UNIVERSITAT POLITÈCNICA DE VALÈNCIA

_ TELECOM ESCUELA TÉCNICA VLC SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería de Telecomunicación

DESPLIEGUE DE UNA NUEVA SOLUCIÓN DE RED PARA TIENDAS, OFICINAS Y ALMACENES DE UNA MULTINACIONAL

Trabajo Fin de Grado

Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación

AUTOR/A: González Martín, Luis Carlos

Tutor/a: Rodríguez Hernández, Miguel Ángel

CURSO ACADÉMICO: 2021/2022

Resumen

En el entorno corporativo la tecnología cumple un rol fundamental. La constante evolución de la misma hace menos predecible un escenario en el que las buenas decisiones resultan claves para el futuro de la empresa. Hoy, en la multinacional en la que está basado este trabajo, los patrones de tráfico han cambiado con la introducción de aplicaciones moviéndose a la nube y para ello es muy importante enrutar de manera más inteligente dicho tráfico y dotar a la red de flexibilidad, seguridad, autonomía y monitorización. En este caso, la virtualización de la red toma un papel protagonista y, más aún, con vistas a un futuro de interconectividad a partir del mencionado IoT (Internet de las cosas).

El objetivo de este trabajo es: llevar a la práctica los procesos de configuración de la nueva solución SD-WAN (Topología redundante, Reglas de Firewall a nivel de la Capa de Red y de Aplicación, VPNs, entre otros) y el dimensionamiento de la WLAN a través de dispositivos capaces de brindar conectividad en el estándar de Wi-Fi 6 (Documentación del mismo) considerando los procesos de negociación con proveedores y la correcta animación a los equipos técnicos para asegurar el proyecto tal y como había sido planificado.

Palabras clave: MPLS, SD-WAN, Meraki, Wi-Fi 6, Firewall.

Resum

En l'entorn corporatiu la tecnologia compleix un rol fonamental. La constant evolució de la mateixa fa menys predictible un escenari en el qual les bones decisions resulten claus per al futur de l'empresa. Hui, en la multinacional en la qual està basat aquest treball, els patrons de trànsit han canviat amb la introducció d'aplicacions movent-se al núvol i per a això és molt important enrutar de manera més intel·ligent aquest trànsit i dotar a la xarxa de flexibilitat, seguretat, autonomia i monitoratge. En aquest cas, la virtualització de la xarxa pren un paper protagonista i, més encara, amb vista a un futur d'interconnectivitat a partir de l'esmentat IoT (Internet de les coses).

L'objectiu d'aquest treball és: portar a la pràctica els processos de configuració de la nova solució SD-WAN (Topologia redundant, Regles de Firewall a nivell de la Capa de Xarxa i d'Aplicació, VPNs, entre altres) i el dimensionament de la WLAN a través de dispositius capaços de brindar connectivitat en l'estàndard de Wi-Fi 6 (Documentació del mateix) considerant els processos de negociació amb proveïdors i la correcta animació als equips tècnics per a assegurar el projecte tal com havia sigut planificat.

Paraules clau: MPLS, SD-WAN, Meraki, Wi-Fi 6, Firewall.

Abstract

In a corporate environment, the constant evolution of technology establishes a non-predictable scenario in which good decisions are essential to define the future of the company. Today, at the multinational corporation on which this work is based, traffic patterns have changed due to applications moving to the cloud, and because of this, it is very important to intelligently direct traffic across the WAN and improve the network in terms of flexibility, security, autonomy, and observability. In this manner, the virtualization of the network takes on a leading role and, even more so, with future perspectives for IoT (Internet of Things) interconnectivity.

The objective of this work is: to put into practice the configuration processes of the new SD-WAN solution (Redundant Topology, Firewall Rules at the Network and Application Layers, VPNs, among others) and the dimensioning of the WLAN through devices capable of providing connectivity in the Wi-Fi 6 standard (Documentation of the dimensioning) considering the negotiation processes with suppliers and the correct guidance of the technical teams to ensure the project as planned.

Keywords: MPLS, SD-WAN, Meraki, Wi-Fi 6, Firewall.

Índice

1. Introducción

Una multinacional ha basado su red en una WAN tradicional que interconectaba sedes de forma privada en los últimos 15 años. De esta forma, a través de una red MPLS la empresa ha podido garantizar una conectividad fiable y segura entre sus sedes y aplicaciones alojadas en servidores en data centers "On Premise" de la propia empresa.

