

UNIVERSIDAD MIGUEL HERNÁNDEZ DE ELCHE

ESCUELA POLITÉCNICA SUPERIOR DE ELCHE

GRADO EN INGENIERÍA DE TECNOLOGÍAS DE
TELECOMUNICACIÓN



PROYECTO DE MIGRACIÓN DE
INFRAESTRUCTURA DE RED PARA
EMPRESA DE LOGÍSTICA CON BACKUP
LTE Y FUNCIONALIDADES DE VPN PARA
CONECTIVIDAD SEGURA EN SEDES

TRABAJO FIN DE GRADO

Diciembre-2024

AUTOR: Juan Fernando Lobato Guaraca

DIRECTOR/ES: Francisco Javier Gimeno Blanes
José Antonio Mora Torres
Raúl García Jiménez



RESUMEN

Hoy en día, el sector de la logística enfrenta grandes desafíos en materia de conectividad segura, una buena gestión de la logística tiene importantes beneficios para las empresas. Permite acceder a la información exacta sobre los materiales, reducir costos y optimizar tiempos de entrega. La creciente demanda de comunicaciones seguras y efectivas en tiempo real ha generado una enorme demanda de soluciones sólidas y escalables. Este proyecto propone una arquitectura de red que prioriza la seguridad y, al mismo tiempo, mejora la disponibilidad de las comunicaciones críticas.

El objetivo de este proyecto es diseñar e implementar la migración de infraestructura de red de una empresa logística con el uso de VPNs (Virtual Private Network) y tecnologías LTE (Long Term Evolution). Facilitar la continuidad del negocio, la comunicación segura y la gestión eficaz de los datos de una empresa logística de la provincia de Cataluña integrada por 20 sedes.

Este proyecto describe las especificaciones técnicas de los equipos necesario, la metodología de la gestión de la red de acceso, detallando los conceptos teóricos y conceptuales. Además, se consideran las limitaciones impuestas de la infraestructura de red inicial y las mejoras que se consiguen en términos de redundancia, seguridad y escalabilidad.

Palabras clave: Migración de red, conectividad segura, logística, VPN, respaldo LTE.

ABSTRACT

Today, the logistics sector faces major challenges in terms of secure connectivity, and good logistics management has significant benefits for companies. It allows access to accurate information about materials, reduces costs and optimizes delivery times. The growing demand for secure and effective real-time communications has generated an enormous demand for robust and scalable solutions. This project proposes a network architecture that prioritizes security while improving the availability of critical communications.

The objective of this project is to design and implement the migration of a logistics company's network infrastructure using VPNs (Virtual Private Network) and LTE (Long Term Evolution) technologies. Facilitate business continuity, secure communication and effective data management for a logistics company in the province of Catalonia made up of 20 locations.

This project describes the technical specifications of the necessary equipment, the methodology for managing the access network, detailing the theoretical and conceptual concepts. In addition, the limitations imposed by the initial network infrastructure and the improvements achieved in terms of redundancy, security and scalability are considered.

Keywords: Network migration, secure connectivity, logistics, VPN, LTE backup.

AGRADECIMIENTOS

Quiero expresar mi más profundo agradecimiento a mis padres y hermanas, quienes han sido mi mayor pilar de apoyo en todo momento. Gracias por creer en mí, y por motivarme a superar cada desafío.

A todas las personas que, de una u otra forma, han estado presentes durante esta etapa universitaria, quiero darles las gracias por su guía, apoyo y palabras de aliento. A mis profesores, tutores y compañeros, gracias por compartir su conocimiento y contribuir al desarrollo de mi formación académica y profesional.

Finalmente, quiero recordar que el esfuerzo constante y la perseverancia son los cimientos de cualquier logro: "El ser humano ha sabido adaptarse a cualquier contingencia, y la adversidad ha sido el motor de la mejora continua. Por ello, los momentos de adversidad siempre son oportunidades de aprender y de crecer". A todos los que me han inspirado a dar lo mejor de mí, mi más sincero agradecimiento.

LISTADO DE ACRÓNIMOS

ANS	Acuerdo de Nivel de Servicio
BE	Best Effort
CTO	Caja Terminal Óptica
CPE	Equipo cliente (Customer Premises Equipment)
FTTH	Fibra hasta el hogar (Fiber to the Home)
GPON	Red óptica pasiva Gibabit (Gigabit Passive Optical Network)
LAG	Agrupación lógica de enlaces (Link aggregation)
NEBA	Nuevo Ethernet de Banda Ancha (Servicio Mayorista de acceso indirecto)
LAGL	LAG del servicio NEBA LOCAL
OLT	Equipo de terminación de línea óptica (Optical Line Termination)
ONT	Equipo de terminación de red óptica (Optical Network Termination)
PAI-L	Punto de acceso indirecto-NEBA LOCAL
PTRO	Punto Termina Red Óptica
Q-in-Q	Técnica de encapsulado de VLANes de conformidad con la norma IEEE 801.1ad
RT	Real Time

ÍNDICE

ABSTRACT	4
LISTADO DE ACRÓNIMOS.....	6
ÍNDICE DE FIGURAS.....	10
ÍNDICE DE TABLAS.....	12
1. MEMORIA.....	13
1.1 MARCO TEÓRICO Y CONCEPTUAL.....	13
1.1.1 PROTOCOLOS DE ENRUTAMIENTO DINÁMICOS.....	13
1.1.2 BASES DE DATOS DE PROTOCOLOS DE ENRUTAMIENTO	15
1.1.3 TABLAS DE ENRUTAMIENTO DE JUNOS OS.....	15
1.1.4 REDES Y SUBREDES	17
1.1.5 TABLAS DE REENVÍO.....	17
1.1.6 SINCRONIZACIÓN ENTRE LAS TABLAS DE ENRUTAMIENTO Y ENCAMINAMIENTO	19
1.1.7 DESCRIPCIÓN DE LAS INSTANCIAS DE ENRUTAMIENTO.....	19
1.1.8 VRF.....	22
1.2 NEBA	22
1.2.1 DESCRIPCIÓN DEL SERVICIO	22
1.2.2 CALIDADES DE SERVICIO	24
1.2.3 RED DE ACCESO.....	25
1.2.4 TRÁFICO UNICAST	25
1.2.5 TRANSPORTE HASTA LOS PUNTOS DE ENTREGA DE TRÁFICO	26
1.2.6 VLAN DE CLIENTE Y SERVICIO.....	26
1.2.7 TRÁFICO UNICAST	27
1.2.8 INTERFAZ FÍSICA DE LA ENTREGA DEL SERVICIO.....	29
1.2.9 PUNTO DE ENTREGA Y DISTRIBUCIÓN GEOGRÁFICA.....	30
1.2.10 IDENTIFICADORES DE ACCESOS.....	36
1.2.11 FLUJOS DE CONEXIONES NEBA LOCAL	39
1.2.12 PARÁMETROS TÉCNICOS	39
1.2.13 ALTA DE CONEXIONES NEBA LOCAL.....	41
1.2.13.1 ALTA SOBRE VACANTE.....	41
1.2.14 INGRAESTRUCTURA PREVIA DEL CLIENTE	43
1.2.15 DESCRIPCIÓN GENERAL DE LA INFRAESTRUCTURA	44
1.2.16 CONFIGURACIÓN DE RED INICIAL.....	46
1.2.17 LIMITACIONES DE LA CONFIGURACIÓN INICIAL.....	46
1.2.18 INTEGRACIÓN CON RED MPLS.....	47

1.2.18.1	ARQUITECTURA DE RED	48
1.2.18.2	RENDIMIENTO.....	48
1.2.18.3	GESTIÓN	48
1.2.18.4	ESCALABILIDAD.....	48
1.2.18.5	RESUMEN COMPARATIVO.....	48
1.2.19	LTE.....	49
2	MAPA DE RED PROPUESTO	50
2.1	EQUIPO CORE PARA RED DE ACCESO FTTH	57
2.2	EQUIPO BACKBONE PARA EL TRÁFICO DEL ISP.....	57
2.3	DISPOSITIVO DE SEGURIDAD PERIMETRAL.....	58
2.4	RED 4G	58
2.5	FTTH.....	59
2.6	ONT	59
2.7	ROUTER 4G	60
2.8	LAN DE LA SEDE DEL CLIENTE	60
3	PLIEGO DE CONDICIONES.....	61
3.1	REQUISITO TÉCNICOS GENERALES	61
3.2	EQUIPO CORE PARA RED DE ACCESO FTTH	62
3.2.1	DESCRIPCIÓN GENERAL.....	64
3.2.2	HARDWARE, CARACTERÍSTICAS GENERALES.....	65
3.2.3	DESCRIPCIÓN DEL CHASIS.....	66
3.2.4	REDUNDANCIA DE COMPONENTES.....	67
3.2.5	INDICADORES LED DE ALARMA Y BOTÓN DE PRUEBA EN LA INTERFAZ MX480 CRAFT	69
3.2.6	SOPORTES Y ADMINISTRACIÓN DE CABLES.....	71
3.2.7	DESCRIPCIÓN DEL MOTOR DE ENRUTAMIENTO MX480	72
3.2.8	PUERTOS DE INTERFAZ DEL MOTOR DE ENRUTAMIENTO.....	74
3.3	EQUIPO BACKBONE PARA TRÁFICO ISP.....	74
3.3.1	DESCRIPCIÓN GENERAL.....	75
3.3.2	HARDWARE, CARACTERÍSTICAS GENERALES.....	75
3.3.3	DESCRIPCIÓN DEL CHASIS.....	78
3.3.4	REDUNCIA DE COMPONENTES	81
3.3.5	DESCRUPCIÓN DE LA INTERFAZ CRAFT MX960	82
3.3.6	DESCRIPCIÓN DEL ADMINISTRADOR DE CABLES	82
3.3.7	PROCEDIMIENTO DE MANTENIMIENTO DE RUTINA PARA EL ENRUTADOR MX960	86
3.3.8	INDICADORES LED DE ALARMA	86

3.4	DISPOSITIVO DE SEGURIDAD PERIMETRAL.....	87
3.4.1	WATCHGUARD T85	88
3.4.2	DESCRIPCIÓN GENERAL.....	89
3.4.3	ESPECIFICACIONES TÉCNICAS.....	92
3.4.4	ASPECTOS LEGALES Y NORMATIVA APLICABLE	93
4	PRESUPUESTO	95
4.1	OBRA CIVIL	95
4.2	INSTALACIONES DE FIBRA ÓPTICA.....	99
4.3	CANALIZACIONES	101
4.4	RESUMEN	105
5	CONCLUSIONES	106
6	BIBLIOGRAFIA	107



ÍNDICE DE FIGURAS

Figura 1: Protocolos IGP, EGP [2]	14
Figura 2: EGP, IGP [3]	15
Figura 3: Red y subred [5].....	17
Figura 4: Sincronización de tablas de enrutamiento y encaminamiento en Juno OS ..	19
Figura 5: Estructura de protocolos para conexiones FTTH [7]	25
Figura 6: Trama de Usuario 802.1Q [7].....	28
Figura 7: Puntos de entrega y distribución geográfica [7].....	31
Figura 8: Ubicación de nuevos PAI-L debido al incremento de la demanda [9]	32
Figura 9: Escenario debido al crecimiento de OLT y PAI-L [7]	33
Figura 10: Escenario donde un PAI-L y la OLT se ubican en centrales diferentes [7] .	34
Figura 11: Instalación de un PAI-L en otra central [7].....	35
Figura 12: PTRO rotulado con IUA [10]	38
Figura 13: Core MPLS	47
Figura 14: Mapa de red general propuesto para la conexión de sedes	51
Figura 15: BGP FAMILY INET	52
Figura 16: BGP Export 0.0.0.0/	53
Figura 17: BGP export 192.168.1.0/24.....	54
Figura 18: Public prefixes static routes to WAN	55
Figura 19: Static route 0.0.0.0/0 to LAN	55
Figura 20: Static route 0.0.0.0/0 to WAN.....	56
Figura 21: Private prefixes static routes to LAN	56
Figura 22: Equipo para gestionar la red de acceso FTTH	57
Figura 23: Equipo Backbone para la gestión del tráfico del ISP	57
Figura 24: Dispositivo que aplica políticas de firewall.....	58
Figura 25: Red 4G	58
Figura 26: Red FTTH.....	59
Figura 27: ONT (Optical Network Terminal)	59
Figura 28: Router con módem LTE	60
Figura 29: Red de Area Local del Cliente.....	60
Figura 30: Plataforma de enrutamiento universal MX480 [19].....	62
Figura 31: Plataforma de enrutamiento universal MX480 [19].....	63
Figura 32: Vista frontal del chasis completamente configurado [20].....	66
Figura 33: Vista trasera del MX480 con alimentación CA completamente configurado [20]	67
Figura 34 Soportes de administradores de cables [20]	71

Figura 35: Soportes de administración de cables instalados en el equipo [20].....	72
Figura 36: Motor de enrutamiento RE-S-1800 [20].....	73
Figura 37: Vista frontal del motor de enrutamiento RE-S-X6-64G	73
Figura 38: Panel frontal [22].....	82
Figura 39: Administrador de cables estándar [22]	83
Figura 40: Administrador de cables extendido [22]	84
Figura 42: Base de la seguridad de la información [23].....	88
Figura 43: Firebox T85 [24].....	89

1



ÍNDICE DE TABLAS

Tabla 1: Calidades de servicio	24
Tabla 2: p-bit 802.1p	26
Tabla 3: Longitud de onda utilizada en cada sentido	30
Tabla 4: Parámetros técnicos obtenidos de [10]	40
Tabla 5: Tipos de código GESCAL [11]	41
Tabla 6: Listado de sedes y ubicaciones. El listado por razones de confidencialidad ha sido alterado no respondiendo a la real configuración del cliente.	45
Tabla 7: IPsec y MPLS.....	49
Tabla 8: Indicadores LED de alarma y botón de prueba alarma/ luz	70
Tabla 9: Motor de enrutamiento RE-S-X6-64G	73
Tabla 10: Capacidad MX960 enrutador de red [22].....	76
Tabla 11: Capacidad de tarjeta de control para puertos [22].....	77
Tabla 12: Indicadores LED de alarma y botón de prueba de lámpara/corte de alarma.	87
Tabla 13: Comparativa Basic y Total Security.....	91
Tabla 14: Especificaciones Firebox T85 [24].....	92
Tabla 15: Especificaciones Firebox T85 [24].....	93

1. MEMORIA

En el ámbito de las telecomunicaciones, los protocolos representan la columna vertebral que permite la interconexión y comunicación eficiente entre dispositivos y redes. Actualmente, los protocolos más utilizados, como TCP/IP, son fundamentales para la transmisión de datos en Internet y redes privadas. Además, tecnologías emergentes como el 5G han impulsado el desarrollo de nuevos protocolos de acceso y transporte, optimizados para latencias ultrabajas y altas velocidades de transferencia. Esto ha llevado a una evolución en los estándares, integrando soluciones más dinámicas y adaptables para gestionar el tráfico creciente y diverso que demanda el entorno actual.

1.1 MARCO TEÓRICO Y CONCEPTUAL

En este apartado se presentan los fundamentos teóricos que respaldan el diseño y configuración de la solución de red propuesta. Se introducen conceptos clave como los protocolos de enrutamiento dinámico, las tablas de reenvío y los mecanismos de virtualización de instancias de enrutamiento (VRF), los cuales son esenciales para la gestión y optimización del tráfico en redes avanzadas.

Este marco teórico no solo explica las herramientas y metodologías empleadas, sino que también ofrece una visión técnica integral de cómo se interrelacionan los elementos del sistema para garantizar una conectividad segura, eficiente y escalable.

1.1.1 PROTOCOLOS DE ENRUTAMIENTO DINÁMICOS

El enrutamiento es el proceso de dirigir paquetes desde una dirección origen a una dirección destino. Los protocolos de enrutamiento dinámico, que se implementan en un sistema autónomo (AS) o “dominio de routing”, se clasifican en Protocolo de Gateway interior (IGP) y Protocolo de puerta de Gateway exterior (EGP).

Los IGP como OSPF, IS-IS, EIGRP y RIP se implementan dentro de un AS y

realizan enrutamiento interno. Por el contrario, el enrutamiento entre AS lo realiza EGP; BGP es el protocolo principal de EGP y se ejecuta entre redes autónomas para gestionar el flujo de tráfico [1].

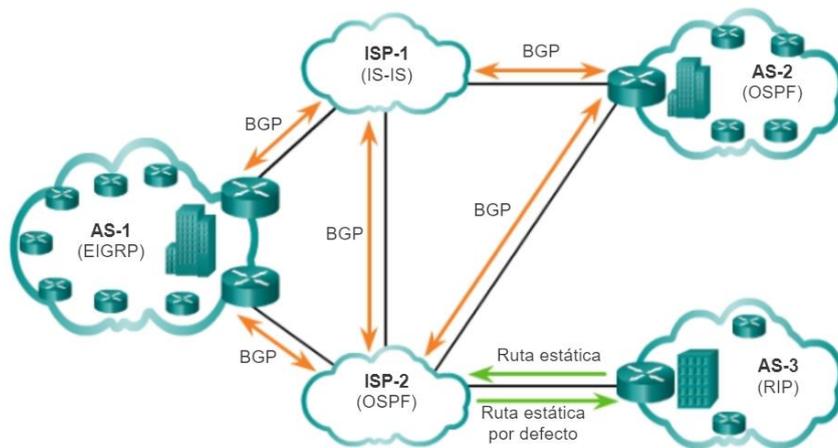


Figura 1: Protocolos IGP, EGP [2]

El sistema operativo Junos OS gestiona dos principales bases de datos para gestionar la información de enrutamiento:

- La tabla de enrutamiento que contiene toda la información aprendida por todos los protocolos de enrutamiento.
- La tabla de reenvío que contiene las rutas realmente utilizadas para el reenvío de paquetes.

Los protocolos IGP, como IS-IS y OSPF, utilizan bases de datos de estado de enlace para almacenar información sobre la topología de la red.

1.1.2 BASES DE DATOS DE PROTOCOLOS DE ENRUTAMIENTO

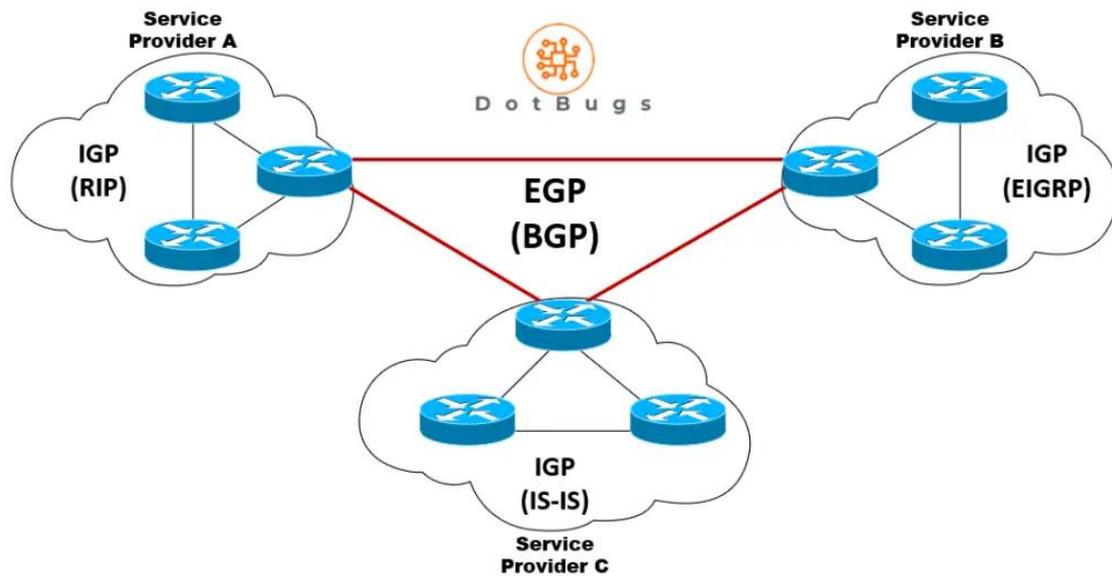


Figura 2: EGP, IGP [3]

Cada protocolo de enrutamiento IGP, como RIP, mantiene una base de datos propia que contiene la información de enrutamiento que ha recibido de otros routers que ejecutan el mismo protocolo.

Todos estos IGP son bastante rápidos y seguros ya que se ejecutan en un entorno totalmente confiable. BGP requiere que estas conexiones individuales se configuren manualmente en ambos extremos del enlace. Esto implica que cada router debe establecer explícitamente los parámetros de sesión, para el intercambio de tráfico. A diferencia de los protocolos de gateway interior, BGP no utiliza descubrimiento dinámico de vecinos. Por lo que se garantiza un control estricto y una mayor seguridad en la conexión.

1.1.3 TABLAS DE ENRUTAMIENTO DE JUNOS OS

En Junos OS, las tablas de enrutamiento almacenan información sobre tres tipos de rutas:

- **Rutas estáticas:** Configuradas manualmente por un administrador.

Especifican un destino y una ruta fija a través de la cual se pueden alcanzar las redes o dispositivos. Las rutas estáticas no se adaptan automáticamente a los cambios en la red.

- **Rutas directas o de interfaz:** Estas son rutas asociadas directamente a las interfaces físicas o lógicas del dispositivo. Una interfaz conectada a una red crea automáticamente una ruta en la tabla de enrutamiento para esa red.
- **Rutas aprendidas dinámicamente:** Estas rutas son adquiridas a través de protocolos de enrutamiento dinámico, como BGP, OSPF, IS.

Los dispositivos intermedios deben conocer la ruta para enviar paquetes desde un host origen a un host destino. Las tablas de enrutamiento almacenan todas las rutas posibles que un dispositivo A conoce para llegar al destino B.

Por defecto, Junos OS mantiene tres tablas de enrutamiento: una para unidifusión, otra para multidifusión y otra para MPLS. Cuando se necesita mayor flexibilidad o separar rutas, se pueden configurar tablas de enrutamiento adicionales.

A cada tabla de enrutamiento se le asigna un nombre compuesto por la familia de protocolos, como inet (Internet), iso (ISO) o mpls (MPLS), seguido de un número entero no negativo.

- inet.0: Tabla de enrutamiento de unidifusión de IP predeterminada versión 4 (IPv4)
- instance-name. inet.0: tabla de enrutamiento de unidifusión para una instancia de enrutamiento determinada
- inet.3Tabla de enrutamiento MPLS para información de rutas

1.1.4 REDES Y SUBREDES

Una red es un conjunto de dispositivos interconectados con la capacidad de comunicarse entre sí, bajo el control de una sola entidad. Las redes facilitan el intercambio de datos y el enrutamiento del tráfico entre hosts. Una subred es una partición lógica de esta red más grande, creada para optimizar la organización y gestión del espacio de direcciones IP. Esto permite una mayor flexibilidad en la asignación de direcciones y mejora la eficiencia del enrutamiento, segmentando la red en unidades más pequeñas [4].

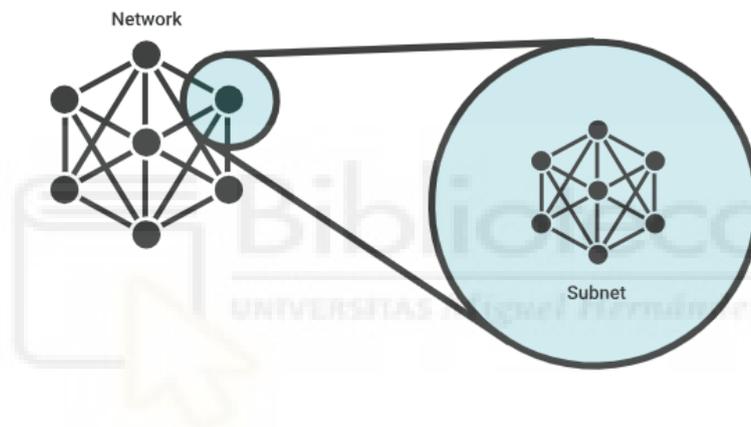


Figura 3: Red y subred [5]

1.1.5 TABLAS DE REENVÍO

El enrutamiento es el proceso por el cual los paquetes de datos son transmitidos desde una dirección origen hacia una dirección destino, en la mayoría de los casos a través de múltiples redes interconectadas. Este proceso se basa en dos componentes:

- Intercambio de información de enrutamiento: Los routers comparten información entre sí para construir y actualizar sus tablas de enrutamiento.
- Procedimiento de reenvío de paquetes: Una vez que se ha determinado la ruta óptima, los routers se encargan de reenviar los

paquetes a lo largo de esa ruta hasta alcanzar el destino final.

Para garantizar que los paquetes lleguen correctamente al host adecuado, cada dispositivo en la red debe tener un identificador numérico único, es decir, una dirección IP (dirección del Protocolo de Internet). Estas direcciones IP de destino se utilizan para crear entradas en la tabla de enrutamiento, que son esenciales para decidir por dónde se debe encaminar un paquete desde su origen hasta su destino.

Mientras que la tabla de enrutamiento contiene una lista exhaustiva de todas las rutas posibles que un paquete puede tomar, la tabla de reenvío se enfoca únicamente en las mejores rutas hacia destinos específicos. La determinación de la mejor ruta depende del protocolo de enrutamiento, pero generalmente se considera que la ruta con el menor número de saltos entre el origen y el destino es la más eficiente.



