RENOVACIÓN DEL EQUIPAMIENTO DE LA RED TRONCAL DE COMUNICACIONES OT DE ETS

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES

ÍNDICE

1 OBJETO DEL PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES 1

2 RELACIONES ENTRE ETS Y EL CONTRATISTA. DEFINICIONES 2

3 DESARROLLO GENERAL DE LOS TRABAJOS 3

3.1 CONTROL DE LOS TRABAJOS 3

3.2 PROGRAMA DE TRABAJOS 3

4 ANTECEDENTES, SITUACIÓN ACTUAL, DOCUMENTOS DE REFERENCIA 4

4.1 ANTECEDENTES 4

4.2 SITUACIÓN ACTUAL 6

4.3 DOCUMENTACIÓN DE REFERENCIA 16

5 TRABAJOS A REALIZAR POR EL CONTRATISTA 17

5.1 ALCANCE 17

5.2 ANÁLISIS DE LA SITUACIÓN ACTUAL Y EVOLUCIÓN DE RED 17

5.3 PLANTEAMIENTO DE ARQUITECTURA 18

5.4 DESCRIPCIÓN DE LOS NODOS A SUMINISTRAR 21

5.5 SISTEMA DE GESTIÓN 25

5.6 DOCUMENTACIÓN Y FORMACIÓN 27

5.7 SOPORTE DEL ADJUDICATARIO 27

5.8 GARANTÍA 29

6 ESPECIFICACIONES EQUIPAMIENTO RED 30

6.1 ROUTER *CORE* MPLS-IP MODULAR: ATXURI Y AMARA 30

6.2 ROUTER *CORE* MPLS-IP DE CHASIS FIJO 42

6.3 EQUIPOS DE ACCESO PARA EL *CORE* MPLS-IP 46

7 PLANIFICACIÓN 48

8 CERTIFICACIONES 49

9 PRECIOS DE CONTRATO 50

10 VALORACIÓN Y ABONO DE LOS TRABAJOS REALIZADOS 51

11 PRESUPUESTO DEL CONTRATO 52

12 ANEJO: CUADRO DE PRECIOS 53

1 OBJETO DEL PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES

El objeto del presente Pliego de Prescripciones Técnicas Particulares es el de establecer las condiciones técnicas que han de regir la adjudicación y, en su momento, del servicio para **la renovación del equipamiento de CORE de la red troncal de comunicaciones OT de ETS, así como la evolución de una Red IP a una red MPLS-IP en el ámbito del CORE para crear las bases para una migración total (Core y Acceso) de la red a MPLS-IP.**

2 RELACIONES ENTRE ETS Y EL CONTRATISTA. DEFINICIONES

A los efectos de fijar las relaciones contractuales se definen las siguientes figuras jurídicas:

- PROPIEDAD.- ETS, Ente Público del Gobierno Vasco.
- RESPONSABLE DEL PROYECTO.- ETS designará un Responsable del Contrato, bajo la supervisión de la Dirección de Instalaciones Y Mantenimiento. Dada la complejidad de los trabajos, el Responsable del Contrato podrá rodearse del equipo técnico necesario que le asesorará y en su caso podrá actuar por delegación del mismo.
- CONTRATISTA.- Licitador Adjudicatario del contrato de prestación de servicio, persona natural o jurídica que adquirirá esa condición a la firma del Contrato.
- DELEGADO/A DEL CONTRATISTA.- Técnico Superior, designado por el Contratista para hacerse cargo de la coordinación técnica de los trabajos y representar a éste frente a ETS. Todo el equipo del Contratista dependerá del Delegado, quien informará directamente y cuantas veces sea requerido al Responsable del Proyecto.

3 DESARROLLO GENERAL DE LOS TRABAJOS

3.1 Control de los trabajos

Al menos una vez por mes, el Contratista informará por escrito al Responsable del Proyecto sobre el estado de los trabajos hasta entonces realizados, y solicitará de él las instrucciones pertinentes para la continuación o nueva presentación de aquellos.

Siempre que el Contratista solicite alguna instrucción o decisión, deberá proponer a su vez, aquélla que a su entender considere como más apropiada. En cualquier momento el Equipo Técnico del Responsable del Proyecto, podrá inspeccionar la marcha de los trabajos, en la oficina del Contratista.

Las observaciones o prescripciones que se deriven de la inspección serán comunicadas al Contratista a través del Responsable del Proyecto.

De todas las reuniones que se mantengan entre el Equipo Responsable del Proyecto y el Contratista se levantarán ACTAS donde se recojan las propuestas, modificaciones, instrucciones y conclusiones que se adopten.

3.2 Programa de trabajos

Completada la revisión de los documentos y datos básicos, el Contratista hará entrega al Responsable del Proyecto del Programa de trabajo, que detallará a nivel operativo el Plan de Trabajo que hubiese sido presentado en la proposición.

El programa de trabajos contendrá los siguientes elementos:

A) La metodología pormenorizada según la cual se propone al Contratista realizar los trabajos, desarrollada a nivel operativo y acompañada de las justificaciones pertinentes.

B) La organización del equipo del Contratista para el desarrollo de los trabajos, incluyendo la relación de personas, la relación de medios materiales y la descripción organizativa del equipo.

C) El Plan de Trabajo, incluyendo Cronograma completo para la ejecución de los trabajos de redacción que sea compatible con lo establecido en el presente Pliego y acorde con lo indicado en la propuesta económica

4 ANTECEDENTES, SITUACIÓN ACTUAL, DOCUMENTOS DE REFERENCIA

4.1 Antecedentes

En ETS coexisten dos redes de comunicaciones bien diferenciadas. La red corporativa, sistemas u ofimática y la red de explotación o multiservicio.

La primera red está gestionada por el departamento de sistemas y en ella se encuentran los servidores y ordenadores donde se ejecutan las aplicaciones corporativas (correo electrónico, intranet, SAP, aplicaciones de gestión, almacenamiento etc.) así como los PC de trabajo de cada usuario de ETS. Esta red dispone de sus sistemas de seguridad tanto perimetrales (firewall) como a nivel de usuario final (endpoint) dado que se relaciona con redes externas.

La segunda red está gestionada por el departamento de mantenimiento y sobre ella se soportan todos los sistemas relacionados con la explotación ferroviaria. Esto incluye sistemas críticos como son los relacionados con la señalización ferroviaria, telemandos de energía e instalaciones, sistemas de seguridad, etc.

Los elementos troncales de esta red multiservicio están compuestos por equipamientos ya obsoletos y descatalogados por el fabricante.

4.1.1 La red multiservicio en la infraestructura de telecomunicaciones fijas de una red ferroviaria

La red multiservicio da soporte tanto a los sistemas de explotación ferroviaria como a los administrativos y de gestión, por lo que es uno de los elementos más importantes dentro de toda la infraestructura de telecomunicaciones fijas. Éste se diseña de forma global para prestar soporte y proveer todos los servicios de telecomunicaciones necesarios para la operación, gestión y mantenimiento de la línea ferroviaria.

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

Se estructura sobre la base de niveles jerárquicos, que corresponden a volúmenes crecientes de transporte de información, según el siguiente diagrama y descripción:

- Nivel físico: provee de puntos de conectividad o acceso a la red de telecomunicaciones a lo largo de las diferentes ubicaciones de las instalaciones de la línea ferroviaria.

- Nivel de transmisión: ha de soportar las telecomunicaciones de interconexión entre los distintos centros de la línea y entre éstos y los puestos centrales de gestión tanto del subsistema de telecomunicaciones como del resto de técnicas a las que este subsistema da soporte.
- Nivel de servicios: proporciona los servicios finales a los diferentes sistemas de explotación de la Línea.
- Nivel de gestión de red: incluye los diferentes gestores de cada una de las redes y de los sistemas.

El nivel de transmisión incluye tanto las redes troncales (CORE), como las redes de ACCESO con la tecnología necesaria para cada uno de los servicios a soportar.

4.1.2 Estructura jerárquica

Las redes que forman parte del nivel de transmisión no son redes aisladas, sino que están interconectadas entre sí de forma jerárquica (core, distribución y acceso):

La fiabilidad de estas redes es fundamental ya que son la espina dorsal de las comunicaciones por lo que deben estar dotadas 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.

En las redes ferroviarias actuales, las redes de datos que forman parte del nivel de transmisión se estructuran jerárquicamente con un core y distribución basado en tecnología MPLS-IP y un acceso basado en redes de nivel 2 – 3 (Ethernet – IP) que forman anillos que habitualmente se cierran sobre los equipos de la capa superior.

En los siguientes apartados veremos la situación actual de la red multiservicio de ETS (core y acceso), las tecnologías que la soportan y su posible evolución hacia una red MPLS-IP manteniendo así la analogía con otros operadores ferroviarios.

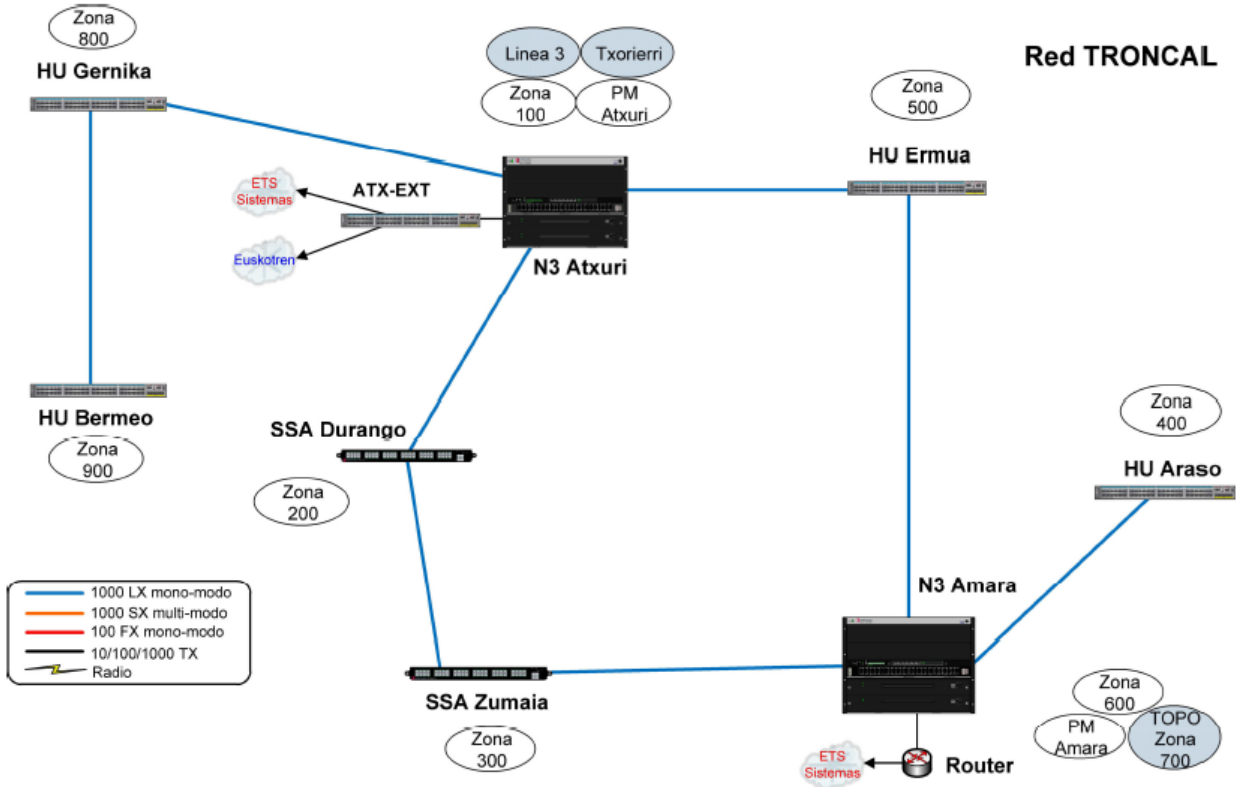
4.2 SITUACIÓN ACTUAL

4.2.1 *CORE* de la red Multiservicio

Atendiendo a la estructura jerárquica expuesta anteriormente, la red multiservicio consta de un *CORE* formado por un anillo, del que cuelgan o al que se enlazan diferentes lineales y anillos secundarios. Se trata de un *CORE*-IP tradicional que implementa **routing OSPF**. El *CORE* hace además en este caso las veces de *CORE* y distribución.

El ***CORE*** de la red Multiservicio de ETS es un anillo de 1 GbE formado por los equipos de Atxuri, Ermua, Durango, Zumaia y Amara. Este anillo tiene dos lineales de 1GbE: uno a Gernika y Bermeo por el lado de Atxuri, y otro a Araso por el lado de Amara.

La topología es la que se muestra en la siguiente figura:



Cada uno de los 8 equipos mencionados anteriormente son routers que dan servicio de routing a todos los equipos dentro de su segmento de red.

Cada router tiene varias redes IP configuradas y separadas a nivel 2 mediante VLANs coincidiendo con cada uno de los servicios de red implementados (CCTV, Información al viajero, interfonía, gestión, expendición, etc…)

Estos routers utilizan OSPF en el área 1.0.0.0 como protocolo de enrutamiento para propagar las rutas entre ellos.

El *CORE* está formado por una electrónica de red muy heterogénea, con routers de distintos fabricantes y con distintas características tanto hardware como software:

EMPLAZAMIENTO	FABRICANTE	MODELO
ATXURI	ENTERASYS (EXTREME NETWORKS)	MATRIX N3
DURANGO	ENTERASYS (EXTREME NETWORKS)	SSA
ERMUA	HUAWEI	S5720-56C-PWR-EI
ZUMAIA	ENTERASYS (EXTREME NETWORKS)	SSA
AMARA	ENTERASYS (EXTREME NETWORKS)	MATRIX N3
ARASO	HUAWEI	S5720-36C-EI
GERNIKA	HUAWEI	S5720-56C-PWR-EI
BERMEO	HUAWEI	S5720-56C-PWR-EI

Algunos de esos modelos están ya en phase-out (descatalogados) mientras que otros son equipos más recientes que cuentan ya con funcionalidades MPLS-IP, en concreto los equipos de Huawei. Son equipos estos últimos de nivel 3 (con plenas funcionalidades de routing: RIP, OSPF, BGP, IS-IS) que soportan además MPLS L3VPN, MPLS L2VPN (VPWS\VPLS), MPLS-TE y MPLS QoS. **Estos equipos quedarán disponibles para su uso como repuestos de la red de ETS**, ya que siguen en estado operativo y permitirán servir para la fase de transición que se generará a partir de la implementación del nuevo *core*.