En paralelo a este hecho, la transformación tecnológica y la necesidad de procesado de datos han hecho que las sedes hayan empezado a utilizar aplicaciones alojadas en la nube. El tráfico de datos se ha volcado a Internet en prácticamente un 90%. Con esta situación, las sedes han empezado a sufrir saturación como consecuencia de las limitaciones que empieza a presentar la MPLS con este uso de la red.

Ante tal situación, la empresa ha decidido dejar de trabajar con la topología de red que tan buenos resultados había traído en los últimos años y optar por una nueva solución de red, con todo lo que eso conlleva a nivel de una multinacional. En este contexto, este Trabajo de Fin de Grado encuentra su motivación en exponer la transformación que requiere dicha multinacional (en la que ha realizado sus prácticas curriculares Luis Carlos González Martín) a nivel de red y todos los procesos que debe planificar y luego verificar para finalmente desplegar de forma masiva.

1.1 Objetivos

En esta sección se presentan los objetivos generales de este trabajo, de manera que sirva como guía para leer y entender su desarrollo y conclusiones finales. Dichos objetivos son los siguientes:

- Aprender la teoría sobre la arquitectura de la red mediante el estudio de la misma para así poder compararla con la arquitectura aplicada a nivel corporativo.
- Exponer todas las limitaciones que presenta la arquitectura actual para la empresa.
- Definir las ventajas y desventajas de SD-WAN en comparación con la MPLS.
- Exponer todo lo que conlleva un despliegue masivo de una nueva solución de red no sólo desde el punto de vista técnico sino también desde el lado organizacional de un ingeniero.
- Mostrar a modo de ejemplo, la tecnología que verifica el funcionamiento de la nueva solución antes planteada de manera teórica.

1.2 Estructura

Este Trabajo de Fin de Grado sigue la siguiente estructura:

Capítulo 1. Introducción al trabajo. Se plantea la necesidad y los objetivos a desarrollar en él. Se deja claro la metodología de trabajo seguida para poder llevarlo a cabo.

Capítulo 2. Contexto actual y sus limitaciones. Parte teórica que explica la tipología de red que luego se ve ejemplificada por la arquitectura actual de la empresa.

Capítulo 3. Solución SD-WAN. Parte teórica que explica la nueva tipología de red y los cambios que ella conlleva.

Capítulo 4. Meraki SD-WAN. Se presenta la nueva solución de red escogida y sus características más importantes con respecto a la red WAN tradicional.

Capítulo 5. Nueva solución de red planteada. Aquí se desarrollan los cambios en la arquitectura de la red de la empresa y las nuevas configuraciones a nivel WAN y LAN.

Capítulo 6. Primeras pruebas (Laboratorio). Por primera vez se entra en contacto con la tecnología de la solución de red escogida. Se dan los primeros pasos necesarios antes de pensar en un despliegue. Se realiza diseño tanto a nivel LAN como WLAN.

Capítulo 7. Reuniones con proveedores y pruebas piloto. Después de realizar las primeras pruebas, se establecen comunicaciones con los proveedores de acceso a Internet para proponer pruebas piloto. Se desarrolla la primera prueba en una sede.

Capítulo 8. Conclusiones y próximos pasos. Luego de las pruebas y sedes piloto necesarias, la empresa está lista para migrar de forma masiva. Se plantean las conclusiones más importantes de este trabajo.

Capítulo 9. Bibliografía. Referencias de las fuentes de las citas de texto y figuras.

1.3 Metodología

Para la realización de este trabajo, se siguió una metodología que abarcó el tiempo de 4 meses de prácticas en la empresa a la que refiere este despliegue.

- Estudio de la teoría: La primera tarea ha sido la de estudiar gran parte de la rama de telecomunicaciones referida a las redes telemáticas y las comunicaciones. Esta parte se ha tomado como un reto, dado que el estudiante ha decidido optar por asignaturas de la rama de Sistemas de Telecomunicaciones en los últimos cursos del grado.
- Entender la tipología de red de la empresa. Parte fundamental para aplicar la teoría a un caso real de una multinacional. Esta era la única forma de entender la necesidad de migrar a una nueva solución de red.
- Contacto con los equipos impactados por el desempeño de la red. De esta forma se podía visualizar el contexto actual y las necesidades/ventajas existentes. Con vistas a ser ingeniero, esta visión del contexto es fundamental antes de tomar cualquier tipo de decisión o proyecto.