1.1.6 SINCRONIZACIÓN ENTRE LAS TABLAS DE ENRUTAMIENTO Y ENCAMINAMIENTO

El proceso de sincronización entre las tablas de enrutamiento y tablas de reenvío en Junos OS funciona de la siguiente manera: el protocolo de enrutamiento selecciona las mejores rutas activas de la tabla de enrutamiento y las instala en la tabla de reenvío. Posteriormente, la tabla de reenvío se copia al PFE (Packet Forwarding Engine), que es el componente encargado de reencaminar físicamente los paquetes a sus destinos a través de las rutas seleccionadas.

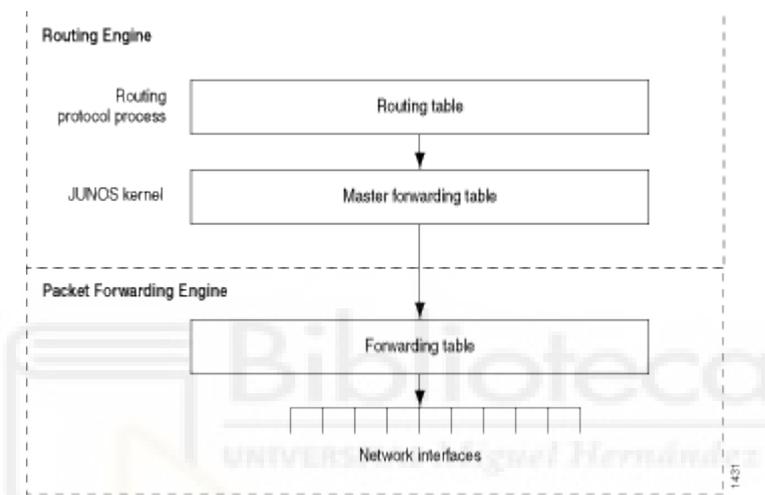


Figura 4: Sincronización de tablas de enrutamiento y encaminamiento en Junos OS

1.1.7 DESCRIPCIÓN DE LAS INSTANCIAS DE ENRUTAMIENTO

En el contexto de redes con Junos OS, se pueden crear varias instancias de protocolos como BGP, OSPF, IS-IS, RIP, y otros, especificando comandos en los niveles de jerarquía correspondientes.

Sin embargo, cada instancia de enrutamiento solo puede tener una instancia de cada protocolo. Esto permite segmentar tablas de enrutamiento y políticas de forma eficiente.

Una instancia de enrutamiento es una agrupación de tablas de enrutamiento, interfaces y los parámetros del protocolo de enrutamiento que controlan la información de dichas tablas.

Una sola instancia de enrutamiento puede contener múltiples tablas, como unidifusión IPv4, unidifusión IPv6 y multidifusión IPv4. Cada instancia tiene un nombre único y una tabla IP unicast asociada. Por ejemplo, si la instancia se llama "my-instance", la tabla será "my-instance.inet.0", donde se instalan todas las rutas asociadas.

En Junos OS, se pueden configurar 13 tipos de instancias de enrutamiento, cada una diseñada para cumplir funciones específicas dentro de la red:

- **Ethernet VPN (EVPN) (solo en routers de la Serie MX):** Este tipo de instancia se utiliza para conectar un grupo de sitios de clientes dispersos geográficamente mediante un puente virtual de Capa 2. EVPN permite extender una red LAN a través de una infraestructura MPLS, facilitando servicios como la movilidad de máquinas virtuales y la interconexión eficiente de centros de datos.
- **Forwarding:** Este tipo de instancia es empleado en aplicaciones de reenvío basado en filtros PFE (Packet Forwarding Engine). A diferencia de otras instancias, aquí no existe una asignación uno a uno entre una interfaz y una instancia de enrutamiento. Todas las interfaces pertenecen a la instancia predeterminada inet.0, y el reenvío de paquetes se decide en función de filtros configurados que determinan el camino que deben seguir los paquetes dentro de la red.
- **Internet Multicast over MPLS:** diseñado para soportar túneles de replicación de entrada (ingress replication provider tunnels), permitiendo transportar datos de multidifusión IP entre routers a través de una nube MPLS. Esto se logra mediante protocolos como MBGP (Multiprotocol BGP) o MVPN (Multicast VPN) de nueva generación, optimizando la distribución de tráfico multicast en entornos donde la eficiencia y el ancho de banda son críticos.

- **Layer 2 Backhaul VPN:** Maneja paquetes VLAN mayoristas sin interfaz lógica existente. Aprende tanto etiquetas externas como internas de los paquetes.
- **Layer2-control:** Usado para protocolos de árbol de expansión como RSTP o MSTP en interfaces del borde del cliente en una instancia VPLS. No se puede usar si hay conexiones multihomed.
- **Layer 2 VPN:** Implementa VPN de capa 2 para conectar redes a través de un backbone de proveedor.
- **MAC-VRF:** Configura múltiples instancias específicas de clientes EVPN con tablas VRF, manejando direcciones MAC en redes EVPN-VXLAN.
- **MPLS Forwarding:** Proporciona protección contra spoofing de etiquetas en los enrutadores de borde de sistemas autónomos (ASBRs).
- **Nonforwarding:** Instancia sin tabla de reenvío correspondiente, utilizada para separar la información de las tablas de enrutamiento. En IS-IS, estas instancias no reenvían.
- **Virtual Router:** Similar a una instancia VRF, pero utilizada en aplicaciones no relacionadas con VPN. No tiene requisitos de importación/exportación de rutas ni de diferenciadores.
- **Virtual Switch:** Aísla un segmento LAN con su propio protocolo STP y separa el espacio de identificadores VLAN.
- **Virtual Private LAN Service:** este tipo de instancia permite la implementación de conexiones LAN de punto a multipunto entre múltiples sitios en una VPN, emulando una red LAN a través de una infraestructura de proveedor.
- **VRF (VPN Routing and Forwarding):** se utiliza en VPNs de capa 3. En este caso, cada instancia VRF tiene su propia tabla de enrutamiento y una tabla de reenvío asociada. Existe una asignación uno a uno entre una interfaz y la instancia de enrutamiento, lo que permite gestionar

rutas de manera independiente.

1.1.8 VRF

Los VRF (Instancia de enrutamiento virtual) ofrecen una solución escalable y flexible para la segmentación de redes, permitiendo a los administradores asignar interfaces físicas a diferentes VRF y así controlar el flujo de tráfico entre distintos dominios de red.

1.2 NEBA

Mediante lo establecido en la Resolución de la CNMC (Comisión Nacional de los Mercados y la Competencia) del 24 de febrero de 2016, por la que se aprueba la definición y análisis de los mercados 3 y 4, el servicio mayorista de acceso indirecto NEBA LOCAL se configura como un servicio similar al servicio NEBA provincial, que incluye además puntos de entrega, PAI, a nivel local, adaptando el resto de los parámetros en consecuencia. Este servicio se soporta sobre la FTTH desplegada por Telefónica, y la tecnología GPON utilizada en el despliegue y no permite la desagregación física real del bucle de fibra óptica. NEBA LOCAL establece una emulación lógica de la desagregación del bucle que permite a los operadores configurar de forma flexible ofertas comerciales a sus clientes independientemente de las ofertadas por Telefónica.

1.2.1 DESCRIPCIÓN DEL SERVICIO

El servicio NBA LOCAL es un servicio mayorista e Banda Ancha de Acceso indirecto con las siguientes características principales:

- Conexiones sólo sobre fibra óptica.
- Servicio de transporte de tramas Ethernet.
- Con diferentes Calidades de tráfico en una única VLAN de cliente y en un mismo acceso.
- Mediante el protocolo IGMP se permite el transporte del tráfico Multicast por una VLAN Multicast.

- El equipo de cliente y la ONT no están incluidos en el servicio.
- La contratación del servicio NEBA LOCAL se realiza en NEON mediante Web Services (WS).

El servicio NEBA LOCAL, comprende dos servicios en sí mismo:

1. Las conexiones NEBA LOCAL, es decir los enlaces físicos y lógicos que conectan a los abonados de un operador alternativo a la infraestructura de acceso de Telefónica.

Ejemplo práctico: En aquellos casos en los que el cliente de un operador alternativo contrate un servicio de Internet en aquella zona en la que el operador no dispone de infraestructura propia, NEBA LOCAL permite la conexión del cliente final con la OLT situada en la central de Telefónica.

2. Los servicios de soporte que proporciona NEBA LOCAL son las funciones que permiten la conexión entre la red de Telefónica y la red del operador alternativo. Con el objetivo de encaminar las conexiones individuales de cada cliente del operador alternativo, hacia su red propia.

1.2.2 CALIDADES DE SERVICIO

Se definen 3 calidades de servicio, ordenadas de menor a mayor prioridad.

Calidad de servicio	Parámetros
Best Effort (BE)	-
Oro	Pérdida de tramas y retardo.
Real Time (RT)	Pérdida de tramas, retardo y jitter.

Tabla 1: Calidades de servicio

Best Effort (BE): Es el nivel de servicio más básico y sin garantías. No tiene requisitos específicos en cuanto a pérdida de tramas, retardo o jitter (Variación de retardo). Esto significa que el tráfico puede ser entregado sin ninguna prioridad, siendo adecuado para aplicaciones no críticas, como la navegación web o correo electrónico.

Oro: Este nivel ofrece mayor calidad que Best Effort y garantiza un menor impacto en parámetros clave como la pérdida de tramas y el retardo. Es ideal para aplicaciones sensibles al retardo, como streaming de video.

Real Time (RT): Es el nivel más alto de prioridad porque está diseñado para aplicaciones en tiempo real que son extremadamente sensibles a la pérdida de tramas, el retardo y el jitter (variación del retardo). Este tipo de tráfico incluye aplicaciones como llamadas VoIP o videoconferencias, donde una variación mínima en los tiempos de entrega puede degradar gravemente la calidad del servicio.

Los caudales de las modalidades BE, ORO y RT estarán sujetos a la velocidad contratada (velocidad máxima) mediante mecanismos de "rate limit" implementados en la OLT.

1.2.3 RED DE ACCESO

La conexión se realizará a cualquier equipo del emplazamiento que esté conectado a la ONT. Los equipos del cliente y la propia ONT no serán proporcionados por Telefónica. Las ONT deben ser tele-supervisadas y tele-configuradas remotamente desde la OLT. Este monitoreo y aprovisionamiento remotos son parte del servicio mayorista. Se proporcionará a los Operadores una herramienta de tele diagnosis para supervisar la ONT de sus conexiones NEBA LOCAL [6].

1.2.4 TRÁFICO UNICAST

La Figura 5 refleja la pila de protocolos del servicio que se construye en la interfaz GPN/FTTH.

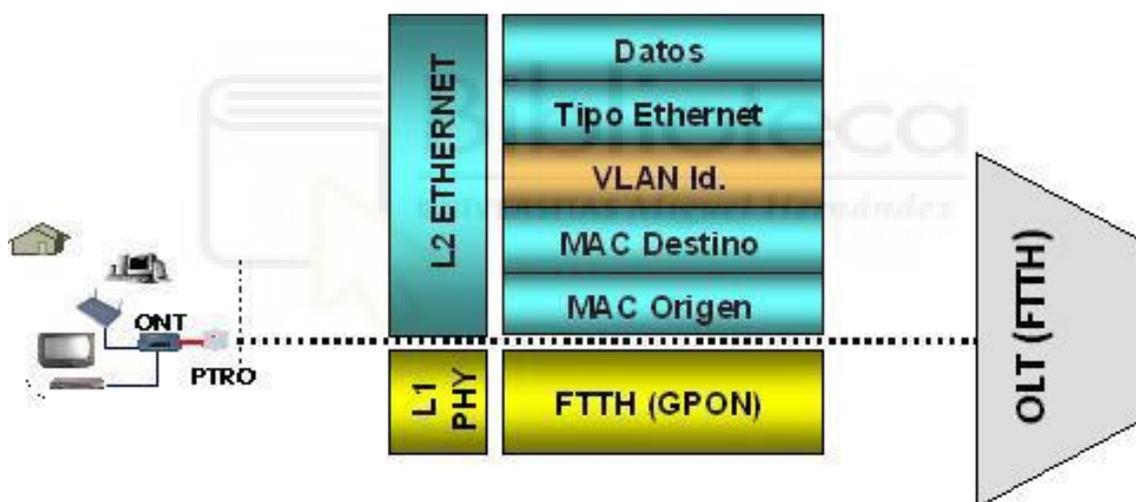


Figura 5: Estructura de protocolos para conexiones FTTH [7]

Se contempla una única VLAN por usuario que alberga las tres calidades de servicio.

La calidad de servicio será determinada por el equipo del cliente, que gestionará esta selección a través de la cabecera Ethernet. Esto se realiza marcando el bit p (bit 802.1p) dentro del campo identificador de la VLAN (VLAN ID). Los valores asignados al bit p y su correspondiente calidad de servicio están detallados en la siguiente tabla:

Valores de bit p-bit 802.1p	Calidades de servicio asociada por Telefónica
0	BE
3	ORO
5	RT

Tabla 2: p-bit 802.1p

Todas aquellas tramas que no vengan marcadas con el bit p con cualquier valor de los de la tabla serán descartadas por la OLT.

1.2.5 TRANSPORTE HASTA LOS PUNTOS DE ENTREGA DE TRÁFICO

La solución técnica implementada para el tráfico Unicast establece una conectividad punto a punto entre cada OLT y el equipo responsable del punto de entrega de tráfico del Operador asociado a dichas OLT.

El servicio NEBA LOCAL agrega el tráfico de los clientes y lo entrega al Operador en un Punto de Acceso Indirecto Local (PAI-L). En este PAI-L, el Operador debe disponer de un servicio de soporte (LAGL) contratado para gestionar el tráfico de las conexiones de sus clientes.

Además, el Operador está obligado a manejar el tráfico Unicast y Multicast a través de VLANs separadas, configuradas específicamente para cada tipo de tráfico.

1.2.6 VLAN DE CLIENTE Y SERVICIO

Es posible configurar la parte lógica de la red de administración de suscriptores mediante redes de área local virtual (VLAN).

- **VLAN de clientes: Las C-VLAN (Customer VLAN):** son una solución de conectividad que asigna una VLAN única a cada cliente (modelo 1:1), lo que facilita la gestión y configuración de la red. Este enfoque permite identificar a cada cliente de manera única, proporcionando simplicidad

operativa y visibilidad de las aplicaciones utilizadas por el cliente en tiempo real. Además, cada cliente tiene una ruta dedicada de capa 2 desde su equipo hasta el enrutador del operador.

- **VLAN de servicio:** Las S-VLAN (Service VLAN) proporcionan conectividad de tipo N:1, donde una VLAN se dedica a un servicio específico (como datos, video o voz) y es compartida por múltiples usuarios. En este modelo, cada servicio tiene su propia VLAN, lo que facilita su gestión. Por ejemplo, para añadir un nuevo servicio, basta con crear una nueva VLAN y asignarle el ancho de banda correspondiente [8].

1.2.7 TRÁFICO UNICAST

Las tramas Ethernet se gestionarán con doble etiqueta VLAN conforme al estándar 802.1ad (Q-in-Q), lo que permite encapsular una VLAN dentro de otra para crear una jerarquía.

En sentido ascendente: La OLT añadirá una etiqueta S-VLAN a las C-VLAN de las conexiones NEBA LOCAL de un mismo operador, sin alterar la VLAN original del cliente (C- VLAN). Tanto la S-VLAN como la C-VLAN serán informadas al Operador al provisionar las conexiones NEBA LOCAL.

El encapsulado Q-in-Q permite conectar a los usuarios a la red del Operador a través de la red de acceso de Telefónica, manteniendo intacta la VLAN original del cliente (C-VLAN). La Figura 6 ilustra cómo se construye la trama 802.1ad a partir de una trama 802.1Q generada por el usuario.

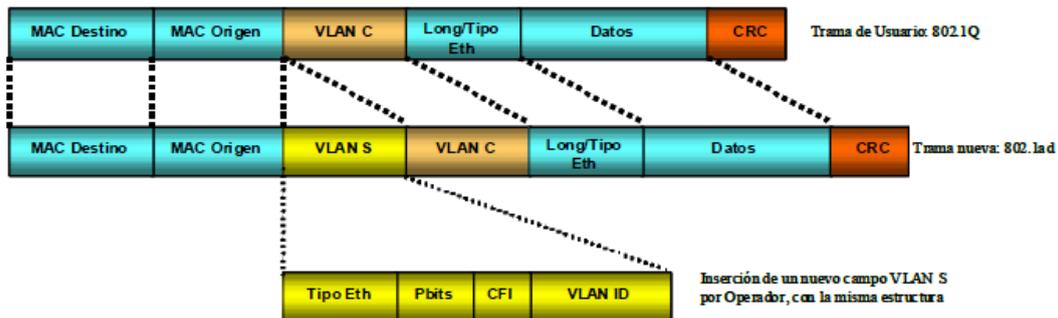


Figura 6: Trama de Usuario 802.1Q [7]

En el LAGL, el Operador recibirá el tráfico de todas las conexiones NEBA LOCAL asociadas a una OLT específica y a ese LAGL, encapsulado con la S-VLAN correspondiente. Dentro de esa S-VLAN, el tráfico de cada conexión individual será diferenciado mediante la C-VLAN, la cual se asigna a medida que se provisionan las conexiones para un Operador, OLT, LAGL y S-VLAN específicos.

El valor de los bits de prioridad 802.1p de la etiqueta C-VLAN, generados por la OLT, se mantendrá intacto en las tramas Ethernet. Además, por cada LAGL y Operador, se asignará una nueva S-VLAN cuando se solicite la primera conexión para una OLT distinta que no haya sido previamente accedida desde ese LAGL y Operador.

En el PAI-L, se mantendrán los valores de los bits de prioridad 802.1p de la etiqueta C-VLAN establecidos por el Operador en las tramas Ethernet enviadas desde su red.

El PAI-L también se interpretará los bits 802.1p de la etiqueta S-VLAN marcados por la OLT (en sentido ascendente) y por el equipo del Operador (en sentido descendente) para aplicar el tratamiento adecuado de calidad de servicio (QoS) a cada trama. Además, reescribirá los valores de estos bits al enviarlos hacia la OLT o hacia la red del Operador, asegurando que se respete la calidad de servicio asignada.

1.2.8 INTERFAZ FÍSICA DE LA ENTREGA DEL SERVICIO

La interconexión entre el equipo de red del Operador y el punto de entrega de tráfico se realizará a través de los puertos del equipo ubicado en el PAI-L. Las interfaces disponibles para esta interconexión varían según la capacidad y el alcance, y se clasifican de la siguiente manera:

Interfaces disponibles:

- 1000 Base-LX: Alcance de hasta 10 km.
- 1000 Base-EX: Alcance de hasta 40 km.
- 1000 Base-ZX: Alcance de hasta 80 km.

- 1000 Base-BX10-D/U: Alcance de hasta 10 km.
- 1000 Base-BX40-D/U: Alcance de hasta 40 km.
- 1000 Base-BX80-D/U: Alcance de hasta 80 km.

- 10GBase-LR: Alcance de hasta 10 km.
- 10GBase-ER: Alcance de hasta 40 km.
- 10GBase-ZR: Alcance de hasta 80 km.

Para las interfaces BX monofibra, las longitudes de onda utilizadas en cada sentido se mantendrán constantes, independientemente del alcance.

Dependencias	Denominación	Longitud Onda TX	Longitud Onda RX
Telefónica	1000BASE-BX-D	1490nm	1310nm
Operador	1000BASE-BX-U	1310nm	1490nm

Tabla 3: Longitud de onda utilizada en cada sentido

1.2.9 PUNTO DE ENTREGA Y DISTRIBUCIÓN GEOGRÁFICA

En la red de Telefónica, los equipos de acceso (OLT) de una central están conectados directamente a un punto de entrega de tráfico, generalmente ubicado en la misma central. Desde este punto, el tráfico es encaminado hacia la red de transporte de Telefónica, gestionando las conexiones correspondientes al servicio NEBA LOCAL y dirigiéndolas hacia la red del Operador.

Estos puntos de entrega de tráfico, denominados PAI-L, son donde Telefónica entrega el tráfico al Operador, quien posteriormente lo gestiona según corresponda. Este proceso se ilustra en la Figura 7.

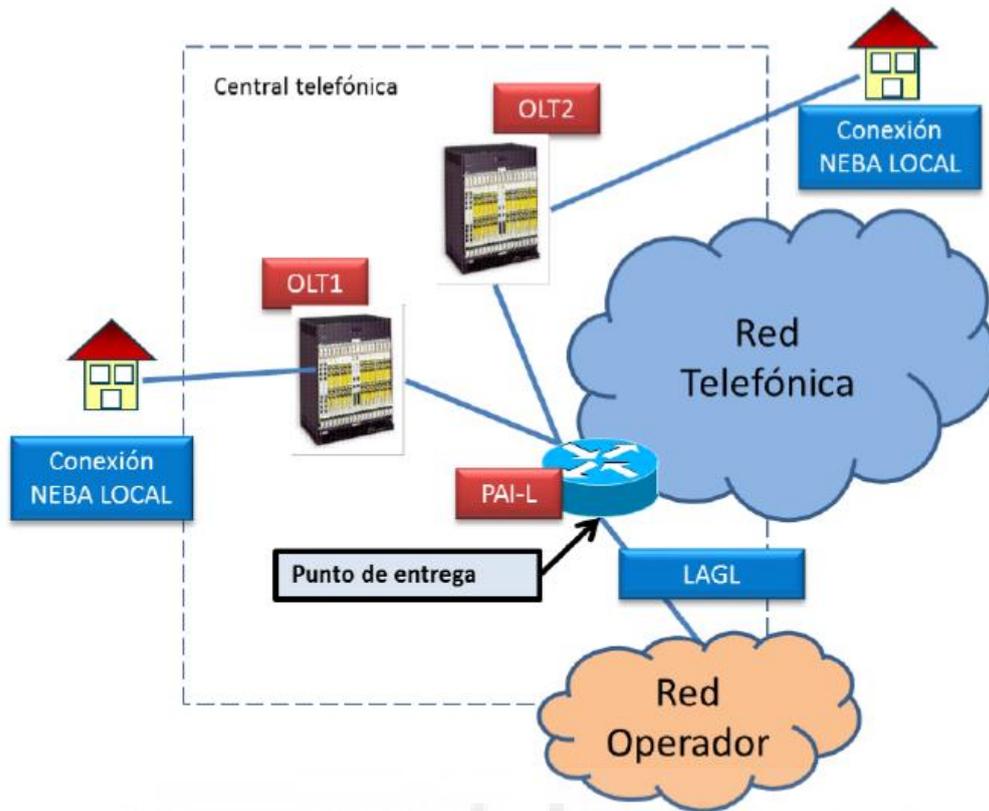


Figura 7: Puntos de entrega y distribución geográfica [7]

Aunque el esquema anterior representa el caso genérico, el crecimiento de la demanda y el despliegue de infraestructura por parte de Telefónica podrían dar lugar a escenarios distintos. Por ejemplo, como se muestra en la Figura 8 cuando se alcanza el límite de OLTs que puede gestionar un PAI-L, se requiere la instalación de un nuevo PAI-L para dar soporte a las OLTs adicionales.

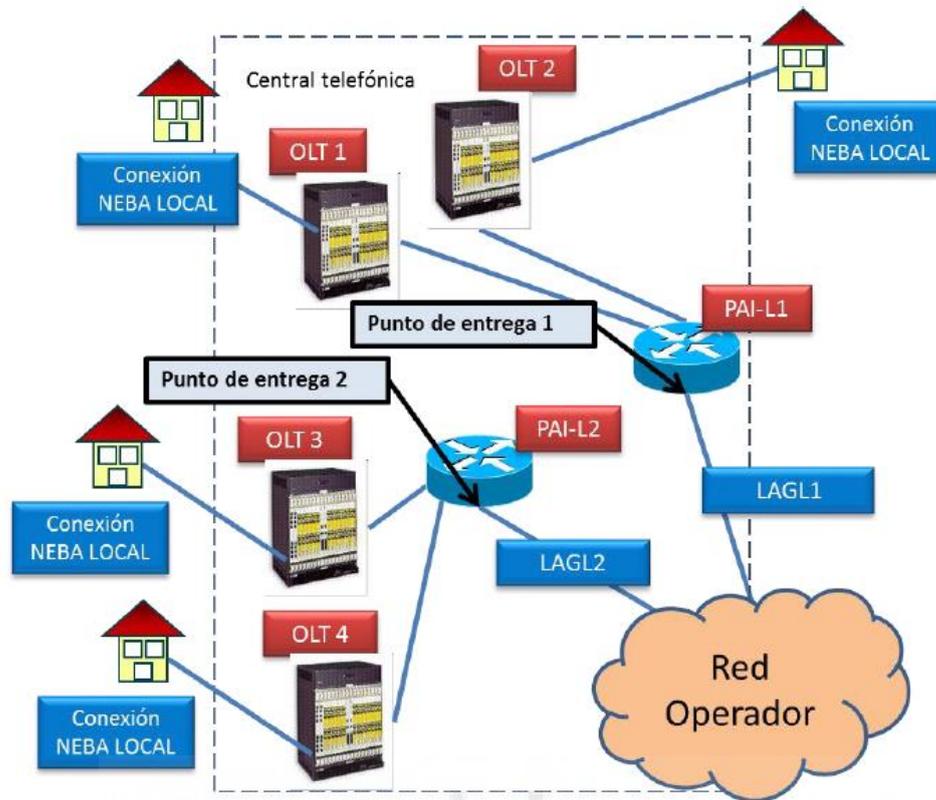


Figura 8: Ubicación de nuevos PAI-L debido al incremento de la demanda [9]

En este caso específico, si el Operador desea ofrecer servicio a las conexiones asociadas a las nuevas OLTs (OLT 3 y OLT 4), será necesario contratar un servicio de soporte en el nuevo PAI-L (PAI-L2).