En Atxuri y en Amara hay sendos routers para comunicar la red Multiservicio con el exterior:

- En Atxuri hay un Huawei S5720 que permite comunicar la red Multiservicio con las redes de ETS-Sistemas y de Euskotren. Este router tiene listas de acceso (ACLs) para dar un nivel de seguridad a las conexiones entrantes.
- En Amara hay un router (de ETS Sistemas) cuya función principal es la entrada de las VPN para las empresas mantenedoras de ETS.

4.2.2 Red de acceso

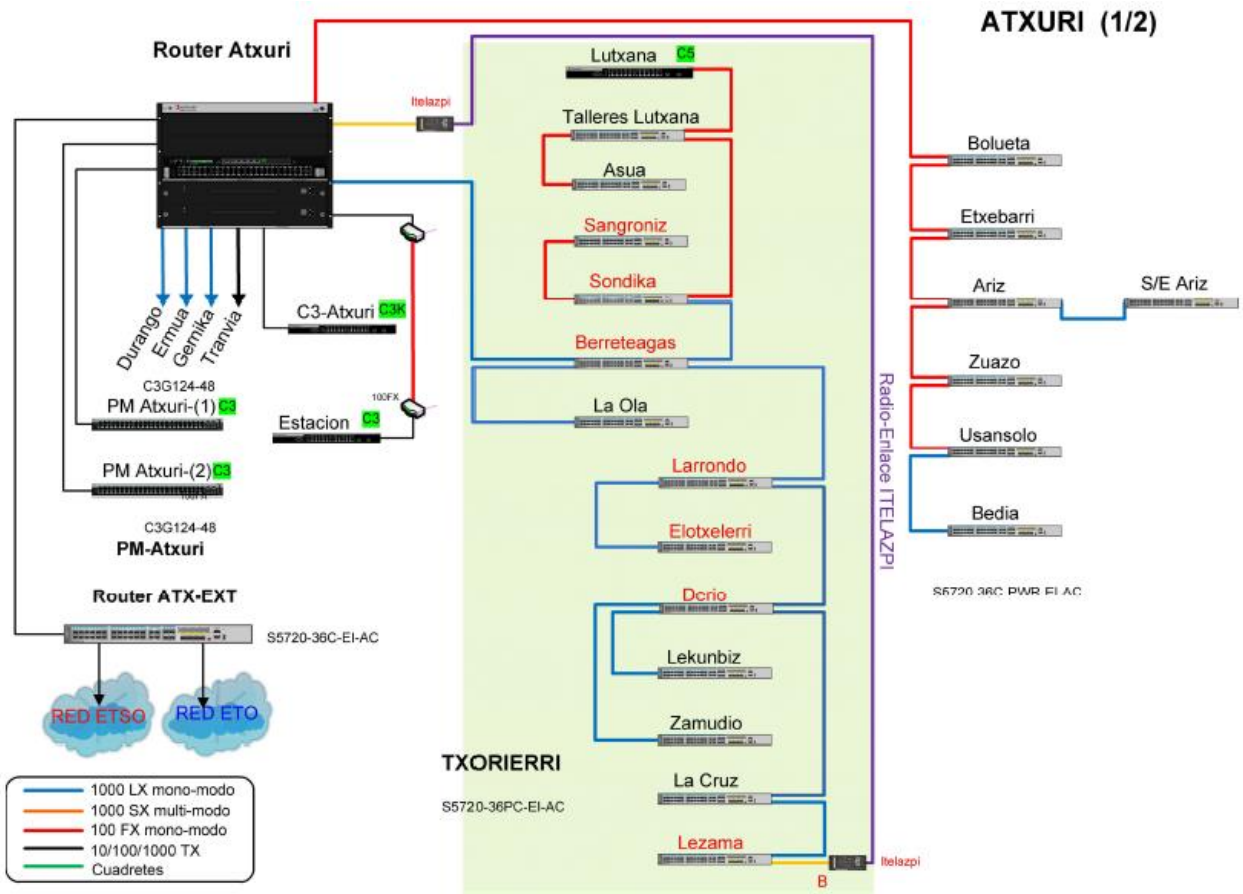
Adicionalmente, de cada router del *CORE* cuelgan/se conectan todos los switches de **ACCESO** (estructura jerárquica) que dan servicio de red a cada estación, subestación y apeadero. Estos switches se conectan a nivel 2 en topología de estrella y en algunos casos en anillo como en el Txorierri, tranvía de Bilbao, Línea 3 y Topo.

La electrónica de red presente en la capa de ACCESO de la red de ETS es igualmente heterogénea con switches de distintos fabricantes y con distintas características tanto hardware como software:

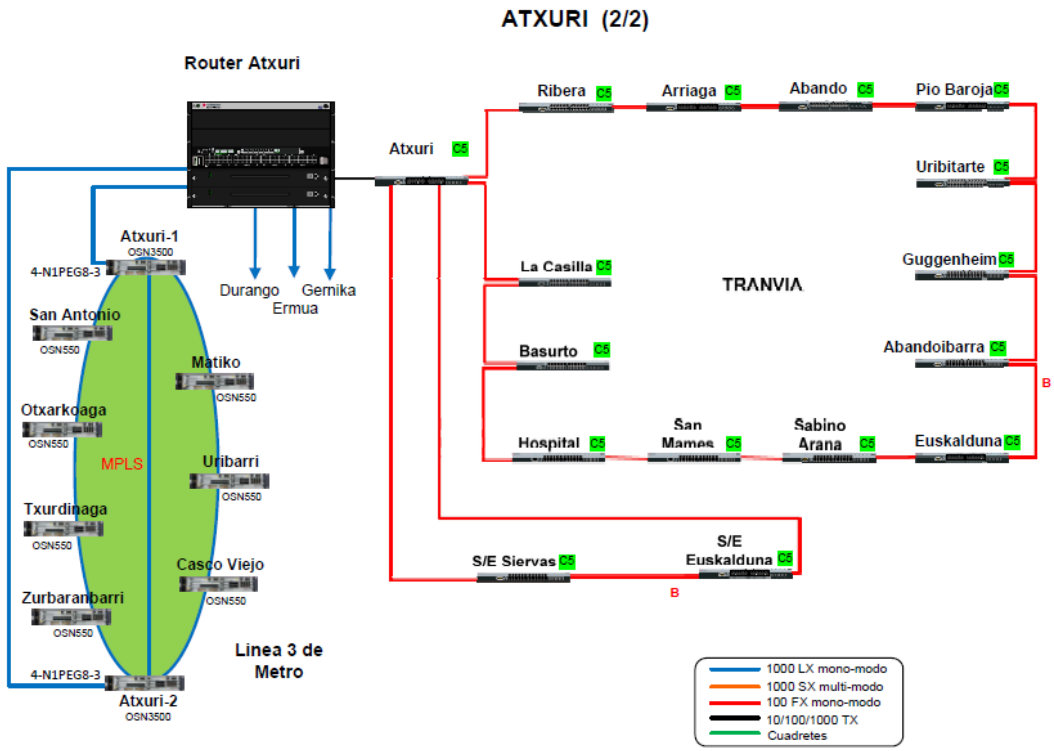
EMPLAZAMIENTO	FABRICANTE	MODELO
ESTACIÓN/SSEE/APEADERO	ENTERASYS (EXTREME NETWORKS)	C3
ESTACIÓN/SSEE/APEADERO	ENTERASYS (EXTREME NETWORKS)	C5
ESTACIÓN/SSEE/APEADERO	HUAWEI	S5720- EI

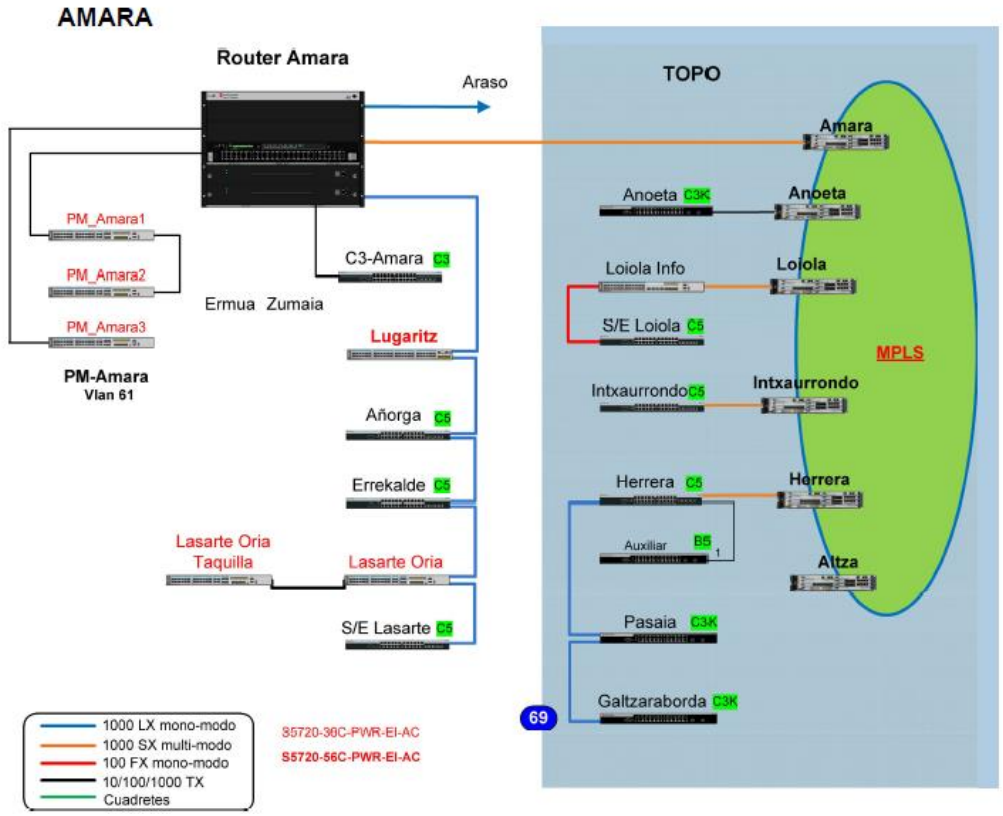
Algunos de los modelos desplegados son equipos obsoletos, con escasas posibilidades de mantener y de obtener repuestos. Dada la importancia que tiene la red IP, dando soporte a múltiples sistemas relacionados con la explotación ferroviaria, la necesidad de disponer de una red en perfecto estado de mantenimiento ha obligado en los últimos años a abordar la renovación continua de toda aquella electrónica de red que impedía su mantenimiento y evolución. Se trata de nodos secundarios de la red IP (nodos de acceso/distribución), que a su vez direccionan todo el tráfico IP hacia las instalaciones que dependen de ellos (como son estaciones y subestaciones). La nueva electrónica de red que se ha ido añadiendo a través de dichas renovaciones ha permitido por un lado soportar la segmentación de VLANs necesaria dentro del tráfico IP de ETS y por otro unificar la velocidad de transmisión a 1Gbps en toda la red, eliminando equipos con puertos de uplink limitados a 100Mbps.

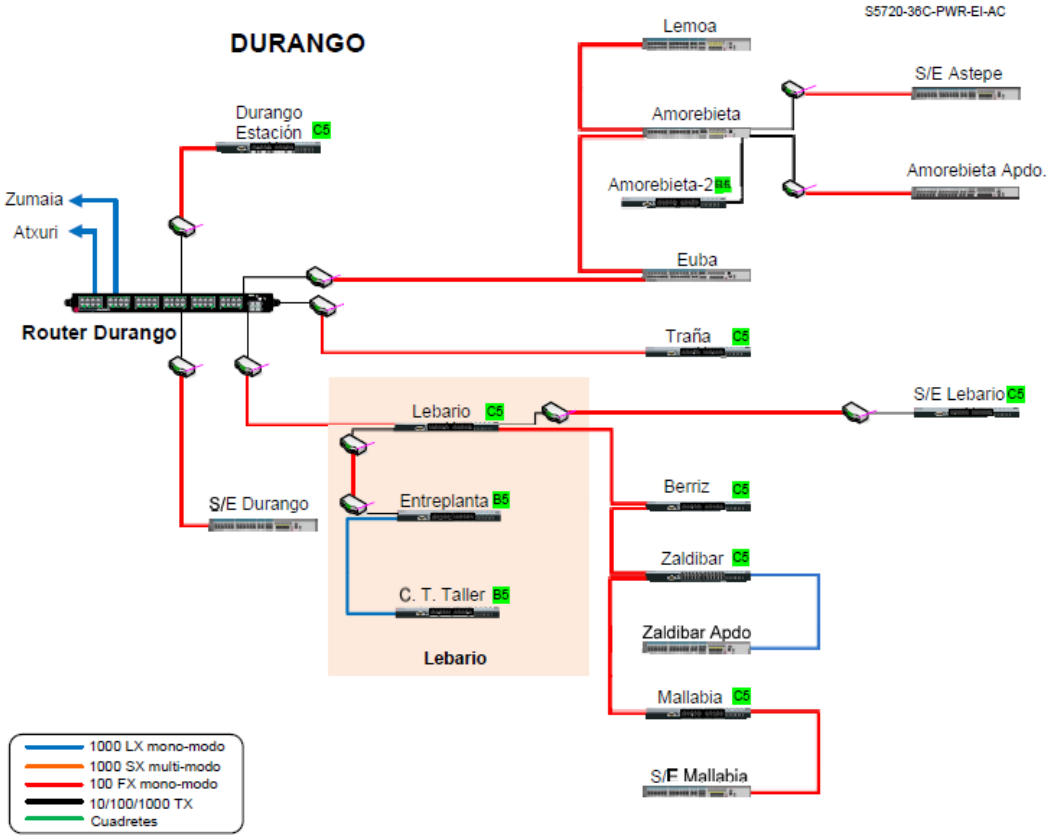
Los siguientes esquemas nos muestran cómo es la topología de la red de ACCESO, tanto en los distintos anillos (Txorierri, tranvía de Bilbao, Topo, anillos MPLS-TP) como en los lineales que cuelgan de los nodos del CORE de Ermua, Durango, Zumaia, Gernika y Bermeo.

