C144/15-SV Programa Escuelas Conectadas

Solución Técnica Islas Baleares

30 de Julio de 2020

FICHA DEL DOCUMENTO

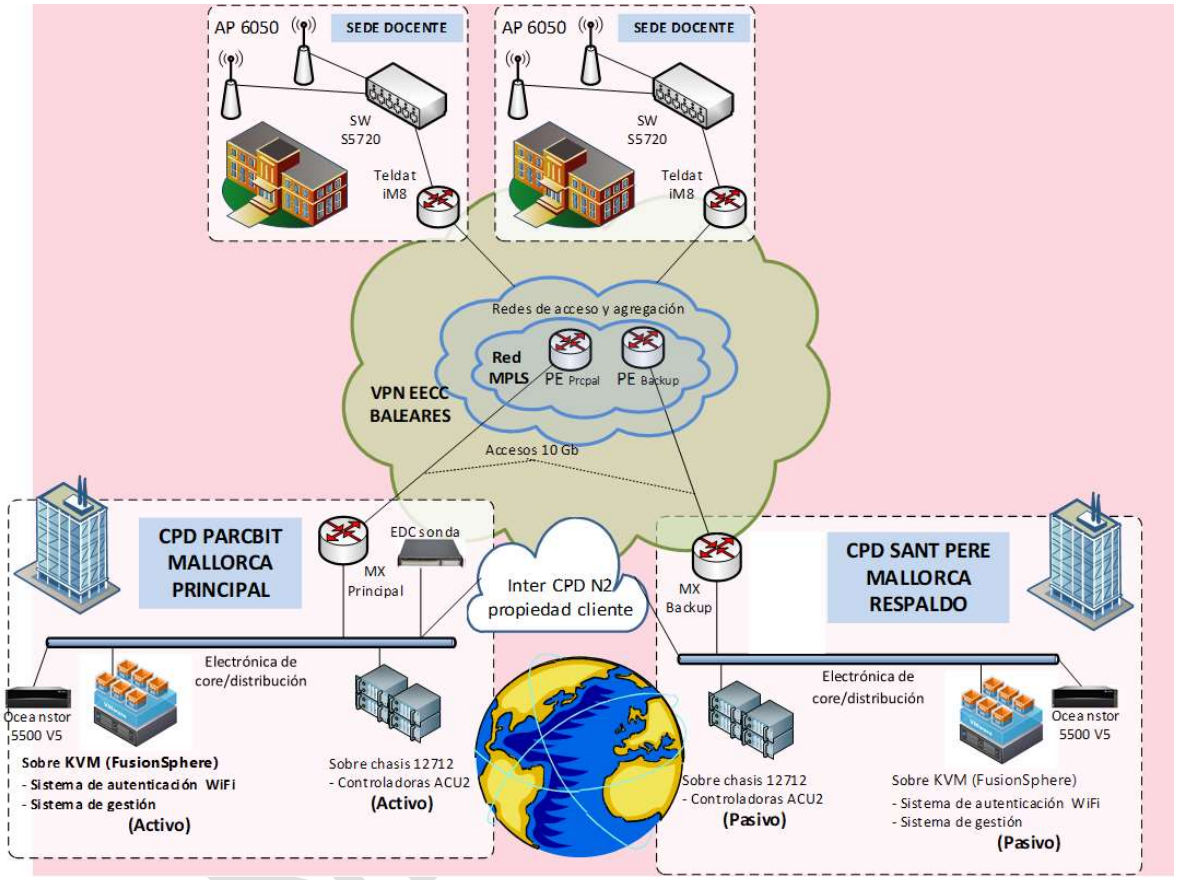
AUTOR:	Telefónica
APROBADO POR:	[Nombre] [Organización]
NOMBRE DEL DOCUMENTO:	PEC_CON_BAL_Solucion_Tecnica_Conectividad_Final.docx
CONTROL DE VERSIONES:	xx-xxx-xx⇒ PA_N [Comentarios / Comentarios / Comentarios / Comentarios / Comentarios / Comentarios / Comentarios / Comentarios / Comentarios / Comentarios] xx-xxx-xx⇒ PA_N [Comentarios] xx-xxx-xx⇒ PA_N [Comentarios]

ÍNDICE

1 DISEÑO GENERAL DE LA SOLUCIÓN

A continuación, se muestra un esquema donde se puede visualizar la solución técnica presentada por Telefónica tanto en el ámbito de las comunicaciones de datos como en el de WIFI:

SEDES DOCENTES PÚBLICAS



En lo que se refiere a las comunicaciones, todas las sedes docentes públicas a excepción de dos, alcanzan hasta un máximo de 990 Mb simétricos de Caudal Nominal (tanto ascendente como descendente), y el mismo valor para el Caudal Garantizado. En el esquema se aprecia que existirá una única VPNs para dar servicio a todas las sedes docentes públicas. El tráfico agregado de todos los centros docentes públicos se entrega en el CDP principal en condiciones normales, o en el CPD de Backup en caso de quedar indisponible el CPD principal. Cada CPD contará con un acceso troncal con su equipo terminal, y que actuarán en configuración de principal / backup.