Además, es posible que, debido al crecimiento en el número de OLTs y PAI-Ls, se generen escenarios diseñados para mejorar la calidad del servicio, como el que se muestra en la Figura 9.

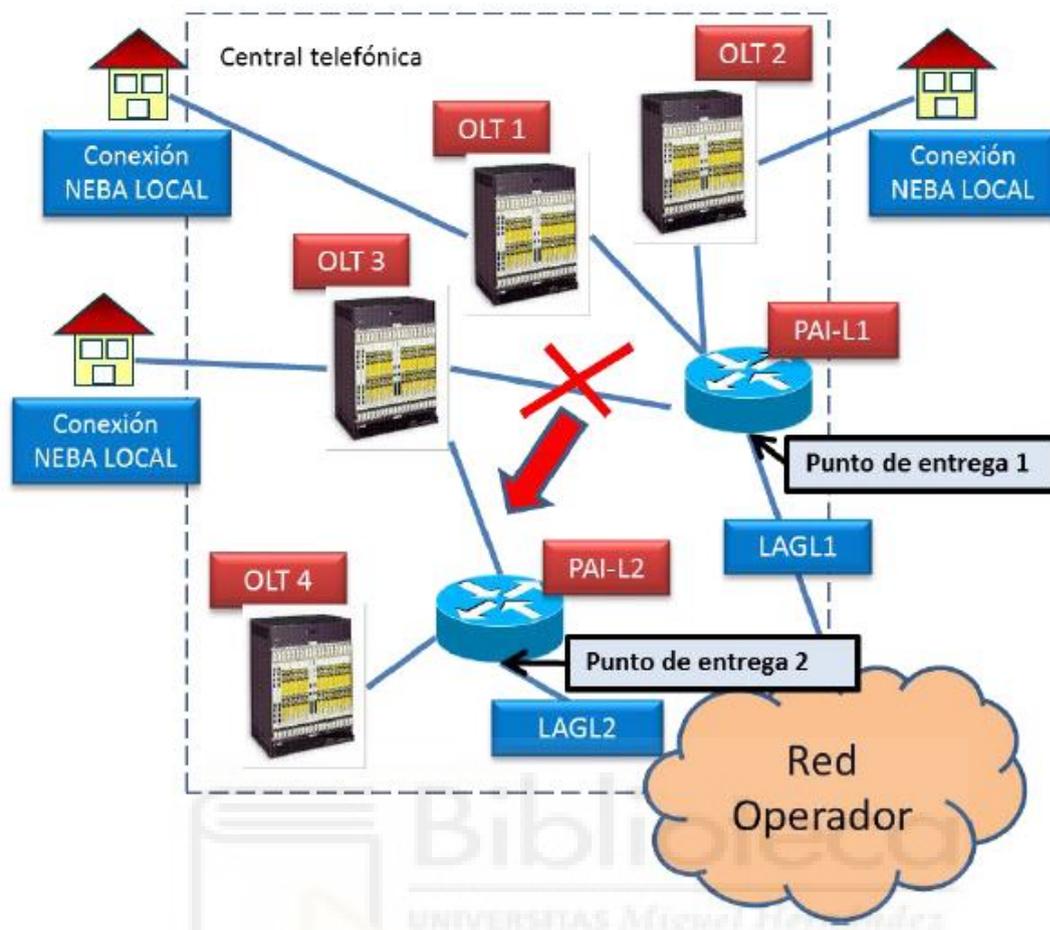


Figura 9: Escenario debido al crecimiento de OLT y PAI-L [7]

En el caso de la Figura 7, el tráfico de los clientes asociados a la OLT 3, que anteriormente era entregado al Operador a través del LAGL1 en el PAI-L1, será transferido al LAGL2 en el PAI-L2. Este cambio será debidamente comunicado y coordinado con los Operadores.

Otro posible escenario, derivado de la estructura de red desplegada por Telefónica, es aquel en el que una OLT se conecta a un PAI-L ubicado en una central distinta a la de la propia OLT, como se ilustra en la Figura 10.

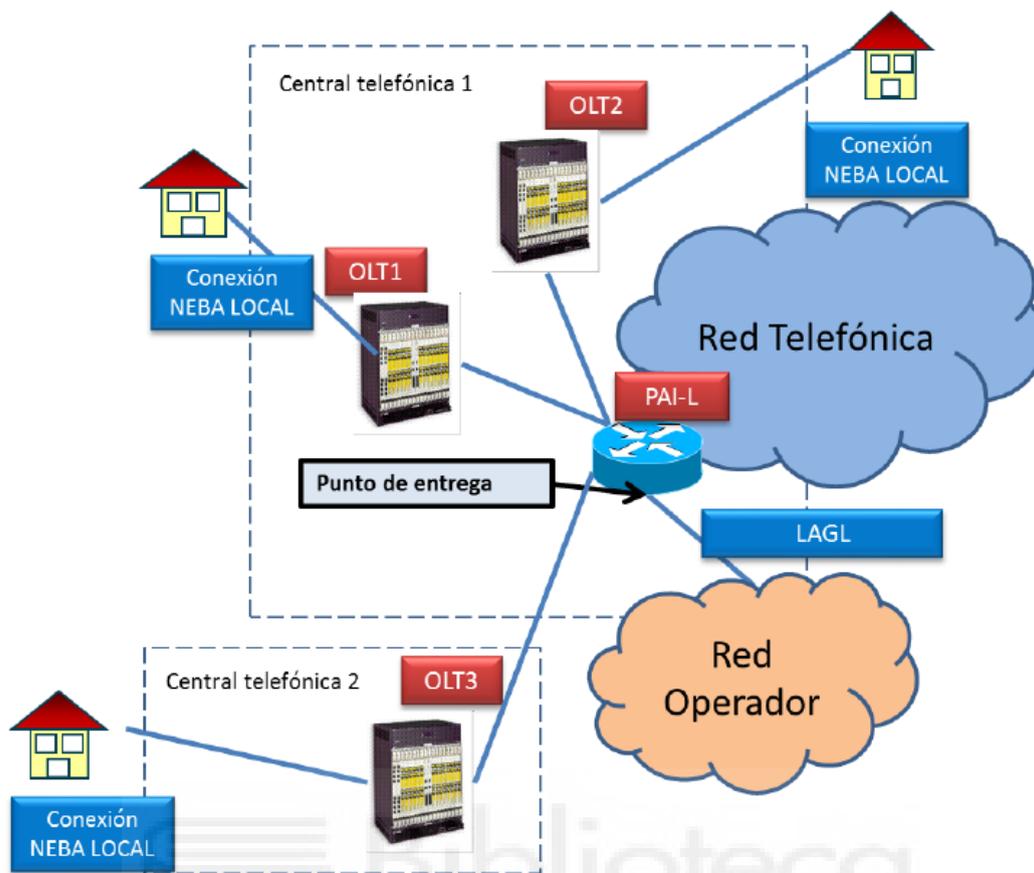


Figura 10: Escenario donde un PAI-L y la OLT se ubican en centrales diferentes [7]

En este escenario, aunque la OLT se encuentra en una central diferente a la del PAI-L, el Operador solo necesitará contratar un LAGL en la ubicación del PAI-L, ya que este actúa como el punto de entrega del tráfico generado por esa OLT (OLT3 ubicada en la central Telefónica 2).

Finalmente, debido al crecimiento de la demanda y la expansión de la red, podría surgir la necesidad de instalar un nuevo PAI-L en la otra central, como se muestra en la Figura 11.

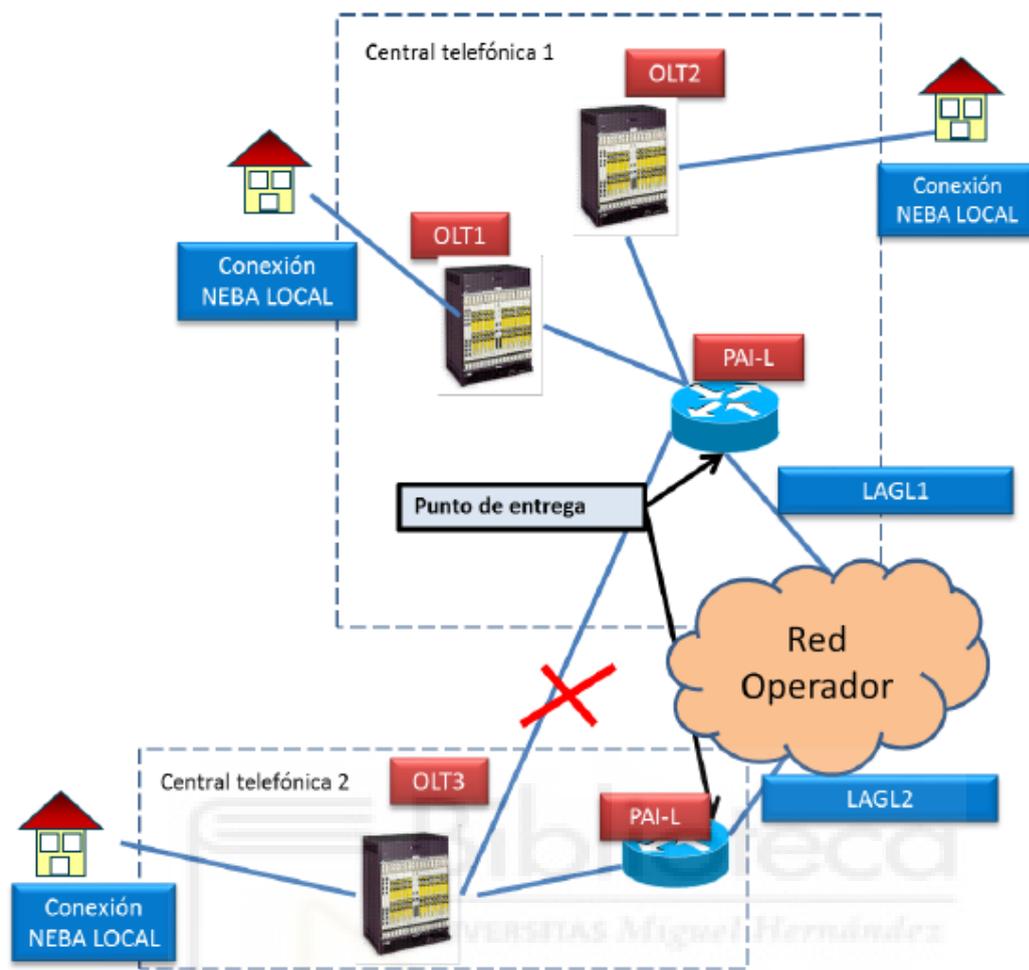


Figura 11: Instalación de un PAI-L en otra central [7]

De esta manera el punto de entrega del "OLT3-central telefónica 2", estará en la misma central, reemplazando a "PAI-L-central telefónica 1" como punto de enlace de tráfico.

Este cambio será comunicado y acordado con el Operador, quien contratará el servicio de soporte en el nuevo punto de entrega identificado como "PAI-L-Central Telefónica 2".

Telefónica proporcionará a los Operadores la información necesaria sobre la relación entre OLT, central y PAI-L, con el objetivo de facilitar la gestión de sus solicitudes de servicios de soporte y la planificación para ofrecer servicio a sus clientes. Esta información se incluirá en el fichero de fincas pasadas FTTH, detallando, para cada GESCAL 17, el código MIGA de la central cabecera y el

PAI-L correspondiente donde se entregará el tráfico al Operador. Además, en las consultas de cobertura realizadas a través de Web Services, se indicará el PAI-L asociado. De acuerdo con el proceso de migración cuando conexiones de cliente de un PAI-L deban ser migradas a un nuevo PAI-L, Telefónica avisará previamente con tres meses de antelación, que también será remitido a la CNMC. Durante este período, los Operadores deberán provisionar el LAGL (y entrega de señal). Finalizado el plazo establecido, se identificará la infraestructura afectada y se otorgará un periodo de 1 mes para completar la migración de las conexiones desde el LAGL original al nuevo. Posteriormente, las OLT vinculadas al PAI-L original serán desconectadas. Los costes de migración de estas conexiones serán asumidos por Telefónica.

1.2.10 IDENTIFICADORES DE ACCESOS

La identificación del acceso para el servicio NEBA LOCAL dependerá del tipo de solicitud, distinguiendo entre Alta sobre Vacante y Alta sobre Ocupado.

Alta sobre Vacante:

En el caso de Alta sobre Vacante, la solicitud debe tramitarse indicando el domicilio mediante el código GESCAL. Este proceso aplica en los siguientes casos:

- No existe acceso de fibra en el domicilio o se requiere un nuevo acceso.
- El acceso de fibra existente está vinculado a un operador distinto a Telefónica.
- El servicio actual se proporciona a través de acceso de cobre o cable.

Los operadores pueden utilizar herramientas como el buscador GESCAL de NEON o servicios ofrecidos por Telefónica para obtener el código GESCAL necesario.

Restricciones y gestión de incidencias:

Telefónica no podrá tramitar altas en domicilios afectados por incidencias de tipo “SIN RED” o “Ampliación de recursos”, extendiendo esta restricción a todos los domicilios conectados a la misma CTO (Caja Terminal Óptica) afectada.

Las solicitudes pendientes deberán atenderse en orden una vez resuelta la incidencia.

Telefónica deberá mantener actualizados sus sistemas sobre el estado de las CTO tras cualquier intervención física.

Procesos en áreas de cierre de centrales:

En zonas afectadas por el cierre de centrales, si una solicitud de Alta sobre Vacante enfrenta incidencias como “SIN RED” o “Ampliación de recursos”, Telefónica deberá instalar o ampliar los recursos necesarios en un plazo máximo de 15 días laborables desde la solicitud del operador.

Alta sobre Ocupado:

En el caso de una instalación de línea ocupada (Alta sobre Ocupado), es decir, cuando el acceso de fibra ya dispone de servicio de Telefónica, ya sea mayorista o minorista, el acceso deberá identificarse unívocamente mediante el Identificador Único del Acceso (IUA).



Figura 12: PTRO rotulado con IUA [10]

La IUA es una clave que identifica de forma única el punto de terminación de red asociado a un acceso físico con una interfaz óptica. Telefónica facilitará a los operadores alternativos el algoritmo necesario para generar el código de control IUA previa solicitud.

El IUA se proporciona al Operador durante el proceso de provisión de un servicio NEBA LOCAL (tanto en el alta sobre vacante, como sobre ocupado), y también se etiqueta en el PTRO (Punto de Terminación de Red Óptica) desde el momento de la instalación.

Para obtener el IUA el Operador tiene las siguientes opciones:

- Visualizarlo en el PTRO, donde está rotulado.
- Utilizar el Servicio Web (WS) “Servicio de consulta para identificación de accesos”, proporcionando la dirección del cliente en su forma GESCAL apropiada.
- Revisar las facturas de los clientes, ya que tanto Telefónica como los operadores alternativos están obligados a incluir en sus facturas de

clientes minoristas el IUA de las conexiones FTTH activas.

1.2.11 FLUJOS DE CONEXIONES NEBA LOCAL

- **Alta sobre Vacante:**

Se solicita para un acceso FTTH que no tiene servicio activo de Telefónica (ni mayorista ni minorista). Implica la instalación de una acometida y un PTRO, lo que requiere desplazamiento al domicilio del cliente. El PTRO se instalará siguiendo los mismos criterios que en una alta minorista. Si un operador desea desplegar sus propias acometidas, deberá alcanzar un acuerdo previo con Telefónica en términos razonables.

- **Alta sobre Ocupado:**

Se solicita sobre un acceso FTTH que ya cuenta con servicio activo de Telefónica, ya sea mayorista o minorista. Tanto la acometida como el PTRO ya están instalados.

Este tipo de alta puede incluir portabilidad (ya sea del servicio actual o entre terceros), lo que permite sincronizar la portabilidad con las tareas necesarias para la provisión del NEBA LOCAL.

- **Modificación (Posventa):**

El Operador puede solicitar cambios en parámetros técnicos (como OPVLAN o perfil), migraciones de una conexión NEBA LOCAL de un LAGL a otro, o incluso la reinstalación del PTRO, lo que requerirá un desplazamiento al domicilio del cliente.

- **Baja**

No requiere desplazamiento al domicilio del cliente.

1.2.12 PARÁMETROS TÉCNICOS

Los parámetros comunicados al Operador durante la provisión como tras la

finalización de la solicitud son los siguientes:

Parámetro	Valor
Identificador ONT	Código numérico de 11 cifras
IUA	Número identificador del IUA generado en la provisión
Id. Servicio	Número Administrativo del servicio generado en la provisión
OP-VLAN	20 a 24
S-VLAN	De 1000 a 4000(*1)
C-VLAN	De 4 a 503 (*2)
VLAN MCAST	(*3)
Q-VLAN	(*4)

Tabla 4: Parámetros técnicos obtenidos de [10]

(1*) La S-VLAN será única para un operador para un mismo LAG, pudiéndose repetir para el mismo operador en distintos LAG.

(2*) La C-VLAN es exclusiva dentro de una misma S-VLAN. Esto significa que, dentro de una S-VLAN específica, cada C-VLAN identifica de manera única a un cliente o conexión.

Sin embargo, el mismo identificador de C-VLAN puede reutilizarse para diferentes clientes del mismo operador, siempre y cuando estos clientes estén conectados a distintos nodos de acceso (por ejemplo, diferentes OLT).

Esto es posible porque el tráfico de cada nodo se transporta a través de una S-VLAN distinta, lo que garantiza que no haya conflicto entre las C-VLAN que comparten el mismo identificador en diferentes nodos.

(*3) La VLAN MCAST será la misma etiqueta para todos los Operadores, y será comunicada a los Operadores que soliciten la funcionalidad Multicast.

(*4) La Q-VLAN será única por Operador, y será acordada con Telefónica cuando se solicite la funcionalidad Multicast.

1.2.13 ALTA DE CONEXIONES NEBA LOCAL

En este apartado se explica una de las principales modalidades de alta en el servicio NEBA.

1.2.13.1 ALTA SOBRE VACANTE

Las solicitudes de alta de vacantes incluyen el código GESCAL como parámetro principal de identificación de la residencia.

Entidad Geográfica		Nombre	Formato	Observaciones			
Provincia	PP	Código de la provincia	Num.	Obligatorio	GESCAL 17	GESCAL 24	GESCAL 37
Población	EEEE	Nº de Entidad de Población	Num.	Obligatorio			
Calle	CCCC	Nº de Calle	Num.	Obligatorio			
Finca	FFFF	Nº de Finca	Num.	Obligatorio			
	B	Bis/duplicado	Alfanum.	Opcional			
	TXX	Bloque	Alfanum.	Opcional			
	OY	Portal/Puerta	Alfanum.	Opcional			
	L	Letra de la finca	Alfanum.	Opcional			
Escalera	SS	Identificador de escalera	Alfanum.	Opcional			
Domicilio	AAA	Planta	Alfanum.	Obligatorio			
	MMMM	Mano 1 del domicilio	Alfanum.	Opcional			
	NNNN	Mano 2 del domicilio	Alfanum.	Opcional			

Tabla 5: Tipos de código GESCAL [11]

La solicitud de entrada incluirá el GESCAL 37 para identificar inequívocamente el domicilio de instalación. Para disponer de dicho código, el operador dispone de las siguientes opciones:

1. Para recuperar el GESCAL 37 de un domicilio, el operador podrá utilizar el correspondiente "Web Service".
2. En caso de que el domicilio no estuviera un Gescalizado o si el operador no localiza el GESCAL 37, se puede utilizar el GESCAL 24 (Finca), cumplimentando un conjunto de campos adicionales (equivalentes a los utilizados en las posiciones 25 a 37 del GESCAL 37), con la información que el operador disponga del domicilio de instalación.

Descripción del proceso:

1. Solicitud del Operador: El operador debe presentar su solicitud indicando los datos de contratación requeridos.
2. Validación por TE: Telefónica (TE) recibe la solicitud, la valida, asigna un número y verifica cobertura.
3. Notificación: TE informa al operador si la solicitud es aceptada o rechazada, y proporciona un número administrativo si es aprobada.
4. Activación de la orden: TE asignará y activará la orden de servicio. En caso de que el operador proporcione el OP-VLAN se asignará dicho valor. En caso contrario se asignará un valor que se comunicará al operador.
5. Datos técnicos: Se comunican al operador los parámetros técnicos necesarios para activar el servicio, como ID ONT, S-VLAN, C-VLAN, OP-VLAN, junto con el número Administrativo e IUA de la conexión previamente comunicado.
6. Agendamiento con el cliente: TE contacta al cliente para acordar la fecha o ventana de instalación (VIL). Si el contacto con el cliente fuera infructuoso, se generará parada de reloj y se abrirá una incidencia al Operador y esperará que este reitere o anule.
7. Confirmación de VIL: TE notifica al operador la fecha agendada junto con la información previa, número administrativo y el IUA asignado.

8. Instalación: En la fecha programada, TE realiza la instalación y verifica el funcionamiento mediante una ONT de prueba.
9. Finalización: Tras la instalación, TE informa al operador del cierre de la solicitud.
10. Cancelación por el cliente: Si el cliente final decide no proceder, TE notifica al operador, quien debe reiterar o anular la solicitud.
11. Trabajos necesarios en domicilio: Si se detectan obstáculos para la instalación (ej. canalizaciones obstruidas), TE detiene el proceso y notifica una incidencia al operador. El operador tiene 15 días para resolver la incidencia junto con el cliente. Si no se resuelve en este plazo, TE cancela la solicitud [12].

1.2.14 INGRAESTRUCTURA PREVIA DEL CLIENTE

Telefónica es una compañía multinacional de telecomunicaciones con operaciones en 17 países y presencia en 24 en total. Es una empresa privada y líder en su sector en España.

Para la distribución de sus productos y servicios, Telefónica emplea tres marcas comerciales principales:

- Movistar, presente en España y en numerosos países de América Latina.
- O2, operativa en Alemania, Reino Unido y recientemente en España como una opción centrada en fibra y móvil.

Vivo, su marca exclusiva en Brasil [13] Telefónica Tech es un conglomerado de empresas bajo la propiedad del grupo Telefónica. Ofrece una amplia gama de servicios y soluciones tecnológicas integradas en áreas como ciberseguridad, cloud, IoT, big data y blockchain.

Acens, integrada en Telefónica Tech, es una empresa pionera en soluciones Cloud dirigidas a pequeñas y medianas empresas, brindando opciones flexibles,

seguras y efectivas tanto en entornos de cloud privados, públicos como híbridos. Fundada en 1997, actualmente opera en España, Brasil, Perú y México. Dispone de dos centros de datos en España con una superficie superior a 6.000 metros cuadrados y cuenta con una cartera de clientes que supera los 100.000 [14].

1.2.15 DESCRIPCIÓN GENERAL DE LA INFRAESTRUCTURA

Los operadores logísticos se encargan de llevar a cabo actividades de almacenaje, gestión y distribución de productos.

Existen distintos tipos de operadores logísticos según sus ámbito y capacidad:

- Operadores logísticos internacionales: Transportan y distribuyen mercancías a nivel internacional, gracias a una red logística que abarca varios países.
- Operadores logísticos nacionales: En España, el sector logístico es uno de los sectores que más empleo genera, La contribución del sector logístico a la economía española representó el 2.74% del PIB en 2021 [15]
- Operadores logísticos regionales: Son empresas que se dedican a llevar a cabo todo el proceso de suministro y distribución de mercancías. Se caracterizan por disponer de varios almacenes situados en una sola Comunidad Autónoma [16].

El cliente es un operador logístico regional con 20 sedes distribuidas estratégicamente en los polígonos industriales más relevantes de Cataluña, optimizando sus rutas de transporte y cobertura. Actualmente, las sedes se encuentran localizadas en:

Sede	Ubicación (Polígono Industrial)	Ciudad
Transporte Norte	Polígono Zona Franca	Barcelona
Transporte Tarragona	Polígono Francolí	Tarragona
Transporte Vallés	Polígono Can Magarola	Mollet del Vallés
Transporte Delta	Polígono Les Salines	Sant Boi de Llobregat
Transporte Empordà	Polígono Vilamalla	Figueres
Transporte Garraf	Polígono Mas Alba	Sant Pere de Ribes
Transporte Manresa	Polígono Bufalvent	Manresa
Transporte Martorell	Polígono Can Cases	Martorell
Transporte Sabadell	Polígono Sant Pau de Riu-Seco	Sabadell
Transporte Vic	Polígono El Sot dels Pradals	Vic
Transporte Baix Llobregat	Polígono El Plà	Sant Feliu de Llobregat
Transporte Reus	Polígono Agro-Reus	Reus
Transporte Lleida	Polígono Camí dels Frares	Lleida
Transporte Alt Penedès	Polígono Clot de Moja	Olèrdola
Transporte Girona	Polígono Fornells	Fornells de la Selva
Transporte Mataró	Polígono Pla d'en Boet	Mataró
Transporte Granollers	Polígono Congost	Granollers
Transporte Igualada	Polígono Les Comes	Igualada
Transporte Castelldefel	Polígono Can Vinader	Castelldefels
Transporte Rubí	Polígono Cova Solera	Rubí

Tabla 6: Listado de sedes y ubicaciones. El listado por razones de confidencialidad ha sido alterado no respondiendo a la real configuración del cliente.