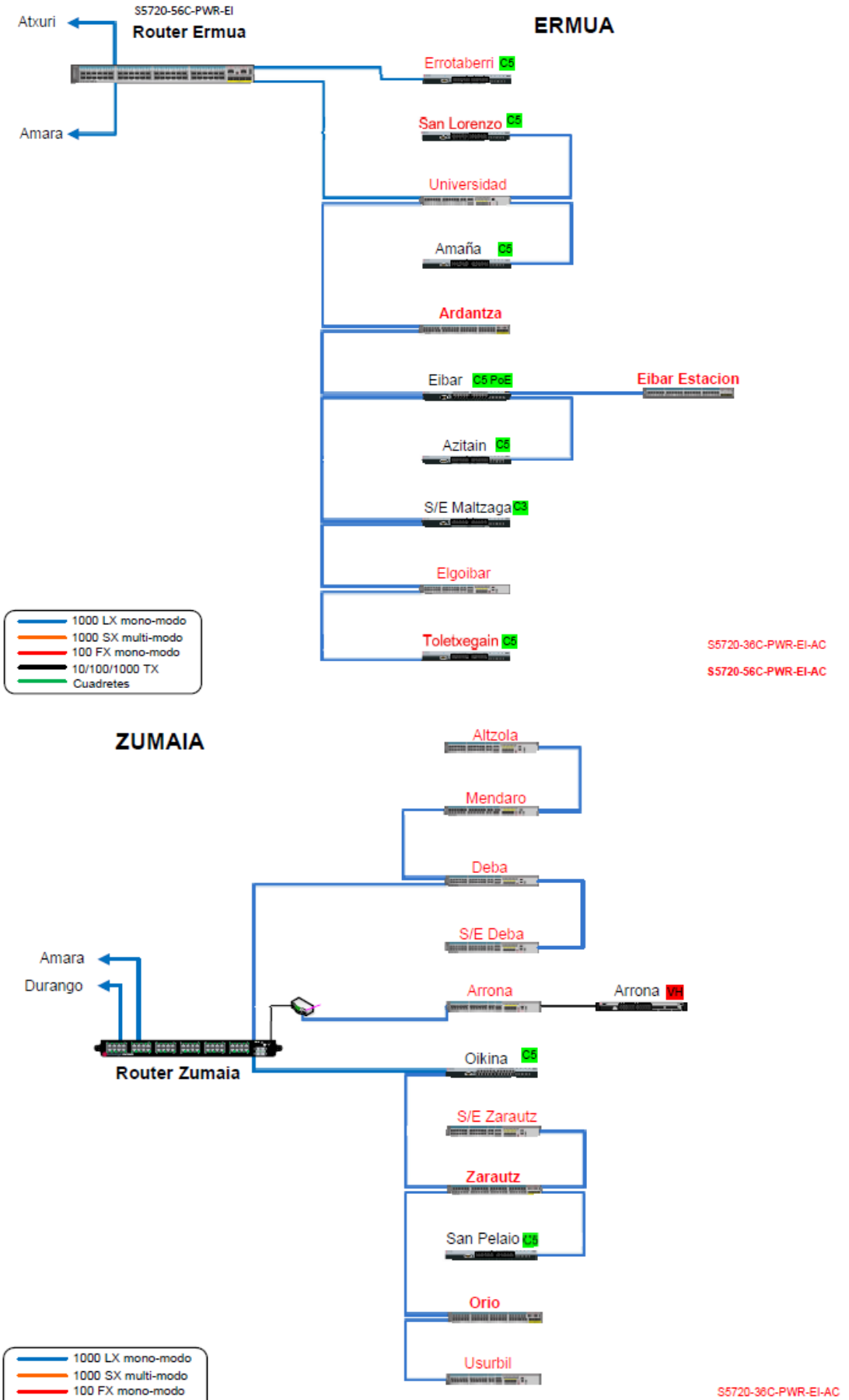


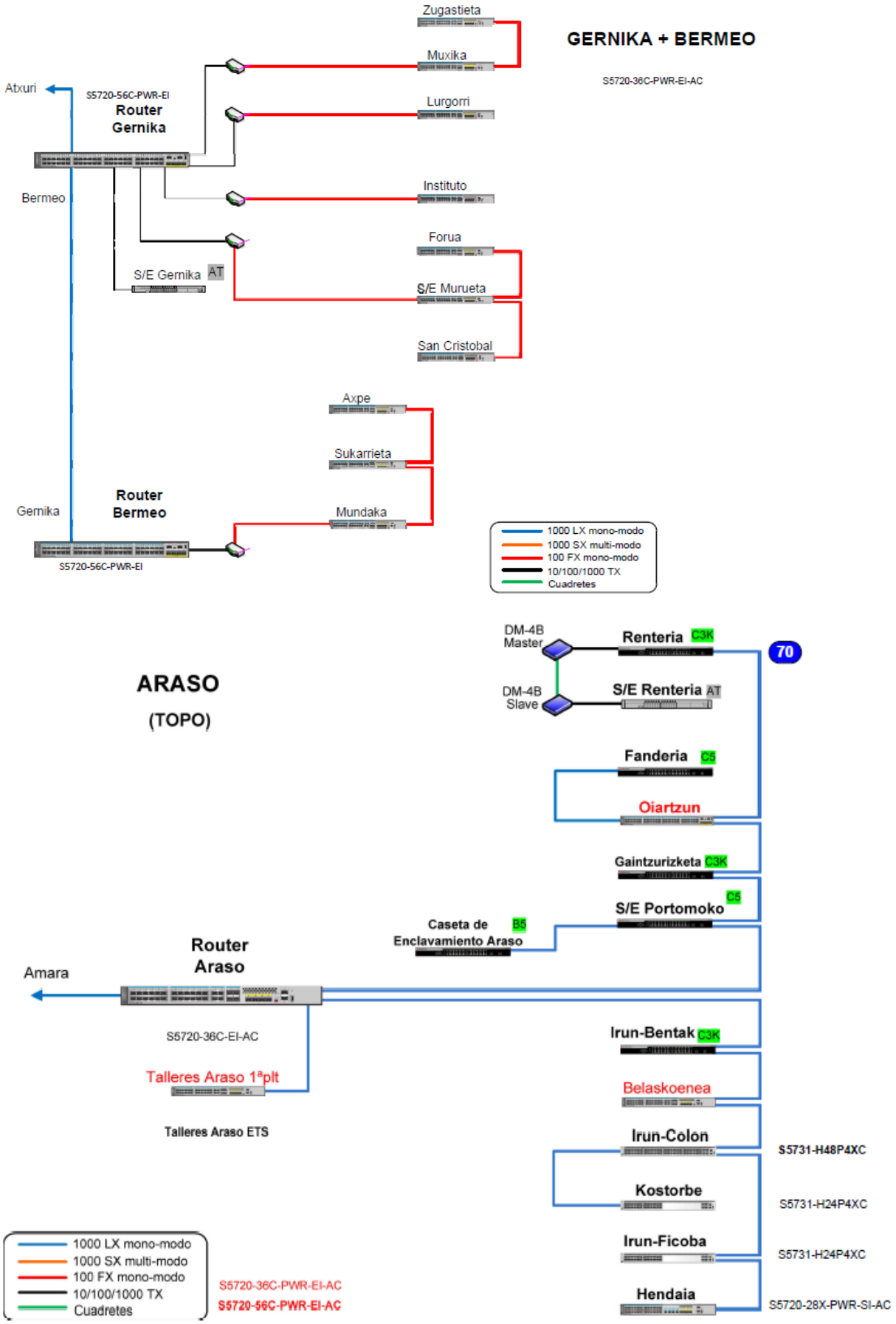
Los anillos del Txorierri y del Tranvía de Bilbao conectan con el router de Atxuri y tienen configurado MSTP (Multiple Spaning Tree) para prevenir bucles.




AMARA
Router Amara
Araso
PM_Amara1
PM_Amara2
PM_Amara3
PM-Amara
Vlan 61
C3-Amara
Ermua Zumaia
Lugaritz
Añorga
Errekalde
Lasarte Oria Taquilla
Lasarte Oria
S/E Lasarte
TOPO
Amara
Anoeta C3K
Anoeta
Loiola Info
Loiola
S/E Loiola C5
MPLS
Intxaurrondo C5
Intxaurrondo
Herrera C5
Herrera
Auxiliar B5
Altza
Pasaia C3K
Galtzaraborda C3K
69
1000 LX mono-modo
1000 SX multi-modo
100 FX mono-modo
10/100/1000 TX
Cuadretes
S5720-36C-PWR-EI-AC
S5720-56C-PWR-EI-AC


S5720-36C-PWR-EI-AC
DURANGO
Lemoa
S/E Astepe
Durango Estación C5
Amorebieta
Amorebieta Apdo.
Amorebieta-2 B5
Zumaia
Atxuri
Euba
Router Durango
Traña C5
S/E Lebario C5
Lebario C5
Berriz C5
S/E Durango
Entreplanta B5
Zaldibar C5
C. T. Taller B5
Zaldibar Apdo
Lebario
Mallabia C5
S/E Mallabia
1000 LX mono-modo
1000 SX multi-modo
100 FX mono-modo
10/100/1000 TX
Cuadretes


S5720-56C-PWR-EI
Router Ermua
ERMUA
Atxuri
Amara
Errotaberri C5
San Lorenzo C5
Universidad
Amaña C5
Ardantza
Eibar C5 PoE
Eibar Estacion
Azitain C5
S/E Maltzaga C3
Elgoibar
Toletxegain C5
1000 LX mono-modo
1000 SX multi-modo
100 FX mono-modo
10/100/1000 TX
Cuadretes
S5720-36C-PWR-EI-AC
S5720-56C-PWR-EI-AC
ZUMAIA
Altzola
Mendaro
Deba
S/E Deba
Amara
Durango
Arrona
Arrona VH
Router Zumaia
Oikina C5
S/E Zarautz
Zarautz
San Pelaio C5
Orio
Usurbil
1000 LX mono-modo
1000 SX multi-modo
100 FX mono-modo
10/100/1000 TX
Cuadretes
S5720-36C-PWR-EI-AC
S5720-56C-PWR-EI-AC


GERNIKA + BERMEO
S5720-36C-PWR-EI-AC
Zugastieta
Muxika
Lurgorri
Instituto
Forua
S/E Murueta
San Cristobal
Atxuri
S5720-56C-PWR-EI
Router
Gernika
Bermeo
S/E Gernika AT
Axpe
Sukarrieta
Mundaka
Gernika
Router
Bermeo
S5720-56C-PWR-EI
1000 LX mono-modo
1000 SX multi-modo
100 FX mono-modo
10/100/1000 TX
Cuadretes
ARASO
(TOPO)
DM-4B
Master
DM-4B
Slave
Renteria C3K
S/E Renteria AT
70
Fanderia C5
Oiartzun
Gaintzurizketa C3K
S/E Portomoko C5
Caseta de
Enclavamiento Araso B5
Router
Araso
Amara
S5720-36C-EI-AC
Talleres Araso 1ªplt
Talleres Araso ETS
Irun-Bentak C3K
Belaskoenea
Irun-Colon
S5731-H48P4XC
Kostorbe
S5731-H24P4XC
Irun-Ficoba
S5731-H24P4XC
Hendaia
S5720-28X-PWR-SI-AC
1000 LX mono-modo
1000 SX multi-modo
100 FX mono-modo
10/100/1000 TX
Cuadretes
S5720-36C-PWR-EI-AC
S5720-56C-PWR-EI-AC

4.2.3 Los anillos MPLS-TP de Línea 3 y el Topo

Dentro de esos anillos de nivel 2 cabe destacar los casos especiales de los anillos de Línea 3 de Metro y del Topo. Se trata en ambos casos de anillos que forman dos redes **MPLS-TP** independientes.

La electrónica de red encargada de dar soporte a estos anillos es de Huawei:

EMPLAZAMIENTO	FABRICANTE	MODELO
ATXURI/AMARA	HUAWEI	OSN3500
ESTACIONES	HUAWEI	OSN550

La red MPLS-TP de Línea 3 conecta con el router de Atxuri para el servicio de routing, mientras que la red MPLS-TP del Topo conecta con el router de Amara para el servicio de routing. De esa manera se integran ambas redes dentro de la red completa de ETS.

4.2.4 Red de backup MPLS-IP

En los anteriores apartados hemos visto el estado actual de la red Multiservicio, tanto en el *CORE* como en el ACCESO.

A día de hoy ya se ha llevado a cabo en una primera etapa la implementación de una red MPLS-IP periférica capaz de proporcionar un **backup MPLS-IP del *CORE* existente**. El anillo Gigabit troncal tiene un sistema de backup para garantizar continuidad de la red entre nodos de routing ante un doble corte de la fibra del anillo que deje el anillo segmentado en dos partes.

Esta actuación es fundamental para dotar a la red de la robustez necesaria elevando la fiabilidad de la misma al permitir utilizar esquemas de protección de tráfico.

El medio físico que habilita los caminos redundantes para dicho backup ha sido proporcionado mediante radioenlaces, capaces de proporcionar un ancho de banda de unos 200Mbps. Los radioenlaces se han habilitado utilizando la infraestructura de antenas de ITELAZPI.

La electrónica de red que ha permitido implementar dicho backup se ha basado ya en equipamiento con capacidad completa MPLS-IP y funcionalidades de nivel 3. Dada la limitación de ancho de banda que proporcionan los radioenlaces, la electrónica de red que soporta el backup está sujeta a interfaces de 1GbE.