Para el funcionamiento de la solución de alta disponibilidad entre ambos CPDs, hay configurada una interconexión a nivel 2 de varias VLANs entre la electrónica de ambos CPDs. Esta interconexión ha sido proporcionada por el Gobierno Balear y tiene un ancho de banda de 10Gbps compartidos con tráfico de servicio del propio Gobierno Balear.

Sobre estas comunicaciones se podrán seguir proporcionando todos los servicios que existen en la actualidad tales como el acceso a aplicaciones y recursos corporativos de la Comunidad Autónoma de las Islas Baleares, voz sobre IP, etc…

La salida a Internet pública será proporcionada por la Comunidad Autónoma de las Islas Baleares desde su CPD principal.

Respecto a la arquitectura WiFi, se diferencian dos escenarios:

- equipamiento en los CPDs
- equipamiento en las sedes docentes remotas

En cada CPD se implantarán las controladoras, la herramienta de gestión de la infraestructura y la herramienta de control de acceso que darán servicio a todas sedes docentes públicas de manera centralizada. Telefónica aportará al proyecto todas las prestaciones y todos los elementos hardware, software, accesorios y materiales necesarios para la implementación de las plataformas de gestión y autenticación objeto del proyecto.

REDUNDANCIA DE LA SOLUCIÓN PARA LAS SEDES DOCENTES PÚBLICAS

Independientemente del software que se ejecute sobre las máquinas virtuales que prestan el servicio, la redundancia de estas máquinas virtuales la ofrecerá el sistema de virtualización distribuido entre ambos CPDs.

En el caso de la **plataforma de gestión**, que está compuesto por 4 máquinas virtuales (3 colectoras y una consola) la redundancia en este caso la ofrecerá el sistema de virtualización distribuido entre ambos CPDs.

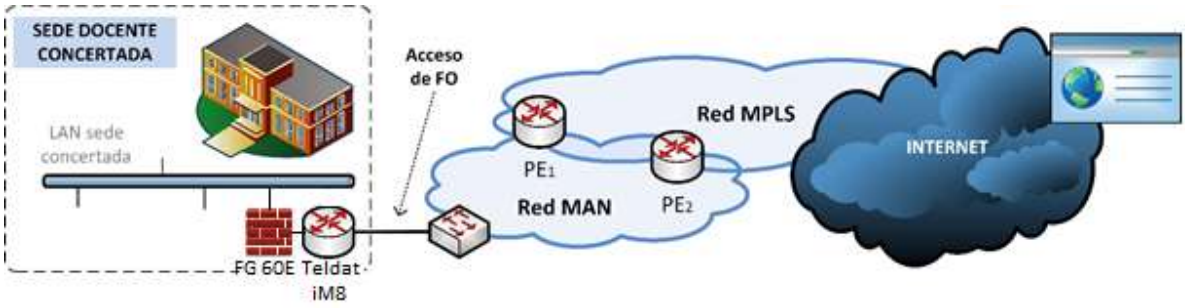
En el caso de la **plataforma de autenticación**, tenemos un clúster de 4+1 (4 máquinas en funcionamiento y una de backup) con las 5 máquinas activas en el CPD principal. La máquina de backup dará servicio en el caso de fallar alguna de las 4 principales. No obstante, en caso de fallo de CPD, las 5 máquinas levantarán en el CPD de backup por tener también la redundancia del sistema de virtualización distribuido.

De las 16 **controladoras**, las 8 que están en el CPD principal estarán dando servicio, y cada una de las 8 que hay en el CPD de backup dará redundancia a una de las 8 del CDP principal.

En cualquier caso, los sistemas de redundancia implementados consiguen que en caso de fallo hardware o software, el servicio se continúe dando con las prestaciones necesarias para que no haya discontinuidad del servicio que reciben los usuarios finales. En las sedes docentes estará desplegada la red de puntos de acceso conectados a los switches, que serán los que proporcionen la cobertura WiFi requerida.

SEDES DOCENTES CONCERTADAS

La conectividad directa de las ocho sedes concertadas a Internet seguirá un esquema como el presentado en la siguiente figura:



Todas las sedes docentes concertadas, a excepción de una, alcanzan hasta un máximo de 990 Mb simétricos de Caudal Nominal (tanto ascendente como descendente), y el mismo valor para el Caudal Garantizado.

Telefónica entregará las comunicaciones al switch principal pre-existente en cada una de las sedes docentes concertadas, mediante un interfaz de cobre 1GigaBit Ethernet RJ45.

El punto de entrega del servicio de acceso a Internet será la frontera entre el último equipo propiedad del operador que da el servicio y el switch principal pre-existente sede.

2 DESCRIPCIÓN TÉCNICA DE LA SOLUCIÓN

2.1 SOLUCIÓN DE COMUNICACIONES

A continuación, se describe la solución ofertada tanto para los CPDs como para las sedes docentes públicas y concertadas.

