

Respaldo en una red Provincial (SD-WAN multiVRF)



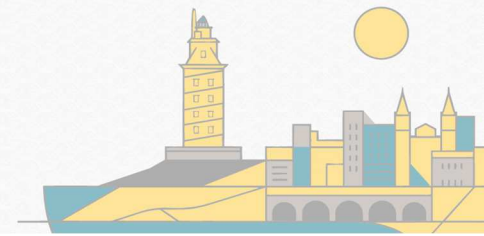
Eladio Maqueda Gil

Jefe de Sección de Sistemas
emaqueda@dip-badajoz.es



Miguel Ángel Muñoz Ruiz

Ingeniero CGE



Preámbulo

- Qué es una Diputación: <http://es.wikipedia.org/wiki/Diputaci%C3%B3n> (o preguntar a vuestra IA favorita).
- Diputación: arquitecto del ayuntamiento, abogado, informático, asesor, carreteras, depuradoras ...
- Nuestro cliente tipo: un ayuntamiento con alcalde, secretario a ratos y un administrativo. Hacen de todo.
- Nuestro área (IAD): proporcionamos asesoramiento informático, aplicativos, redes:

<https://www.dip-badajoz.es/diputacion/delegaciones/apnt/>



Qué es la RPCS

Es un servicio más de los que Diputación presta a las EELL **gratis**.

En los servicios administrativos de las EELL se dispone de:

- **Una línea de comunicaciones en fibra óptica** que comunica con la Diputación de Badajoz.
- **Un router de comunicaciones.**
- Diputación proporciona (o incluso realiza) configuración de los ordenadores y switches de la entidad.
- En Diputación se encuentra el equipamiento para garantizar la seguridad, integridad y fiabilidad de las conexiones



¿Quiénes está en la RPCS?

- Todos los edificios de la Diputación de Badajoz (capital y sedes remotas)
- Ayuntamientos (165 municipios)
- ELM con servicios administrativos.
- Mancomunidades (14)
 - ~ 200 sedes de EELL sobre un total de ~ 300 sedes.
 - > 300 routers remotos, > 400 switches y > 7.000 puntos de red
 - > 2.000 extensiones telefónicas → + 70 EELL (>800 extensiones)



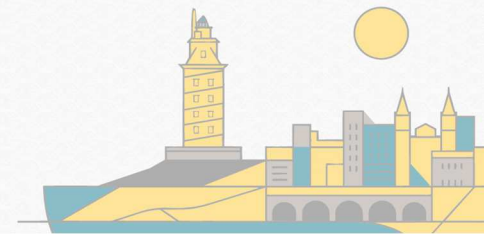
Servicios en la RPCS

- Acceso directo a los principales servicios de Diputación: tributos (OAR), correo corporativo para más de 4000 usuarios, padrón de habitantes, alojamiento web, administración electrónica, registro telemático, procedimientos, perfil contratante, publicación en BOP, gestión remota (Diputación y EELL),...
- Acceso a datos y servicios mediante virtualización de aplicaciones o directamente web.
- Acceso autenticado a Internet a más de 2000 usuarios