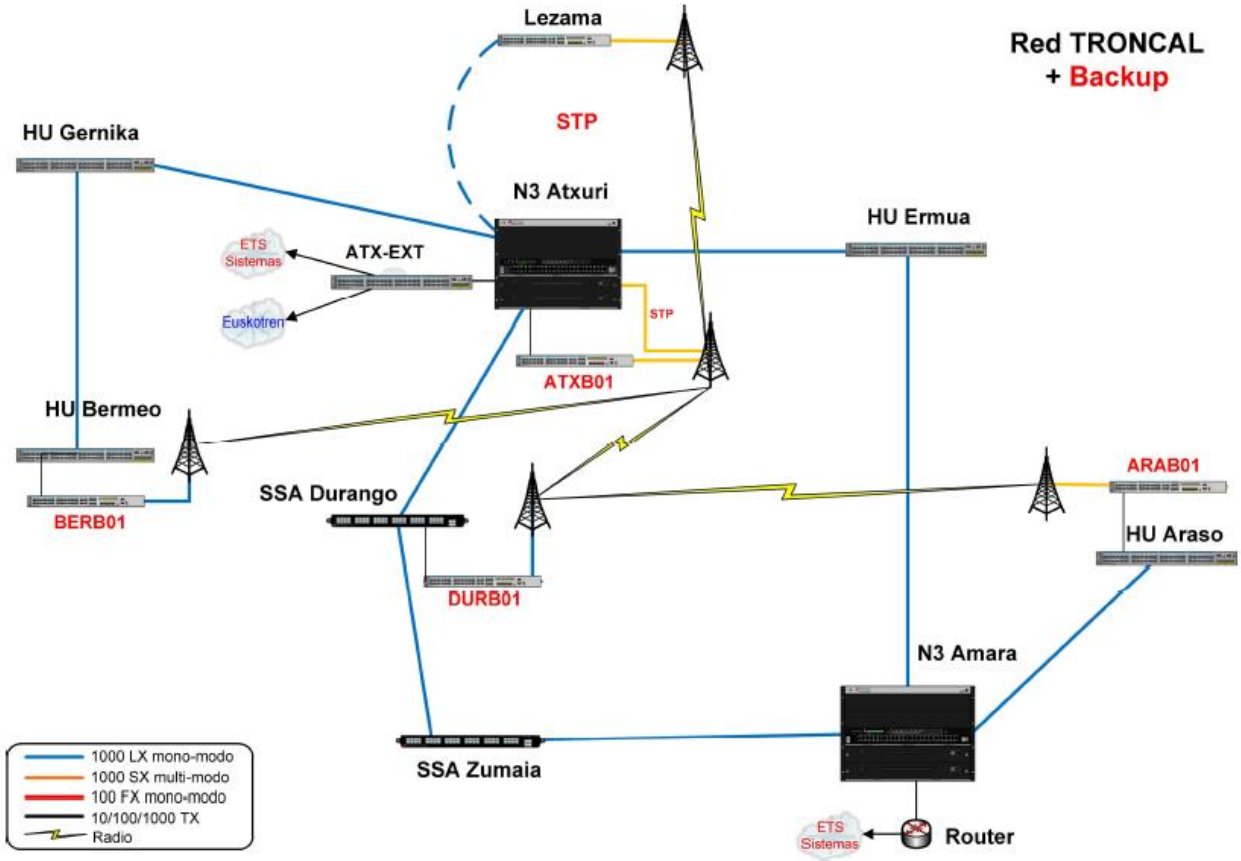
El backup está formado por 5 switches Huawei S5720-EI colocados en Atxuri, Bermeo, Durango, Araso y Lezama (este último para cerrar el anillo del Txorierri vía MPLS VPNL2):

EMPLAZAMIENTO	FABRICANTE	MODELO
ATXURI	HUAWEI	S5720-EI
BERMEO	HUAWEI	S5720-EI

DURANGO	HUAWEI	S5720-EI
ARASO	HUAWEI	S5720-EI
LEZAMA	HUAWEI	S5720-EI

El backup crea una red MPLS-IP periférica capaz de enrutar el tráfico entre sus nodos (vía MPLS VPNL3) conectados por radioenlace cuando se detecta un corte total de la fibra del anillo (excepto en el Txorierri que el backup se hace a nivel 2 vía MPLS VPNL2).

Lo que se ha pretendido con ese diseño de red de backup MPLS-IP es que la conmutación a la red de backup sea automática y cubra todo el tramo de fibra afectado en el menor tiempo posible. Se cubre sólo el tramo cortado usando un enlace de capacidad limitada (200Mbps) frente a la capacidad agregada de la red, 1GE (se dispone de un vano inalámbrico con ancho de banda reducido cubriendo el corte mientras que el resto de la red operaría con el cableado de fibra). De este modo, el offload de tráfico al enlace radio se minimiza, reduciendo la probabilidad de saturación por tráfico en pico.
El siguiente esquema muestra la topología de la red trocal junto con los switches encargados de soportar el backup MPLS (aquellos etiquetados en rojo en Atxuri, Lezama, Bermeo, Durango y Araso):



4.3 Documentación de referencia

Los trabajos objeto del presente concurso comprenderán todas las labores necesarias para la "Renovación del equipamiento de la red troncal de comunicaciones OT de ETS", tendrán como referencia la siguiente documentación:

- Proyecto de remodelación de la red de comunicaciones de ETS en el escenario 2010 (2007)
- Auditoría de Seguridad ICS (2020)
- Pliego de prescripciones técnicas de actualización de medidas de ciberseguridad en la red de explotación de ETS (2021)

5 TRABAJOS A REALIZAR POR EL CONTRATISTA

Los trabajos a realizar por el contratista se describen en los siguientes puntos

5.1 Alcance

En el punto 4.2 del documento (Situación actual) se ha hecho una descripción de la red actualmente en funcionamiento a nivel de CORE y ACCESO, así como del back-up. De forma similar, este punto 5 trata de describir la evolución de toda la red en su conjunto, CORE y ACCESO. El alcance principal de este pliego es únicamente la renovación del equipamiento de CORE, así como la evolución de una Red IP a una red MPLS-IP en el ámbito del CORE para crear las bases para una migración total (Core y Acceso) de la red a MPLS-IP que se probará en aquellas ramas de acceso cuyo equipamiento actual lo permita. Sin embargo, esta renovación se plantea llevarla a cabo de tal manera que se permita optimizar la inversión desde diversos ángulos:

1) Por una parte se pretende aprovechar durante una fase de transición que puede ser larga, todos los elementos IP-MPLS ya instalados; principalmente los de cabecera de estación. Se recuerda en este punto que los equipos que cumplen esta funcionalidad generalmente pertenecen a la familia 5720 de Huawei (actualmente en *phase-out*). En el caso concreto del *core*, en las estaciones de Ermua, Araso, Gernika y Bermeo hay sendos dispositivos de esta familia que se quedarán a disposición de ETS y que permitiría su implementación en otras estaciones como equipos de cabecera o bien como equipos de repuesto.

2) La presente licitación permite dotar de un sistema de monitorización y gestión a la red IP, al modo como ya se hace con la red de transporte SDH. Por esta razón, dentro del alcance deberá incluirse un SW con esta funcionalidad dirigido a los nuevos nodos del *core* pero que también permitan integrar, al menos, todos los nodos de cabecera que dispongan de capacidad IP-MPLS. Para homogeneizar la solución se considerarán 100 licencias para equipos IP-MPLS. Esta cantidad permitirá abarcar todos los nodos propios de este concurso, todos los nodos de cabecera de la red actual con funcionalidad IP-MPLS, así como una pequeña reserva para nodos de acceso secundario que resulte de interés monitorizar. Este SW de gestión, en cualquier caso, permitirá establecer una política de adquisición de licencias por si en el futuro ETS desea incorporar dispositivos adicionales al sistema de monitorización y gestión.

Queda fuera del alcance de esta licitación el equipamiento de seguridad así como las políticas de la misma, que serán objeto de otro expediente completo que abarque seguridad perimetral, *endpoints* y servidores.

5.2 Análisis de la situación actual y evolución de red

Se propone como primera acción de este apartado el actualizar/renovar el actual *CORE*-IP que realiza el routing de red, por un *CORE* MPLS-IP. También será necesaria la ***migración de los servicios de nivel 2*** que actualmente se proporcionan en la red de Acceso (Estaciones) a una red que trabaje igualmente en un entorno MPLS-IP que llegue a todos los extremos remotos de la red.

Esto requiere de un análisis previo para confirmar que la realización de esta arquitectura con elementos de nivel 3 de tipo router/switch es viable.

Adicionalmente habría que añadir / intercalar equipos routers modulares adicionales de nueva generación con todos sus elementos redundados, que se ubicarían al menos en los emplazamientos clave de Atxuri y Amara, donde actualmente hay nodos Enterasys (Matrix N3) de la misma categoría de fiabilidad (en cuando a redundancia de elementos).

En muchas de las estaciones (Red de Acceso) hay switches Huawei S5720-EI con capacidades completas MPLS y funcionalidades de nivel 3 capaces de ser migrados un entorno MPLS-IP. Las distintas topologías de lineales y anillos (Red de Acceso) que actualmente dan servicios de nivel 2 (Vlans) se migrarán a servicios MPLS-IP de nivel 3 (L3VPN) aislados unos de otros. Esta nueva topología permitirá marcar con una calidad de servicio para priorizar servicios críticos y además en caso necesario permitirá solapamiento de rangos IP siempre que se usen en servicios L3VPN distintos.

Se entiende que la evolución de la red pretende tanto la mejora de prestaciones y escalabilidad, como la sustitución de equipamiento obsoleto y sin soporte (sin RMAs, repuestos, etc.).

Una vez realizada la migración de la red de CORE y Acceso de IP a MPLS-IP, el siguiente paso consistiría en interconectar el resto de subredes y elementos anteriormente descritos en los puntos 4.2.3 y 4.2.4.

Por otro lado, la conexión del *CORE*-MPLS-TP no debería presentar ningún inconveniente, ya que hay un estándar que define el procedimiento para conectar MPLS-TP con MPLS-IP, siendo en este caso la recomendación el modelo llamado "peering-model" (una red no contiene a la otra, sino que son lineales y se conectan para enlazar elementos de una y de otra). Esta definición se halla en la RFC "*Interworking between MPLS-TP and IP/MPLS; IETF Draft draft-martinotti-mpls-tp-interworking-02; June 2011*".

Habría que definir tanto la arquitectura, como las situaciones intermedias, así como el procedimiento de evolución/migración ordenado.

5.3 Planteamiento de arquitectura

La nueva arquitectura deberá estar formada por dos tipos de redes. Una red de *CORE* o backbone formada por los nodos principales y la red de ACCESO que son el conjunto de

anillos/lineales que conforman toda la red de estaciones de ETS. **Este análisis se centra única y exclusivamente en la red de *CORE*, en su migración de un *CORE* IP nativo a un *CORE* IP-MPLS**. **La extensión de la red MPLS hasta el acceso queda fuera del ámbito de esta licitación.** Cabe únicamente reseñar que para poder extender MPLS hasta el acceso se necesitaría disponer de electrónica de red en todo el acceso capaz de soportar MPLS.

A continuación, se plantea un posible diseño de la arquitectura global de la red ETS que estará sujeta a modificaciones en base a las propuestas alternativas que puedan realizar los distintos licitadores.

La nueva red de *CORE* estará compuesta por un anillo principal de routers IP/MPLS de 10GbE comunicados con fibra óptica y situados en los emplazamientos oportunos para el correcto diseño de la red. Su objetivo es servir de red de *backbone* para las redes de datos existentes y los servicios disponibles en la línea (servicios de voz, servicios de alta disponibilidad, servicios de propósito general, telemando de energía, servicios de detectores, protección y seguridad, corporativos, etc.).

Se asegurará así 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.

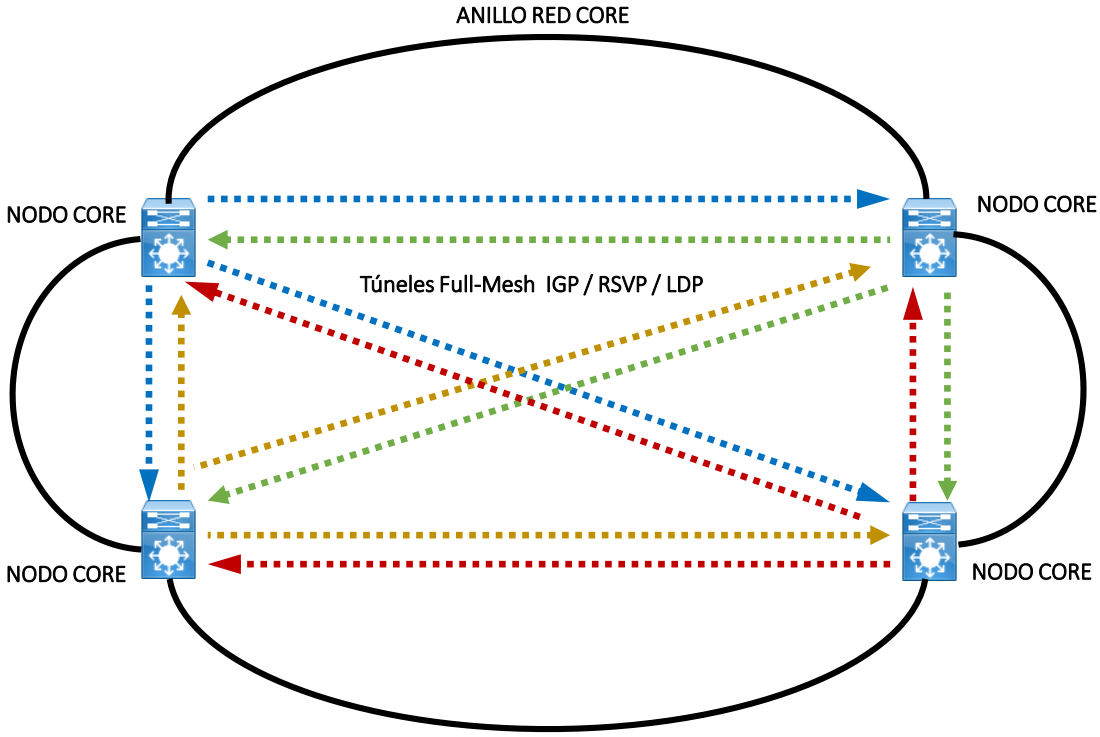
La red de *CORE* será IP/MPLS para mejorar los tiempos de convergencia, latencias y poder implementar VPNs, QoS e Ingeniería de Tráfico y se apoyará en la red de cables de fibra óptica para comunicar sus equipos.

Sobre ella se implementarán VPN N3 sobre MPLS o VPLS según conveniencia del servicio de telecomunicaciones a proporcionar. Se configurará para permitir obtener tiempos de restablecimiento ante fallos inferiores a 50 ms extremo a extremo para todos los servicios que lo demanden. Para el servicio de CCTV deberá soportar multicast.