2.1.1 SOLUCIÓN DE LOS CPDs

Como se ha indicado anteriormente, en condiciones normales, el CPD principal de la Comunidad Autónoma de las Islas Baleares recibirá el tráfico agregado de todas las sedes docentes públicas. Cada CPD contará con 2 enlaces de 10Gb Ethernet en fibra óptica que conectará directamente con un equipo PE de la red MPLS de Telefónica (PE -> Provider Edge: router frontera de conexión con el núcleo IP/MPLS de la red de Telefónica). Cada pareja de estos enlaces terminará en un equipo de acceso independiente, de forma que el equipo y su acceso asociado en el CPD principal actuarán como conexión principal del servicio, y el equipo y la pareja de accesos asociados en al CPD de backup actuarán como conexión de backup del servicio. Por lo tanto, el modo de funcionamiento de las pajeras de accesos será activo/pasivo. Es decir, si los accesos del CPD principal están activos, los accesos del CPD de backup permanecerán operativos pero no cursarán tráfico porque éste será encaminado por los accesos principales. Si los accesos principales fallan, se encaminará tráfico por los accesos de backup hasta que se reestablezcan los enlaces principales.

Telefónica proporcionará conexión a nivel 3 a las sedes docentes descritas anteriormente. Se dispondrá un único ID-VPN para todos los centros, y la topología será full-mesh.

Los equipos de Telefónica instalados en cada CPD presentarán hacia la red de la Comunidad Autónoma de las Islas Baleares dos interfaces Ethernet 10 Gb de fibra óptica multimodo.

Los equipos utilizados para dar el servicio de comunicaciones en los CPDs son Juniper MX, y serán gestionados por Telefónica. Se trata de equipos propiedad de Telefónica, ya que son una extensión de su red, y por lo tanto no serán serigrafiados y podrán ser sustituidos si el crecimiento del tráfico del proyecto o la evolución de la red de Telefónica lo requieren. Las interfaces hacia cliente del equipo principal y el equipo de backup deberán conectarse a la misma vlan para poder implementar el protocolo VRRP como método para la conmutación del servicio en caso de fallo en el acceso o equipo principal.

Además de los routers Juniper MX, se instalará en cada CPD un servidor específico para realizar las medidas de puesta en marcha de las sedes remotas, recibiendo el tráfico de pruebas inyectado por los generadores de tráfico empleados en el transcurso de dichas pruebas. Adicionalmente se instalará en el CPD principal un router Teldat iM8 que servirán para recibir el tráfico de las sondas configuradas en los routers de las sedes remotas con el objetivo de recopilar la información necesaria para los informes periódicos de calidad de servicio.

Los equipos Juniper MX, el servidor de medidas y los routers receptores de las sondas forman parte de la solución de comunicaciones. En el CPD de Sant Pere, el router Juniper MX se instalará en un rack de comunicaciones. En el CPD de Parc Bit, el router Juniper MX, el servidor de medidas y el

router Teldat iM8 se instalarán en el rack donde se van ubicados el resto de los equipos de la solución Wifi. Todos estos equipos serán gestionados por Telefónica.

En los equipos EDCs Macrolan hemos definido varias VLANs:

- VLAN 1305 se utiliza para interconetar los EDCs con:
    - La sonda SLA, con la que se testean parámetros de calidad entre la sede central y las sedes remotas.
    - Los servidores de medidas de ancho de banda.
- VLAN 1306 se utiliza para la interconexión entre los EDCs y los switches de CPD (CE6856).

Estas VLANs tienen definidos grupos VRRP con IPs virtuales para obtener alta disponibilidad en caso de fallo del EDC principal o de las líneas WAN conectadas a él.

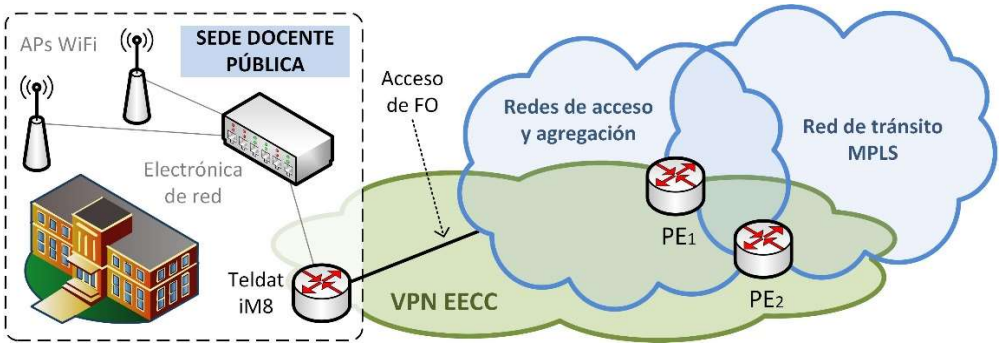
Para el encaminamiento del tráfico entre los usuarios de los centros y la red del Gobierno Balear se publica desde los EDCs de CPD la ruta por defecto hacia la red Macrolan del Gobierno Balear.

