-40ºC a 75ºC).
- Alta fiabilidad.
- Factor de potencia unidad.
- Refrigeración forzada con velocidad controlada.
- Alto rendimiento.
- Paralelable con reparto activo de carga.
- Arranque lento (ETSI ETS 300 132-1).
- Muy reducido de peso y volumen.
- Protección frente a sobretemperatura, sobrecarga y cortocircuito.

10.2.2. Módulo de control

El módulo de control digital está basado en un microprocesador para la supervisión y configuración de funciones en los sistemas de corriente continua.

Las características y prestaciones del módulo de control se desglosan a continuación:

- Enchufable y desenchufable con el sistema en marcha.

- Alarmas proporcionadas (locales – leds + display y remotas – PC), parámetros de funcionamiento y operaciones del sistema programables por el usuario.
- Alarma acústica.
- Control y medida de la temperatura de los módulos rectificadores del sistema.
- Control de encendido-apagado de los módulos rectificadores del sistema.
- Control del sistema de onduladores
- Supervisión y gestión local y remota mediante PC.
- Almacenamiento de eventos.
- Actualización remota del software.
- Posibilidad de carga rápida (manual o automática) de baterías.
- Gestión inteligente de baterías (compensación automática de la tensión de flotación con la temperatura, limitación de la corriente máxima de carga de batería, desconexión automática de batería o utilizaciones por baja tensión y test de capacidad de baterías).

10.2.3. Baterías

En ausencia de tensión alterna de entrada, ausencia de red, las baterías son las encargadas de proporcionar la alimentación en corriente continua a las cargas alimentadas en 48 Vcc. Estarán dimensionadas para garantizar la alimentación a los consumos críticos al menos un tiempo de 6 horas en ausencia de red.

Se podrán instalar hasta 4 bandejas de baterías en el bastidor de energía, con las siguientes características:

- Baterías de plomo hermético de recombinación de gases.
- Sin mantenimiento.
- Alta capacidad de ciclaje.
- Compuestas por monobloques de 12 V, 100 Ah y 190 Ah.
- Alta densidad de energía.
- Larga vida (hasta doce años de caducidad).
- Parte frontal de conexiones rápido y fácil de instalar y mantener.
- Amplio rango de temperatura de funcionamiento: -40°C a +50°C.

Las baterías se instalarán en las secciones necesarias en función de las necesidades de cada emplazamiento, estando normalmente compuesta por 4 monobloques de 12 Vcc. Excepcionalmente, en los casos en los que las necesidades de energía sean superiores, sobrepasando las 4 secciones de baterías, se presupuestará un armario de energía adicional donde se alojarán las baterías necesarias.

10.2.4. Módulo de distribución de corriente continua 48 Vcc a utilizaciones

El sistema de energía permitirá alimentar inicialmente unas utilizaciones en 48 Vcc de 2500 W, mediante la instalación de 1 hasta 21 interruptores magnetotérmicos (2 a 63 A).

Se instalarán dos interruptores de reserva en cada emplazamiento.

10.2.5. Sistema de Onduladores

Estará compuesto por, al menos, dos módulos onduladores de 1500 W cada uno. Estos son los encargados de transformar la tensión continua de -48 Vcc, proveniente de la salida del Sistema de Alimentación Ininterrumpida (SAI), en tensión alterna de 230 Vca 50 Hz, con las características de calidad requerida por las utilizaciones. Contará con protecciones de las salidas en alterna, con un by-pass manual y un by-pass estático.

Todos los Módulos Onduladores que equipen el sistema de onduladores, trabajarán en paralelo repartiéndose la carga, con su tensión de salida perfectamente sincronizada en fase, amplitud y frecuencia.

10.3. CÁLCULO DE LOS COMPONENTES DEL SISTEMA DE ENERGÍA.

Los diferentes emplazamientos, desde el punto de vista eléctrico, irán equipados con el equipamiento de energía anteriormente descrito y con sus respectivas protecciones (de entrada 230 V desde el cuadro de conmutada, de protección de baterías, de salidas en continua y de salidas en alterna). Este sistema de energía será el encargado del suministro eléctrico a los consumos requeridos por los equipos de la red de Telecomunicaciones Fijas. El licitador indicará en su oferta el detalle de los componentes necesarios del sistema de energía por emplazamiento en función del consumo del equipamiento propuesto. En el presupuesto adjunto se incluye una estimación basada en consumos típicos por tipo de equipo.

Dependiendo del tipo de emplazamiento se requerirán diferentes consumos de potencia y se optará, en todos los casos, por la instalación de módulos rectificadores de la misma potencia e idénticas características, tanto si se requiere un consumo de potencia pequeño o grande. Ello se debe a la homogeneización del sistema de energía en todas sus partes: repuestos, formación de personal y supervisión remota centralizada. También en aras de la homogeneidad se ha elegido un conjunto de baterías, de todas las disponibles en el mercado, con las que se implementarán las distintas configuraciones necesarias en cada tipo de emplazamiento. Las capacidades elegidas son: 100 Ah y 190 Ah.

10.3.1. Protección de las personas contra contactos directos.

Las personas que trabajan en contacto con los equipos de energía descritos anteriormente deben ser protegidas contra accidentes causados por contactos indirectos con cualquiera de las tensiones que se encuentran en la instalación.

Los equipos interiores garantizan la protección de las personas contra contactos indirectos mediante la puesta a tierra de todas las partes metálicas accesibles de los equipos de energía. Se realizará, dentro del mismo cuarto, una conexión en anillo de todos los equipos y a su vez, éste se conectará a la barra principal de tierra, la cual está conectada a la tierra del carril. La tierra en ningún caso sobrepasará el valor de 10 Ω.