Las principales ventajas que ofrecerá la red MPLS-IP son las siguientes:

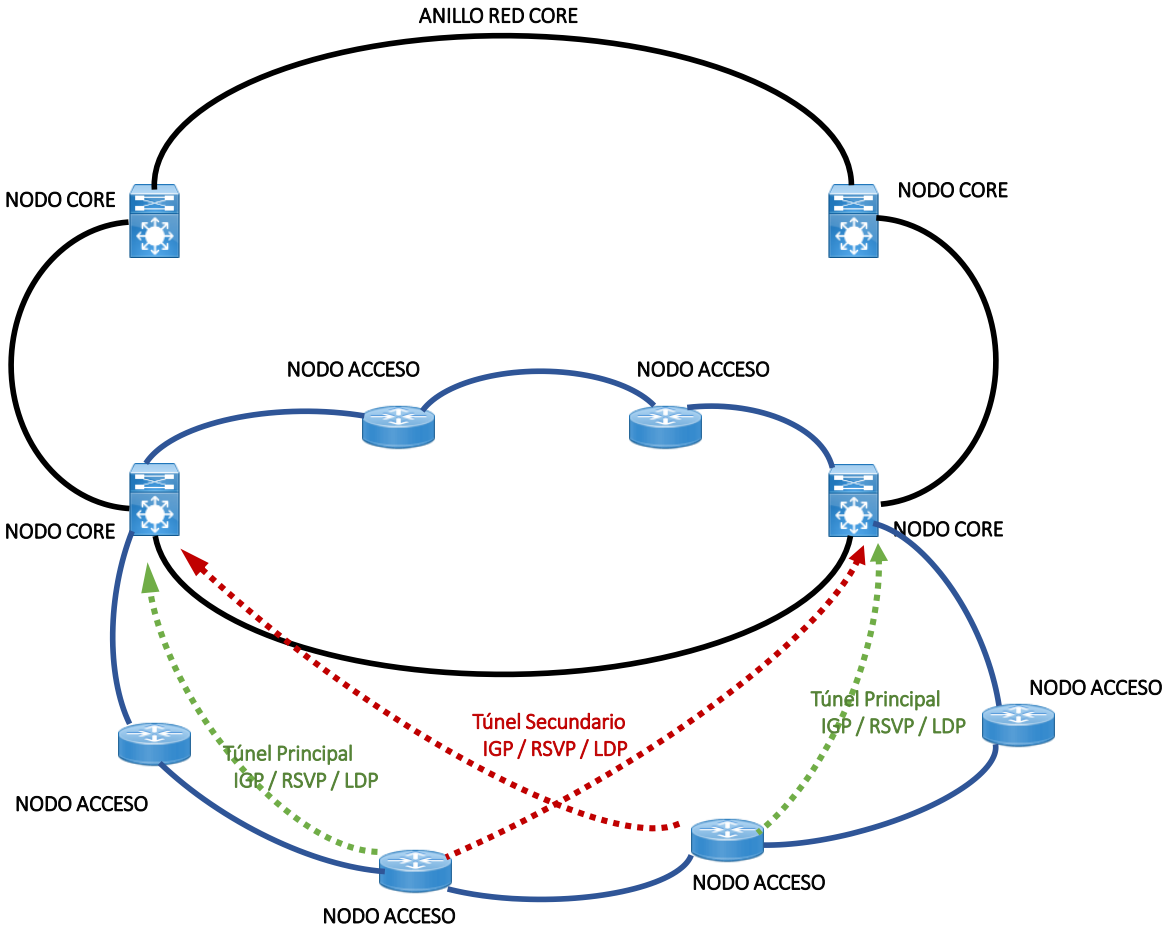
- Permite un uso eficiente del ancho de banda y gran granularidad. Permite concentrar el tráfico de los diferentes servicios evitando el problema de reservar ancho de banda inutilizado.
- Presenta mecanismos de Calidad de Servicio (QoS) mediante la asignación de prioridades, lo que permite que los servicios 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 VLANs.
- Permite una gestión sencilla del ancho de banda mediante las diferentes VLANs y VPNs que se configuren, asociando a cada una de ellas diferentes prioridades.

Dentro de la Red de *CORE* se establecerá una topología full-mesh de túneles end-to-end entre todos los nodos del *CORE*. Esta topología protegerá ante cualquier caída de uno de los equipos o enlaces del *CORE*.



De la misma forma dentro de la Red de acceso se establecerán mecanismos de protección para proteger el tráfico del anillo. Pero en este caso la propuesta no es hacer un full-mesh de túneles entre todos los nodos del anillo (poco escalable y gran consumo de recursos) sino que se establecerán dos túneles contra los nodos principales (Nodo *CORE*) del anillo de backbone, uno principal y otro que actuará como respaldo.

En este punto hay que indicar que en la actualidad la mayor parte de los anillos no están establecidos entre dos nodos de *CORE* sino que el anillo comienza y termina sobre un mismo nodo de *CORE*. En otros casos realmente no es un anillo sino que es un lineal con una única conexión a un equipo de *CORE*. La propuesta de la nueva arquitectura deberá incluir allí donde sea posible crear anillos y no lineales con una conexión que forme un anillo pasando por dos nodos de *CORE* tal y como se muestra en la siguiente figura:



De esta forma cada nodo de la Red de *CORE* actuará como reflector de rutas de los anillos de la Red de Acceso consiguiendo un diseño jerárquico de VPNs que permite la protección del tráfico de la Red de Acceso ante cualquier caída de nodos de la Red de *CORE*. Este diseño evita que los nodos de *CORE* tengan que mantener conexiones con el resto de nodos de la Red de Acceso de los diferentes anillos al suyo, y por tanto conservar los recursos de los equipos de *CORE* y también de Acceso (estos últimos solo tendrán que establecer dos sesiones contra los routers de *CORE*).

Tal y como se ha indicado para los servicios de nivel 3 se empleará un diseño de VPNs de nivel 3 jerárquicas apoyadas por mecanismos de rápida convergencia en el protocolo BGP. Esto permitirá crear rutas de respaldo en las tablas de forwarding para dotar de una rápida convergencia ante cualquier caída de enlace o equipo. Todos los nodos de Acceso enviarán el tráfico a los nodos del *CORE* y estos decidirán si el tráfico se queda dentro del mismo anillo o se tiene que enviar a otro nodo del *CORE* u otro anillo.

Para los servicios especiales que requieran una conexión VPN de nivel 2 (VPLS) se seguirá el mismo esquema jerárquico estableciendo conexiones principal y redundante contra los nodos del CORE

5.4 Descripción de los nodos a suministrar

Todos los nodos de la red serán nodos de alta capacidad con enlaces 10GbE en el lado *Backbone* y enlaces 1GbE en el lado acceso. Para mejorar los tiempos de convergencia, todos los interfaces entre los nodos del *CORE* y entre éstos y los nodos principales de estación es conveniente que sean ópticos.

El diseño del nuevo *CORE* MPLS-IP mantendrá la aproximación ya existente en el *CORE* actual de la red, diferenciando por un lado los nodos más importantes (Atxuri y Amara) del resto de los nodos que conforman el *CORE*.

Los nodos de Atxuri y Amara, donde se encuentran ubicados los centros de control, **se instalarán en configuración de alta disponibilidad,** con todos los elementos vitales, procesadoras, alimentación y tarjetas de línea redundadas. Serán, por tanto, equipos modulares, potentes y versátiles.

El resto de los nodos del *CORE* serán equipos de chasis fijo con alimentación redundante. Todos ellos con capacidades completas MPLS, funcionalidades de nivel 3 e interfaces ópticos de 10GbE.

Los nodos de la red de Acceso serán equipos de chasis fijo con alimentación redundante. Todos ellos con capacidades completas MPLS, funcionalidades de nivel 3 e interfaces ópticos de 10GbE o 1GbE según las necesidades.

5.4.1 Descripción de los nodos de Atxuri y Amara

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

La arquitectura hardware y software de los nodos tendrá 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.

1. 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.

2. 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.

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.

3. 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.

4. 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).

5.4.2 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.

A/Protección en los equipos

Los equipos 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)
- Fuente de alimentación redundada.
- Ventilación redundada.
- Slots de expansión para tarjetas insertables y extraíbles en caliente.
- Los interfaces del anillo estarán en tarjetas diferentes.

B/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.

C/ Protección en la puerta de enlace (VRRP)

Virtual Router Redundancy (VRRP) es un protocolo estándar diseñado para eliminar el punto único de fallo que existe cuando en una red sólo hay un dispositivo actuando como ruta por defecto o puerta de enlace (Default Gateway). Cuando un grupo de enrutadores están configurados con VRRP, el protocolo asigna dinámicamente a uno de ellos la función de enrutador virtual. El enrutador que controla la IP asociada al enrutador virtual será el master del grupo VRRP.

Por tanto, una vez formado el grupo VRRP, tendremos una IP virtual asociada al grupo, que será la que haga de DG para los dispositivos de la LAN. Se asignará también un enrutador de respaldo que asumirá el rol de DG si el enrutador que actúa como master deja de estar disponible. De esta manera, se aporta redundancia a nivel de puerta de enlace.

Al enrutador virtual se le asocia una dirección IP virtual y una MAC virtual. Esta IP y esta MAC nunca cambian independientemente del enrutador físico que el protocolo escoja como master.

5.4.3 Seguridad de la red

Algunas de las propiedades de los LSR 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´s de IPSec de Nivel 3 y las VPN´s 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´s 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.

5.5 **Sistema de gestión**

Conjuntamente con la evolución hacia una red MPLS-IP, el proyecto aborda la necesidad de incorporar un sistema de gestión de red capaz de gestionar tanto los nuevos equipos del *CORE* MPLS-IP como el resto de equipamiento de red ya existente.

Como hemos comentado anteriormente, se trata de una red heterogénea en cuanto a la electrónica de red presente en la red (distintos fabricantes) por lo que la solución propuesta deberá ser capaz de gestionar equipamiento multifabricante.

El sistema de gestión de red o NMS (Network Management System) deberá basarse en los siguientes conceptos:

- Estar centrado en la topología
- Permitir una gestión simplificada
- Ofrecer una eficiencia mejorada en la operación y mantenimiento (O&M, Operation and Maintenance)

Los administradores de la red deben ser capaces de obtener una visión global del estado de la red observando la topología de la misma. Así, el NMS no sólo deberá proveer capacidades básicas de gestión de la red (alarmas, topología, rendimiento o configuración), sino que deberá ofrecer de forma proactiva avisos sobre posibles fallos de red. Adicionalmente deberá proporcionar distintos métodos para la localización de fallos, ayudando de una forma efectiva a los administradores de la red a encontrar y solucionar fallos.

Las características principales que deberá cumplir el sistema de gestión de red serán:

- Facilidad de uso:
  - Interfaz de usuario (GUI, Graphical User Interface) amigable
  - Monitorización activa y O&M visible

- Interfaz flexible, ágil y abierto

- Gestión unificada
  - Capaz de gestionar múltiples dispositivos

- O&M inteligente
  - Plug and play
  - Detección automática de la calidad de la red

A medida que tanto la red como las aplicaciones van creciendo también lo hacen los dispositivos que se van desplegando (electrónica de red fija, APs, controladores, dispositivos IoT) pertenecientes a diferentes fabricantes. Cada uno de ellos tiene su propio sistema de gestión de red lo que genera una gran confusión y una problemática para los administradores de la red.

Para poder abordar esos problemas, se instalará un sistema de gestión de red unificado capaz de proveer gestión de toda la red, de todos los recursos, asegurando la estabilidad de la misma y aumentando la eficiencia en el O&M.

El sistema de gestión de red deberá estar compuesto de una plataforma unificada capaz de incorporar componentes opcionales que puedan ser añadidos en función de las necesidades que puedan ir surgiendo, facilitando así una rápida expansión. Por ejemplo, en el caso de incorporar dispositivos móviles a la red (APs, controladoras WLAN) se podrá añadir la correspondiente funcionalidad al sistema de gestión que permita gestionar los nuevos dispositivos e incorporarlos a su monitorización.

Deberá contener herramientas que mejoren la eficiencia de configuración, evitando a los administradores de red el tener que memorizar comandos y permitiéndoles en su lugar utilizar herramientas inteligentes de configuración para completar la configuración de dispositivos por lotes.

Deberá incorporar soluciones que permitan monitorizar el rendimiento basado en grupos, de manera que se puedan agrupar dispositivos con las mismas características en un mismo grupo y se monitoricen en todos ellos los mismos parámetros.

Ya hemos señalado anteriormente que el sistema de gestión y monitorización que proponga el licitador tiene que integrar, por una parte, los equipos de la propia licitación (que en la solución planteada suman 18 equipos), así como al menos los nodos de cabecera IP-MPLS existentes en la red de ETS. Para homogeneizar, se considera un mínimo de 100 licencias que se deberán dar de alta así como configurar.

Este Sistema podría, en el futuro, convertirse en el único elemento de gestión de la capa IP, routing y transporte.

5.6 Documentación y Formación

El contratista deberá a entregar a ETS toda la documentación resultado de la implantación realizada, incluyendo:

- Actualización de la topología física y lógica de la red de ETS, conteniendo los hitos previos del proceso de migración de la red CORE
- Datasheets de los equipos implantados e interfaces ópticos
- Documentación de diseño y configuración del sistema del CORE
- Documentación funcional de los aplicativos implantados
- Procedimientos para las tareas habituales por el administrador de la red de explotación de ETS y en especial de los aplicativos del sistema de gestión implementado, tanto en los aspectos operativos como de seguridad
- Creación de rutas
- Creación de reglas
- Políticas básicas de seguridad
- Mejores prácticas para la configuración de los equipos
- Procedimiento para restablecer una configuración mal aplicada
- Procedimiento para renovación de certificados y licencias

Toda información adicional que sea necesaria para el correcto funcionamiento de la instalación

Adicionalmente, durante todo el proceso de instalación, configuración, y pruebas, el adjudicatario transferirá el conocimiento necesario a los técnicos de ETS para que estos sean autónomos en la gestión del nuevo sistema.

La formación comenzará con una sesión inicial, previa a la configuración del sistema.

La instalación y configuración de los aplicativos identificados se realizará conjuntamente con las personas que ETS determine, formando en la realización de las tareas tipo y de mantenimiento.

Todo el proceso se realizará en las instalaciones de ETS.

5.7 Soporte del Adjudicatario

El contratista deberá llevar a cabo el soporte asociado a las actualizaciones de red indicadas, como pueden ser:

- Actualización de licencias de los sistemas integrados en la red de explotación
- Monitorización de los sistemas y elementos que componen la red de explotación, atendiendo a eventos y alarmas generados en la red:
- Estado de las máquinas
- Estado de la CPU

- Estado de la memoria
- Error de paquetes
- Sesiones
- Etc.

- Realización periódica de verificaciones de seguridad
- Propuesta de implantación de medidas para las vulnerabilidades adicionales que se hayan identificado
- Operación remota de la plataforma en 10x5:
- Se realizarán todas las tareas de gestión necesarias para el mantenimiento de la plataforma ya definida:
  - *Creación y Modificación de rutas y reglas*
  - *Modificación de perfiles de acceso*
  - *Aplicación de la solución ante incidencias*
  - *Actualización y parches*
- La operación será realizada de forma peticionada por ETS o consensuado entre ambas partes cuando el adjudicatario lo proponga de forma proactiva. Todas las tareas que pudieran suponer un riesgo para la disponibilidad del servicio ferroviario, tendrán que ser realizadas en horario nocturno.
- Actualizaciones de los diferentes sistemas incluidos en este servicio:
- Estas intervenciones se realizarán en horario laboral (8x5), o en una franja horaria en la que no haya servicio ferroviario en caso de poderse ver este afectado, minimizando al máximo los cortes del servicio. Se procederá de la siguiente forma:
  - *Se acordará con ETS la fecha para la actualización y se le explicará las implicaciones que tiene.*
  - *Ejecución de la actualización sobre la solución y verificación del correcto funcionamiento del servicio.*
  - *Notificación a ETS de la finalización del proceso de actualización*
- Aplicación de medidas extraordinarias contra amenazas
- Informes de servicio trimestrales en los que se reflejará el estado de la red y las recomendaciones de mejora

Todas estas actuaciones se deberán llevar a cabo de forma coordinada con ETS y con su previa autorización y se podrán prolongar por un plazo de 2 años desde la fecha de finalización de la implantación de las medidas indicadas en este pliego.