- Estudio y aplicación de la nueva solución. Así como se ha mencionado en el punto anterior, este punto es fundamental para entender la nueva tecnología, la inteligencia detrás de ella, y todas las consecuencias positivas que traería a la empresa.
- Propuestas de diseño e implementación basados en la nueva tipología. Aquí entra en vigor la importancia del trabajo, pues se ve el aporte real del estudiante.

2. Contexto actual y sus limitaciones

2.1 Red MPLS

La Conmutación de Etiquetas Multiprotocolo o Multiprotocol Label Switching (MPLS) “is a networking technology that routes traffic using the shortest path based on labels, rather than network addresses, to handle forwarding over private wide area networks” [1] En otras palabras, es una técnica en la cual los datos que son transmitidos llevan un encabezado incorporado, de forma que son reenviados por los enrutadores según el tipo de operación para la cual están destinados, en lugar de requerir búsquedas complejas en una tabla de enrutamiento en cada parada hasta llegar a su destino.

La configuración de la cabecera consiste en:

- Label (20 bits): Valor de etiqueta MPLS.
- Traffic Class (3 bits): Identifica la clase de servicio.
- Stack (1 bit): Si este valor es 0, significa que hay más etiquetas añadidas al paquete. Si el valor es 1, significa que es la última etiqueta del “stack”.
- TTL (8 bits): Tiempo de vida.

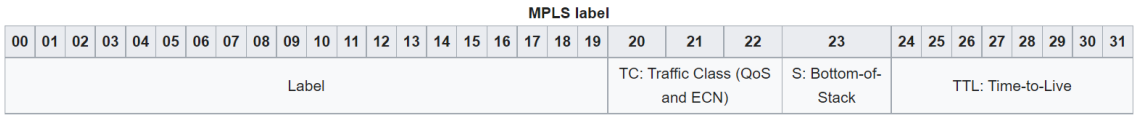


Figura 1. Cabecera MPLS. [2]

Una red MPLS opera entre la capa 2 y la capa 3 del conocido modelo OSI [3], es decir, entre la capa de enlace de datos (transporta tramas de datos entre dispositivos de una misma LAN) y la capa de red (utiliza direccionamiento y enrutamiento de internet a partir de protocolos IP). La mencionada conmutación por etiqueta proporciona a las redes IP el poder cursar tráfico con diferentes grados de calidad de servicio (QoS). Para ello, la red MPLS está compuesta principalmente por dos tipos de routers/switches o nodos:

- Enrutadores Conmutadores de Etiqueta (LSR): Nodos que se ubican en el medio de la red MPLS y efectúan el enrutamiento basado únicamente en las etiquetas de los paquetes. Los LSR emplean su funcionamiento tanto en el plano de control como en el plano de datos.
- Enrutadores de borde de Etiqueta (LER): Son los puntos de entrada/salida de la red MPLS desde otras redes, encargados de incorporar o extraer la cabecera a cada paquete.

De esta forma, las etiquetas MPLS se establecerán teniendo en cuenta las tablas de encaminamiento que los nodos MPLS contienen y que comparten a través de protocolos

de encaminamiento estándar al igual que sucede en routers IP “comunes”. Al establecerse dichas etiquetas, también se establece el LSP o Intercambio de rutas por Etiqueta, que no es más que el camino unidireccional de tráfico a través de la red MPLS. Así, un LER clasifica y etiqueta un paquete IP entrante a la red, definiendo el LSP que debe seguir dicho paquete a lo largo de la red considerando su IP de destino y su QoS. El LER entonces envía el paquete a un LSR ubicado en el núcleo de la red, que determinará el siguiente nodo al que debe ser enviado a partir de la conmutación por etiqueta. En caso de tratarse de un paquete que debe salir de la red MPLS, es decir, que debe ser enviado a un LER, el LSR extrae la cabecera de la MPLS antes mencionada.