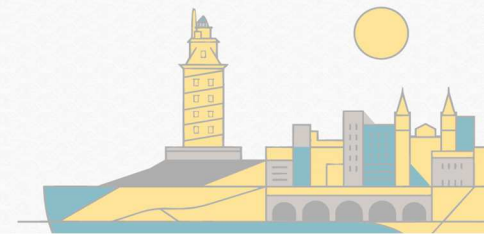
Para qué la RPCS

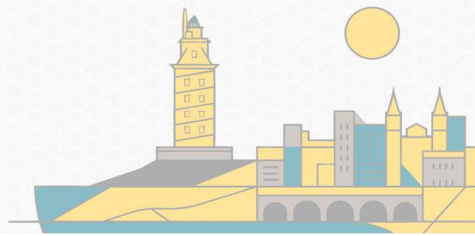
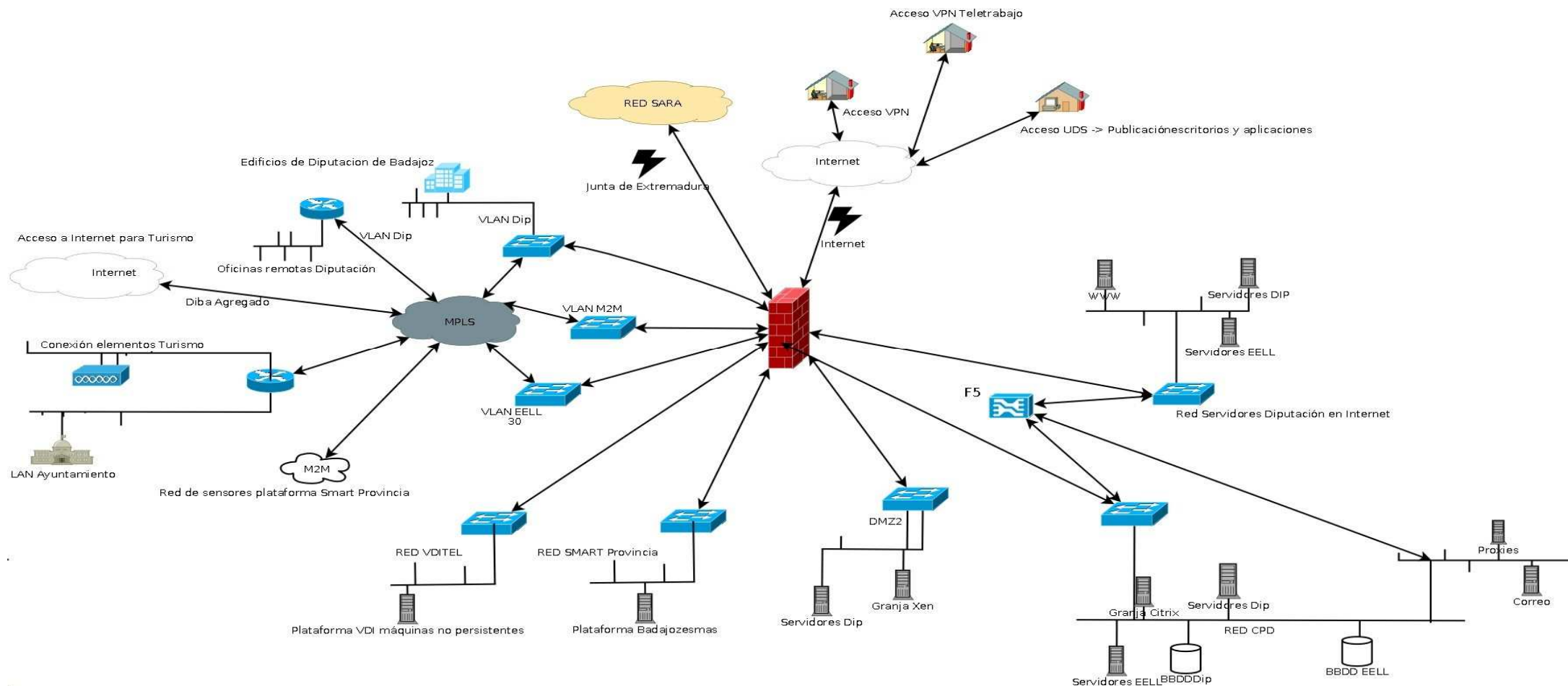
- Equipos y programas de los servicios administrativos de las EELL en una red protegida.
- Dotada de elementos de protección de red (FW, proxies,...) + distribución y gestión antivirus, EDR, microClaudia, ...
- Proporciona acceso controlado a la red corporativa de la Junta de Extremadura, a red SARA (DGT, Hacienda, cl@ve, @firma, SIRAJ, Seguridad Social, Ministerio de Justicia, INE, MAP, Catastro, ...) y a otras redes europeas.
- Punto Neutro Interadministrativo: EELL → Diputación → Junta de Extremadura → AGE.
Direccionamiento Ip de red SARA.