1.2.16 CONFIGURACIÓN DE RED INICIAL



La infraestructura de red del cliente se basa en una VPN diseñada para conectar de manera segura, las 20 sedes distribuidas estratégicamente en Cataluña. Esta red utiliza una topología basada en túneles IPsec que enlazan las sedes remotas al firewall centralizado, ubicado en un Data Center.

Detalles de la configuración:

- Túneles IPsec: Todas las sedes remotas se conectan a través de túneles IPsec al firewall central, proporcionando una comunicación segura y cifrada sobre Internet.
- Firewall centralizado: Firewall como núcleo de la seguridad de la red, con capacidad para aplicar políticas avanzadas de filtrado, prevención de intrusiones.

1.2.17 LIMITACIONES DE LA CONFIGURACIÓN INICIAL

- Existe una dependencia del nodo central para todas las comunicaciones. La caída del firewall central afecta todas las operaciones de red.
- Latencia alta debido a que el tráfico entre sedes debe pasar obligatoriamente por el nodo central, lo que incrementa la latencia y afecta el rendimiento de aplicaciones críticas.

- Cada sede mantiene un túnel IPsec activo hacia el nodo central, lo que puede aumentar la carga en los dispositivos de borde.
- La configuración inicial requiere direcciones IP públicas o configuraciones NAT para establecer los túneles.
- Aunque la administración se centraliza, el monitoreo y mantenimiento de los túneles IPsec es más complejo y consume más recursos operativos.
- Agregar nuevas sedes aumenta la carga operativa sobre el firewall central, dificultando el escalado de la red.

Esta configuración inicial, basada en túneles IPsec, presenta posibilidades de mejora futura hacia un diseño más robusto, como la integración con redes MPLS y Backup LTE.

1.2.18 INTEGRACIÓN CON RED MPLS.

Con la integración de la red MPLS encontramos mejoras significativas en aspectos como arquitectura, rendimiento, gestión y escalabilidad.

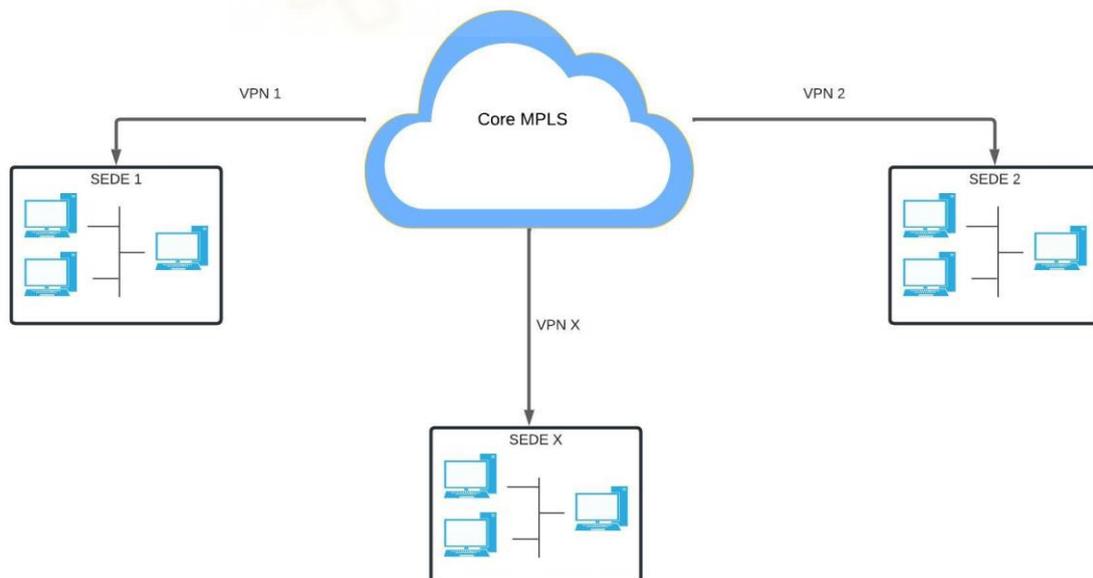


Figura 13: Core MPLS

1.2.18.1 ARQUITECTURA DE RED

Topología Any-to-Any: Con la implementación de MPLS, las sedes se conectan directamente entre sí, eliminando la dependencia del nodo central para la intercomunicación.

1.2.18.2 RENDIMIENTO

Optimización del Tráfico: MPLS permite conexiones directas entre sedes con baja latencia.

MPLS crea un entorno aislado y seguro, eliminando la dependencia de conexiones públicas para la interconexión de las sedes.

1.2.18.3 GESTIÓN

Escalabilidad Operativa: La integración de nuevas sedes en la red MPLS es sencilla, y las configuraciones de seguridad se aplican de manera uniforme desde el Firewall.

1.2.18.4 ESCALABILIDAD

Alta Capacidad de Crecimiento: MPLS y el Firewall permiten una expansión fluida de la red, integrando nuevas sedes sin afectar el rendimiento o la seguridad general.

La solución admite una combinación de diferentes tipos de enlaces (FTTH, 4G) y permite ajustes en función de las necesidades futuras del cliente.

1.2.18.5 RESUMEN COMPARATIVO

Característica	IPSec	MPLS
Propósito Principal	Garantizar la seguridad de los datos durante el tránsito por redes públicas.	Proveer conectividad de alto rendimiento entre sedes a través de redes privadas.

Capa OSI	Opera en la Capa 3 (Red).	Opera en la Capa 2.5 (entre Enlace y Red).
Seguridad	Ofrece cifrado extremo a extremo para proteger la confidencialidad de los datos.	Depende de la red MPLS del proveedor; no incluye cifrado por defecto.

Eficiencia de tráfico	Puede introducir latencia debido al cifrado y descifrado.	Bajo retardo y alta capacidad de transmisión.
Escalabilidad	Escalable, pero puede complicarse con un gran número de túneles.	Altamente escalable, especialmente para redes con múltiples sedes
Facilidad de implementación	Relativamente fácil de implementar sobre Internet existente	Requiere infraestructura específica proporcionada por el ISP.
Requerimientos de infraestructura	No requiere infraestructura específica, se basa en firewalls o routers.	Necesita hardware específico y soporte por parte del ISP.

Tabla 7: IPSec y MPLS

1.2.19 LTE

LTE, siglas de "Long Term Evolution" y conocido como 4G, es un estándar para comunicaciones inalámbricas de banda ancha. Fue concebido como una tecnología de radiocomunicación principalmente orientada al uso humano.

Su diseño se centra en proporcionar altas velocidades de datos y baja latencia, características ideales para soportar servicios de banda ancha en dispositivos móviles, como navegación por internet y transmisión de video.

En el ámbito del Internet de las Cosas (IoT), LTE se aplica a casos que demandan estas prestaciones, como los vehículos conectados.

2 MAPA DE RED PROPUESTO

El siguiente mapa de red presenta una infraestructura diseñada para conectar las 20 sedes del cliente de manera eficiente y segura. Este diseño prioriza la continuidad operativa y la optimización de la gestión del tráfico. Además, la arquitectura propuesta destaca por su escalabilidad y adaptabilidad, lo que permite futuras modificaciones según las necesidades del cliente.



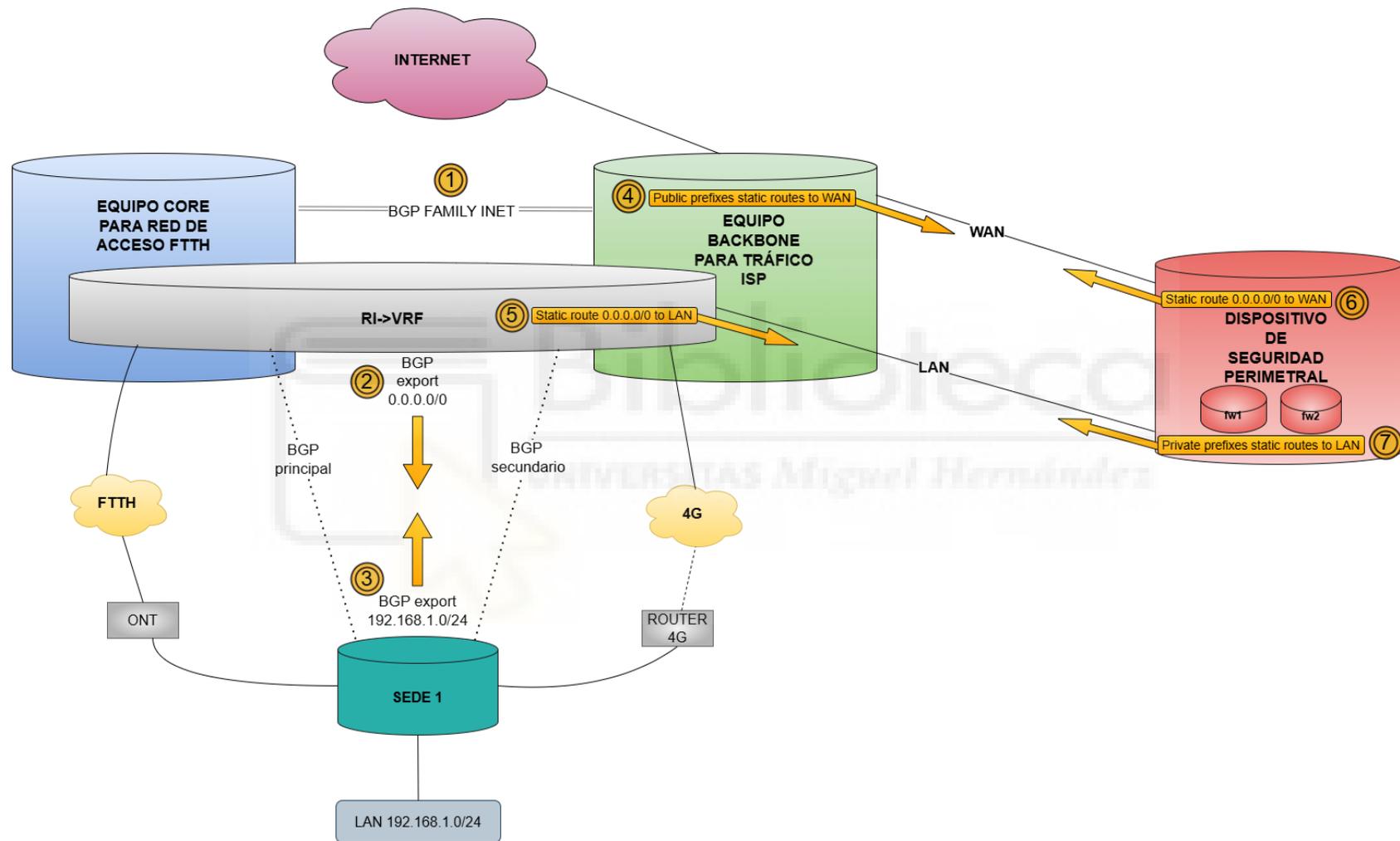


Figura 14: Mapa de red general propuesto para la conexión de sedes

1. BGP family inet:

BGP family inet es una funcionalidad específica del protocolo BGP, orientada al intercambio de rutas IPv4. Permite que diferentes sistemas autónomos compartan información de enrutamiento para garantizar la conectividad entre redes. En este proyecto, BGP FAMILY INET establece la base para que el equipo Core, encargado de gestionar la red de acceso FTTH, y el equipo Backbone, que maneja el tráfico hacia y desde Internet, puedan comunicarse de manera eficiente. A través de esta familia de direcciones, se garantiza la propagación de rutas globales e internas necesarias para mantener la conectividad tanto en la red del ISP como hacia redes externas. Es una pieza clave para asegurar que el tráfico fluya de manera ordenada, segura y optimizada dentro de toda la arquitectura.



Figura 15: BGP FAMILY INET

2. BGP Export 0.0.0.0/0:

La exportación de la ruta predeterminada 0.0.0.0/0 permite que todo el tráfico cuyo destino no coincida con rutas más específicas sea redirigido a través del backbone del ISP. De esta manera se asegura que el tráfico de cada sede con destinos externos o no definidos tenga una salida preestablecida hacia Internet, proporcionando una solución eficiente para la gestión del enrutamiento global.

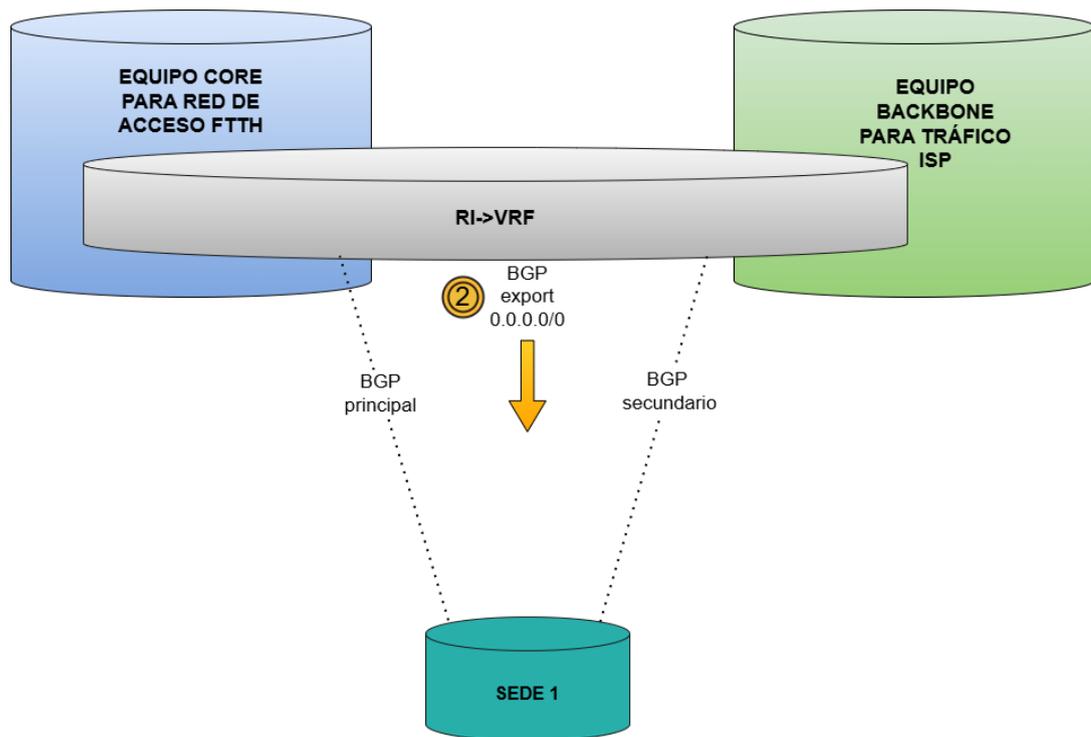


Figura 16: BGP Export 0.0.0.0/

3. BGP export 192.168.1.0/24:

En la Figura 17 observamos el proceso mediante el cual la subred local de la sede 1, 192.168.1.0/24, se anuncia desde la Routing Instance configurada en la red del proveedor. Este anuncio permite que la subred de la sede 1 sea visible y accesible desde otras partes de la red, tanto dentro de la infraestructura del proveedor como a través de los enlaces hacia otras redes. De esta manera, se garantiza que los dispositivos y servicios de la sede 1 puedan comunicarse eficientemente con redes externas e internas.

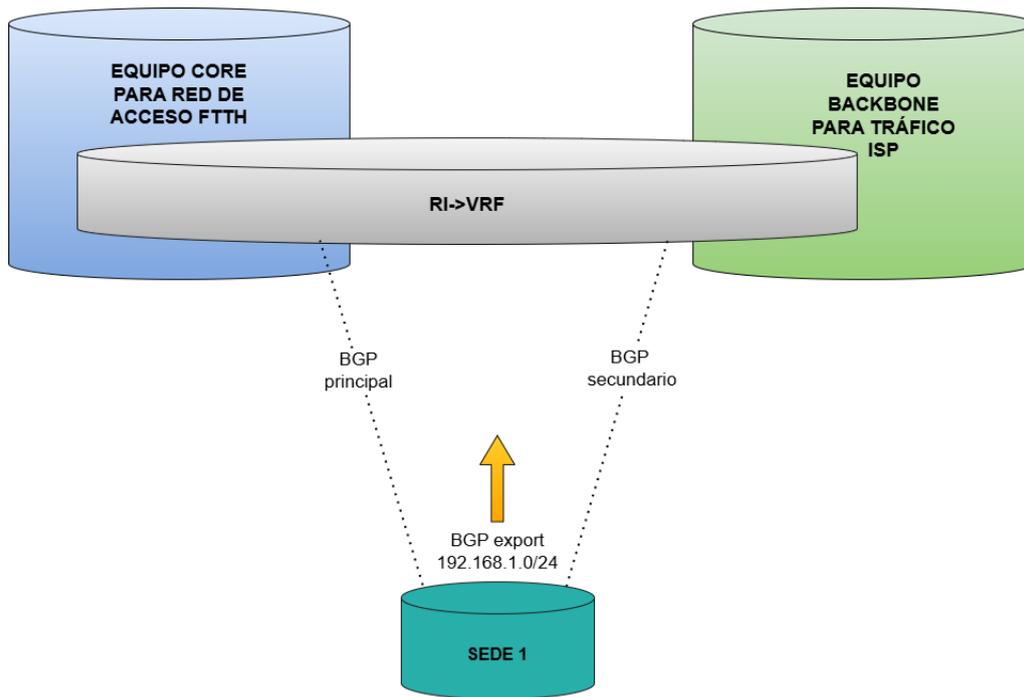


Figura 17: BGP export 192.168.1.0/24

4. Public prefixes static routes to WAN:

En la Figura 18 se indica la configuración de rutas estáticas utilizadas para dirigir los prefijos públicos hacia la red WAN. Esto permite que el tráfico destinado a direcciones públicas sea encaminado de manera eficiente desde el equipo backbone hacia Internet. Este mecanismo asegura que los datos provenientes de la red interna puedan alcanzar los destinos públicos correspondientes.

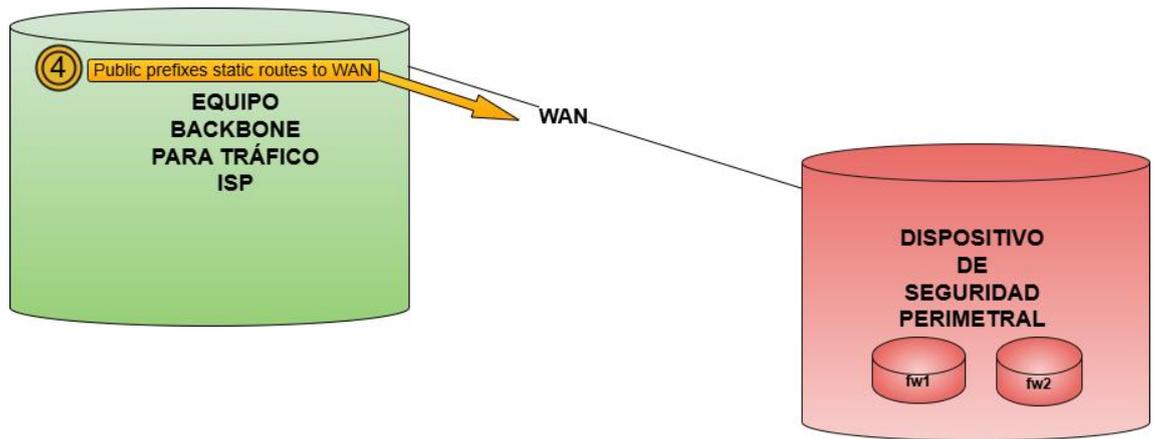


Figura 18: Public prefixes static routes to WAN

5. Static route 0.0.0.0/0 to LAN:

En la Figura 19 se define una ruta estática que actúa como puerta de enlace predeterminada para todo el tráfico que no tenga una ruta específica en la tabla de enrutamiento. Esta configuración dirige el tráfico desde el equipo backbone hacia la red LAN asociada, garantizando que todos los paquetes con destino desconocido o genérico sean redirigidos correctamente a la red local.

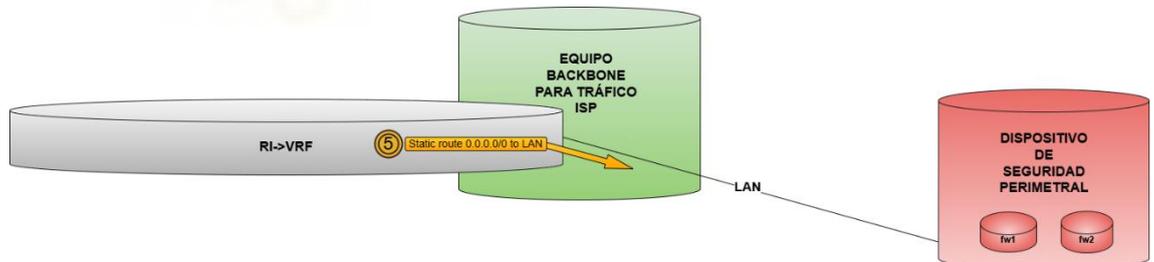


Figura 19: Static route 0.0.0.0/0 to LAN

6. Static route 0.0.0.0/0 to WAN:

En la Figura 20 se establece una ruta estática predeterminada que dirige todo el tráfico saliente, cuyo destino no se encuentra especificado en la tabla de enrutamiento, hacia la red WAN. Esta configuración asegura que el tráfico con origen el dispositivo de seguridad perimetral y con destino a redes externas, como Internet, sea encaminado a través de la interfaz designada hacia el equipo

backbone para tráfico ISP.

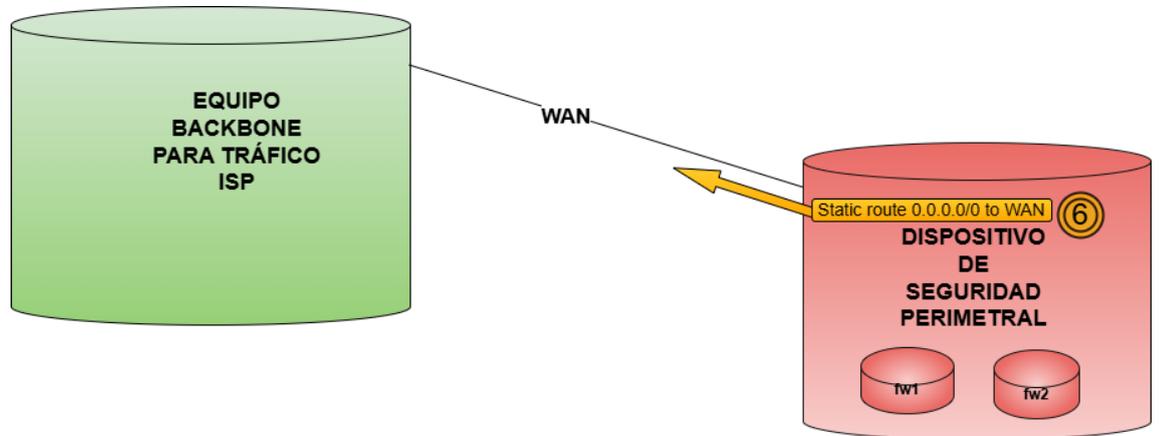


Figura 20: Static route 0.0.0.0/0 to WAN

7. Private prefixes static routes to LAN:

En la Figura 21 define rutas estáticas específicas para prefijos privados que permiten dirigir el tráfico entrante desde la red interna hacia las diferentes subredes locales (LAN) gestionadas por el firewall. Estas rutas garantizan que el tráfico destinado a redes privadas sea correctamente enrutado hacia los segmentos de red adecuados, facilitando una comunicación interna segura y eficiente entre los dispositivos y servicios de todas las sedes.

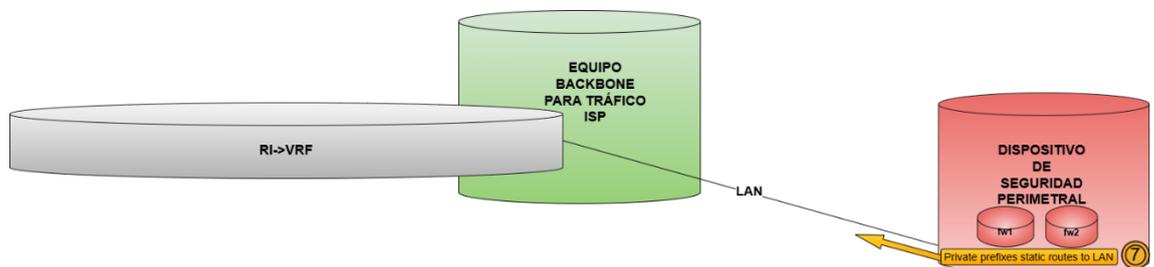


Figura 21: Private prefixes static routes to LAN

2.1 EQUIPO CORE PARA RED DE ACCESO FTTH

Descripción: Este dispositivo actúa como el núcleo de gestión de la red de acceso FTTH. Gestionando el enrutamiento y el flujo de tráfico entre las redes internas y las redes externas.