Este servicio se prestará bajo un modelo de provisión de servicios en el que la gestión y la realización de actividades será responsabilidad del adjudicatario y la prestación del servicio está basado en SLOs (Service Level Objective), de forma que, en el transcurso de su horario de atención, el objetivo de equipo de soporte del adjudicatario será responder ante una incidencia o consulta, en un tiempo máximo establecido:

Alerta	Riesgo de Impacto	Tiempo máximo de respuesta
Alta	Caída del servicio	<= 1 hora
Media	Servicio en riesgo	<= 4 horas
Baja	Bajo rendimiento	<= 16 horas
Consulta	Asistencia General	<= 24 horas

Cualquier actuación realizada por el contratista supondrá la actualización por su parte de la documentación correspondiente.

5.8 Garantía

Todo el equipamiento propuesto se deberá ofrecer con una garantía de dos (2) años y con un tiempo mínimo de cinco (5) años en el que los fabricantes deberán disponer de piezas de repuesto para garantizar su reparación.

6 ESPECIFICACIONES EQUIPAMIENTO RED

6.1 Router *CORE* MPLS-IP modular: Atxuri y Amara

Router IP/MPLS de CORE. Incluye chasis modular con ventiladores, fuentes de alimentación, módulos de interfaces, procesador y routing/forwarding engine todos ellos redundantes, cableado, licencias, software e integración en sistema de gestión. Equipado con una capacidad mínima de 2 tarjetas por equipo de 10 puertos 10GE/GE SFP+ para proveer redundancia interchasis. Posibilidad de incorporar tarjetas de baja velocidad (E1) y de alta velocidad (GE, 10GE, 25GE, 40GE, 50GE, 100GE) permitiendo en un futuro escalar la solución actual mediante la incorporación de los interfaces ópticos correspondientes. El equipo actuará como equipo P/PE en la red MPLS.

El equipo se suministrará con todos los interfaces ópticos al completo.

6.1.1 Descripción del sistema

Algunas de las características generales que deberán tener los nodos de CORE modulares son:

Redundancia multifuncional

Enrutamiento IP/IPS/MPLS

Que en un mismo chasis se soporte la combinación de alta densidad de puertos y diferentes velocidades de funcionamiento (Fast Ethernet, Giga Ethernet, 10Gigabit Ethernet, 25Gigabit Ethernet, 40GigaEthernet, 50GigaEthernet, 100GigaEthernet).

Tendrán mecanismos de reinicio y reenrutamiento de tráfico en caso de fallos, y tecnología FastReroute para minimizar el tiempo de convergencia en caso de caída de algún enlace.

El equipo deberá tener la capacidad de controlar y garantizar el rendimiento con tráfico sensible a retardos, jitter, latencia, etc., o lo que es lo mismo, podrá asignar diferentes niveles de calidad de servicio.

El nodo tendrá posibilidad de separar los niveles de control y reenvío. Esto se consigue haciendo que la arquitectura hardware y software de los nodos Gigabit tenga una clara separación entre las funciones de control (Routing) y reenvío (Forwarding), evitando que dichas funciones compitan por los mismos recursos del sistema y así, cada una de ellas se implemente de forma independiente.

Los nodos tendrán una estructura modular con fuentes de alimentación, matriz de conmutación y tarjetas extraíbles en caliente y soporte avanzado de características MPLS y creación de paths RSVP/LDP. Se entiende por extraíbles en caliente que dicha operación no causa prejuicio alguno ni interrupción en los módulos restantes del equipo y que no hay necesidad de apagar el equipo.

Tendrá capacidad de actualización del firmware sin pérdida de prestaciones.

Algunas de las propiedades relativas a la seguridad serán la utilización de filtros de Firewall de entrada y de salida, gestión de sesiones de tráfico encriptadas, funcionalidades de túneles seguros, logins remotos seguros, niveles de privilegios configurables, filtros de tráfico SNMP, sesiones BGP IPsec para encriptar el control de tráfico o creación de logs del sistema que permitan monitorizar un sistema mediante mensajes codificados.

Los nodos serán routers de alta capacidad de conmutación para equipos de gran densidad de puertos y altas necesidades de fiabilidad por paquete enrutado. Como ya se ha dicho anteriormente, con el objetivo de mejorar los tiempos de convergencia, se proponen nodos de transporte de datos con funcionalidad MPLS.

Los nodos deberán ser capaces de 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).

6.1.2 Características técnicas y funcionales

1. Chasis

El chasis del router debe ser instalable en bastidor ETSI normalizado de 19”. Todos los elementos constructivos del equipo deben cumplir con la directiva 2002/95/CE de Restricción de Sustancias Peligrosas (RoHs) en aparatos electrónicos. El diseño del chasis debe posibilitar la diferenciación de zonas calientes/frías del equipo e incluir un módulo de ventilación redundante que permita la operación normal del equipo en máximo rendimiento.

2. Modularidad

Los nodos deben ser modulares, con fuentes de alimentación, matriz de conmutación y tarjetas extraíbles en caliente sin necesidad de desconectar la alimentación del mismo.

El equipo estará equipado con módulos de proceso y fuentes de alimentación suficientes para su perfecta operatividad en el momento del suministro. Cualquier ampliación posterior no requerirá ninguna ampliación de los elementos constructivos sino meramente la ampliación de tarjetas de entrada/salida en función de los requisitos deseados.

El fallo de alguna de las tarjetas de entrada/salida no debe degradar ni comprometer las prestaciones del resto de módulos del equipo.

3. Capacidad de ampliación

Al ser modular, el nodo tendrá ranuras abiertas/slots en las que se puedan instalar distintas tarjetas de interfaz.

El equipo incluirá tarjetas con posibilidad de puertos Ethernet de alta capacidad como 100GbEthernet, 10GbEthernet, 1GbEthernet, 10/100/1000 Ethernet, E1 o SDH y con interfaces coloreadas que permitan el tráfico WDM.

4. Compatibilidad e inmunidad electromagnética

El equipo cumplirá con la legislación vigente sobre normativa en materia de compatibilidad electromagnética y exposición a campos electromagnéticos y garantizará la eficiencia energética del mismo.

5. Rangos operativos

- Según la norma IEC 68-2-14, los equipos deberán funcionar correctamente a cualquier temperatura que se encuentre dentro del rango: -5° C a +40° C (Operación) -30° C a +70° C (Almacenamiento)
- Deberán soportar una humedad relativa de entre: 5% a 85% (No condensando).

Los fabricantes deberán aportar una justificación de las pruebas llevadas a cabo por medio de las cuales se proporcionan los rangos operativos de los equipos.

6. Número y tipología de puertos a considerar

El nodo deberá tener capacidad de funcionar con puertos de alta capacidad, de al menos 100GbEthernet, 50Gb Ethernet, 40Gb Ethernet, 25Gb Ethernet, 10Gb Ethernet, 1Gb Ethernet, 10/100/1000 Ethernet, E1 o SDH y con interfaces para conexiones mediante cable de cobre o interfaces ópticos coloreadas, es decir, que soportan tecnologías WDM. Respecto al tipo de conectores podrán ser de tipo RJ-45 para el caso de conexiones con cables de cobre o de tipo SC y LC para conexiones de fibra óptica.

7. Alimentación

El equipo se alimentará en AC y contará con redundancia de alimentación en, al menos, configuración 1+1. Las fuentes serán extraíbles y sustituibles en caliente.

El equipo deberá poder admitir dos alimentaciones de origen diferente, de modo que ante el fallo de una entrada el equipo pueda seguir funcionando normalmente con la otra.

La conmutación entre una fuente de alimentación y la de reserva no debe provocar interrupción del servicio ni pérdida de funcionalidad del mismo.

Las fuentes de alimentación deben garantizar la operación del equipo configurado en su máxima capacidad y al máximo rendimiento.

8. Promedio del tiempo entre fallos del sistema (MTBF)

El equipo debe cumplir un MTBF de al menos 250000 horas.

9. Tasa de transferencia (THROUGHPUT) y capacidad de conmutación

La tasa de transferencia total de los nodos será superior a 450 Mpps. Los puertos (100Gbps, 10Gbps, 1Gbps, 10 Mbps, 1000 Mbps, 100 Mbps, etc.) reenviarán los datos a velocidad de línea.

La capacidad de conmutación debe ser de al menos 480Gbps. La capacidad solicitada será para cada una de las matrices que se instalen. Dispondrá de circuitos integrados especializados (ASIC) diseñados expresamente, que proporcionen funciones de reenvío de tramas de la capa MAC y filtrado en todos los puertos del conmutador, de forma totalmente compatible con las normas 802.1D y 802.1w.

10. Requerimientos de nivel 2

En referencia a las normas de funcionamiento con diferentes velocidades, distintos tipos de medios y redes virtuales, los equipos deberán soportar, al menos, los siguientes estándares:

- Estándar IEEE 802.3. Ethernet

- Estándar IEEE 802.3u. FastEthernet

- Estándar IEEE 802.3ab. GigaEthernet

- Estándar IEEE 802.3x. Control de Flujo

- Estándar IEEE 802.1q. VLANs

Se tendrá opción de transportar tráfico sin etiquetar, con etiquetado .q y con etiquetado q in q. y capacidad de modificar etiquetas por puerto.

Los nodos tendrán la capacidad de gestionar al menos 4096 VLANs por puerto y se podrán manejar sin conflicto VLANs con las mismas etiquetas pertenecientes a

clientes diferentes, sin que el rendimiento del equipo se vea afectado por la creación de VLANs en base a ninguno de los criterios, aunque se creen el máximo de ellas.

Se establece que los nodos deben cumplir los siguientes estándares de interconexión relacionados con la gestión de redes:

- Estándar IEEE 802.1D. Protocolo Spanning Tree.

- Estándar IEEE 802.1w Protocolo Rapid Spanning Tree.

- Estándar IEEE 802.1s Protocolo MultiVLAN Spanning Tree.

- Estándar IEEE 802.1x. Autenticación. Control Acceso por puerto.

- RFC 3635, RFC 2665 o RFC 2358. Definitions of Managed Objects for the Ethernet-like Interface Types.

11. Agregación de enlaces

Con la intención de que los nodos cumplan con los requisitos necesarios referentes a la agregación de enlaces, será necesario que los equipos soporten el estándar IEEE 802.3ad (Link Aggregation Control Protocol).

Además, los puertos que pertenezcan a una agregación serán tratados como un único puerto lógico y al caerse uno de los enlaces pertenecientes a la agregación, ésta sigue operativa y los parámetros del tráfico resultan afectados de forma despreciable, recuperándose en menos de 1 segundo tras reponer el enlace caído.

12. Requerimientos de nivel 3

El equipo soportará los protocolos habituales de routing, RIP, BGP, BGPv6, RIPng, OSPF, OSPFv3, IS-IS, IS-ISv6, protocolos de enrutamiento IPv6 unicast estático y dinámico.

Como requerimientos de alta disponibilidad, deben soportar el protocolo VRRP (Virtual Router Redundancy Protocol) y/o SEP (Smart Ethernet Protection).

Los nodos también deben soportar protocolos de enrutamiento multicast IPv6.

Será valorable que los equipos propuestos soporten Segment Routing SRv6.

13. Marcado de paquetes

Para la clasificación y marcado de paquetes los equipos deben soportar IETF DiffServ en función de interfaz, subinterfaz, protocolo, puerto, dirección MAC, tamaño, el estándar IEEE 802.1p y el protocolo DSCP preference.

Por otro lado, los criterios de marcado podrán estar basadas en:

- Dirección MAC origen y destino

- Dirección IP origen y destino

- Puerto

- Protocolo

- VLAN

14. Requerimientos de gestión de ancho de banda

El equipo permitirá controlar el uso de ancho de banda que está utilizando una aplicación impidiendo que en momentos puntuales consuma todo el ancho de banda disponible limitando las prestaciones de otras aplicaciones que comparten con ella la misma prioridad. Se debe poder Controlar el Ancho de Banda por: puerto físico, flujo (L3/L4) y grupo de flujos.

Sobre el tráfico filtrado se debe poder controlar, limitar, priorizar y conformar. Además, debe tener capacidad de controlar, limitar, priorizar y conformar tráfico según su tipo: multicast, unicast, broadcast o desconocido.

Con el fin de proteger la CPU de posibles usos malintencionados o errores de configuración en los protocolos de control, es necesario poder soportar Rate Limiting de los siguientes protocolos:

- ICMP

- LDP

- OSPF

- RSVP

- Telnet

- SNMP

15. Requerimientos de priorización del tráfico

Mediante la asignación de prioridades se garantiza una relación de ancho de banda entre las aplicaciones individuales o protocolos y de esta forma, se asigna una calidad de servicio (QoS) a cada tipo de tráfico, consiguiendo así controlar y gestionar el ancho de banda de las conexiones fijas de la red correspondiente, permitiendo que los servicios prioritarios no se vean afectados por posibles problemas de congestión. Se podrá filtrar por diferentes campos, tanto en el nivel 2 o capa de enlace como en el nivel 3 o capa de red.

Nivel 2

El equipo debe ser capaz de asignar prioridades de tráfico en la capa de enlace (nivel 2) al menos según los campos:

- MAC origen

- MAC destino

- VLAN ID

- EtherType

Nivel 3

En la capa de red (nivel 3) se podrá hacer diferenciación de tipos de tráfico, o lo que es lo mismo, priorizarlo, como mínimo, por los campos que se detallan a continuación:

- IP Origen

- IP Destino

- DSCP (Differentiated Services Code Point)

- Por el campo ToS (Type of Service)

- Por tipo de interfaz.

Nivel 4

El equipo deberá poder priorizar por diferentes tipos de tráfico al menos a nivel 4, y como mínimo según los siguientes criterios:

- Por protocolo TCP/UDP

- Por puerto TCP/UDP origen

- Por puerto TCP/UDP destino

Requerimientos MPLS

En este apartado se enumerarán los estándares específicos del protocolo MPLS que debe cumplir el equipo:

- Estándar RFC 2702, que describe los requisitos para ingeniería de tráfico de MPLS.

- Estándar RFC 3031, referida a la arquitectura MPLS.

- Estándar RFC 3032, trata del cifrado de pila de etiquetas MPLS.

- Estándar RFC 3063, para el mecanismo de prevención de bucles MPLS.

- MPLS fast reroute. Mecanismo de backup.