Evolución RPCS

- Inicio: red plana conectando EELL a aplicativos en Diputación y redSARA, Internet autenticado,...
- Siguiendo paso: comunicaciones MPLS (VPNIP y Macrolan) confiables y seguras → altísima personalización. Limitación a 4 VRF por sede. Cada VRF trámite burocrático complicado.
- Ahora: múltiples servicios (VRF, VLAN, VNI,...) en sedes: Dip, EELL, ToIP, incubadoras empresas, sensores, Internet, placas solares,...
- La seguridad e independencia de las comunicaciones dependía del operador (MPLS). Con SD-WAN nosotros definimos los túneles, cifrado, ...
- Futuro cercano: más VRF (ó Vlan, VNI,...) -> paradigma es la microsegmentación de las redes. Provisión inmediata y directa.





Despliegue SD-WAN

- En 2020 desplegamos la tecnología SDWAN sobre un piloto de 15 sedes, sin intervenciones en campo y costes. No hay más elementos físicos en las sedes remotas, solo una licencia en el router y configuraciones.
- Empezamos por analizar y catalogar el tráfico de cada sede, evidenciando las necesidades de personalización, aplicando políticas de servicio acordes a las aplicaciones. Se ha eliminado mucho ruido (tráfico erróneo, tráfico no autorizado, tráfico filtrado,...) en las conexiones, ganando ancho de banda y seguridad. Hay un ZTP pues aquello que no se define no se procesa.
- Se ha implementado la parte de seguridad, consistente en FW instalados en los CPD de Diputación y dada su integración con la plataforma permiten dotar de seguridad integral a la solución SD-WAN.
- Desplegando seguridad usando SD-WAN, sin cambios en las sedes remotas.



Despliegue SD-WAN

- Complejidad de las redes WAN. Virtualizando la red nos abstraemos de las limitaciones de las infraestructuras, utilizando cualquier tipo de acceso (MPLS, Internet, 4G, 5G, Startlink,...), habilitando redundancia de caminos, implementando garantías de SLA y garantizando la seguridad extremo a extremo.
- La red conmuta paquetes, pero los usuarios usan aplicaciones. Esta nueva tecnología nos permitirá evolucionar de redes IP a redes de Aplicaciones. Se opera en la “Capa de Aplicación”, tomando decisiones de routing basadas en nivel 7. La seguridad se integra completamente pudiendo tomar decisiones como filtrar url, antivirus, IDS, IPS,... La seguridad consiste en un verdadero firewall que actúa a nivel IP, protocolo, servicio o aplicación.
- Implementar cambios es difícil y se tarda. Se trata la gestión de la red como un elemento Software, desacoplando planos de datos y control, traduciendo “deseos” a configuración, proporcionando herramientas de Visibilidad de las Aplicaciones y autoprovisión.



Resiliencia en la RPCS

Tres circunstancias nos permiten plantearnos una redundancia en la red:

- **Oportunidad “política”:** Desgraciadamente las inundaciones de este año nos han sometido a diversos tipos de caídas (fibra arrastrada por el Guadiana y camino alternativo con tirada de kilómetros de fibra, viento que “tira” enlaces, cortes de luz, ...). Se ha comprendido la necesidad de la red todos los días.
- **Oportunidad técnica:** Este año nuestro operador nos ha permitido disponer de Starlink y hemos comprobado unas prestaciones óptimas para el funcionamiento de la red, existe despliegue de fibra de otros operadores en algunas sedes y, lo más importante, nuestra red SDWAN permite abstraernos del operador.
- **Oportunidad económica:** El marco adecuado es el nuevo concurso (inicio en 2027) que nos permite hacer un lote específico para la redundancia de la red que recoge: conexiones de fibra de otro operador, Starlink y estabilidad de la electricidad.



Resilencia en la RPCS

Dentro de las posibilidades que nos ofrece la solución de SDWAN – Teldat, es realizar Backup del acceso principal Macrolan o VPNIP con conexiones alternativas de cualquier operador. En caso de caída del acceso principal Macrolan o VPNIP, el tráfico de forma automática saldría por el acceso alternativo del segundo operador, interconectando con la solución SDWAN vía el DIBA mediante tunelización por IPs públicas.