Rol: Su función es garantizar la conectividad eficiente y fiable entre las diferentes redes.



Figura 22: Equipo para gestionar la red de acceso FTTH

2.2 EQUIPO BACKBONE PARA EL TRÁFICO DEL ISP

Descripción: Este dispositivo actúa como el núcleo principal de la red del ISP, gestionando el enrutamiento y el flujo de tráfico entre las redes internas y las redes externas, incluyendo el acceso a Internet.

Rol: Su función es garantizar la conectividad eficiente y fiable entre las diferentes redes, asegurando un transporte óptimo del tráfico en todo el sistema.



Figura 23: Equipo Backbone para la gestión del tráfico del ISP

2.3 DISPOSITIVO DE SEGURIDAD PERIMETRAL

Descripción: Equipo dedicado a la protección de la red, encargado de realizar funciones como el filtrado de tráfico, aplicación de políticas de acceso y gestión de conexiones seguras.

Rol: Garantiza la seguridad de la red y la separación de dominios de confianza mediante la implementación de políticas de firewall, segmentación y configuración de conexiones seguras entre las diferentes sedes o con redes externas.



Figura 24: Dispositivo que aplica políticas de firewall

2.4 RED 4G

Descripción: La red 4G se utiliza como respaldo (backup LTE) en la infraestructura final, proporcionando conectividad inalámbrica de alta velocidad y baja latencia. También soporta conexiones VPN para garantizar la seguridad y privacidad en la comunicación entre las sedes.

Rol: Funciona como enlace redundante en la red, asegurando la continuidad operativa en caso de fallos de la conexión principal y garantizando una transmisión de datos segura entre las sedes de la empresa de logística.



Figura 25: Red 4G

2.5 FTTH

Descripción: Es la red de acceso primaria que establece la conexión entre las sedes del cliente y el equipo core de la infraestructura.

Rol: Ofrece enlaces de alta velocidad y baja latencia para garantizar una comunicación eficiente entre las sedes, empleando terminales ONT (Optical Network Termination) como interfaz de conexión.



Figura 26: Red FTTH

2.6 ONT

Descripción: La ONT es el dispositivo terminal en una red FTTH que realiza la conversión de señales ópticas en señales eléctricas compatibles con los equipos de usuario. Además, permite la terminación del enlace óptico en el cliente final.

Rol: Es el punto de interconexión entre la red óptica de acceso y la red interna del cliente. Su función es garantizar la transmisión eficiente de información, manteniendo los parámetros de calidad definidos por la infraestructura de la red.



Figura 27: ONT (Optical Network Terminal)

2.7 ROUTER 4G

Descripción: Dispositivo diseñado para utilizar la red 4G como enlace de respaldo en caso de interrupciones en la conexión principal.

Rol: Garantiza la continuidad del servicio al cliente al mantener la conectividad operativa durante fallos en la red FTTH principal, estableciendo la comunicación con la infraestructura del proveedor a través del núcleo 4G.



Figura 28: Router con módem LTE

2.8 LAN DE LA SEDE DEL CLIENTE

Descripción: Infraestructura de red interna implementada en cada sede del cliente para garantizar la conectividad local.

Rol: Facilita la comunicación eficiente entre los dispositivos dentro de la sede y actúa como el enlace hacia la red global mediante las conexiones principales de FTTH o respaldo 4G.

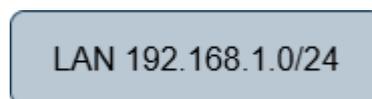


Figura 29: Red de Area Local del Cliente

3 PLIEGO DE CONDICIONES

En este punto se define los requisitos técnicos y funcionales necesarios para la implementación de la red propuesta, diseñada para mejorar la conectividad y la seguridad de la infraestructura de la empresa de logística.

En este apartado se detallan las especificaciones técnicas mínimas de los equipos genéricos que componen la red, garantizando su compatibilidad, rendimiento. Se incluyen los recursos necesarios para soportar protocolos avanzados de enrutamiento, redundancia y segmentación del tráfico.

Se pretende orientar la selección, instalación y configuración de los equipos, asegurando que cumplan con los objetivos del proyecto y las necesidades operativas de la empresa.

3.1 REQUISITO TÉCNICOS GENERALES

El diseño de cualquier infraestructura de red compleja tiene en cuenta el hecho de que el hardware elegido debe cumplir con los requisitos mínimos de capacidad de los protocolos (por ejemplo, BGP).

Los equipos que implementan la segmentación con el uso de VLAN permiten al usuario darle estructura y mayor eficiencia a la red interna. La segmentación de VLAN permite aislar diferentes áreas funcionales dentro de una organización, como administración, y seguridad. Esto aumenta el nivel de seguridad y, al mismo tiempo, mejora las posibilidades de control sobre el tráfico interno.

Finalmente, el equipo de red central, especialmente el de un proveedor de servicios de Internet, debe cumplir con estándares internacionales de rendimiento y disponibilidad muy altos, como deberían definir organizaciones como el IETF [17] y el Metro Ethernet Fórum [18]. Entre ellos se encuentran la compatibilidad con altas velocidades de transmisión (10G, 40G o superior), tolerancia a fallos, redundancia y un tiempo de retardo. Además, es indispensable que se agregue una gran cantidad de funciones de monitoreo, diagnóstico y seguridad a los dispositivos finales para que puedan operar todo el

tiempo de manera continua y confiable en redes críticas. Estas reglas garantizarán que los dispositivos centrales sean adecuados para soportar la carga en la operación y sean escalables en función de las necesidades futuras del cliente.

3.2 EQUIPO CORE PARA RED DE ACCESO FTTH

En este apartado, se describen las especificaciones técnicas mínimas que debe cumplir un equipo genérico destinado a actuar como núcleo de una red de acceso FTTH. A modo de referencia, se considera el equipo Juniper MX480, reconocido en el sector por sus capacidades avanzadas de enrutamiento y alto rendimiento, como ejemplo de un dispositivo que satisface los requisitos planteados en este proyecto.



Figura 30: Plataforma de enrutamiento universal MX480 [19]

El equipo MX480, perteneciente a la plataforma de enrutamiento universal 5G, es un enrutador de borde diseñado específicamente para optimizar el tráfico Ethernet, ofreciendo capacidades avanzadas de conmutación y soporte para servicios Ethernet de Carrier-class. Este dispositivo permite implementar una amplia variedad de aplicaciones y servicios, tanto empresariales como residenciales, entre los que se incluyen transporte de datos de alta velocidad, servicios VPN, soluciones multiplay de banda ancha de última generación, acceso a Internet de alta velocidad y conectividad eficiente para entornos de centros de datos.

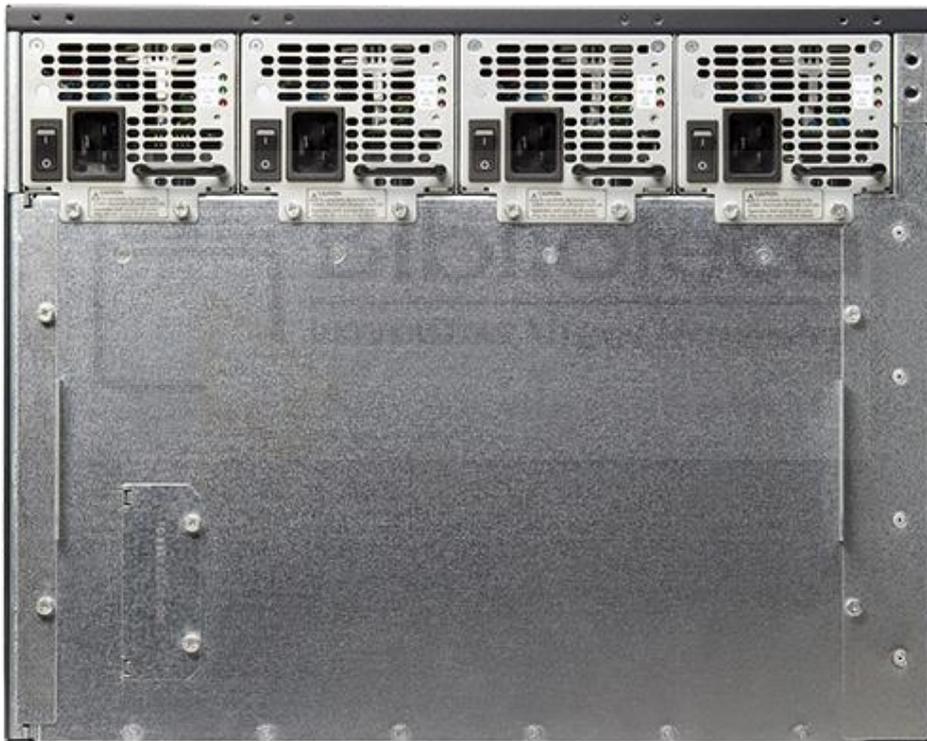


Figura 31: Plataforma de enrutamiento universal MX480 [19]

3.2.1 DESCRIPCIÓN GENERAL

- **System Capacity:** El MX480 proporciona una capacidad de sistema de 9 Tbps, lo que lo hace apto para una amplia gama de aplicaciones en entornos de nube, campus, empresas, centros de datos, proveedores de servicios, redes de cable y servicios móviles.
- **Always-on Infrastructure Base:** Los enrutadores de la serie MX aseguran la disponibilidad tanto de la red como del servicio mediante un conjunto completo de características de resistencia a nivel físico, lógico y de protocolo en múltiples capas. La tecnología de Virtual Chassis de Junos OS en los enrutadores de la serie MX permite redundancia a nivel de chasis, facilitando la gestión de dos enrutadores como una única entidad. Además, la implementación de Multichassis Link Aggregation Group (MC-LAG) proporciona redundancia en el chasis, las tarjetas y los puertos manteniendo el estado activo.
- **Application-Aware Networking:** Los enrutadores de la serie MX permiten la inspección profunda de paquetes para identificar aplicaciones y, a través de políticas definidas por el usuario, determinar el tratamiento del tráfico para cada una de ellas. Esto permite ofrecer servicios altamente personalizados y diferenciados a gran escala.
- **Programmable Chipset:** El chipset de los enrutadores de la serie MX está diseñado con una estructura de datos de reenvío programable que permite realizar cambios rápidos en el microcódigo directamente en el hardware. Además, cuenta con un motor de búsqueda programable que posibilita el procesamiento de servicios en línea. El motor de QoS programable del chip admite colas detalladas y complejas, satisfaciendo los requisitos de los casos de uso en el núcleo, el borde y la agregación.
- **Junos Continuity and Unified In-Service Software Upgrade (Unified ISSU):** Gracias al paquete de continuidad de Junos, es posible realizar actualizaciones de forma fluida cuando se instala nuevo hardware en un enrutador de la serie MX. La Unified ISSU permite actualizaciones y modificaciones de software sin causar interrupciones en el tráfico de la

red.

- **Junos Telemetry Interface:** La interfaz de telemetría de Junos ofrece datos detallados a nivel de componentes para monitorear, analizar y optimizar el rendimiento de la red. Los análisis obtenidos a partir de esta telemetría en tiempo real permiten identificar la congestión actual y tendencias, la utilización de recursos, los volúmenes de tráfico y la ocupación de los búferes.
- **Integrated Hardware-Based Timing:** Los enrutadores de la serie MX no requieren un reloj externo, ya que admiten sincronización basada en hardware altamente escalable y confiable. Esto incluye Synchronous Ethernet para frecuencia y el Precision Time Protocol (PTP) para sincronización de frecuencia y fase. Synchronous Ethernet y PTP pueden combinarse en un modo híbrido, alcanzando una alta precisión de frecuencia (10 ppb) y sincronización de fase (<1.5 μ S).

3.2.2 HARDWARE, CARACTERÍSTICAS GENERALES

El chasis del MX480 está diseñado para ofrecer redundancia. El sistema de hardware incluye componentes completamente redundantes, como fuentes de alimentación, Routing Engines y Switch Control Boards (SCB).

El enrutador MX480 tiene una altura de ocho unidades de rack (U). Es posible apilar hasta cinco enrutadores en un solo rack, desde el suelo hasta el techo, optimizando la densidad de puertos por unidad de espacio en el suelo. El dispositivo cuenta con ocho ranuras, que pueden ser ocupadas por hasta seis Dense Port Concentrators (DPC) o Modular Port Concentrators (MPC), tres Flexible PIC Concentrators (FPC) y dos SCB. Cada FPC puede contener hasta dos CPC, mientras que cada MPC admite hasta dos Modular Interface Cards (MIC).

Cuando está completamente equipado, el enrutador MX480 ofrece una capacidad de switching fabric agregada de hasta 5.76 Tbps y transferencia de datos a velocidad de línea para hasta 240 puertos 10 Gigabit Ethernet, 24 puertos 100 Gigabit Ethernet, o 72 puertos 40 Gigabit Ethernet.

3.2.3 DESCRIPCIÓN DEL CHASIS

El chasis del enrutador está construido como una estructura rígida de hoja metálica que alberga todos los componentes internos del dispositivo. Sus dimensiones son 35,6 cm de altura, 44,3 cm de ancho y 62,2 cm de profundidad, medidas desde la parte frontal hasta la trasera del chasis. Este chasis puede instalarse en armarios cerrados estándar de 800 mm (o más), racks de equipos de 19 pulgadas o racks de marco abierto para telecomunicaciones. En un rack estándar de 48 U, es posible montar hasta cinco enrutadores, siempre que el bastidor soporte su peso combinado, que puede superar los 371,0 kg (818 lb).

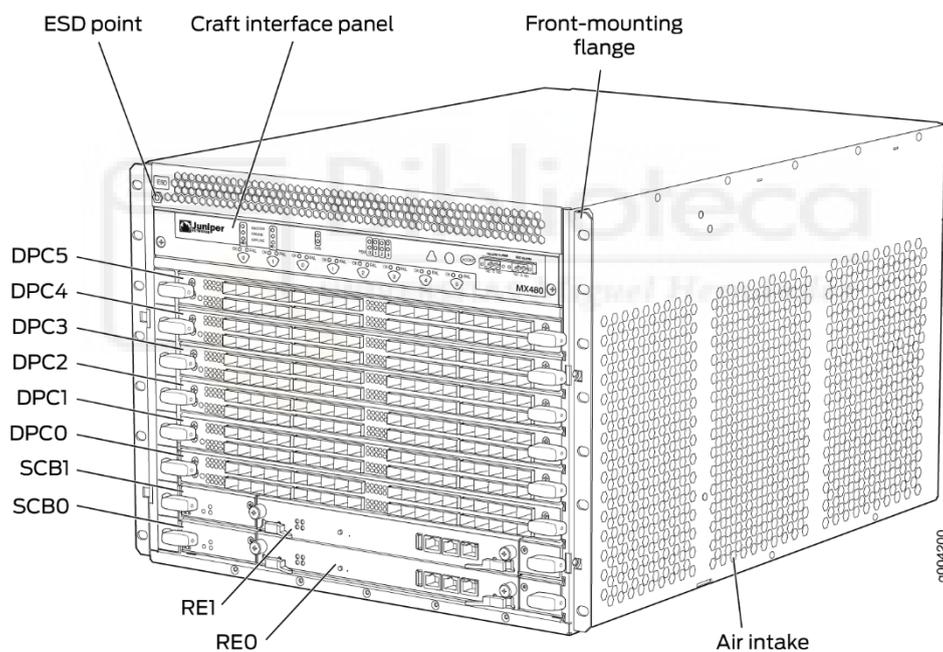


Figura 32: Vista frontal del chasis completamente configurado [20]

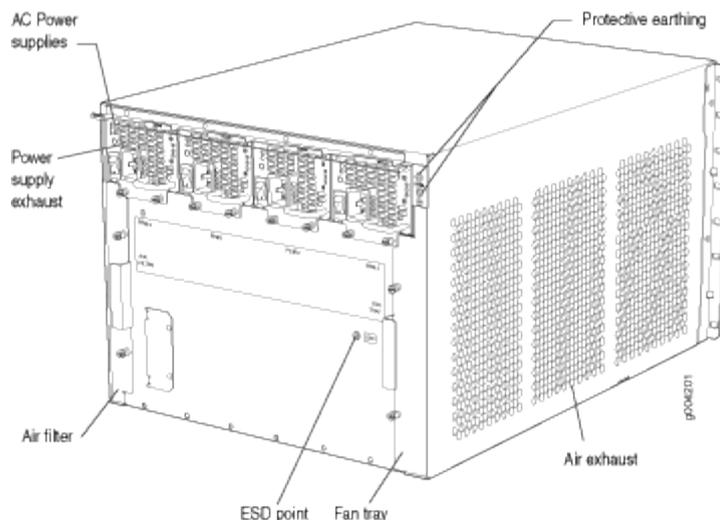


Figura 33: Vista trasera del MX480 con alimentación CA completamente configurado [20]

3.2.4 REDUNDANCIA DE COMPONENTES

Un enrutador completamente configurado está diseñado para garantizar que no exista un único punto de falla que pueda causar la interrupción total del sistema. Solo una configuración completa del enrutador asegura redundancia total, mientras que configuraciones parciales ofrecen redundancia limitada. Los siguientes componentes de hardware críticos cuentan con redundancia:

- **Subsistema de host:** Este subsistema incluye un Routing Engine que trabaja junto con una SCB. El enrutador puede estar equipado con uno o dos subsistemas de host. Si hay dos instalados, uno opera como principal y el otro como respaldo. En caso de que falle el subsistema principal (o cualquiera de sus componentes), el respaldo asume automáticamente el rol principal. Para su funcionamiento, cada subsistema de host requiere un Routing Engine directamente conectado a una SCB.

Si los Routing Engines están configurados para un cambio sin interrupciones, el respaldo sincroniza automáticamente su configuración y estado con el principal. Cualquier actualización en el estado del Routing Engine principal se replica en el respaldo. Si el respaldo toma el rol principal, el reenvío de paquetes continúa sin interrupción.

- **Fuentes de alimentación:** En la configuración de alimentación de CA de línea baja (110 V), el enrutador tiene tres o cuatro fuentes de alimentación de CA ubicadas horizontalmente en la parte trasera del chasis en las ranuras PEM0 a PEM3 (de izquierda a derecha). Cada fuente de alimentación suministra energía a todos los componentes del enrutador. En una configuración con tres fuentes, estas comparten la carga eléctrica equitativamente. Con cuatro fuentes, se alcanza redundancia total. Si una fuente falla o se retira, las restantes asumen automáticamente la carga sin interrupción. Tres fuentes aseguran operación completa durante el tiempo que el enrutador esté en uso.

En la configuración de CA de alta línea (220 V), el enrutador contiene dos o cuatro fuentes de alimentación de CA en las mismas ranuras. Con dos o más fuentes, la carga eléctrica se distribuye equitativamente. Cuatro fuentes aseguran redundancia total, y en caso de falla o retiro de una fuente, las demás asumen la carga sin interrupción. Dos fuentes garantizan el máximo rendimiento operativo.

En la configuración de CC, se requieren dos fuentes de alimentación para un enrutador completamente configurado. Cada fuente cubre aproximadamente la mitad de los componentes. Agregar dos fuentes adicionales ofrece redundancia total. Si una falla o se retira, las otras asumen la carga sin interrupción, asegurando operación completa.

- **Sistema de refrigeración:** El sistema de enfriamiento incluye componentes redundantes controlados por el subsistema de host. Si falla uno de los ventiladores, el subsistema de host incrementa la velocidad de los ventiladores restantes para mantener una refrigeración adecuada de forma indefinida.

3.2.5 INDICADORES LED DE ALARMA Y BOTÓN DE PRUEBA EN LA INTERFAZ MX480 CRAFT

En la esquina superior derecha de la interfaz del dispositivo se encuentran dos indicadores LED de alarma de gran tamaño. Las luces LED circulares de color rojo señalan una condición crítica que podría provocar una desconexión del sistema, mientras que las luces LED triangulares de color amarillo indican una situación menos grave que requiere supervisión o mantenimiento. Es posible que ambos indicadores LED estén encendidos simultáneamente.

Cuando se activa una condición que enciende un LED, también se activa el contacto del relé de alarma correspondiente en la interfaz del dispositivo.

Para desactivar las alarmas rojas y amarillas, se debe presionar el botón etiquetado como ACO/LT (acrónimo de "Alarm Cutoff/Lamp Test"), ubicado a la derecha de los indicadores LED de alarma. Al presionar este botón, se apagan ambos indicadores LED y se desactiva cualquier dispositivo conectado al contacto correspondiente del relé de alarma en la interfaz.

En la tabla 8 se proporciona una descripción detallada de los indicadores LED de alarma y el botón ACO/LT.

Color	Estado	Descripción
Rojo	En constante	LED de alarma crítica: señala una condición severa que podría provocar la interrupción del funcionamiento del enrutador. Entre las posibles causas se encuentran la extracción, fallo o sobrecalentamiento de algún componente.
Amarillo	En constante	LED de alarma de advertencia: indica una condición de error importante, aunque no crítica, como una notificación de mantenimiento o un incremento considerable en la temperatura de un componente.
-	-	Botón de prueba de bloqueo/apagado de alarma: permite desactivar las alarmas rojas y amarillas. Al mantenerlo presionado, enciende todos los indicadores LED de la interfaz del dispositivo para realizar pruebas.

Tabla 8: Indicadores LED de alarma y botón de prueba alarma/ luz

3.2.6 SOPORTES Y ADMINISTRACIÓN DE CABLES

Los soportes de gestión de cables están formados por divisores de plástico situados a los lados izquierdo y derecho de cada ranura CPC, FPC o MPC, así como en la ranura SCB. Estos soportes permiten organizar y dirigir los cables hacia el exterior del enrutador, manteniéndolos alejados de las DPC, MPC, MIC, PIC y la SCB.

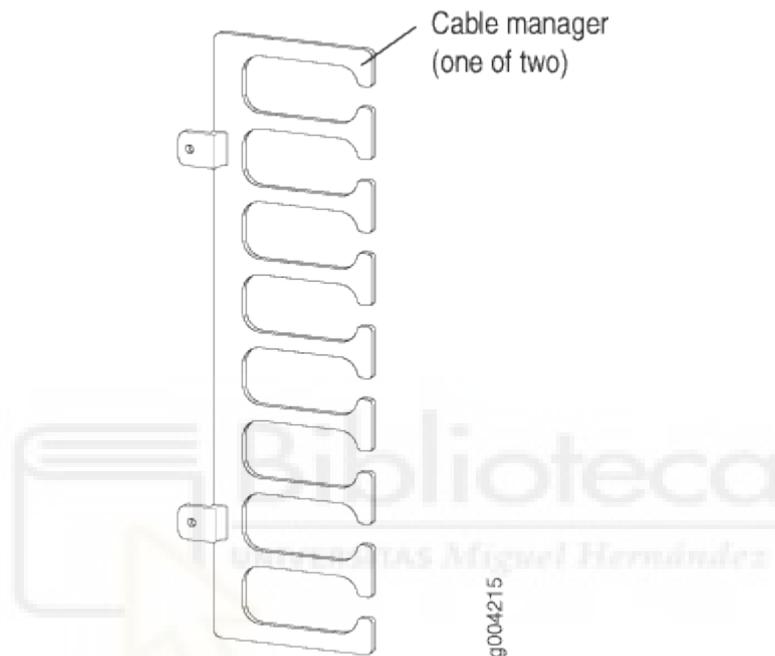


Figura 34 Soportes de administradores de cables [20]

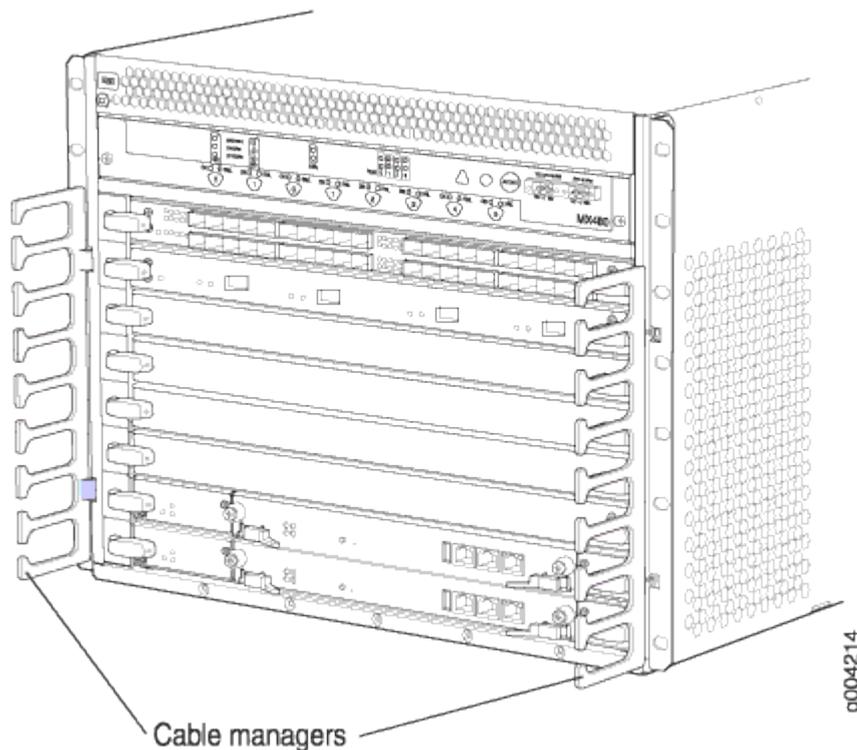


Figura 35: Soportes de administración de cables instalados en el equipo [20]

3.2.7 DESCRIPCIÓN DEL MOTOR DE ENRUTAMIENTO MX480

El motor de enrutamiento es una plataforma basada en Intel que ejecuta Junos OS. Los procesos de software que operan en el motor de enrutamiento gestionan las tablas de enrutamiento, administran los protocolos de enrutamiento utilizados por el dispositivo, controlan las interfaces del enrutador, supervisan algunos componentes del chasis y ofrecen tanto la interfaz para la administración del sistema como el acceso de los usuarios al dispositivo.