En condiciones normales de funcionamiento, el tráfico de usuarios una vez llega al EDC Macrolan principal, se enruta estáticamente hasta el switch de CPD CE6856_A por la VLAN 1305. Desde este switch el tráfico se balancea por las dos VLANs de interconexión (1307 y 1308) que hay definidas entre los switches de CPD y los Firewalls del Gobierno Balear. Este balanceo se consigue configurando dos rutas estáticas con mismo peso, una apunta a la IP del Firewall en la VLAN 1307 y la otra apunta a la IP del Firewall en la VLAN 1308. El tráfico una vez entregado al Firewall principal del Gobierno Balear, este se encarga de enrutarlo por la salida a internet.

Las dos VLANs de interconexión (1307 y 1308) están definidas por los dos enlaces que interconectan los switches de CPD WiFi con los switches de CPD del Gobierno Balear. Cada una de estas VLANs está bloqueada por uno de los dos enlaces de interconexión entre switch CPD WiFi (CE6856_A y CE6856_B) y los switches de CPD del gobierno Balear.

2.1.2 SOLUCIÓN DE LAS SEDES DOCENTES PÚBLICAS

A continuación, se muestra un esquema de las comunicaciones en cada sede docente. La propuesta plantea la utilización de fibra óptica para alcanzar los anchos de banda comprometidos:



El equipamiento empleado como equipo terminal del servicio de comunicaciones en las sedes es el Teldat iM8. Se trata de un potente router con capacidad de ejecutar aplicaciones gracias a una arquitectura hardware de doble núcleo y una arquitectura software de doble Sistema Operativo (tiempo real para el router y Linux para aplicaciones). De pequeño tamaño y no necesita ventiladores, con lo cual no genera ruido y puede instalarse en áreas de trabajo. Tiene potencia para servicios de hasta 1000 Mbps simétricos. Escalable gracias a un slot con una amplia variedad de tarjetas

Teldat iM8

Telefónica propone entregar el servicio mediante tres interfaces de 1Gb Ethernet RJ45 que se conectarán de la siguiente forma:

- Puerto 1: Conexión al switch Administrativo del centro
- Puerto 2: Conexión al nuevo switch Wifi del centro
- Puerto 3: Conexión al equipo de medida de Naudit

Panel trasero de un Teldat iM8

Al puerto 1 se asocia la vlan Administrativa con el direccionamiento IP correspondiente para cada centro, siendo la IP del router la primera IP de la red definida.

Los puertos 2 y 3 se asocian a la vlan de Interconexión, que hará de conexión punto a punto entre el router (puerto 2) y el switch Wifi (puerto 23). Por esta interconexión se enrutarán de manera estática las redes IP conectadas a este switch Wifi, y que son:

- Red Educativa
- Red Educativa Wifi
- Red de Gestión

En estos tres puertos las vlans definidas se configurarán para que no etiqueten el tráfico de red (modo acceso).

El puerto 3 del router se utiliza para la conexión de las sondas de medida. El router tiene configurado el servicio DHCP para que la sonda obtenga dirección IP al conectarse.

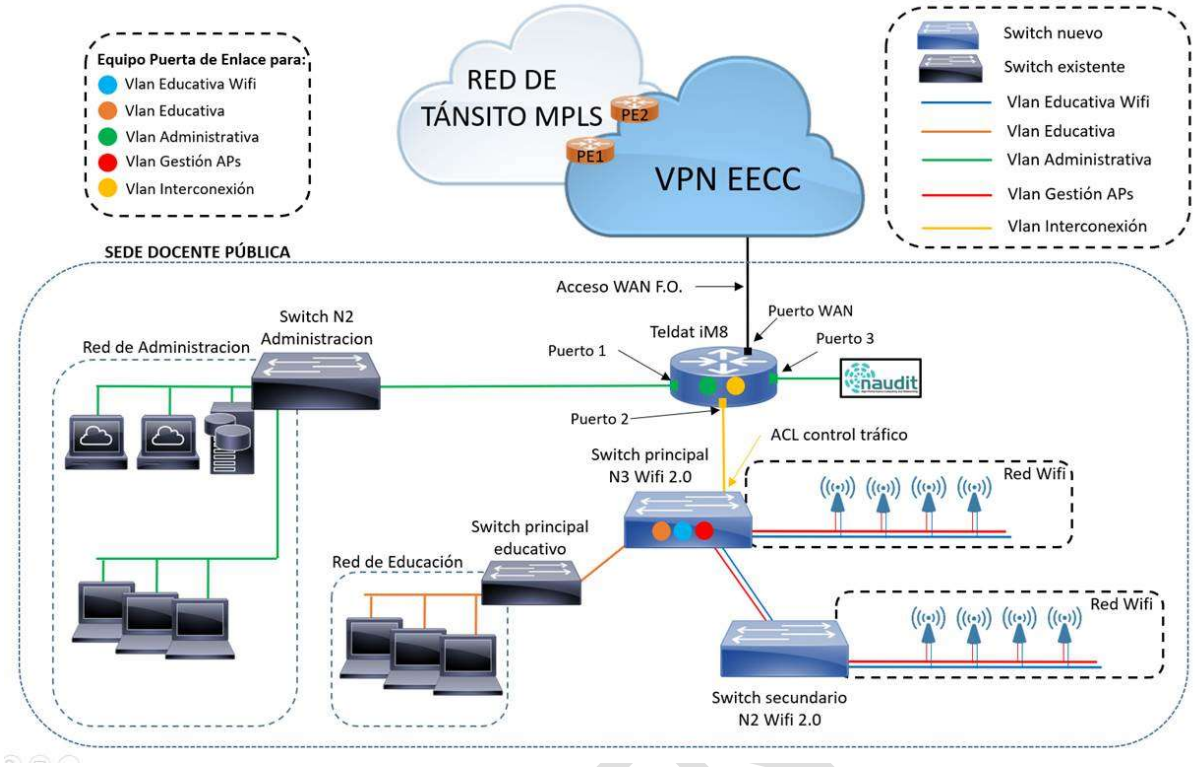
Como gestor del direccionamiento IP de cada sede docente pública, la Comunidad Autónoma de las Islas Baleares ha proporcionado direccionamiento para las siguientes VLANs:

- Vlan Educativa Wifi: Direccionamiento de red suficiente para asignar al volumen de dispositivos inalámbricos concurrentes que tenga previsto soportar.
- Vlan de Gestión: Direccionamiento de red suficiente para asignar a los dispositivos de red a instalar para soportar el nuevo servicio de conectividad Wifi (una IP por cada switch y por cada AP)
- Vlan de Interconexión: Direccionamiento de red suficiente para asignar IP al router de acceso y al switch principal Wifi y a una sonda de medida (red /29).
- Vlan Administrativa: Se reutiliza el direccionamiento ya existente en el centro o se asigna nuevo en caso de sede desdoblada.

El switch principal Wifi de la sede hace de servidor DCHP para los dispositivos de las redes Educativa, Educativa Wifi y de Gestión. Para la VLAN Administrativa la asignación de IPs será estática. La VLAN de interconexión tiene asignada IP estática en el router y el switch, no obstante para que la sonda obtenga IP hay configurado DHCP en el router.

El router de la sede tiene configurado hacia la WAN el protocolo de routing BGP para el anuncio de las redes del centro.

Para poder realizar las pruebas de conectividad una vez concluida la instalación de cada sede, se propone que la oficina técnica del programa de Red.es conecte su equipo de medida de Naudit al puerto 3 del router Teldat. El dispositivo obtendrá una IP automáticamente de la red de interconexión del centro.



Esquema de conexionado para una sede docente pública

Para la VLAN Educativa, el servidor DHCP sirve IPs de la segunda mitad de la red. Los DNS que sirve son 10.215.5.1 y 10.215.5.2.

Para la VLAN Educativa Wifi, el servidor DHCP sirve IPs de todo el rango exceptuando las 20 primeras IPs de la red. Los DNS que sirve son el 8.8.8.8 y el 8.8.4.4.

Para la VLAN de Gestión, el servidor DHCP sirve IPs de todo el rango exceptuando un número variable de las primeras IPs de la red, que será proporcional al tamaño de red asignado al centro. Para esta VLAN no se configuran servidores DNS.

En todas las VLANs, la primera IP del rango se asigna al equipo que tiene el rol de puerta de enlace de la VLAN. Para las VLANs Educativa, Educativa Wifi y de Gestión, la puerta de enlace es el switch principal Wifi, en el cual, se implementan listas de acceso para limitar el tráfico originado en las VLANs Educativa y WiFi según los criterios definidos en la siguiente tabla:

Origen	Destino	Acción
Red Educativa	Red Educativa (remota)	Denegar
Red Educativa	Red Wifi (remota)	Denegar
Red Educativa	Red Wifi (local)	Permitir
Red Educativa	Red Administrativa (remota)	Denegar
Red Educativa	Red Administrativa (local)	ACL
Red Wifi	Red Educativa (remota)	Denegar
Red Wifi	Red Educativa (local)	Permitir
Red Wifi	Red Wifi (remota)	Denegar

Red Wifi	Red Administrativa (remota)	Denegar
Red Wifi	Red Administrativa (local)	ACL
Red Administrativa	Red Administrativa (remota)	Denegar

Las reglas referidas a una "ACL" serán variables por cada centro en base a los servidores y las impresoras conectados a la red Administrativa que deban ser accesibles en cada uno de los centros.