Se admite FTTH de operador alternativo, 5G con SIM/eSIM gestionada, radioenlace o combinación equivalente. Se persigue diversidad lógica y/o física (operador, ruta, medio) cuando exista disponibilidad razonable.



Resilencia en la RPCS

Es importante que este acceso de respaldo FTTH, no comparta ningún elemento del trazado, dado que en caso de incidencia por corte de fibras troncales afectaría a ambos circuitos.

Dicha solución no está actualmente implementada debido a varios factores:

- No tenemos FTTH residenciales en sedes remotas de operador distinto. Requiere contrato con otro operador.
- El acceso del DIBA de Diputación de Badajoz, es limitado a 2Gb, en caso de meter tráfico de sedes que sufren alguna caída, se podría desbordar el acceso.



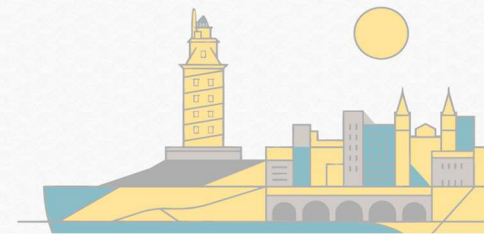
Infraestructura Provincial

Conectividad en ciudades

Diversificación física de fibra óptica hacia múltiples centrales en cabeceras de comarca como Badajoz y Mérida.

Conectividad en zona rural

Dificultad de replicar trazados redundantes en poblaciones dispersas debido a severas limitaciones de infraestructura.



Backup de Primera Fase



Parques Bomberos

Garantía de respaldo inalámbrico inmediato para la coordinación ante siniestros.



Policia Local

Continuidad de comunicaciones clave de la Policía Local y bases críticas.



Servicios Esenciales EELL

Uso en Ayuntamientos medianos para evitar el aislamiento administrativo.



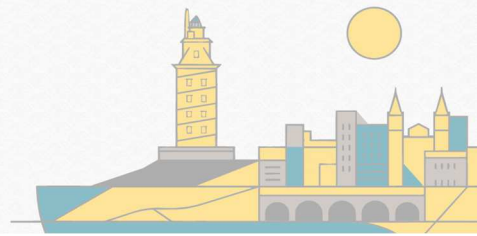
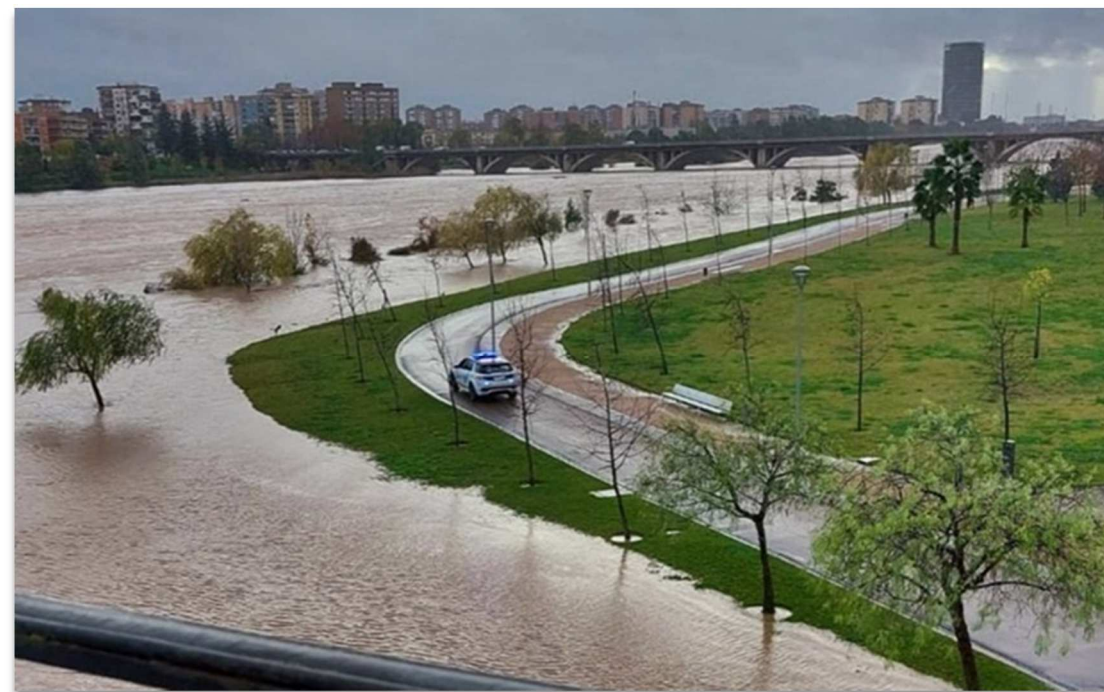
Trampa del enlace troncal común