El enrutador puede equiparse con uno o dos motores de enrutamiento, los cuales se instalan en la parte frontal del chasis, en ranuras horizontales de las SCB etiquetadas como 0 y 1. En configuraciones con dos motores, uno opera como principal mientras el otro funciona como respaldo. Si el motor de enrutamiento principal falla o es retirado, y el respaldo está configurado correctamente, este último asume el rol principal.

Los motores de enrutamiento admiten conexión en caliente y deben instalarse directamente en una SCB. Además, cuentan con un puerto USB que permite

conectar una memoria USB para cargar Junos OS. La Figura 36 presenta el motor de enrutamiento RE-S-1800, mientras que la Figura 37 muestra el modelo RE-S-X6-64G.

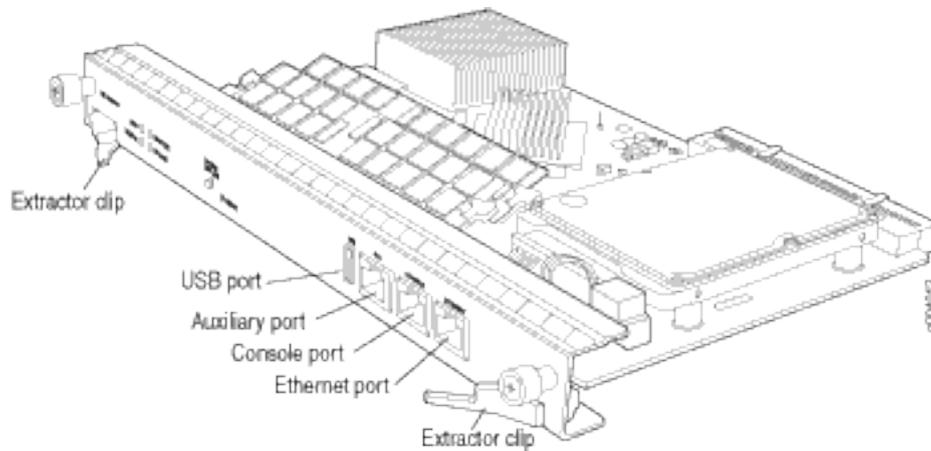


Figura 36: Motor de enrutamiento RE-S-1800 [20]

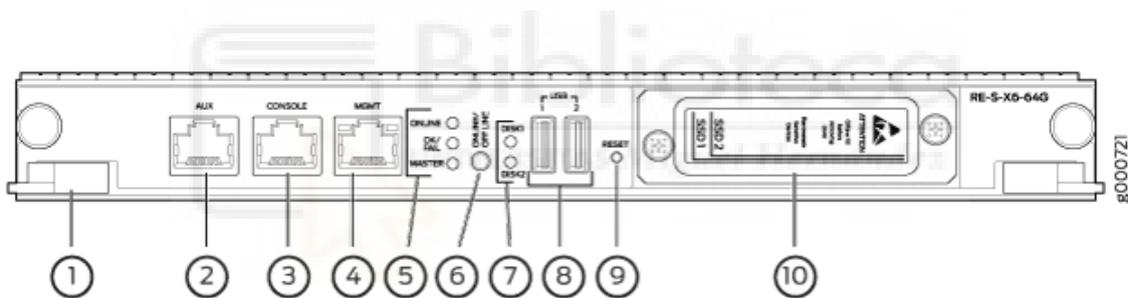


Figura 37: Vista frontal del motor de enrutamiento RE-S-X6-64G

1 - Clips extractores	6 - EN LÍNEA/FUERA DE LÍNEA Botón
número arábigo - Puerto auxiliar (AUX)	7- LED de SSD: DISCO1 y DISCO2
3 - Puerto de consola (Con)	8 - Puertos: USB1 y USB2
4 - Puerto de administración (MGMT)	9 - RESTABLECIMIENTO Botón
5 - LED: En línea, aceptar/fallar y master	10 - Cubierta de ranura para tarjeta SSD

Tabla 9: Motor de enrutamiento RE-S-X6-64G

3.2.8 PUERTOS DE INTERFAZ DEL MOTOR DE ENRUTAMIENTO

En el lado derecho del motor de enrutamiento se encuentran tres puertos que permiten conectarlo a uno o más dispositivos externos. A través de estos puertos, los administradores del sistema pueden ejecutar comandos de la Command Line Interface (CLI) de Junos OS para gestionar el enrutador.

Los puertos etiquetados cumplen las siguientes funciones:

- **AUX:** Permite conectar el motor de enrutamiento a un portátil, módem u otro dispositivo auxiliar mediante un cable serie con conector RJ-45.
- **CONSOLE:** Conecta el motor de enrutamiento a una consola del sistema utilizando un cable serie con conector RJ-45.
- **Ethernet o MGMT:** Facilita la conexión del motor de enrutamiento a una red LAN de administración o a cualquier dispositivo con conectividad Ethernet, proporcionando administración fuera de banda. Este puerto utiliza un conector RJ-45 con detección automática que admite velocidades de 10 Mbps, 100 Mbps y 1000 Mbps. A la derecha del puerto, dos pequeños LED indican el estado de la conexión: El LED izquierdo muestra la velocidad: verde para 1000 Mbps, amarillo para 100 Mbps y apagado para 10 Mbps. El LED derecho indica actividad: parpadea en verde cuando se transmiten paquetes a través del puerto [21].

3.3 EQUIPO BACKBONE PARA TRÁFICO ISP

El equipo backbone para tráfico ISP desempeña un papel crucial en la infraestructura de las redes de operadores, al manejar grandes volúmenes de datos y garantizar la conectividad de alta velocidad entre los diferentes puntos de la red. Estos equipos están diseñados para soportar las demandas de tráfico crecientes asociadas con los servicios modernos de telecomunicaciones, como transmisión de datos, voz y video, proporcionando una capacidad robusta, escalabilidad y alta disponibilidad.

El MX960 de Juniper Networks se toma como referencia debido a su destacada

capacidad como plataforma de enrutamiento universal, específicamente diseñada para redes backbone de ISP. Este equipo ofrece una capacidad de switching fabric de hasta 12 Tbps, lo que lo convierte en una opción ideal para manejar el tráfico de grandes operadores.

3.3.1 DESCRIPCIÓN GENERAL

El MX960 5G Universal Routing Platform es un edge router diseñado específicamente para optimizar redes Ethernet, proporcionando capacidades avanzadas de switching y enrutamiento Ethernet de clase carrier-class. Este enrutador es ideal para una amplia variedad de aplicaciones y servicios, tanto empresariales como residenciales, que incluyen transporte de datos a alta velocidad, servicios VPN, soluciones multiplay de banda ancha de última generación, Internet de alta velocidad y conectividad para centros de datos.

3.3.2 HARDWARE, CARACTERÍSTICAS GENERALES

El chasis del MX960 está diseñado para ofrecer alta redundancia y resiliencia, integrando un sistema de hardware completamente redundante que incluye fuentes de alimentación, bandejas de ventiladores, Routing Engines y Switch Control Boards (SCB).

Con una altura de 16 unidades de rack (U), el MX960 permite apilar hasta tres enrutadores en un único rack estándar, optimizando la densidad de puertos por unidad de espacio físico. Este equipo cuenta con 14 ranuras que pueden configurarse con 11 o 12 Dense Port Concentrators (DPC) o Modular Port Concentrators (MPC), hasta seis Flexible PIC Concentrators (FPC) y dos SCB, según las configuraciones de switching fabric requeridas.

Cuando está completamente equipado, el MX960 alcanza una capacidad de switching fabric de hasta 10.56 Tbps y ofrece transferencia de datos a velocidad de línea en configuraciones que incluyen hasta 264 puertos 10 Gigabit Ethernet, 22 puertos 100 Gigabit Ethernet, 44 puertos 10 Gigabit Ethernet adicionales y 66 puertos 40 Gigabit Ethernet.

Descripción	Capacidad
Capacidad del sistema	Medio dúplex de 10,56 Tbps
Capacidad de estructura de conmutación por ranura	480 Gbps
MPC y DPC por chasis	11 o 12 (según el esquema de protección)
Chasis por bastidor	3

Tabla 10: Capacidad MX960 enrutador de red [22]

Existen varios tipos de Dense Port Concentrators (DPC) disponibles, y cada uno de ellos incluye dos o cuatro Packet Forwarding Engines (PFE). Cada PFE proporciona una capacidad de transferencia de datos de 10 Gbps.

En cada Flexible PIC Concentrator (FPC) se pueden instalar hasta dos DPC, permitiendo que un MX960 completamente equipado soporte hasta 12 DPC.

En el caso de las Modular Port Concentrators (MPC), estas permiten la instalación de hasta dos Modular Interface Cards (MIC) en cada unidad. Cuando está completamente configurado, el MX960 admite hasta 24 MIC.

Los MPC soportan interfaces fijas o hasta dos MIC por unidad, y el MX960, en su máxima capacidad, puede alojar hasta 22 MIC.

Descripción	Ancho de banda de la estructura por ranura	MX960 ancho de banda de la estructura
Mejora de la configuración tarjeta de control MX (modelo SCBE3-MX)	Hasta 1,5 Tbps (configuración de estructura no redundante con tarjetas de línea MPC10E); 1 Tbps (configuración de estructura redundante con tarjetas de línea MPC10E)	Hasta 33 Tbps
Mejora del conmutador MX tarjeta de control (SCBE2-MX)	Hasta 480 Gbps (configuración de estructura no redundante); 340 Gbps (configuración de estructura redundante)	Hasta 10,56 Tbps
Mejora del conmutador MX tarjeta de control (SCBE-MX)	Hasta 240 Gbps (configuración de estructura no redundante); 160 Gbps (configuración de estructura redundante)	Hasta 5,25 Tbps
Conmutador tarjeta de control (SCB-MX)	Hasta 240 Gbps (configuración de estructura no redundante); 120 Gbps (configuración de estructura redundante)	Hasta 2,6 Tbps

Tabla 11: Capacidad de tarjeta de control para puertos [22]

Las conexiones entre las tarjetas de interfaz y las SCB se dividen en tres categorías:

- **Estructura del conmutador:** Estas conexiones enlazan las tarjetas de interfaz, permitiendo el transporte de paquetes entre DPC, FPC y MPC. Para una estructura no redundante, se utilizan dos SCB, mientras que una configuración redundante requiere tres SCB.
- **Plano de control:** Incluye enlaces Gigabit Ethernet entre las SCB, los Routing Engines y cada DPC, FPC o MPC. Toda la información que circula entre las tarjetas y las placas se transmite mediante Ethernet, salvo los comandos y estados de bajo nivel.
- **Señales de administración:** Estas conexiones proporcionan soporte

para diagnósticos de estado a nivel básico.

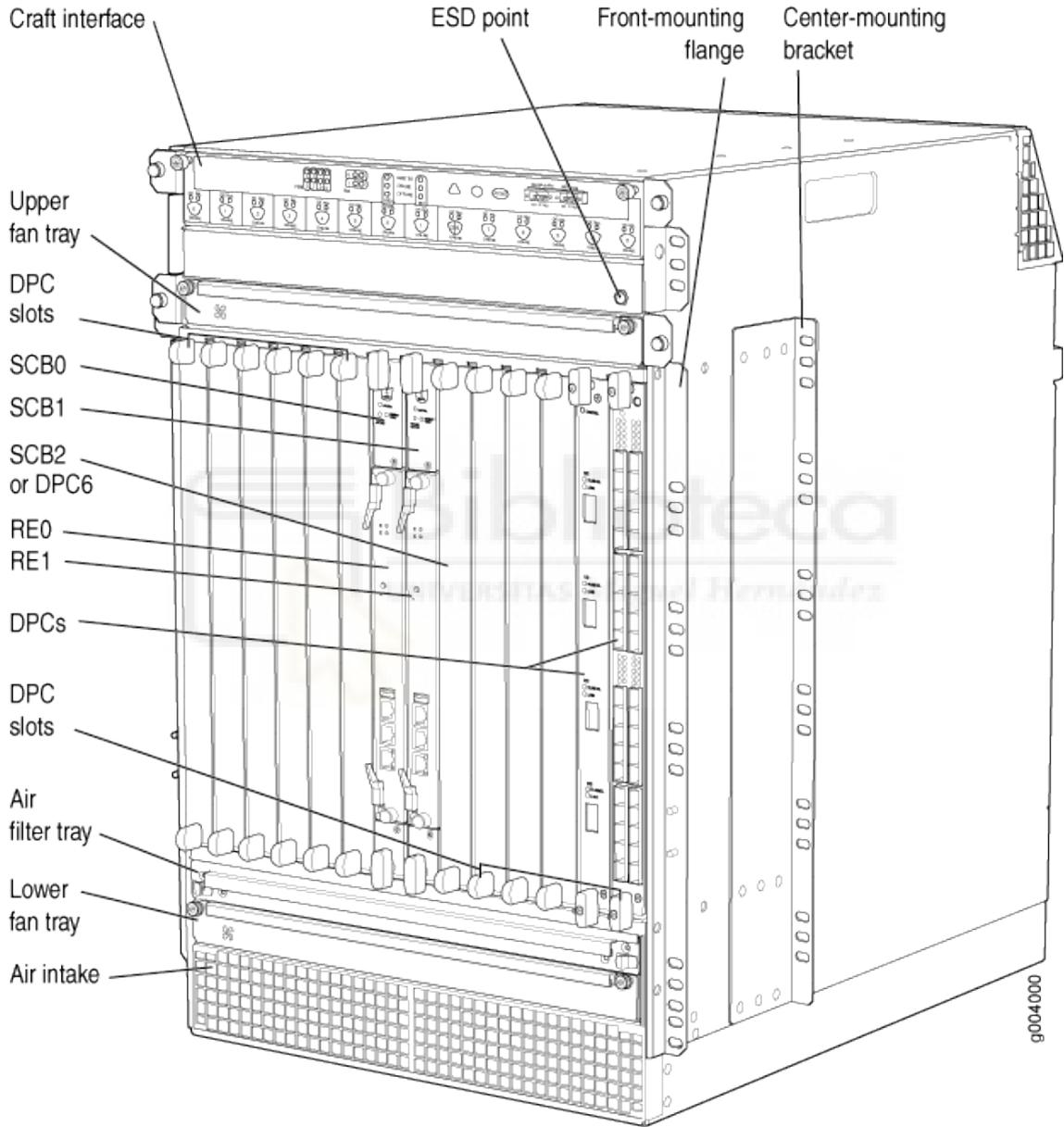
3.3.3 DESCRIPCIÓN DEL CHASIS

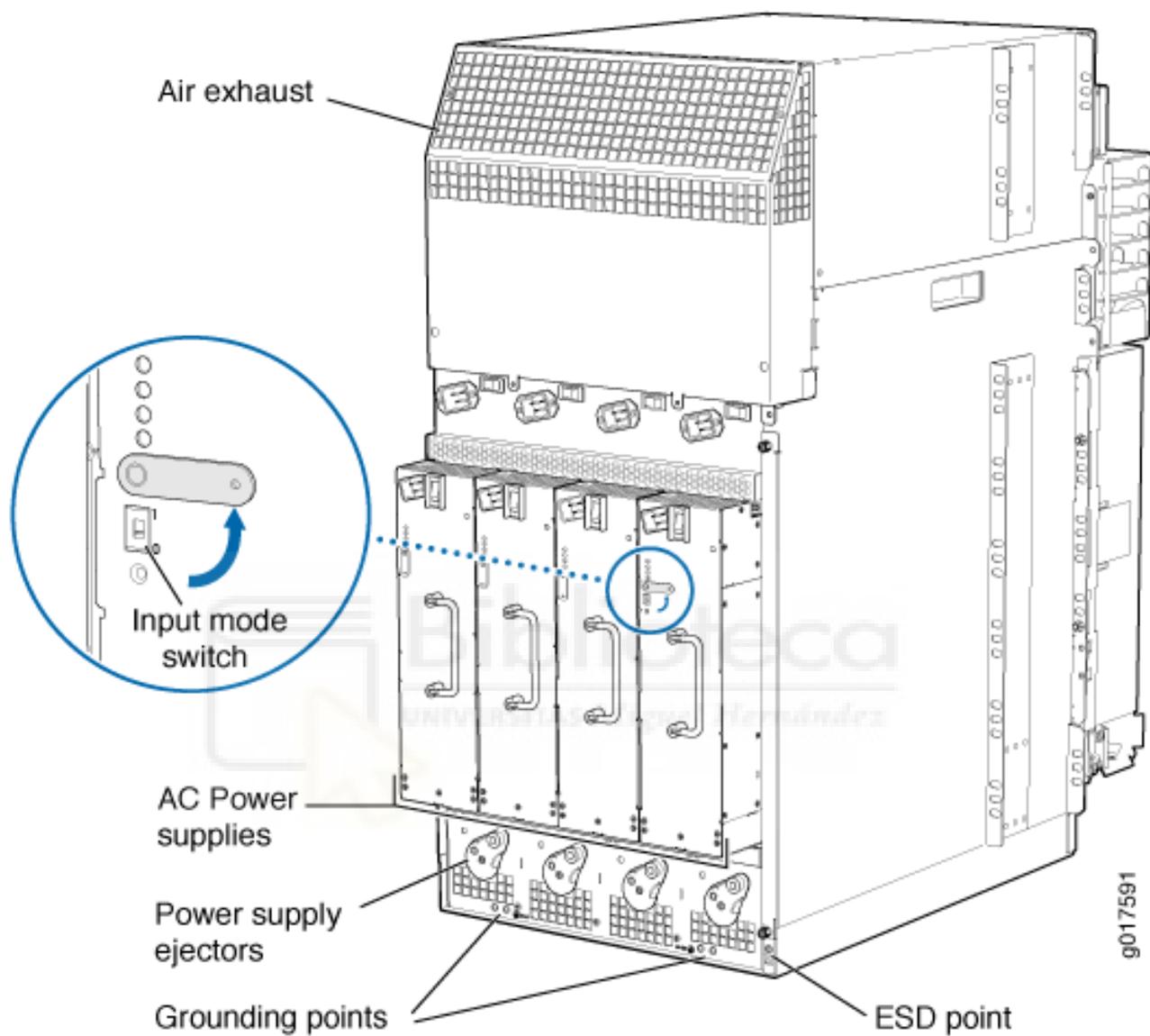
El chasis del enrutador está construido como una estructura metálica rígida diseñada para alojar todos los componentes internos del dispositivo. Este chasis es compatible con diversos tipos de racks, incluidos armarios cerrados con una profundidad de al menos 800 mm, racks estándar para equipos de 48.26 cm y racks de marco abierto utilizados en telecomunicaciones.

Para el enrutador MX960, existen dos variantes de chasis disponibles:

- Chasis estándar: Tiene unas dimensiones de 70,49 cm de altura, 44,11 cm de ancho (sin considerar bridas y soportes de montaje) y 58,42 cm de profundidad desde las bridas de montaje frontal hasta la parte trasera. Al incluir el gestor de cables estándar, la profundidad total alcanza los 71,1 cm. Es posible instalar hasta tres enrutadores en un rack de 48 U, siempre que el rack soporte el peso combinado, que puede superar los 476,3 kg.
- El chasis con el gestor de cables extendido instalado tiene unas dimensiones de 92,7 cm de altura, 44,11 cm de ancho y aproximadamente 73,7 cm de profundidad, considerando la distancia desde las bridas de montaje frontal hasta la parte trasera del gestor de cables extendido. Si el rack es capaz de soportar el peso combinado, es posible instalar hasta dos enrutadores con el gestor de cables extendido en un rack de 48 U, con un peso total que puede superar los 339,28 kg.

El hardware de montaje incluye bridas de montaje frontal situadas en la parte delantera del chasis, además de dos soportes de montaje central fijados en el centro del chasis.





3.3.4 REDUNCIA DE COMPONENTES

Un enrutador completamente configurado está diseñado para garantizar que ningún punto único de falla pueda comprometer el funcionamiento de todo el sistema. Solo una configuración completa asegura redundancia total, mientras que las configuraciones parciales ofrecen una redundancia limitada. Los siguientes componentes clave del hardware cuentan con redundancia:

- **Subsistema de host:** Este subsistema incluye un Routing Engine y una Switch Control Board (SCB). El enrutador puede contar con uno o dos subsistemas de host. Cuando hay dos instalados, uno opera como principal y el otro como respaldo. En caso de fallo en el subsistema principal (o alguno de sus componentes), el respaldo asume automáticamente el control. Para operar, cada subsistema de host necesita un Routing Engine directamente conectado a una SCB.
- **Fuentes de alimentación:** En configuraciones de CA con fuentes de capacidad estándar, se requieren al menos tres fuentes de alimentación para un enrutador completamente configurado. Estas comparten la carga de manera uniforme, y la adición de una cuarta fuente proporciona redundancia total. Si una fuente falla en esta configuración redundante, las otras tres son suficientes para mantener el funcionamiento completo. En configuraciones de CC, CA de alta capacidad, fuentes de segunda generación de alta capacidad y fuentes universales de alto voltaje (HVAC o HVDC), se necesitan dos fuentes de alimentación para soportar un enrutador completamente configurado. Cada una alimenta aproximadamente la mitad de los componentes del dispositivo. La adición de dos fuentes adicionales asegura redundancia total. Si una fuente falla, las restantes asumen toda la carga para mantener el enrutador en funcionamiento.
- **Sistema de refrigeración:** Los componentes de refrigeración cuentan con redundancia y son gestionados por el subsistema de host. Si uno de los ventiladores falla, el subsistema de host incrementa la velocidad de los ventiladores restantes para mantener una refrigeración adecuada y

continúa del enrutador.

3.3.5 DESCRIPCIÓN DE LA INTERFAZ CRAFT MX960

La craft interface permite ver la información de estado y solución de problemas de un vistazo, y realizar muchas funciones de control del sistema. Es insertable y extraíble en caliente. La craft interface se encuentra en la parte frontal del enrutador por encima de la caja de tarjetas y contiene indicadores LED para los componentes del enrutador, los contactos de relé de alarma y el botón de corte de alarma.

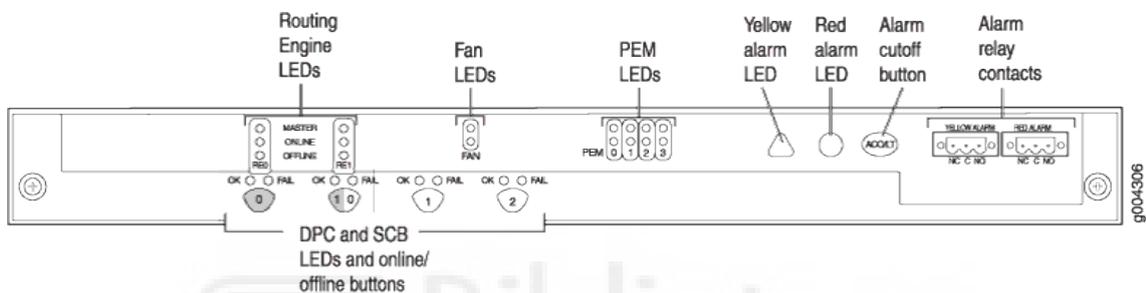


Figura 38: Panel frontal [22]

3.3.6 DESCRIPCIÓN DEL ADMINISTRADOR DE CABLES

El administrador de cables estándar es una bandeja situada debajo de la caja de tarjetas de línea, diseñada con una fila de divisores que permiten organizar los cables de manera individual para cada Dense Port Concentrator (DPC), Modular Port Concentrator (MPC), Modular Interface Card (MIC) o PIC.

Se pueden usar cintas de cable u otros tipos de ataduras para asegurar cuidadosamente los cables en el administrador de cables estándar. Para fijarlos, basta con pasar la atadura por el anclaje del cable y asegurarla firmemente. El administrador de cables estándar puede inclinarse hacia arriba y desplazarse hacia afuera para colocarlo en la posición de mantenimiento, facilitando el acceso tanto a la bandeja inferior de ventiladores como al filtro de aire.