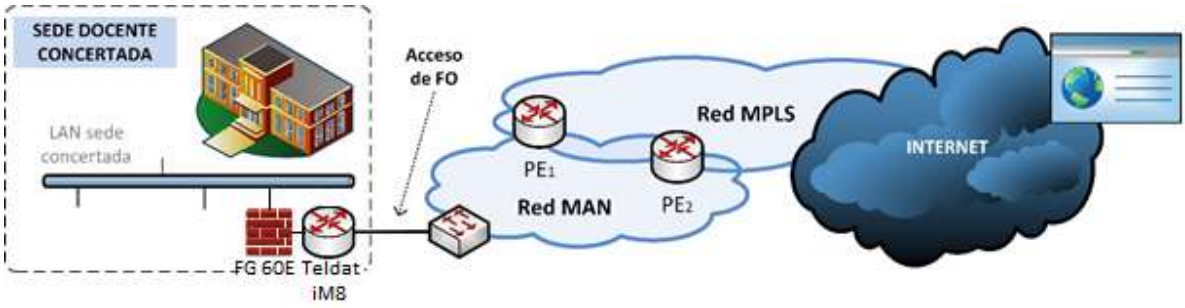
En el Router de cada sede se implementa una lista de acceso para denegar el tráfico hacia las redes Administrativas del resto de centros, a excepción del tráfico entre sedes que pertenecen al mismo centro.

ACL Para VLAN Educativa y WiFi	ACL para VLAN Educativa
regla 10 permite Net_Wifi_sede	regla 10 permite Net_Admin_sede
regla 20 permite Net_Educativa_sede	regla 20 permite Net_CI_10.216.254.0/26
regla 100 permite Impresora_1	regla 30 permite Net_CAIB_10.215.0.0/16
regla 105 permite Impresora_2	regla 50 deniega Net_Admin_10.216.0.0/16
regla 110 permite Impresora_3	regla 100 permite PERMIT_TODO
regla 115 permite Impresora_4	
regla 120 permite Server_DC	
regla 125 permite Server_proxy	
regla 130 permite Server_puppet	
regla 200 permite Net_CI_10.216.254.0/26	
regla 210 permite Net_CAIB_10.215.0.0/16	
regla 220 permite Agile_1	
regla 230 permite Agile_2	
regla 240 permite Agile_3	
regla 250 permite Agile_4	
regla 260 permite Agile_5	
regla 280 deniega Net_wifi_CPD	
regla 400 deniega Net_Admin_10.216.0.0/16	
regla 410 deniega Net_Edu_1_10.218.0.0/16	
regla 420 deniega Net_Edu_2_10.219.0.0/16	
regla 430 deniega Net_Edu_3_10.220.0.0/16	
regla 440 deniega Net_wifi_172.16.0.0/12	
regla 1000 permite PERMIT_TODO	

2.1.3 SOLUCIÓN DE LAS SEDES DOCENTES CONCERTADAS

El proyecto contempla la puesta en marcha de accesos directos a Internet para ocho sedes docentes concertadas. Estas sedes no se conectarán por tanto a la red privada virtual creada para las sedes públicas, ni tendrán comunicación con los CPDs ni con la red corporativa la Comunidad Autónoma de las Islas Baleares.

La solución propuesta se basa en el uso de accesos de fibra óptica y se muestra en el siguiente esquema:



El equipo terminal será "bundle" compuesto por un Firewall de la marcha Fortinet y modelo Fortigate 60E y un router marca Teldat y modelo iM8.

Este "bundle" terminal ofrecerá a una interfaz de cobre 1 Gb Ethernet RJ45 hacia la LAN de la sede. Adicionalmente se disponen de 4 interfaces más para utilizarse en caso de ser necesarias.

En este bundle, el Fortigate 60E hará las funciones de:

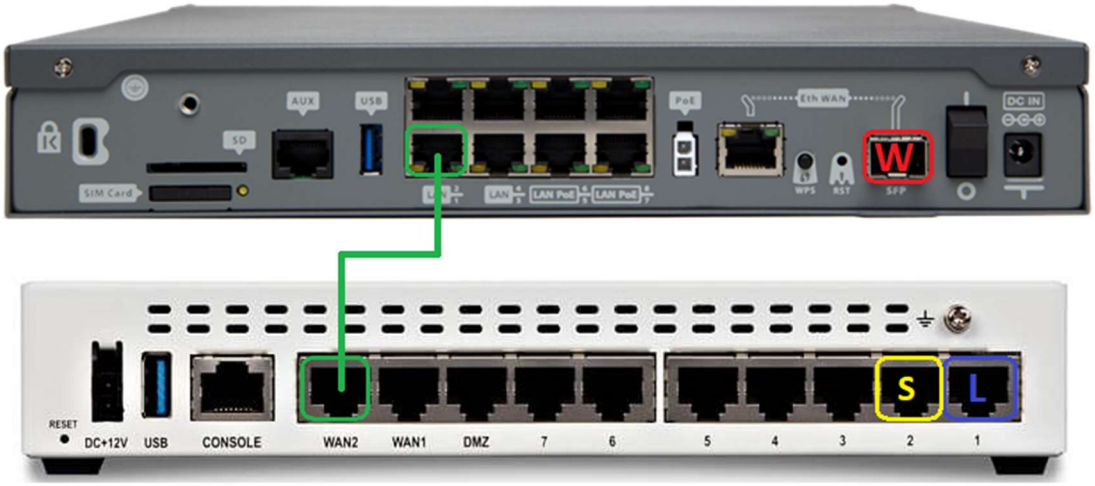
- NAT PAT entre el direccionamiento privado LAN del centro y el direccionamiento público reservado para la sede.
- NAT estático para publicar servicios hacia la WAN (en caso de requerirlo el centro)
- Servidor DHCP para los dispositivos LAN del centro (en caso de requerirlo el centro)