- LSP de backup señalizados y sin señalizar.

- Número máximo de LSP por equipo en LER, de al menos 5000.

Debe soportar el protocolo VPLS, que es un estándar que permite la creación de túneles para comunicaciones multipunto a multipunto. Esto permite crear una gran LAN a partir de múltiples LAN menores y dispersas, interconectándolas mediante una red de conmutación de paquetes.

Respecto a este servicio, es necesario que el equipo soporte:

- Estándar RFC 4761.

- Estándar RFC 4762.

Protocolo de distribución de etiquetas (LDP)

El protocolo LDP (Label Distribution Protocol) es un protocolo para la distribución de etiquetas MPLS entre los equipos de la red de MPLS. Mediante este protocolo los enrutadores de etiquetas intercambian información acerca de la posibilidad de alcanzar otros enrutadores, y las etiquetas que son necesarias para ello.

Los siguientes estándares especifican diferentes aplicaciones del protocolo de distribución de etiquetas, de manera que todas estas características queden normalizadas en el equipo:

- Estándar RFC 5036. Sustituye a la anterior RFC 3036.

- Estándar RFC 3037.

Además, los equipos deberán cumplir con las siguientes características, que mejoran y amplían las funcionalidades del protocolo de distribución de etiquetas LDP:

- Funcionalidad de Fast Re-Route, que acelera la recuperación del tráfico crítico cuando se produce algún fallo en el enlace.

- Mecanismos de Graceful Restart: que permitirá seguir enviando/procesando paquetes aun cuando falle el plano de control de BGP (encargado de definir las mejores rutas) y añade al routing mayores niveles de estabilidad y reduce el consumo de recursos por parte del plano de control.

- VPLS. Es una forma de proporcionar Ethernet multipunto a multipunto basado en la comunicación sobre redes IP / MPLS

- El equipo permitirá también caracterizar los túneles utilizando cualquiera de los siguientes parámetros:

§ Puerto Ethernet

§ VLANs

§ Combinación de puertos y VLANs

§ Rangos de VLANs

§ Combinación de puertos y rangos de VLANs

- H-VPLS (Hierarchical Virtual Private LAN service), que mejora la escalabilidad de VPLS (descrito anteriormente) permitiendo la creación de jerarquías.

Protocolo ISIS

IS-IS (Intermediate System to Intermediate System) es un protocolo de enrutamiento dinámico que trata de la interconexión que permite trabajar con ToS

(Type of Service) para la ingeniería de tráfico. Este protocolo pretende proporcionar grandes dominios de enrutamiento consistentes en combinaciones de varios tipos de subred.

En el caso del equipo de CORE, deberá cumplir las siguientes normas en referencia a dicho protocolo, que forman parte de una serie de normas internacionales realizadas para facilitar la interconexión de sistemas abiertos:

- RFC 1142 OSI IS-IS Intra-domain Routing Protocol.

- RFC 1195 Use of OSI IS-IS for routing in TCP/IP & dual environments.

- RFC 2763 Dynamic Hostname Exchange for IS-IS

- RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS

- RFC 2973 IS-IS Mesh Groups

- RFC 3373 Three-Way Handshake for IS-IS Point-to-Point Adjacencies.

- ISO 10589

- Los nodos soportarán un número mínimo de rutas de, al menos, 250.000.

- El número de rutas en un nivel será de, al menos, 1024.

Protocolo OSPF

OSPF, abreviatura de Open Shortest Path First, es un protocolo de enrutamiento jerárquico de IGP que se encarga de calcular la ruta más corta que deben seguir los paquetes.

A continuación, se detallan las características mínimas que debe cumplir el equipo, de manera que cumpla con las normas suficientes y tenga las características necesarias para las funciones a desarrollar.

- RFC 1765 OSPF Database Overflow

- RFC 2328 OSPF Version 2

- RFC 2370 Opaque LSA Support

- RFC 3101 OSPF NSSA Option

- RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2 (Importante para la QoS en combinación con RSVP-TE)

El número de interfaces que tendrá el equipo será de, al menos, 64.

El número de adyacencias será de, al menos, 250, el mismo número de adyacencias que, como mínimo, tendrá un interfaz individual.

El equipo soportará un mínimo, de 240.000 rutas y tendrá un número de áreas de, al menos, 8.

Para finalizar con las características englobadas dentro del protocolo OSPF cabe destacar que el número máximo de saltos por ECMP (Equal-cost Multi-Path routing), será de al menos 8.

Protocolo RSVP-TE

Es una extensión del protocolo RSVP para la ingeniería de tráfico y proporciona la reserva de recursos a través de una red IP. Se exigirá que el nodo de transporte cumpla, como mínimo, con las siguientes normativas y funcionalidades.

- RFC 2430 A Provider Architecture for DiffServ & TE Page 994

- RFC 3209 Extensions to RSVP for LSP Tunnels

- RFC 3210 Applicability Statement for Extensions to RSVP for LSP Tunnels

- RFC 2961 RSVP Refresh Overhead Reduction Extensions

- RFC 3175 Aggregation of RSVP for IPv4 & IPv6 Reservations

- RFC 3181 Signaled Pre-emption Priority Policy Element

- Fucionalidad Fast Re-Route.

Protocolo BGP-4

El BGP-4 es un protocolo de encaminamiento entre sistemas autónomos y los nodos de transporte de datos deberán cumplir, al menos, según el siguiente listado de normas:

- RFC 1656 BGP-4 Implementation

- RFC 1771 BGP-4. Actualizada por la RFC 4271.

- RFC 1772 Application of BGP in the Internet

- RFC 1997 BGP Communities Attribute

- RFC 2270 Dedicated AS for Sites homed to Single Provider

- RFC 2385 Protection of BGP sessions via MD5

- RFC 2439 BFP Route Flap Damping

- RFC 2547bis BGP/MPLS VPNs

- RFC 2796 BGP Route Reflection: Alternative to Full-mesh IBGP. Actualizada por la RFC 4456.

- RFC 2858 Multi-protocol Extensions for BGP-4

- RFC 2918 Route Refresh Capability for BGP-4

- RFC 3065 Confederations for BGP. Actualizada por la RFC 5065.

- RFC 3392 Capabilities Advertisement

- MP-BGP

Protocolo RIP

RIP son las siglas de Routing Information Protocol (Protocolo de Información de Enrutamiento). Es un protocolo de puerta de enlace interna o IGP utilizado por los routers para intercambiar información acerca de redes IP. En el caso del equipo tratado en la especificación técnica cumplirá, al menos, con las normas:

- RFC 1058 RIP Version 1

- RFC 2082 RIP Version 2

- RFC 2453 RIP-2 MD5 Authentication

Los equipos soportarán un número de rutas RIP de, al menos, 1000.

VPNs

En referencia a las VPNs hay un grupo de normas que especificará el funcionamiento y características del equipo que se deben de cumplir:

- RFC 2547, referente a las VPNs de BGP/MPLS.

- BGP/MPLS VPNs.

- MPLS-based Layer 2 VPNs.

- MPLS/BGP Virtual Private Network Management Information Base Using SMIv2 (only mplsVpnScalars, mplsVpnVrfTable and mplsVpnVrfRouteTargetTable)

- Virtual Private LAN Service.

Protocolo GRE

El protocolo GRE (Generic Routing Encapsulation) es un protocolo para el establecimiento de túneles a través de Internet. Está definido en varias de las normas que deberá cumplir el equipo y que se detallan a continuación:

- RFC 2784

- RFC 1701

- RFC 1702

Requerimientos de seguridad

Para garantizar la seguridad en la aceptación por parte de la red, habrá varias posibilidades para cumplir con los requisitos de cada situación particular. Se podrá configurar el nodo equipo a través de cada puerto y para equipos con usuarios determinados, de manera que pueda denegarse el acceso al resto de usuarios.

Podrá denegarse el acceso a todos los usuarios que no sean uno determinado, se podrá denegar el acceso de usuarios sólo a una VLAN determinada, o podrá filtrarse

el acceso con una prioridad, a través de cada puerto, de equipos con usuarios determinados, denegándose el acceso a los demás.

Además, se debe cumplir con el estándar 802.1X que controla el acceso a la red basándose en los puertos y permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla.

Requerimientos de ip multicast

- Para nivel 2 soportará al menos IGMP v1, v2 y v3

- Para nivel 3 soportará al menos PIM-Dense Mode, PIM-Sparse Mode y MOSPF.

Requerimientos de gestión

El equipo permitirá actualizar la configuración sin necesidad de reinicializar y dispondrá de todas las capacidades necesarias para poder satisfacer los requerimientos de la especificación correspondiente a GESTIÓN. Algunos de ellos son: RMON2 o SNMP v1, 2c y 3.

El equipo debe permitir proveer en tiempo real mediciones de control de flujos, para: flujo IP, VLAN, MPLS LSP.

La obtención de la información referente a los flujos anteriores, debe ser mediante la implementación Hardware, con el fin de no afectar al rendimiento del equipo. El equipo debe facilitar herramientas para realizar:

- Monitorización de umbrales.

- Control de accesos.

- Estadísticas de tráfico.

- Notificación de fallos en la red.

- Gestión remota en banda mediante: SNMP, Cliente Telnet, FTP

El soporte para gestión fuera de banda se realizará mediante un terminal o consola conectada al interface de consola/auxiliar.

Respecto a las políticas de contabilidad, los nodos deberán recolectar las siguientes estadísticas de nivel físico:

- Estadísticas por puerto Ethernet: Octets, Packets, Errors, Unicast packets, Multicast Packets, Broadcast Packets, Discards, Unknown Proto Discards.

- Estadísticas de medio Ethernet: Alignment Errors, FCS Errors, SQE Test Errors, CSE, Too long Frames, Symbol Errors, Single Collisions, Collisions, Late Collisions, Excess Collisions, Int MAC Tx Errors, Int MAC Rx Errors.

- Estadísticas generales Ethernet: Broadcast Packets, Undersize Packets, Oversize Packets, Collisions, Drop Events, CRC/Align Errors, Fragments, Jabbers, Octets, Packets, Packets of 64 Octets, of 65 to 127 Octets, of 128 to 255 Octets, of 256 to 511 Octets, of 512 to 1023 Octets, of 1024 to 1518 Octets, Packets of 1519 or more Octets.

- Estadísticas relativas a la contabilidad de servicios que permitan trabajar en contextos de contabilidad de SLA.

El equipo debe cumplir también los siguientes requerimientos de seguridad de la Gestión:

-SNMP v1, v2 y v3

- TACACS+.

- SSHv2

- RADIUS RFC 2865 Remote Authentication Dial In User Service

- Radius Accounting RFC 2866

6.2 Router *CORE* MPLS-IP de chasis fijo

Router MPLS equipado con diversidad de puertos 10GE/GE/FE ópticos y eléctricos. Fuente de alimentación redundante, software de routing y mecanismos de seguridad para control de los accesos. Con características completas MPLS y creación de paths RSVP/LDP. El equipo actuará como equipo P/PE en la red MPLS.

El equipo permitirá futuras ampliaciones, ya sea mediante apilamiento de un nuevo router de las características definidas en este apartado ya sea mediante la instalación de slots de expansión.

Dispondrá de dos fuentes de alimentación remplazables en caliente. Si una fuente falla, la otra fuente asumirá toda la carga del dispositivo sin interrumpir el tráfico de la red.

Incluirá un agente de gestión basado en SNMP versión 3, que proporcionará gestión en banda y fuera de banda para gestionarlo. El equipo será configurable desde el sistema de gestión.

El equipo se suministrará con todos los interfaces ópticos al completo.

6.2.1 Requerimientos de alta disponibilidad

- Soporte de VRRP y/o SEP

- Capacidad de actualización del firmware sin pérdida de prestaciones/ISSU.

6.2.2 Rendimiento

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

Rendimiento/throughput al menos de 50 Mpps, y sin verse afectado por la creación de VLANs en base a ninguno de los criterios, aunque se creen el máximo de ellas. La generación de VLANs es un factor clave para independizar tráficos acorde a los mecanismos de seguridad.

Capacidad de conmutación mínima de 300 Gbps Full-Duplex (Non-Blocking en cualquier configuración del equipo) y será wire-speed en su máxima configuración.

Control de tormentas de Broadcast

Cumplirá los siguientes estándares:

NIVEL 2

Estándar IEEE 802.3. Ethernet -2005.

Estándar IEEE 802.3i 10Base-T

Estándar IEEE 802.3u. FastEthernet con detección automática de la velocidad.

Estándar IEEE 802.3x. Control de Flujo

Estándar IEEE 802.3z. 1000Base-X

Estándar IEEE 802.3ab. 1000Base-T

Estándar IEEE 802.3af Power over Ethernet (PoE)

Estándar IEEE 802.3ad Agregación de enlaces

Estándar IEEE 802.1p. Priorización de tráfico.

Estándar IEEE 802.1q-2005. VLAN (incorpora 802.1q-1998, 802.1s, 802.1u y 802.1v)

Estándar IEEE 802.1d-2004 MAC Bridges (incorpora 802.1t y 802.1w)

Estándar IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)

Estándar IEEE 802.1s Multiple Rapid Spanning Tree Protocol (MSTP)

Estándar IEEE 802.1x Protocolo de autenticación

Los puertos que pertenezcan a una agregación serán tratados como un único puerto lógico. Al caerse uno de los enlaces pertenecientes a la agregación, ésta seguirá operativa y los parámetros del tráfico resultarán afectados de forma despreciable, recuperándose en menos de 1 segundo tras reponer el enlace caído.

El número de enlaces formando un agregado será de al menos 8. El equipo de datos permitirá mecanismos de balanceo de carga.

ROUTING:

Ipv4 con RIP v1 y v2, OSPF v2, VRRP, IS-IS, BGP, y Rutas Estáticas.

IP Multicast con IGMP v1, v2 y v3, IGMP snooping e IGMP Group Limit, DVMRP, PIM-DM.

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.

ARP para obtención de direcciones físicas preguntando por la dirección IP, NTP para sincronización de todos los equipos de la red.

REQUERIMIENTOS MPLS

- Estándar RFC 2702, Requisitos para ingeniería de tráfico sobre MPLS.
- Estándar RFC 3031, Arquitectura MPLS.
- Estándar RFC 3032, Cifrado de pila de etiquetas MPLS.
- Estándar RFC 3063, Mecanismo de prevención de bucles MPLS.
- LSP de backup señalizados y sin señalizar.
- Protocolo de distribución de etiquetas (LDP)
- Estándar RFC 3036.
- Estándar RFC 3037.
- Funcionalidad Fast Re-Route
- Parámetros utilizados para caracterizar los túneles:

o Puerto Ethernet.

o VLANs.

o Combinación de puertos y VLANs.

o Rangos de VLANs.

o Combinación de puertos y rangos de VLANs.