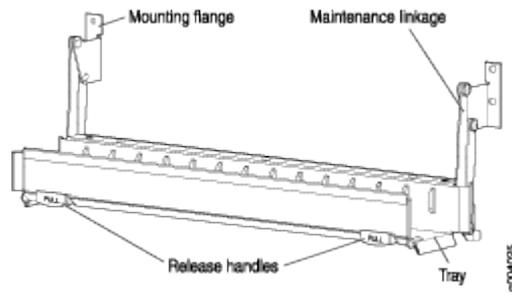
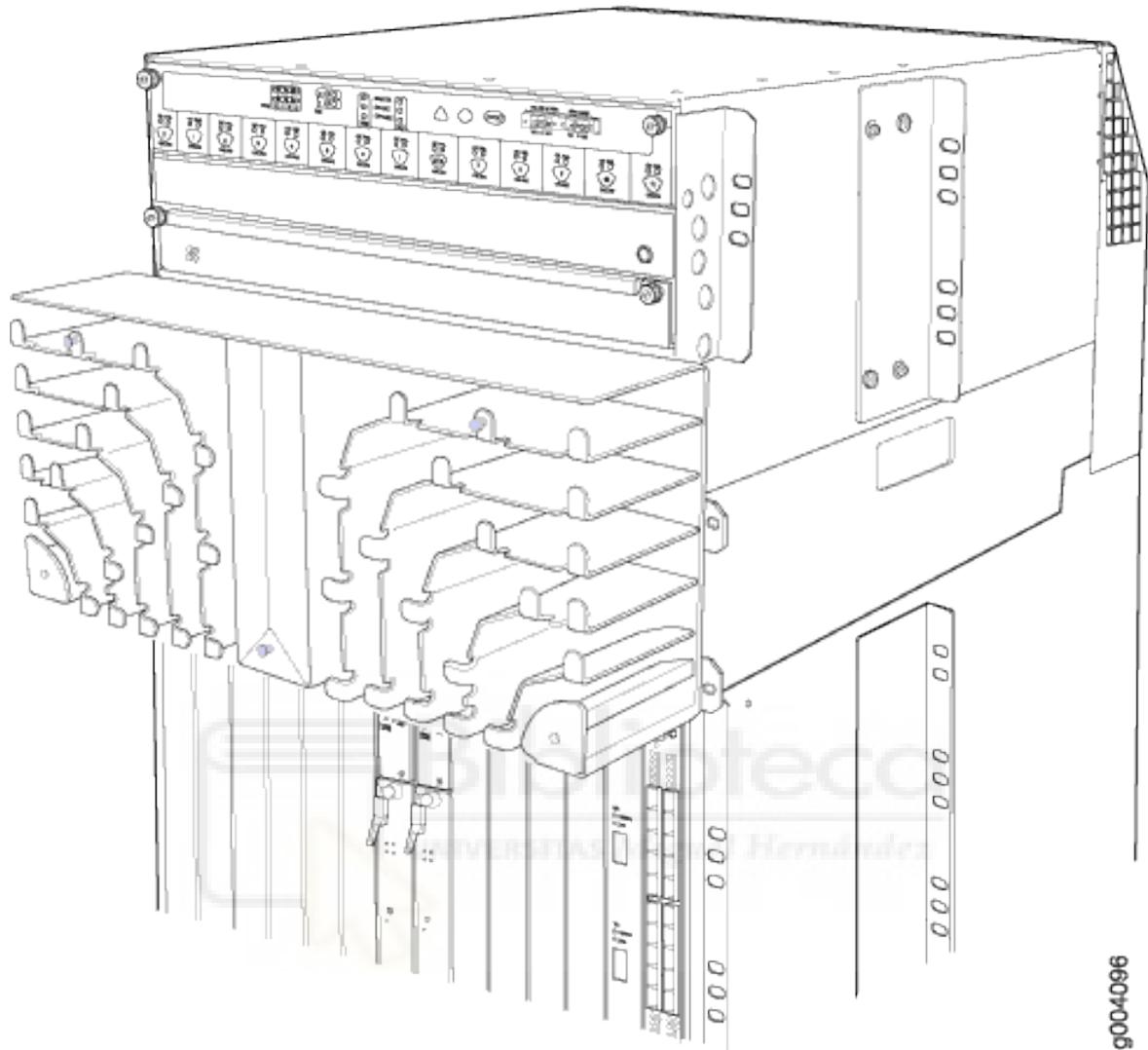


Figura 39: Administrador de cables estándar [22]

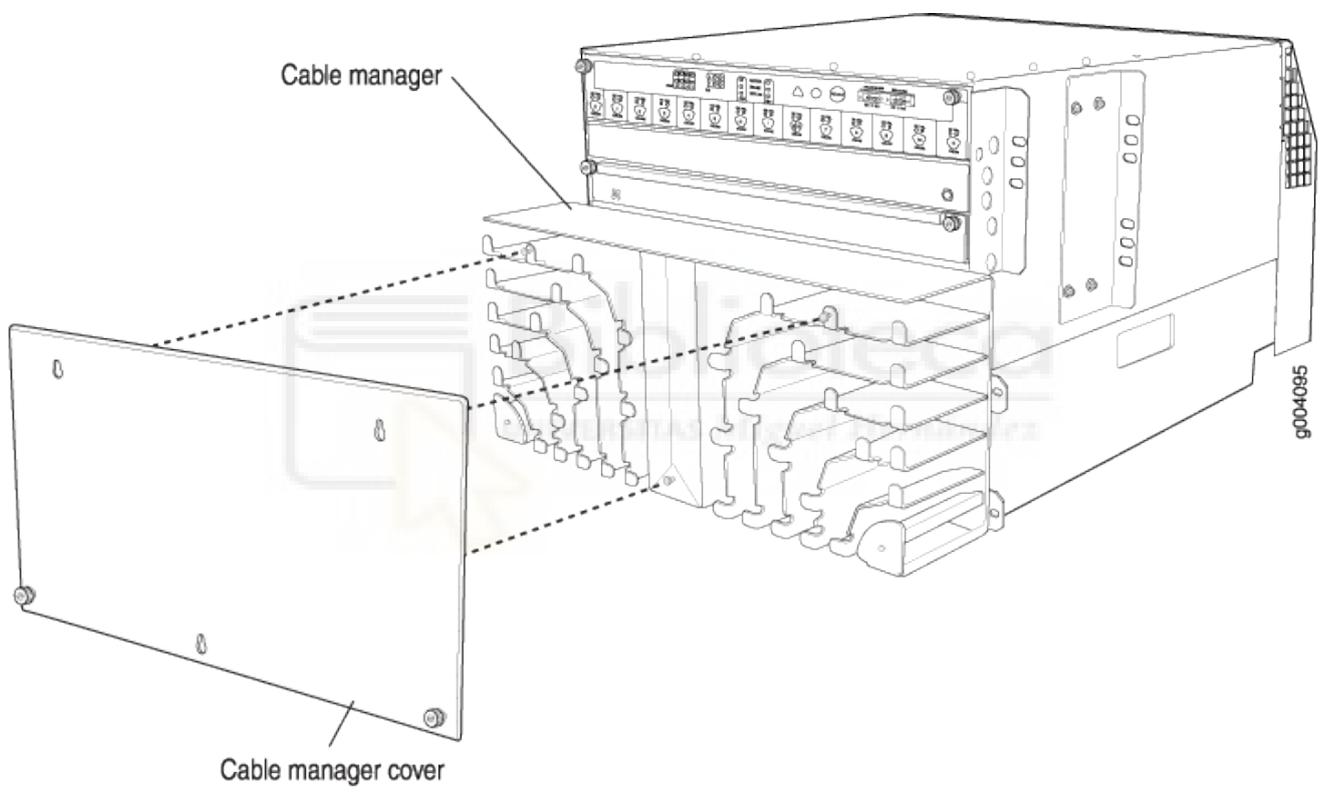
El administrador de cables extendido facilita el enrutamiento de los cables lejos de la parte frontal de las DPC, MPC y MIC, además de ofrecer acceso adicional al sistema.





9004096

Figura 40: Administrador de cables extendido [22]



3.3.7 PROCEDIMIENTO DE MANTENIMIENTO DE RUTINA PARA EL ENRUTADOR MX960

- Realice una inspección del sitio de instalación para detectar posibles problemas como humedad, cables flojos o enredados, y acumulación excesiva de polvo. Verifique que el flujo de aire esté libre de obstrucciones alrededor del enrutador y en las rejillas de ventilación de entrada.
- Revise los indicadores de estado en la interfaz de craft, incluyendo alarmas del sistema y luces LED.
- Examine el filtro de aire ubicado en la parte trasera izquierda del enrutador, y reemplácelo cada 6 meses para garantizar el óptimo funcionamiento del sistema de refrigeración. Evite operar el enrutador por más de unos minutos sin que el filtro de aire esté debidamente instalado.

3.3.8 INDICADORES LED DE ALARMA

En la esquina superior derecha de la interfaz del dispositivo se encuentran dos indicadores LED de alarma de gran tamaño. El LED circular de color rojo se enciende para señalar una condición crítica que podría provocar el apagado del sistema, mientras que el LED triangular de color amarillo indica una situación menos grave que requiere monitoreo o mantenimiento. Ambos indicadores pueden iluminarse al mismo tiempo si las condiciones lo requieren.

Cuando se activa un LED, también se acciona el contacto del relé de alarma correspondiente en la interfaz del dispositivo.

Para desactivar las alarmas rojas y amarillas, se debe presionar el botón etiquetado como ACO/LT (acrónimo de "Alarm Cutoff/Lamp Test"), situado a la derecha de los indicadores de alarma. Al desactivar una alarma, ambos LEDs se apagan y el dispositivo conectado al contacto del relé correspondiente queda desactivado [22].

Color	Estado	Descripción
Rojo	En forma constante	LED de alarma crítica: indica una condición crítica que puede hacer que el enrutador deje de funcionar.
Amarillo	En forma constante	LED de alarma de advertencia: Señala un error importante, pero no crítico, como una alerta de mantenimiento o un incremento notable en la temperatura de los componentes.
-	-	Botón de prueba/corte de alarma: Desactiva las alarmas rojas y amarillas, y enciende todos los indicadores LED para pruebas cuando se mantiene presionado.

Tabla 12: Indicadores LED de alarma y botón de prueba de lámpara/corte de alarma.

3.4 DISPOSITIVO DE SEGURIDAD PERIMETRAL

Los dispositivos de seguridad perimetral son quizás los dispositivos más importantes implementados en cualquier infraestructura de red porque, como primera línea de defensa, protegen toda la red de cualquier amenaza potencial, independientemente de la localización de estas amenazas, externas o internas. Su diseño hace que el flujo de información dentro de la red sea íntegro, confidencial y siempre disponible. Además de proteger contra ataques, estos dispositivos facilitan una gestión eficaz del tráfico para que sólo los usuarios autorizados tengan acceso a los servicios de red.



Figura 41: Base de la seguridad de la información [23]

La función central de cualquier estrategia de seguridad incluye la triada: confidencialidad, integridad y disponibilidad. Proporciona una garantía de que la información, los artículos y los servicios confidenciales están protegidos contra el acceso no autorizado. La integridad proporciona garantía de que los datos están seguros y libres de manipulación no autorizada. Del mismo modo, se deberá garantizar que los sistemas o recursos estén disponibles para el usuario legítimo. Para lograr una protección integral, cada control de seguridad que exista en un dispositivo perimetral debe implementar adecuadamente los tres requisitos anteriores.

3.4.1 WATCHGUARD T85

Se ha seleccionado el Firebox T85 como dispositivo de seguridad debido a su destacada posición en el cuadrante mágico de Gartner, donde ha sido comparado favorablemente con otros firewalls de su categoría. Su rendimiento, escalabilidad y funcionalidad avanzada lo sitúan como una solución idónea para entornos empresariales, ofreciendo una relación calidad-precio superior y capacidades de protección alineadas con las necesidades actuales de seguridad en redes.



Figura 42: Firebox T85 [24]

3.4.2 DESCRIPCIÓN GENERAL

- El Firebox T85 proporciona una solución robusta para gestionar e implementar políticas en redes extendidas, permitiendo ofrecer una protección completa con servicios UTM diseñados específicamente para entornos de pequeñas y medianas empresas, mejorando significativamente su seguridad. Totalmente compatible con el Total Security Suite de WatchGuard, el T85 protege ubicaciones pequeñas mediante servicios de seguridad avanzada como cloud sandboxing, antimalware potenciado por IA, correlación de amenazas y filtrado de DNS.
- Incluye soporte para WatchGuard RapidDeploy, una herramienta basada en la nube que permite configurar y desplegar el dispositivo de forma remota. El dispositivo se conecta a la alimentación y a Internet en la ubicación, y luego obtiene automáticamente las configuraciones necesarias desde la nube.
- Está equipado con dos puertos PoE+ que proporcionan energía a dispositivos periféricos, lo que permite extender la red sin necesidad de alimentación de CA para equipos remotos. Además, incorpora una plataforma de expansión de puertos que incluye un puerto SFP+ para

conectividad de fibra óptica integrada, ofreciendo mayor flexibilidad en la configuración de red.

- El framework Unified Security Platform de WatchGuard está diseñado como una solución integral para el aprovisionamiento, implementación, administración y supervisión de un portafolio de servicios avanzados de ciberseguridad. Este ecosistema incluye soluciones de seguridad de red, autenticación multifactor, protección de endpoints y Wi-Fi, integrando dispositivos como los firewalls Firebox. Su arquitectura permite proteger usuarios, dispositivos y entornos frente a amenazas como intentos de explotación de vulnerabilidades, ransomware, intrusiones, suplantación de identidad y malware avanzado. Este enfoque unificado reemplaza modelos de seguridad fragmentados y extiende las capacidades de protección a todos los entornos operativos de una empresa.
- El Firebox T45 incluye soporte para SD-WAN integrado, lo que permite optimizar el uso de la red al reducir la dependencia de conexiones MPLS o celulares de alto costo. Además, facilita la inspección del tráfico en pequeñas oficinas, mejorando tanto la resiliencia como el rendimiento general de la red.

Las soluciones de WatchGuard están diseñadas para proteger contra amenazas como malware avanzado, ransomware, botnets, troyanos, virus, ataques mediante descargas maliciosas y suplantación de identidad. Ofrecen compatibilidad con los paquetes Total Security Suite y Basic Security Suite, disponibles en todas las soluciones Firebox, proporcionando diferentes niveles de seguridad según las necesidades específicas.

	SOPORTE	BASIC SECURITY	TOTAL SECURITY
Firewall con Control de Estado	✓	✓	✓
VPN	✓	✓	✓
SD-WAN	✓	✓	✓
Portal de Acceso*	✓	✓	✓
Servicio de Prevención de Intrusiones (IPS)		✓	✓
Control de Aplicaciones		✓	✓
WebBlocker (Filtrado de Contenido/URL)		✓	✓
spamBlocker (Filtro de Correo No Deseado)		✓	✓
Gateway AntiVirus		✓	✓
Reputation Enabled Defense		✓	✓
Network Discovery		✓	✓
APT Blocker			✓
DNSWatch			✓
IntelligentAV™			✓
ThreatSync (XDR)			✓
EDR Core			✓
WatchGuard Cloud Visibility Retención de datos	1 Día	1 Día	30 Días
Soporte	Estándar (24x7)	Estándar (24x7)	Gold (24x7)

Tabla 13: Comparativa Basic y Total Security

3.4.3 ESPECIFICACIONES TÉCNICAS

Categoría	Especificaciones
Rendimiento	
UTM (análisis completo)	943 Mbps
Firewall (IMIX)	2.40 Gbps
VPN (IMIX)	680 Mbps
Inspección de Contenido HTTPS (IPS habilitado)	576 Mbps
Antivirus	1.53 Gbps
IPS (análisis completo)	1.28 Gbps
Firewall (UDP 1518)	4.96 Gbps
VPN (UDP 1518)	2.04 Gbps
Capacidad	
Interfaces I/E (10/100/1000)	8
Interfaces I/E (SFP)	1 serie / 2 USB
Conexiones concurrentes	3,850,000
Conexiones concurrentes (proxy)	3,850,000
Nuevas conexiones por segundo	75,500
VLAN	75
Licencias del Administrador de Sistemas de WatchGuard (WSM incl.)	1
Licencias EDR Core	50
Túneles de VPN	
VPN de sucursal	60
VPN móvil	60
Funcionalidades de seguridad	
Firewall	Inspección de paquetes con control de estado, descifrado de TLS, firewall de proxy
Proxies de aplicación	HTTP, HTTPS, FTP, DNS, TCP/UDP, POP3S, SMTPS, IMAPS y proxy web general
Protección contra amenazas avanzadas	Ataques DoS, paquetes fragmentados, y anomalías en aplicaciones
Opciones de filtrado	Búsqueda segura en exploradores, Google para Negocios.

Tabla 14: Especificaciones Firebox T85 [24]

Categoría	Especificaciones
VPN	
VPN sitio a sitio	IKEv2, IPSec, túneles basados en políticas y rutas, concentrador y radio de TLS
VPN de acceso remoto	IKEv2, IPSec, L2TP, TLS
VISIBILIDAD	
Inicio de sesión y notificaciones	WatchGuard Cloud y Dimension, Syslog, SNMP v2/v3
Generación de reportes	WatchGuard Cloud incluye más de 100 reportes predefinidos, resúmenes ejecutivos y herramientas de visibilidad
CERTIFICACIONES	
Seguridad	Pendiente: CC, FIPS 140-2
Protección	NRTL/CB
Red	IPv6 Ready Gold (enrutamiento)
Control de sustancias peligrosas	WEEE, RoHS, REACH
REDES	
SD-WAN	Conmutación por error Multi-WAN, selección de ruta dinámica, medición de vibración, pérdida y latencia
Enrutamiento dinámico	RIP, OSPF, BGP
Redundancia	Activa/pasiva, activa/activa
QoS	802.1Q, DSCP, precedencia de IP
Administración de tráfico	Por política o aplicación
Asignación de dirección IP	Estática, DHCP servidor/cliente, relé, PPPoE y DynDNS
NAT	Estática, dinámica, 1:1, IPsec transversal, traducción de puertos
Agregación de enlaces	802.3ad dinámico, estático, activo/de respaldo

Tabla 15: Especificaciones Firebox T85 [24]

3.4.4 ASPECTOS LEGALES Y NORMATIVA APLICABLE

En el entorno actual, los Proveedores de Servicios de Internet (ISP) desempeñan un papel crítico al proporcionar conectividad y servicios esenciales para individuos y organizaciones. Este rol implica una enorme responsabilidad en términos de calidad, seguridad de la información, gestión de servicios y sostenibilidad. Para cumplir con estas demandas, los ISP deben adherirse a estándares internacionales que establecen directrices claras para operar de manera eficiente, segura y responsable.

Entre estas normas, la ISO/IEC 27011:2024 se destaca como una guía específica para el sector de telecomunicaciones, complementando la ISO/IEC 27001:2023 con un enfoque particular en los riesgos y desafíos únicos del sector. Juntas, estas normas garantizan un nivel elevado de seguridad de la información,

protegiendo datos sensibles frente a ciberamenazas y asegurando la continuidad de los servicios esenciales en redes de telecomunicaciones.

Además, la ISO/IEC 20000-1:2018 permite a los ISP implementar sistemas de gestión de servicios efectivos, optimizando procesos y asegurando que los servicios cumplan con las expectativas de los clientes. Por su parte, la actualización ISO 9001:2015/Amd 1:2024 introduce un enfoque renovado hacia la sostenibilidad y el cambio climático, reflejando la necesidad de operar con calidad mientras se minimiza el impacto ambiental. La implementación de estas normas no solo asegura el cumplimiento regulatorio, sino que también fortalece la confianza de los clientes y mejora la competitividad de los ISP en un mercado global exigente.



4 PRESUPUESTO

El presente presupuesto ha sido elaborado utilizando el software Arquímedes, una herramienta especializada para la gestión de proyectos en el ámbito de la ingeniería y la construcción. Este software permite realizar cálculos detallados de costes, generar presupuestos precisos y garantizar la trazabilidad de las mediciones a través de un sistema integrado de bases de datos. Además, Arquímedes facilita la organización y el desglose de materiales, equipos y mano de obra, asegurando una visión completa y profesional del proyecto.

Para este proyecto, se ha desarrollado un presupuesto que abarca tanto los materiales necesarios como los costes asociados a la instalación por sede. Este enfoque garantiza que los recursos y las inversiones estén adecuadamente planificados, optimizando así la ejecución de la solución propuesta. La estructura detallada y transparente del presupuesto busca reflejar fielmente las necesidades específicas del proyecto y sus implicaciones económicas

4.1 OBRA CIVIL

La siguiente tabla presenta un desglose de conceptos relacionados con obras civiles, específicamente en la instalación de arquetas y canalizaciones bajo diferentes superficies (asfalto y adoquinado). Se incluyen detalles de cantidades, precios unitarios y totales por cada actividad.

CONCEPTO	UD.	Ctd	PRECIO	IMPORTE
ARQUETA PREFAB. TIPO M CON TAPA DE METÁLICA PARA ASFALTO Suministro e instalación de arqueta prefabricada registrable de hormigón armado TIPO M, de 30x30x61 cm. de medidas interiores completa, incluso con tapa de fundición D-400 UNE-EN 124 , colocada sobre solera de hormigón en masa HM-15/B/40, de 15 cm. de espesor, incluso p.p. de formación de agujeros para conexionado de tubos, y con p.p. de medios auxiliares, incluyendo la excavación, y el relleno perimetral	UD	44	297,89	13.107,34
ARQUETA PREFAB. HGÓN. 80x67x80 Arqueta prefabricada registrable de hormigón armado, de 80x60x80 cm. de medidas interiores, completa, incluso con tapa de fundición D-400 UNE-EN 124 en el caso de situarse en calzadas y con marca Junta de Extremadura ref. 01999TM800junta, colocada sobre solera de hormigón en masa HM-15/B/40, de 15 cm. de espesor, incluso p.p. de formación de agujeros para conexionado de tubos, y con p.p. de medios auxiliares, incluyendo la excavación, y el relleno perimetral posterior.	UD	5	533,38	2.666,89
MICROZANJA BAJO ASFALTO Canalización en microzanja, de 0,05 x 0,30 m para 1 haz de 7 miniconductos de polietileno de 50 mm de diámetro, incluso tubos, con relleno de hormigón HM-20/B/20 de 30 cm de espesor hasta el rasante del terreno	ML	741,72	23,52	17.448,39
MICROZANJA BAJO ADOQUINADO Demolición de Adoquines a Mano y reposición de los mismos. Canalización en microzanja, de 0,05 x 0,30 m para 1 haz de 7 miniconductos de polietileno de 50 mm de diámetro, incluso tubos, con relleno de hormigón HM-20/B/20 de 30 cm de espesor hasta el rasante	ML	151,80	37,12	5.634,16

4.2 INSTALACIONES DE FIBRA ÓPTICA

La siguiente tabla presenta un desglose detallado de los elementos relacionados con la instalación de cableado de fibra óptica y elementos auxiliares como torpedos de empalme. En ella se especifican las características, unidades, cantidades, precios unitarios e importes totales para cada uno de los conceptos, proporcionando una visión clara de los materiales y servicios necesarios para el desarrollo del proyecto

CONCEPTO	UD.	CANTIDAD	PRECIO	IMPORTE
CABLE DE 12 FO Cable de FO totalmente instalado, por metro lineal de instalación	ML	1.873,90	1,85	3.462,97
CABLE DE 32 FO Cable de FO totalmente instalado, por metro lineal de instalación	ML	6.030,40	2,27	13.676,95
CABLE DE 64 FO Cable de FO totalmente instalado, por metro lineal de instalación	ML	5.252,20	2,77	14.538,09
CABLE DE 96 FO Cable de FO totalmente instalado, por metro lineal de instalación	ML	524,00	3,39	1.775,31
CABLE DE 128 FO Cable de FO totalmente instalado, por metro lineal de instalación	ML	510,78	4,15	2.118,72
TORPEDO TIPO CAJA 96 FIBRAS, para fusión de 64 fo Contiene 6 puertos de entrada/salida ideal. Para aplicaciones aéreas o subterráneas. Su diseño permite instalarlo en registros bajo tierra o sobre el tendido del cable aéreo. Incluye accesorios para facilitar la instalación: ESPECIFICACIONES: Largo : 396mm, Ancho: 200mm,Alto: 126mm, Peso: 2.5, Puertos: 6, Diámetro mín. Cable: 8 mm, Diámetro max. Cable: 20 mm, Cassete: LM-CH24 (capacidad de 4 cassetes), Capacidad de Fibras: 96, IP 67 NEMA 6s. Comprende todos los trabajos, materiales y medios auxiliares necesarios para dejar la unidad completa, totalmente instalada, rotulada, probada y en perfecto estado de funcionamiento, según los planos, pliego técnico y memoria del proyecto, indicaciones de la dir. facultativa y normativa vigente, incluso p.p. de ayudas de albañilería	UD	3	1.106,01	3.318,03

<p>TORPEDO TIPO CAJA 48 FIBRAS, para fusión de 32 fo</p> <p>CaContiene 6 puertos de entrada/salida ideal. Para aplicaciones aéreas o subterráneas. Su diseño permite instalarlo en registros bajo tierra o sobre el tendido del cable aéreo. Incluye accesorios para facilitar la instalación:</p> <p>ESPECIFICACIONES: Largo : 396mm, Ancho: 200mm,Alto: 126mm, Peso: 2.5, Puertos: 6, Diámetro min. Cable: 8 mm, Diámetro max. Cable: 20 mm, Cassete: LM-CHH24 (capacidad de 4 cassetes), Capacidad de Fibras: 48, IP 67 NEMA 6s. Comprende todos los trabajos, materiales y medios auxiliares necesarios para dejar la unidad completa, totalmente instalada, rotulada, probada y en perfecto estado de funcionamiento, según los planos, pliego técnico y memoria del proyecto, indicaciones de la dir. facultativa y normativa vigente, incluso p.p. de ayudas de albañilería.</p>	UD	3	730,01	2.190,03
<p>TORPEDO TIPO CAJA 96 FIBRAS,para fusión de 96 fo</p> <p>CaContiene 6 puertos de entrada/salida ideal. Para aplicaciones aéreas o subterráneas. Su diseño permite instalarlo en registros bajo tierra o sobre el tendido del cable aéreo. Incluye accesorios para facilitar la instalación:</p> <p>ESPECIFICACIONES: Largo : 396mm, Ancho: 200mm,Alto: 126mm, Peso: 2.5, Puertos: 6, Diámetro min. Cable: 8 mm, Diámetro max. Cable: 20 mm, Cassete: LM-CHH24 (capacidad de 4 cassetes), Capacidad de Fibras: 96, IP 67 NEMA 6s. Comprende todos los trabajos, materiales y medios auxiliares necesarios para dejar la unidad completa, totalmente instalada, rotulada, probada y en perfecto estado de funcionamiento, según los planos, pliego técnico y memoria del proyecto, indicaciones de la dir. facultativa y normativa vigente, incluso p.p. de ayudas de albañilería..</p>	UD	2	1.393,01	2.786,02
<p>TORPEDO TIPO CAJA 144 FIBRAS, para fusión de 128 fo</p> <p>Caja de empalme-fusión estanca tipo FTX-6228 1 500-20 de ADCKRONE o equivalente con capacidad máxima de 288 fusiones, diámetro 28,2 cm y longitud 72 cm, con 7 bocas máximo de entrada / salida. Equipado para 5 accesos (1 acceso simple para cables de 21,6 a 25,4 mm -cable de 256 fo- y 4 accesos simples para cables de 15,2 a 21,6 -cables de 64 fo-). Dispondrá de 32 bandejas de 12 fusiones cada una de ellas, organizadas para fusiones de 32 tubos holgados. Incluye soporte de pared, protector de 35 mm, instalación de la caja de empalme y fusión de 256 fibras. Comprende todos los trabajos, materiales y medios auxiliares necesarios para dejar la unidad completa, totalmente instalada, rotulada, probada y en perfecto estado de funcionamiento, según los planos, pliego técnico y memoria del proyecto, indicaciones de la dir. facultativa y normativa vigente, incluso p.p. de ayudas</p>	UD	2	1.746,01	3.492,02
<p>Caja de conexiones para fibra óptica de 8 puertos IP69</p> <p>Caja distribuidora de fibra óptica para ser montada en pared. Fabricada en plástico de color gris y con protección IP69 anti-humedades y apta para ser instalada en el exterior. Soporta la gestión de 8 conexiones de fibra óptica procedentes un único cable multi-fibra.</p>	Ud	11	50,79	558,65

4.3 CANALIZACIONES

Las siguiente tablas presenta en detalle los importes del material de canalizado ,cada partida está organizada con información detallada sobre el tipo de concepto, unidad de medida, precio unitario, cantidades, origen, y subconceptos involucrados, permitiendo calcular los subimportes correspondientes.