Punto de fallo único terrestre: Aunque el respaldo final fuese inalámbrico, dependía en última instancia del mismo troncal de fibra.

Causas de interrupción:

- Inundaciones y desbordamientos.
- Incendios descontrolados.
- Labores agrícolas agresivas.

Consecuencia: Caída simultánea del enlace principal y de la estación base de telefonía móvil de la zona.



Limitaciones Satelitales VSAT

- **Telefonía IP impracticable:** Retardo inasumible para comunicaciones verbales ágiles
- **Degradación por congestión:** Colapso del rendimiento general bajo tráfico concurrente
- **Altos costes fijos:** Tafias elevadas por anchos de banda muy reducidos.

600 - 800ms

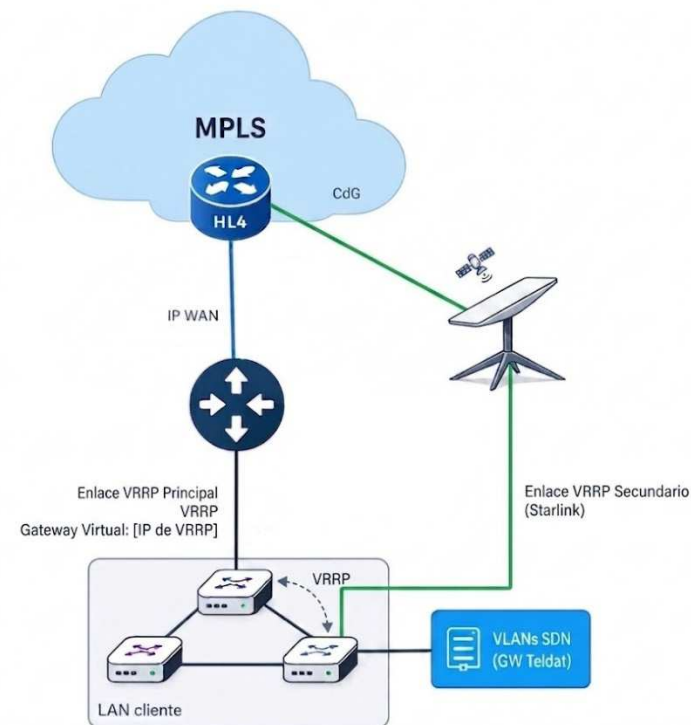
Latencia de satélite VSAT



Starlink: Estándar LEO

Ventajas del Nuevo Paradigma

- Latencia reducida, debido a una conectividad con satélites de baja altura.
- Independencia absoluta de la planta de cableado local.
- Facilidad de implantación en zonas rurales complejas.
- Banda ancha bidireccional de alto rendimiento.

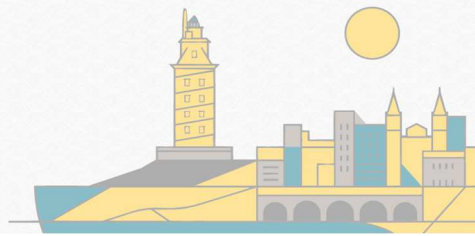


Satelital VSAT

750 ms

Starlink LEO

35 ms



Integración con SD-WAN Teldat



Autonomía de tecnología

Fin de la dependencia cautiva de una única tecnología o proveedor en ubicaciones rurales.