- Protocolo RSVP-TE
- RFC 3209 Extensions to RSVP for LSP Tunnels
- RFC 3210 Applicability Statement for Extensions to RSVP for LSP Tunnels
- RFC 2961 RSVP Refresh Overhead Reduction Extensions

VPNs

RFC 2547, BGP/MPLS VPNs

BGP/MPLS VPNs

MPLS-based Layer 2 VPNs

MPLS/BGP Virtual Private Network Management Information Base Using SMIv2,

CALIDAD DE SERVICIO (sin penalización del rendimiento)

Mínimo 4 colas hardware por puerto

IEEE 802.1p

IP DSCP (Diffserv) / IP Precedence con gestión de colas

SEGURIDAD

Soporta autenticación basada en 802.1x (con PEAP/EAP/TLS/TTLS) para dispositivos con usuario y MAC para dispositivos sin usuario en todos los puertos, y de manera simultánea. Para permitir accesos restringidos a usuarios que no tengan acceso directo a la red, alguno de los puertos debe permitir acceso WEB con petición de nombre de usuario y contraseña.

Soporte de multi-autenticación de dispositivos por puerto, al menos dos.

Tendrá la capacidad de aprender las direcciones MAC de equipos que ya han superado el proceso de autenticación, soportando MAC Adress Learning Limit para evitar denegación de servicio.

Permite bloqueo o denegación de acceso por prohibición de MAC, dirección IP y/o puerto para usuarios y/o dispositivos no autorizados.

Gestión de VLAN Dinámicas, Rate Limit por puerto y VLAN y configuración de Guest VLAN para usuarios invitados.

Soportará 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.

Para dispositivos sin usuario, existirá un gestor de MACs con conectividad con el switch y con el Radius, que almacene la base de datos con las direcciones físicas autorizadas y agilice el proceso de autenticación.

Prevendrá ataques de DoS y soportará ACLs.

Port mirroring, para poder monitorizar el tráfico enviado desde un puerto o VLAN a través de otro puerto del switch.

Al menos 4 colas hardware de prioridad por puerto.

Capacidad para generar VLAN, con soporte de IEEE 802.1q

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.

Mecanismos de prevención ante DoS (Deny of Service) para evitar mecanismos de ataque como DHCP Spoofing, ARP Spoofing, etc.

El equipo soportará las RFC 3579, 3580, 4675 y 4849.

GESTIÓN

Soportará estándar CLI (Command Line Interface) o servidor web propio.

RMON para monitorización del equipo de manera remota.

SNMPv3

Acceso Telnet mediante encriptación securizada SSH.

Puerto serie RS-232 (conector DB-9) para gestión fuera de banda.

Soporta FTP y TFTP

Soporta gestión unificada de logs.

Soporta comandos ping y tracert

NORMAS APLICABLES:

El equipo cumplirá con la legislación vigente sobre normativa en materia de compatibilidad electromagnética y exposición a campos electromagnéticos y garantizará la eficiencia energética del mismo.

6.3 Equipos de Acceso para el *CORE* MPLS-IP

En este tipo de redes de alta capacidad, con unas funcionalidades tan claramente definidas para los equipos del core es habitual incluir equipos de alta gama que actúen como elementos de acceso al mismo. Todo dependerá, en cualquier caso, de la solución tecnológica elegida por el oferente ya que hay fabricantes que pueden incorporar estos puertos de acceso dentro de los nodos de los routers modulares (en este caso los de Atxuri y Amara). En este pliego hemos optado por separarlos funcionalmente por simplicidad y para que se entienda mejor la solución que se plantea. Adicionalmente, la inclusión de estos nodos independientes aporta una serie de ventajas inherentes, como son la modularidad de cara a las ampliaciones así como a la reutilización de los equipos en función de las necesidades reales. Por la propia naturaleza de la propuesta técnica, en la que se adapta la arquitectura y las características de los equipos al proyecto, nos encontramos con routers compactos

en 6 ubicaciones y con routers modulares en dos de ellas. Para homogeneizar la solución de acceso, es preferible utilizar equipos independientes, de manera que en Atxuri y Amara se dispongan de un mínimo de 96 puertos y en las restantes ubicaciones, de 24 puertos.

Los equipos deben estar fabricados con hardware de alto rendimiento de última generación y han de ofrecer funciones avanzadas, como funcionalidad de la capa 3 optimizada, tareas simplificadas de O&M, networking Ethernet flexible y capacidades IPv6 perfeccionadas.

Los equipos (ambos modelos) se plantean con funcionalidad PoE+. Deben disponer de:

Funciones MAC

- Conformidad con IEEE 802.1d
- Aprendizaje y envejecimiento de direcciones MAC
- Entradas de direcciones MAC estáticas, dinámicas y de agujero negro
- Filtrado de paquetes en función de las direcciones MAC de origen

Funciones VLAN

- 4094 VLAN
- VLAN invitada, VLAN de voz
- GVRP
- MUX IAN
- Asignación de VLAN en función de direcciones MAC, protocolos, subredes IP, políticas y puertos.
- Mapeo de VLAN 1:1 y N:1

Routing IP

- Ruta estática, RIPv1/v2, RIPng, OSPF, OSPFv3, ECMP, IS-IS, IS-ISv6, BGP, BGP4+

Rendimiento de reenvío

96 Mpps para los equipos de 24 puertos y 132 Mpps para los equipos de 48 puertos.

Capacidad de switching del dispositivo

128 Gbps para los equipos de 24 puertos y 176 Mbps para los de 48 puertos

7 PLANIFICACIÓN

Dado que el proceso de migración del *CORE* básicamente se puede afrontar de varias formas, desde un punto de vista teórico, el licitador deberá explicitar claramente el proceso de migración propuesto. En el presupuesto se plantea el desglose que deberá utilizarse para dar una explicación detallada de la propuesta de migración y puesta en servicio, en función de la solución tecnológica aportada.

La duración máxima del proyecto se establece en 8 meses, con los siguientes hitos principales:

- Replanteo e ingeniería previa: 1 mes
- Acopio de materiales: 3 meses
- Prueba piloto de configuración: 1 mes
- Puesta en servicios de la red de *core*: 2 meses
- Migración de servicios: 2 meses

En función de la solución propuesta por el licitador se podrán optimizar los tiempos individuales y los globales por superposición de tareas.

Deberá tenerse en cuenta que el proceso de migración no puede afectar al servicio ferroviario por lo que es previsible el realizar varias labores en horario nocturno, sin circulación ferroviaria y de acuerdo con ETS.

8 CERTIFICACIONES

Para la ejecución de los trabajos se deberá disponer de las siguientes certificaciones:

• ISO 9001 (Calidad), ISO 14001 (Medio Ambiente) y OHSAS 18000 (Seguridad laboral).

Las personas incluidas en el equipo de trabajo de la propuesta deberán contar con las certificaciones del fabricante de los productos propuestos en su oferta o, en su defecto, la empresa licitante deberá aportar carta de compromiso de la contratación de los servicios profesionales del fabricante correspondiente.

Los recursos que participen en la ejecución de los trabajos contarán con la siguiente certificación:

- CCNA (Cisco Certified Network Associate) o equivalente del fabricante
- CCNP (Cisco Certified Network Professional) o equivalente del fabricante

Se requerirá una declaración responsable disponiendo que para la prestación del servicio de soporte del adjudicatario, los tiempos máximos de respuesta según el riesgo del impacto indicados en la tabla del apartado "soporte del adjudicatario", se cumplirán completamente.

Adicionalmente, se podrán incluir otras certificaciones técnicas relacionadas y adecuadas a este servicio de las que disponga la empresa.

9 PRECIOS DE CONTRATO

Los concursantes fijarán los precios unitarios designados en el anexo conforme al modelo de presupuesto desglosado en el Anejo III.2 del PCAP [VER ANEJO 12 DE ESTE PLIEGO], que serán de aplicación para su abono en las correspondientes certificaciones, no sufriendo variación por concepto alguno.

Estos precios serán de contrata, de modo que en ellos estén incluidos todos los beneficios, cargas sociales, gastos, impuestos, excepto IVA, etc.

Con la oferta se entregará además la proposición económica según modelo del Anejo III.1 del PCAP.

10 VALORACIÓN Y ABONO DE LOS TRABAJOS REALIZADOS

La valoración y abono de los trabajos realizados por el Contratista se efectuará por certificaciones mensuales en función del avance de los trabajos de cada uno de los apartados desglosados.

Antes del día 20 de cada mes el adjudicatario indicará al Responsable del Contrato una medición del avance previsto en cada tarea al terminar el mes en curso. Una vez aceptada dicha medición, antes del último día del mes, el adjudicatario enviará la hoja de mediciones firmada para su validación, y emitirá la correspondiente factura digital por el importe acordado.

A la puesta en marcha de todo el equipamiento se realizará una recepción parcial, iniciándose en ese momento el periodo de garantía y el soporte que se certificará trimestralmente hasta su finalización, en la que se emitirá la recepción definitiva.

11 PRESUPUESTO DEL CONTRATO

El Presupuesto máximo de licitación, IVA no incluido, es el indicado en el apartado 3 de la Carátula del concurso y asciende a **336.901,81euros** (IVA no incluido).

12 ANEJO: CUADRO DE PRECIOS

Pos	Concepto	Uds	Precio Ud. Euros	Importe Total EJECUCIÓN MATERIAL Euros
	UNITARIOS EJECUCIÓN			
1	**Nodo de cabecera** Equipo modular en chasis con doble controladora. A ubicar en ATXURI y AMARA. Modelo de NetEngine8000 M8 de HUAWEI o similar, con alimentación en AC redundante, doble controladora (IPU) y 6 slots de servicio disponibles. Procesadora con capacidad mínima de 480 Gbps. Para cubrir las necesidades de conectividad actuales se propone instalar al menos 2 tarjetas por equipo de 10 puertos10GE/GE SFP+ para redundancia interchasis permitiendo así mismo una evolución fluida ya que las interfaces de 10G soportan velocidades de 10GE/GE/FE, módulos eléctricos y MACSec. El equipo se suministrará con todos los interfaces ópticos al completo, considerando capacidad 10G por interfaz y para garantizar distancias de 80 KM. La partida incluye latiguillos y trabajos de instalación en cuarto de comunicaciones, así como conexionado en repartidor existente. Los tendidos de cable, por canalización/bandejas existentes. La alimentación eléctrica se tomará del cuadro actual.	**2**	**56.678,50**	**113.357,00**
2	**Nodo de CORE COMPACTO** Para los nodos de cabecera ubicados en Durango, Ermua, Zumaia, Araso, Gernika y Bermeo, se propone el modelo de router fijo NetEngine8000 M1A de Huawei o similar dotado con capacidad de 4 x 10GE/GE/FE + 12 x GE/FE(o). Switching Capacity: 352Gbps. El equipo se suministrará con todos los interfaces ópticos al completo, considerando: 16 interfaces 10G/G para garantizar distancias de 80 KM. interfaces G para distancias de 10 Km. La partida incluye latiguillos y trabajos de instalación en cuarto de comunicaciones, así como conexionado en repartidor existente. Los tendidos de cable, por canalización/bandejas existentes. La alimentación eléctrica se tomará del cuadro actual.	**6**	**8.540,04**	**51.240,24**

3	**Nodo de ACCESO 48 PUERTOS** Nodos de acceso. Capacidad mínima 48 puertos 10/100/1000 + 4 x10GE(ópticos). PoE+, con doble fuente de alimentación. Modelo S5735-S48P4x de Huawei o similar. Conexión 10 GE con router de cabecera.	**4**	**3.001,29**	**12.005,16**
4	**Nodo de ACCESO 24 PUERTOS** Nodos de acceso. Capacidad mínima 24 puertos 10/100/1000 + 4 x10GE(ópticos). PoE+, con doble fuente de alimentación. Modelo S5735-S24P4x de Huawei o similar. Conexión 10 GE con router de cabecera.	**6**	**2.350,62**	**14.103,72**
5	**Sistema de gestión** Como sistema de gestión se propone instalar en modo appliance un clúster de servidores físicos, que aporte redundancia entre los diferentes componentes de la plataforma, por ej. iMasterNCE-IP Lite. Este gestor deberá tener la capacidad para gestionar conjuntamente toda la base instalada de Switches, Routers por supuesto y también los equipos de transmisión del fabricante, mediante la incorporación de una política de licencias. Se proporciona con las licencias para los nodos de core y acceso de la presente licitación.	**1**	**28.68973**	**28.689,73**
6	**Licencias para switches de cabecera existentes en la red** Conjunto de 100 licencias para los switches de cabecera en el aplicativo de gestión integral.	**1**	**14.875,00**	**14.875,00**
7	**Replanteo con toma de datos de red física y lógica actual con marcaje y mapeado de todos los interfaces** Incluye visita a las ubicaciones objeto de esta licitación y preparación de la documentación de arranque con planos de preingeniería.	**1**	**7.735,00**	**7.735,00**
8	**Puesta en servicio de la red de Core** Incluye la configuración del nuevo core con las funcionalidades de IP-MPLS y las interfaces con los demás elementos de la red principal de ETS. Incluye Curso de Formación de operación, administración y mantenimiento de 16 horas de duración en las instalaciones que determine ETS.	**1**	**31.134,60**	**31.134,60**
9	**Prueba piloto de configuración** Factory Acceptance Test con la configuración propuesta. Escala 1:1. Todos los equipos objeto de la licitación conectados con la malla a implementar. Obtención de estadísticas, validación de escenarios y verificación de caminos de back-up con simulaciones de redundancias y carga de red.	**1**	**11.305,00**	**11.305,00**

10	**Migración de servicios del core existente a nueva red** Migración y actualización de servicios garantizando la continuidad de los servicios, estableciendo las políticas de migración y vuelta atrás segura. La partida incluye una propuesta previa con diferentes alternativas de estudio para su validación por ETS y finalmente la migración con los seguimientos correspondientes y cumplimiento de hitos.	**1**	**14.604,55**	**14.604,55**
11	**Documentación as built** Incluye planos de red, listado de interfaces ópticas y configuración de los equipos del core de la red de ETS, así como de los hitos previos del proceso de migración de red del core.	**1**	**7.051,86**	**7.051,86**
12	**Soporte** Soporte anual del adjudicatario, según indicado en pliego técnico.	**2**	**15.400,00**	**30.800,00**

TOTAL EJECUCIÓN	336.901,81
TOTAL EJECUCIÓN CONTRATA	**336.901,81**
IVA 21%	70.749,38
TOTAL CON IVA	407.651,19