CANALIZACIÓN BAJO CALZADA CON MBC	ML	27,30							
Canalización en zanja, de 0,25 x 0,80 m para 1 conducto tritubo de 40 mm. de diámetro interior cada uno, embebido en prisma de homigón HL-150/P/20 de central de 5 cm. de recubrimiento superior e inferior, incluso tritubo, homigón y relleno de la capa superior con tierras procedentes de la excavación, en tongadas <25 cm., compactada al 95% del P.N., así como reposición del pavimento existente sobre solera de homigón HM-20/B/20 de 30 cm de espesor y capa de mezcla bituminosa en caliente S-12 de 6 cm de espesor, con mandrilado y tendido de hilo-guía en conductos y subconductos.			P27TW110A	Instelca	MANDRILADO	ML	3,000	3,50	10,50
			E02ZM010	Preoc 2009	EXC.ZANJA A MÁQUINA T. DISGREG.	M3	0,024	5,88	0,14
			P27TT040	Nav / Plom	Tritubo polietileno D=40 mm	ML	1,660	1,66	2,76
			P27TT180	Instelca	Hilo acerado 0,8 mm para guía	ML	3,000	0,59	1,77
			P01HD150	Preoc 2009	Horn.elem. no resist.HM-15/P/20 central	M3	0,000	49,69	0,00
			P1470	Plomyplas	Cinta señalización de zanja	ML	1,000	0,33	0,33
			P01HC003	Preoc 2009	Hormigón HM-20/P/20/I central	M3	0,020	57,20	1,14
			U04CM025	Navarino	M.B.C. TIPO AC16 surf S DESG.ÁNGELES<25	Tm	0,024	16,18	0,39
			P27TT050		Soporte separador 40 mm 4 aloj.	Ud	1,000	0,3	0,30
			P27TT1501		Tapón obturador conductos D=40mm	Ud	2,000	2,14	4,28
			O01A090		Cuadrilla A	h	0,050	32,87	1,64
			P27TT200		Limpiador unión PVC	Kg	0,001	2,06	0,00
			P27TT210		Adhesivo unión PVC	Kg	0,001	2,63	0,00
			O01E010		Arqueólogo	h	0,100	40,43	4,04
CANALIZACIÓN BAJO ACERADO CON BALDOSA HM SIN PULIR	ML	44,85							
Canalización en zanja, de 0,05 x 0,20 m para 1 conducto tritubo de 40 mm. de diámetro interior cada uno, embebido en prisma de homigón HL-150/P/20 de central de 5 cm. de recubrimiento superior e inferior, incluso tritubo, homigón y relleno de la capa superior con tierras procedentes de la excavación, en tongadas <25 cm., compactada al 95% del P.N., así como reposición del pavimento existente sobre solera de homigón HM-20/B/20 de 15 cm de espesor y reposición de solera y tendido de hilo-guía en conductos y subconductos.			P27TW110A	Instelca	MANDRILADO	ML	3,000	3,50	10,50
			E02DA030		EXC.VAC.MANUAL.TERR.COMPACTOS	m3	0,09	27,2	2,45
			P27TT040	Nav / Plom	Tritubo polietileno D=40 mm	ML	1,660	1,66	2,76
			P27TT180	Instelca	Hilo acerado 0,8 mm para guía	ML	3,000	0,59	1,77
			P01HD150	Preoc 2009	Horn.elem. no resist.HM-15/P/20 central	M3	0,020	49,69	0,99
			P1470	Plomyplas	Cinta señalización de zanja	ML	1,000	0,33	0,33
			E01EPS030	Preoc 2009	DEMOL Pav. Homigón Impreso	M3	0,500	10,03	5,02
			P08TE030	Navarino	Baldosa reliev. 40x40x3,7 1ª cal	Tm	0,500	19,95	9,98
			P27TT050		Soporte separador 40 mm 4 aloj.	Ud	1,000	0,3	0,30
			P27TT1501		Tapón obturador conductos D=40mm	Ud	1,600	2,14	3,42
			O01A090		Cuadrilla A	h	0,100	32,87	3,29
			P27TT200		Limpiador unión PVC	Kg	0,001	2,06	0,00
			P27TT210		Adhesivo unión PVC	Kg	0,001	2,63	0,00
			O01E010		Arqueólogo	H	0,100	40,43	4,04

CONCEPTO	UD.	PRECIO	Cód.	Origen	Subconcepto	Ud.	Cantidad	Precio	Subimporte
ARQUETA PREFAB. TIPO M CON TAPA DE METÁLICA PARA ASFALTO	UD	297,89							
Suministro e instalación de arqueta prefabricada registrable de hormigón armado TIPO M, de 30x30x61 cm. de medidas interiores completa, incluso concon tapa de fundición D-400 UNE-EN 124 , colocada sobre solera de hormigón en masa HM-15/B/40, de 15 cm. de espesor, incluso p.p. de formación de agujeros para conexionado de tubos, y con p.p. de medios auxiliares, incluyendo la excavación, y el relleno perimetral			O010A030	Navarino	Oficial primera	H	0,600	13,42	8,05
			O010A060	Navarino	Peón especializado	H	1,200	12,91	15,49
			P01HD150	Preoc 2009	Horm.elem. no resist.HM-15/P/20 central	M3	0,049	40,00	1,98
			P27TA100	Bedec	Arqueta pref.hgón. 30x60x30 cm.	UD	1,000	156,33	156,33
			P27TA130	Bedec	Tapa arqueta FD 30x60 cm. D-400	UD	1,000	73,22	73,22
			M05RN030		Retrocargadora neum. 100 CV	h	0,250	47,26	11,82
			E02PM030		EXC.POZOS A MÁQUINA T.COMPACT	M3	1,000	10,81	10,81
			O01E010		Arqueólogo	h	0,500	40,43	20,22
ARQUETA PREFAB. HGÓN. 80x67x80	UD	533,38							
Arqueta prefabricada registrable de hormigón armado, de 80x60x80 cm. de medidas interiores, completa, incluso con tapa de fundición D-400 UNE-EN 124 en el caso de situarse en calzadas y con marca Junta de Extremadura ref. 01999TM800junta, colocada sobre solera de hormigón en masa HM-15/B/40, de 15 cm. de espesor, incluso p.p. de formación de agujeros para conexionado de tubos, y con p.p. de medios auxiliares, incluyendo la excavación, y el relleno perimetral posterior.			O010A030	Navarino	Oficial primera	h	0,600	13,42	8,05
			O010A060	Navarino	Peón especializado	h	1,200	12,91	15,49
			P01HD150	Preoc 2009	Horm.elem. no resist.HM-15/P/20 central	M3	0,049	40,00	1,98
			P27TA060	Bedec	Arqueta pref.hgón. 80x70x80 cm. Con Tapa	UD	1,000	462,67	462,67
			M05RN030		Retrocargadora neum. 100 CV	h	0,300	47,26	14,18
			E02PM030		EXC.POZOS A MÁQUINA T.COMPACT	M3	1,000	10,81	10,81
			O01E010		Arqueólogo	h	0,500	40,43	20,22
MICROZANJA BAJO ASFALTO	ML	23,52							
Canalización en microzanja, de 0,05 x 0,30 m para 1 haz de 7 miniconductos de polietileno de 50 mm de diámetro, incluso tubos, con relleno de hormigón HM-20/B/20 de 30 cm de espesor hasta el rasante del terreno			P27TT010A	Emtelle 7DBmf	Tubo rígido PVC 40x1,2 mm. Subconductado en	ML	1,000	2,38	2,38
			P01HC003	Preoc 2009	Hormigón HM-20/P/20/I central	M3	0,013	57,20	0,74
			E02ZM010AA		Alquiler Microzanjadora Marais Side CUT	h	0,150	66,02	9,90
			E02ZM010AA		Alquiler Máquina de soplado JDSU AirBlow FO 8	h	0,032	79,82	2,55
			O01BT161	H	Oficial 1º Instalador telecomunicación	h	0,100	20,56	2,08
			O01BT162	H	Ayudante Instalador telecomunicación	h	0,100	18,45	1,85
			O01E010		Arqueólogo	H	0,100	40,43	4,04

CANALIZACIÓN EN TERRENO NO URBANIZADO									
Canalización en zanja, de 0,20 x 0,39 m para 1 tubo corrugado de polietileno de 40 mm de diámetro, embebido en prisma de arena de 5 cm. de recubrimiento inferior, 9 cm lateral y 25 cm superior, incluso tubos, y reposición del terreno existente de 30 cm de espesor con mandrilado y tendido de hilo-guía en conductos y subconductos.									
ML	30,80								
		P27TW110A	Instelca	MANDRILADO	ML	3,000	3,50		10,50
		E02ZM010	Preoc 2009	EXC.ZANJA A MÁQUINA T. DISGREG.	M3	0,024	5,86		0,14
		P27TT040	Nav / Plom	Tritubo polietileno D=40 mm	ML	1,660	1,66		2,76
		P27TT180	Instelca	Hilo acerado 0,8 mm para guía	ML	3,000	0,59		1,77
		P01AA080	Preoc 2015	ARENA DE RÍO (0-2 mm)	M3	0,145	14,59		2,12
		E02SZ060	Navarino	RELL.TIERR.ZANJA MANO S/APORT	M3	0,200	6,39		1,28
		P1470	Plomyplas	Cinta señalización de zanja	ML	1,000	0,33		0,33
		P27TT050		Soporte separador 40 mm 4 aloj.	Ud	1,000	0,3		0,30
		P27TT1501		Tapón obturador conductos D=40mm	Ud	2,000	2,14		4,28
		O01A090		Cuadrilla A	h	0,100	32,87		3,29
		P27TT200		Limpiador unión PVC	Kg	0,001	2,06		0,00
		P27TT210		Adhesivo unión PVC	Kg	0,001	2,63		0,00
		O01E010		Arqueólogo	H	0,100	40,43		4,04
CANALIZACIÓN TUBO DE ACERO AÉREO									
Canalización aérea para 1 tubo de acero galvanizado de 2 1/2", DN 65 mm., de diámetro interior, con mandrilado y tendido de hilo-guía en conductos y subconductos.									
Ud	51,88								
		P27EW140	Preoc 2009	Poste tubo 3 m. galv.para espejo	ud	1,000	29,47		29,47
		P27TT180	Instelca	Hilo acerado 0,8 mm para guía	ML	3,000	0,60		1,80
		O01BT162	Navarino	Peón especializado	h	1,000	18,45		18,45
		P27EW160		Anclaje hito y tomillería	Ud	1,000	2,16		2,16

CANALIZACIÓN EN TERRENO NO URBANIZADO									
Canalización en zanja, de 0,20 x 0,39 m para 1 tubo corrugado de polietileno de 40 mm de diámetro, embebido en prisma de arena de 5 cm. de recubrimiento inferior, 9 cm lateral y 25 cm superior, incluso tubos, y reposición del terreno existente de 30 cm de espesor con mandrilado y tendido de hilo-guía en conductos y subconductos.	ML	30,80							
			P27TW110A	Instelca	MANDRILADO	ML	3,000	3,50	10,50
			E02ZM010	Preoc 2009	EXC.ZANJA A MÁQUINA T. DISGREG.	M3	0,024	5,88	0,14
			P27TT040	Nav / Plom	Tritubo polietileno D=40 mm	ML	1,660	1,68	2,76
			P27TT180	Instelca	Hilo acerado 0,8 mm para guía	ML	3,000	0,59	1,77
			P01AA080	Preoc 2015	ARENA DE RÍO (0-2 mm)	M3	0,145	14,59	2,12
			E02SZ060	Navarino	RELL.TIERR.ZANJA MANO S/APORT	M3	0,200	6,39	1,28
			P1470	Plomyplas	Cinta señalización de zanja	ML	1,000	0,33	0,33
			P27TT050		Soporte separador 40 mm 4 aloj.	Ud	1,000	0,3	0,30
			P27TT1501		Tapón obturador conductos D=40mm	Ud	2,000	2,14	4,28
			O01A090		Cuadrilla A	h	0,100	32,87	3,29
			P27TT200		Limpiador unión PVC	Kg	0,001	2,08	0,00
			P27TT210		Adhesivo unión PVC	Kg	0,001	2,63	0,00
			O01ED10		Arqueólogo	H	0,100	40,43	4,04
CANALIZACIÓN TUBO DE ACERO AÉREO									
Canalización aérea para 1 tubo de acero galvanizado de 2 1/2", DN 65 mm., de diámetro interior, con mandrilado y tendido de hilo-guía en conductos y subconductos.	Ud	51,88							
			P27EW140	Preoc 2009	Poste tubo 3 m. galv.para espejo	ud	1,000	29,47	29,47
			P27TT180	Instelca	Hilo acerado 0,8 mm para guía	ML	3,000	0,60	1,80
			O01BT162	Navarino	Peón especializado	h	1,000	18,45	18,45
			P27EW160		Anclaje hito y tomillería	Ud	1,000	2,16	2,16

4.4 RESUMEN

La tabla presentada muestra un resumen económico detallado de un proyecto de obra, desglosando las principales partidas, como obra civil, elementos pasivos y electrónicos de red, seguridad y salud, y gestión de residuos. También incluye el cálculo de gastos generales, beneficio industrial y el importe total de ejecución, tanto sin IVA como con IVA.

RESUMEN			
TOTAL PARTIDA DE OBRA CIVIL (OC)		71039,05	€
TOTAL PARTIDA DE ELEMENTOS PASIVOS Y ELECTRÓNICA DE RED		51228,87	€
TOTAL PARTIDA DE SEGURIDAD Y SALUD (SS)		3.041,74	€
TOTAL GESTIÓN DE RESIDUOS		2.431,41	€
IMPORTE TOTAL DE EJECUCIÓN (TE1)		127.741,07	€
13% DE GASTOS GENERALES SOBRE (OC +SS) (GG)		10.800,34	€
6% DE BENEFICIO INDUSTRIAL SOBRE (OC +SS) (BI)		7.664,48	€
TOTAL DE GASTOS GEN. Y BENEFICIO IND. (GG + BI)		152.011,87	€
TOTAL DE EJEC. + GASTOS GEN. + BENEFICIO IND. (TESI)		152.011,87	€
IMPORTE TOTAL DE EJECUCIÓN DE LA OBRA SIN IVA (TE)		152.011,87	€
21% DE IVA SOBRE TO		31.922,49	€
IMPORTE TOTAL DE EJECUCIÓN DE LA OBRA CON IVA		183.934,37	€

5 CONCLUSIONES

A lo largo de este trabajo fin de grado se ha desarrollado una solución integral para la migración de la red de una empresa logística hacia un entorno más robusto y seguro, que incluye respaldo LTE y funcionalidades avanzadas de VPN. Este diseño no solo responde a los requerimientos actuales del cliente, sino que también sienta las bases para futuras ampliaciones y adaptaciones, garantizando flexibilidad y sostenibilidad en un sector tan dinámico como el de la logística.

La implementación de tecnologías como BGP, MPLS y dispositivos de seguridad perimetral permite optimizar el tráfico, garantizar la continuidad operativa y proteger los datos críticos de la organización. Asimismo, se ha demostrado la viabilidad técnica y económica de la propuesta, evaluando cuidadosamente los costes de los equipos y su instalación, así como el cumplimiento de normativas y estándares internacionales.

Este proyecto destaca la importancia de una infraestructura de red bien diseñada como base para el éxito de las operaciones logísticas. A través de un análisis técnico riguroso y la colaboración entre diversas disciplinas, se ha logrado desarrollar una solución que no solo satisface las necesidades actuales, sino que también prepara a la empresa para enfrentar los retos futuros de conectividad y ciberseguridad.

6 BIBLIOGRAFIA

- [1] Sapalomera, "Protocolos de routing IGP y EGP." Accessed: Oct. 20, 2024. [Online]. Available: <https://www.sapalomera.cat/moodlecf/RS/2/course/module7/7.1.4.2/7.1.4.2.html>
- [2] Redesconfiguracion, "Redes Informat, Router ,switch, Lan ,Wan ,Man y más: Protocols IGP y EGP." Accessed: Oct. 11, 2024. [Online]. Available: <https://redesconfiguracion.blogspot.com/2018/05/protocols-igp-y-egp.html>
- [3] F. Álvarez, "Protocolos de Enrutamiento de Red," Routing and Switching. Accessed: Dec. 14, 2024. [Online]. Available: <https://dotbugs.com/protocolos-enrutamiento-de-red/>
- [4] P. Tsuchiya Bellcore, "Request for Comments: 1219 ." Accessed: Oct. 16, 2024. [Online]. Available: <https://www.rfc-es.org/rfc/rfc1219-es.txt>
- [5] Cloudflare, "¿Qué es una subred? | Cómo funciona una subred," ¿Qué es una subred? Accessed: Dec. 14, 2024. [Online]. Available: <https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-subnet/#:~:text=Una%20subred%20es%20una%20red%20dentro%20de%20una%20red.,para%20llegar%20a%20su%20destino.>
- [6] Movistar, "Servicio NEBA LOCAL," Descripción técnica y Procedimientos V1.4. Accessed: Dec. 12, 2024. [Online]. Available: https://www.cnmc.es/sites/default/files/2421046_8.pdf
- [7] Telefónica, "Servicio NEBA LOCAL," Descripción técnica y Procedimientos V1.4. Accessed: Dec. 12, 2024. [Online]. Available: https://www.cnmc.es/sites/default/files/2421046_8.pdf
- [8] Juniper Networks, "Subscriber Management VLAN Architecture Overview | Junos OS | Juniper Networks," Broadband Subscriber VLANs and Interfaces User Guide. Accessed: Dec. 06, 2024. [Online]. Available: <https://www.juniper.net/documentation/us/en/software/junos/subscriber->

mgmt-vlan/topics/concept/subscriber-management-vlan-architecture.html

- [9] Telefónica, “NEBA LOCAL,” Descripción técnica. Accessed: Dec. 10, 2024. [Online]. Available: https://www.cnmc.es/sites/default/files/2421046_8.pdf
- [10] Movistar, “Descripción PTRO,” Blog Movistar. Accessed: Dec. 12, 2024. [Online]. Available: <https://comunidad.movistar.es/t5/Hogar-Fijo-Internet-TV/Para-qu%C3%A9-es-esta-caja-de-pared/td-p/4919499>
- [11] WatchGuard T85, “WatchGuard Firebox T85,” Seguridad de alto rendimiento que evoluciona con su red. Accessed: Dec. 12, 2024. [Online]. Available: <https://www.watchguard.com/es/wgrd-products/tabletop/firebox-t85>
- [12] Telefónica España, “Servicio NEBA LOCAL Descripción técnica y Procedimientos V1.11,” 2023. Accessed: Dec. 04, 2024. [Online]. Available: https://www.cnmc.es/sites/default/files/editor_contenidos/Telecomunicaciones/Ofertas/NEBA%20Local/Texto%20NEBA%20Local%20vigente.pdf
- [13] S. A. Telefónica, “Marcas - Telefónica.” Accessed: Nov. 06, 2024. [Online]. Available: <https://www.telefonica.com/es/nosotros/marcas/>
- [14] acens, “Sobre acens,” Acens Part of Telefónica Tech. Accessed: Nov. 06, 2024. [Online]. Available: <https://www.acens.com/corporativo/>
- [15] Ministerio de transportes y movilidad sostenible., “6.1.1 Valor Añadido Bruto | OTLE,” Informe anual 2023 OTLE. Accessed: Dec. 14, 2024. [Online]. Available: <https://otle.transportes.gob.es/inform/es/2023/6logistica/61-peso-economico-del-sector-logistico/611valor-anadido-bruto>
- [16] Flexpacio, “Mejores operadores logísticos en España: cuáles son y ejemplos,” Logística Ecommerce. Accessed: Dec. 14, 2024. [Online]. Available: <https://www.flexpacio.com/post/principales-operadores-logisticos-en-espana-cuales-son-y-ejemplos>

- [17] IETF, "IETF | Security & privacy," IETF. Accessed: Dec. 02, 2024. [Online]. Available: <https://www.ietf.org/technologies/security/>
- [18] MEF, "MEF 3.0 Optical Transport Service Standards," The standard for automated optical transport services. Accessed: Dec. 02, 2024. [Online]. Available: <https://www.mef.net/service-standards/underlay-services/optical-transport/>
- [19] Juniper, "Plataforma de enrutamiento universal MX480 | Juniper Networks," Plataforma de enrutamiento universal MX480. Accessed: Dec. 06, 2024. [Online]. Available: <https://www.juniper.net/mx/es/products/routers/mx-series/mx480-universal-routing-platform.html>
- [20] Juniper Network, "MX480 descripción del enrutador | MX480 Plataforma de enrutamiento universal guía de hardware | Juniper Networks TechLibrary," 2024. Accessed: Dec. 03, 2024. [Online]. Available: <https://www.juniper.net/documentation/mx/es/hardware/mx480/topics/concept/mx480-description.html>
- [21] Juniper, "Guía de hardware de la plataforma de enrutamiento universal MX480a plataforma de enrutamiento universal MX480," Juniper Documentation. Accessed: Dec. 14, 2024. [Online]. Available: <https://www.juniper.net/documentation/mx/es/hardware/mx480/index.html>
- [22] Juniper Networks, "MX960 Universal Routing Platform Hardware Guide," Hardware Guide. Accessed: Dec. 10, 2024. [Online]. Available: <https://www.juniper.net/documentation/us/en/hardware/mx960/topics/task/mx960-qs.html>
- [23] Universidad Cumillas., "Confidencialidad, Integridad y Disponibilidad," Stic. Accessed: Dec. 04, 2024. [Online]. Available: <https://ciberseguridad.comillas.edu/confidentiality-integrity-and-availability/>

[24] WatchGuard, "WatchGuard Firebox serie T85," WatchGuard Solutions.
Accessed: Dec. 14, 2024. [Online]. Available:
<https://www.watchguard.com/es/wgrd-products/tabletop/firebox-t85>