En este bundle, el Teldat iM8 hará las funciones de:

- Interconexión entre la red MAN de Telefónica y la sede
- Enrutamiento WAN contra la red MPLS de Telefónica

Esta pareja de equipos que forman el bundle se interconectará entre si mediante una interfaz ethernet de 1Gbps, quedando tal y como se muestra en la fi

gura:



Interconexiones del bundle formado por un Teldat iM8 y un Fortigate 60E

El detalle de los puertos utilizados:

- Puertos del 1 al 5 Fortigate: Punto de entrega del servicio
- Puerto 1 Fortigate: Conexión al switch principal del centro (etiqueta L)
- Puerto 2 Fortigate: Conexión al equipo de medida de Naudit (etiqueta S)
- Puerto WAN2 Fortigate: Interconexión contra el puerto 1 del Teldat iM8
- Puerto SFP Teldat iM8: Conexión WAN del centro con fibra óptica (etiqueta W)

A nivel de red, la interconexión entre los dos equipos del bundle se realizará mediante una única VLAN punto a punto con el mismo direccionamiento para todos los centros (195.76.102.0/30). Este direccionamiento de interconexión es público reservado por telefónica y no enrutado en internet, por lo que no supondrá ningún problema de solapamiento con los direccionamientos LAN de los centros.

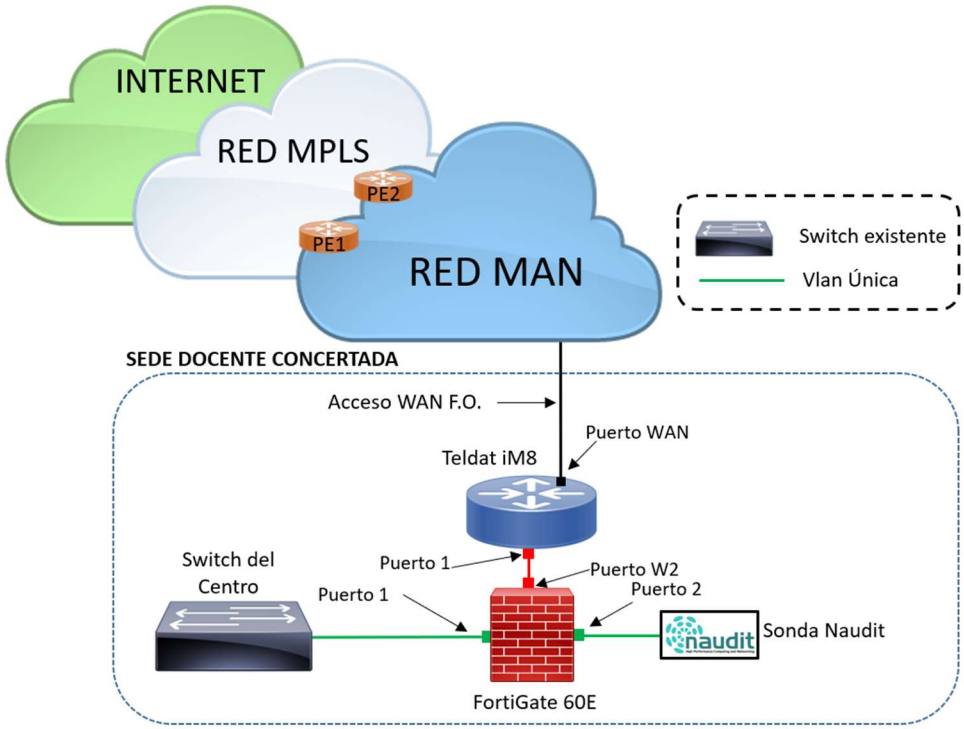
Para cada sede, el servicio provee una subred de 8 direcciones IP públicas estáticas para la navegación por internet del centro. Este direccionamiento, a priori, se asignará en un único pool para la navegación por internet de todos los dispositivos del centro. No obstante, si el centro requiere de la publicación del algún servicio en internet, se extraerá de ese pool una IP para la asignación estática del NAT para el servicio.

Telefónica se encargará de consultar con los responsables de red de cada uno de los centros los parámetros a configurar:

- Direccionamiento IP privado empleado en la sede
- Arquitectura (Redes directamente conectadas al equipo terminal vs Conexión a FW u otro equipo con capacidad de routing pre-existente)
- Enrutamiento hacia la LAN (protocolo de routing dinámico / enrutamiento estático / redes directamente conectadas)

- Si el servicio de DHCP lo realizará el propio equipo terminal o un equipo dedicado ya existente en la sede.
- Necesidad de realizar NAT estático para publicar algún servicio.