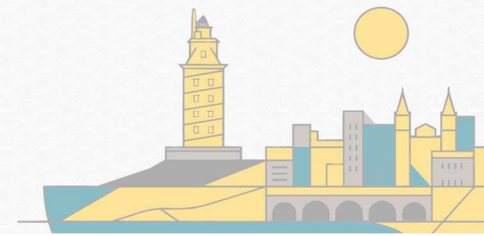
Eficiencia de Costes

Permite realizar redundancia con circuitos FTTH o Starlink residenciales.



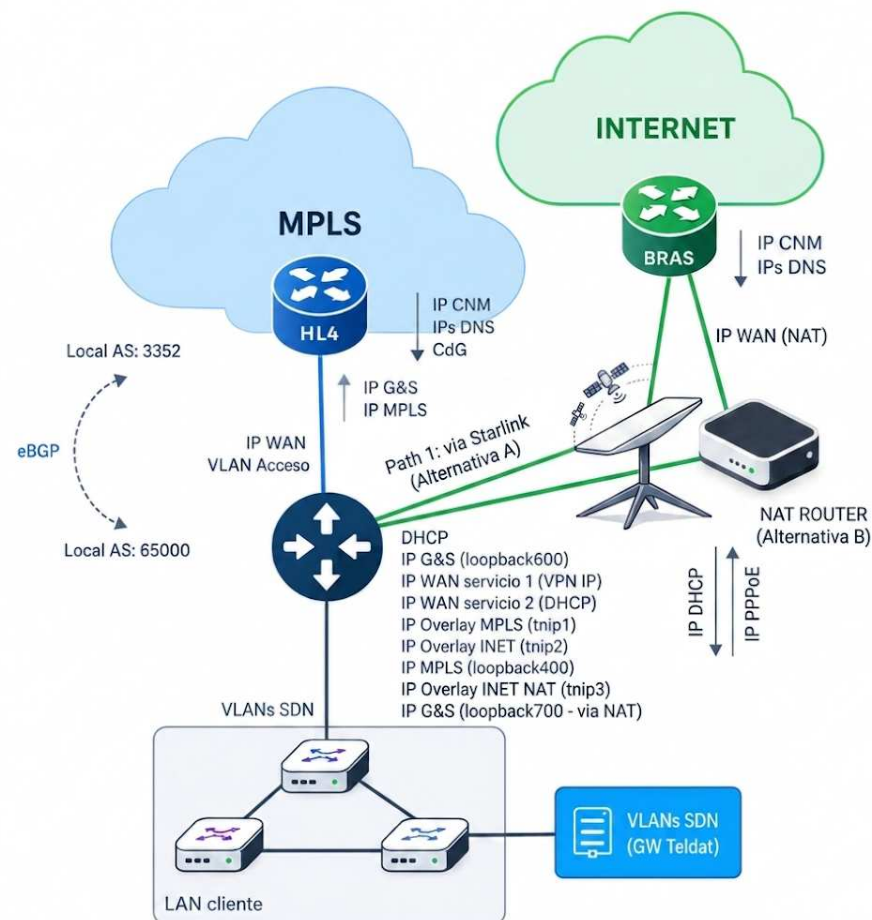
Inmunidad Física

Resistencia real de servicio frente a averías de un operador y cableado terrestre.