Al igual que en las sedes docentes públicas, para poder realizar las pruebas de conectividad una vez concluida la instalación de cada sede, se propone que la oficina técnica del programa de Red.es conecte su equipo de medida de Naudit al puerto 2 del Fortigate 60E. El Firewall Fortigate 60E proporcionará dirección IP automáticamente a la sonda para las pruebas.



Esquema de conexionado para el bundle “Fotigate 60E - Teldat iM8”

2.1.4 DESCRIPCIÓN DEL SERVICIO VPN SOBRE MPLS

El servicio de comunicaciones que Telefónica ofrece para el Proyecto de Escuelas Conectadas, permitirá que se sigan prestando sobre los centros educativos públicos todos los servicios que se dan en la actualidad y que se detallan a continuación:

- Acceso a Internet a través de la conectividad de la Comunidad Autónoma de las Islas Baleares que tiene en los CPDs.
- Acceso a contenidos y servicios en los CPDs
- Videoconferencia
- Tráfico de gestión/monitorización
- Gestión remota de la infraestructura de las sedes

Telefónica garantiza que el servicio de conectividad, tanto en subida como en bajada, cumple con los parámetros establecidos en el pliego:

- Pérdida de paquetes inferior o igual al 1%
- Latencia extremo a extremo inferior o igual a 100ms
- Jitter inferior o igual a 50 ms

Para la solución propuesta, Telefónica ha definido una única case de servicio dentro de la RPV, de modo que todo el tráfico generado por cada una de las sedes tendrá el mismo tratamiento en la red.

A esta calidad de servicio se le asignará el total del ancho de banda definido para cada sede.

2.1.5 EQUIPO TERMINAL

El equipo terminal de la sede docente tiene la función de realizar la conexión entre la LAN y el acceso al servicio de conectividad. El modelo propuesto es el router Teldat iM8, que cumple con las características técnicas exigidas en el pliego.

El equipo terminal de cada sede será gestionado por Telefónica

El equipo terminal del servicio de conectividad de cada sede se podrá integrar, de ser necesario, con los sistemas de monitorización y gestión de la Comunidad Autónoma de las Islas Baleares.

2.1.6 SEGURIDAD DE LAS COMUNICACIONES

Telefónica dispone de un documento de Normativa Corporativa de la Seguridad que es de aplicación en todas las fases del ciclo de vida de la información (generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción) y en las infraestructuras (sistemas y redes) que la procesan (análisis, diseño, desarrollo, implantación, explotación y mantenimiento), y tiene como marco de referencia las siguientes normas:

- ISO/IEC 27001:2005 -> Requisitos para implantar un SGSI
- ISO/IEC 27002:2005 -> Controles para implantar un SGSI
- ISO/IEC 27005:2008 -> Criterios para análisis de riesgos
- ISO/IEC 18028-1(2,3,4 y 5):2006 -> Criterios recomendables en la gestión de redes de comunicaciones
- ISO/IEC 24762:2008 -> Criterios recomendables para los planes de contingencia y recuperación
- ISO/IEC 20000-2:2005 -> Criterios recomendables de seguridad en la gestión de servicios TI
- PCI DSS v1.2. PCI Data Security Estándar
- BS 25999-1(2):2006(2007) -> Controles para implantar la Continuidad de Negocio
- Sarbanes-Oxley Act of 2002 (SOX)

La Normativa Corporativa de Seguridad de Telefónica ofrece un control y gestión de la seguridad de características similares a la ISO 27001.

La gestión y operativa en los desarrollos en red se basan en un modelo SGSI. La gestión de la seguridad de la red incluye un conjunto de principios o políticas sobre los objetivos y activos que se deben proteger. Igualmente el despliegue de nuevos servicios en la red o servicios de clientes sustentados en la red es gestionado mediante un proceso de análisis de riesgos en la red. Los equipos de la red son inventariados y auditados a nivel de seguridad mediante herramientas internas de Telefónica. Esto incluye especificar requisitos de seguridad en los activos, en el diseño y en la implementación de controles de seguridad en la red y sus dispositivos, ejecutar auditorías y test de penetración, por último los informes y resultados son sometidos a revisión para su evolución.

A continuación se describen los controles de seguridad que se aplican en la red de acuerdo a lo establecido en la ISO 27002:

- Política de Seguridad de la Información
- Organización de la Seguridad de la Información y Seguridad en los accesos de terceras partes
- Responsabilidad sobre los Activos y Clasificación de la información
- Seguridad de los Recursos Humanos
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Adquisición, desarrollo y mantenimiento de sistemas de la información
- Gestión de los incidentes de seguridad de la información
- Gestión de continuidad del negocio
- Cumplimiento de los requerimientos legales de las revisiones de la política y estándares de seguridad y de la conformidad técnica, y de las consideraciones sobre la auditoría de sistemas