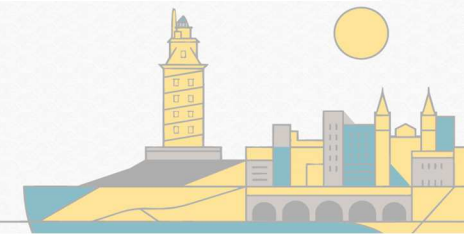
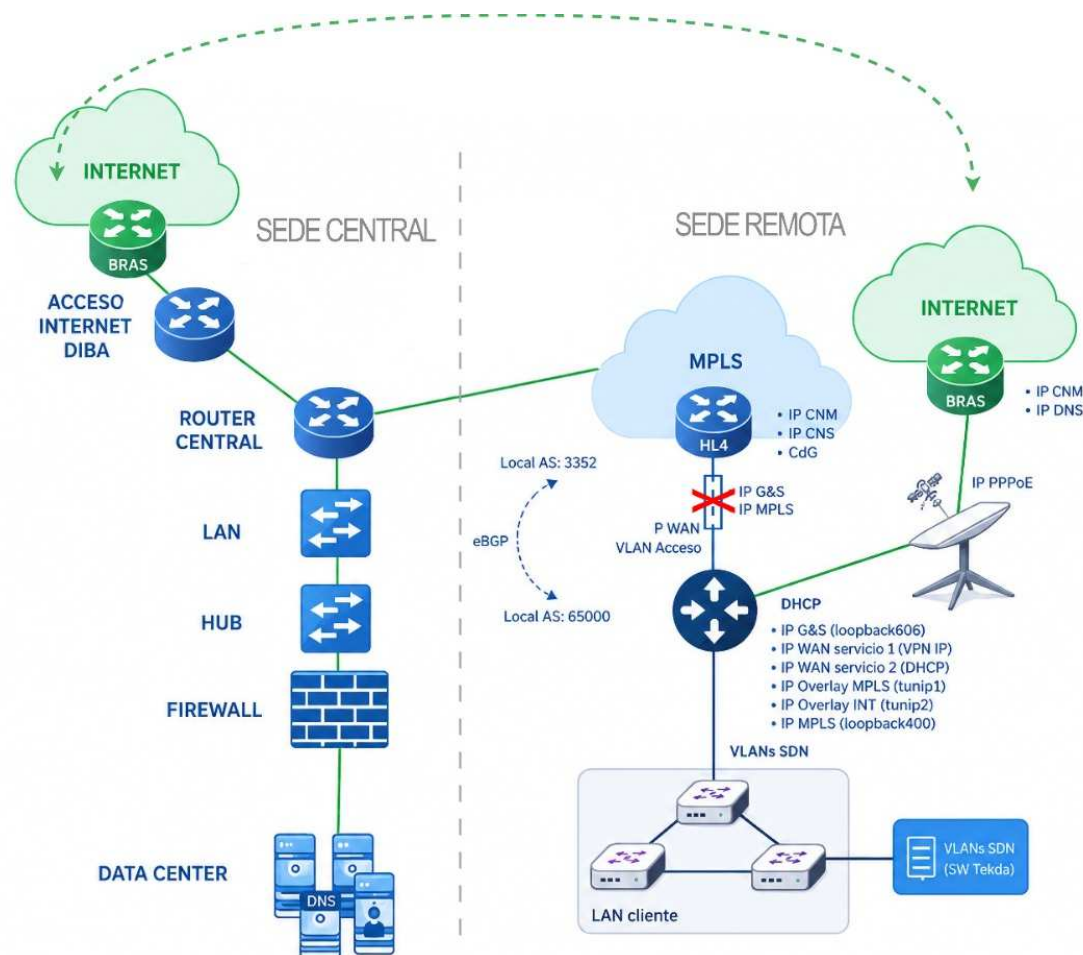
Integración con SD-WAN Teldat

- **Enlace principal (MPLS corporativa)**
 - Conexión directa por fibra óptica.
 - Enrutamiento dinámico (BGP)
 - Calidades de servicio (QoS)
- **Enlace respaldo (FTTH o Starlink residencial)**
 - Agnóstico de acceso.
 - Interconexión sencilla (DHCP, NAT)
 - Tunnelización IPsec automático.
- **Inteligencia de enrutamiento SD-WAN**
 - Enrutamiento el tráfico hacia una IP Pública.
 - Conmutación rápida.
 - Redimensionamiento acceso a internet principal.



SD-WAN enrutamiento inteligente

- **Modo normal**
 - Datos y gestión circulan por el enlace principal (WAN1)
- **Modo contingencia**
 - Conmuta todo el tráfico por la WAN2 (Tunel IPsec)
 - Se mantiene la monitorización y gestión de forma remota.



Un poco de publicidad

Preguntas

Eladio Maqueda Gil

Jefe de Sección de Sistemas

Área de Innovación y
Administración Digital

emaqueda@dip-badajoz.es