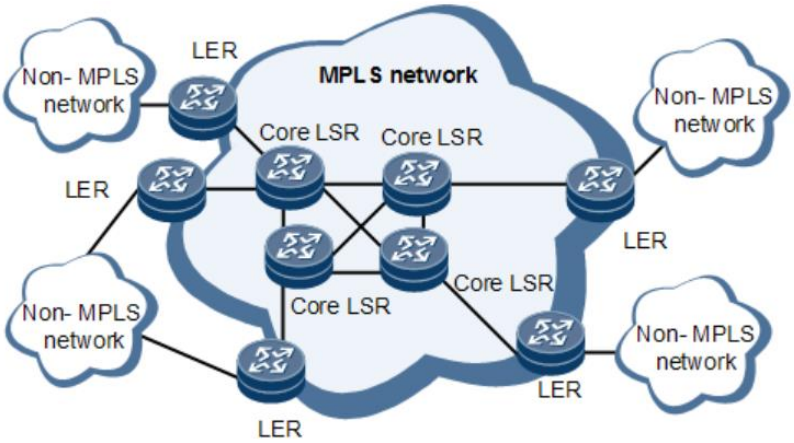


Figura 2. Red MPLS. [4]

Organizaciones y empresas utilizan esta tipología de red cuando tienen múltiples sucursales o “branch offices” remotas que necesitan acceso a un centro de datos o a ciertas aplicaciones que se pueden alojar tanto en estos centros de datos, como en otra sucursal, como en sus oficinas corporativas o “Headquarters”. En este sentido, la MPLS permite a las empresas beneficiarse de una solución que es: escalable, capaz de posibilitar redes virtuales privadas basadas en IP (VPN), que proporciona un mejor rendimiento y ancho de banda al ser una red privada, y también segura ya que se basa en circuitos dedicados/privados. En la siguiente figura 3, se ejemplifica esta privacidad que provee una red de este tipo: Dos clientes independientes A y B se conectan vía VPN a través de circuitos separados, por lo tanto, los enlaces rojos están aislados para el cliente A y los enlaces azules están aislados para el cliente B.

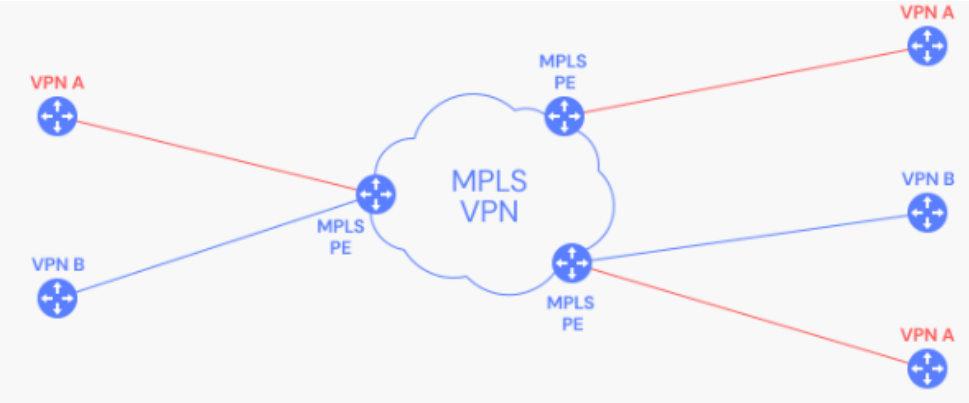


Figura 3. Conexiones de clientes A y B con MPLS. [5]

Para un proveedor de servicios de Internet (ISP) resulta más que viable el utilizar la MPLS como una forma de aislar el tráfico y así ofrecer un servicio de VPN acorde para sus clientes. Aun así, deberán garantizar la securización de los datos a través de firewalls o cortafuegos y de protocolos de encriptación de las comunicaciones como por ejemplo IPsec o SSL.

A nivel de arquitectura de la red, como se ha mencionado anteriormente, WAN tradicionales como la MPLS están diseñadas en torno a esta construcción: las empresas deben transportar todo el tráfico desde sus distintas ubicaciones a un centro de datos centralizado, donde se alojan las aplicaciones a las que cada sede pretende acceder. Y es en esta construcción donde empiezan a verse las limitaciones de la MPLS con la realidad "cloud" del mundo actual, ya que el tráfico que va desde las sedes a través de la red de retorno o "backhaul" pasa por las HQ o un centro de datos centralizado antes de acceder al entorno "cloud" o antes de acceder a Internet.

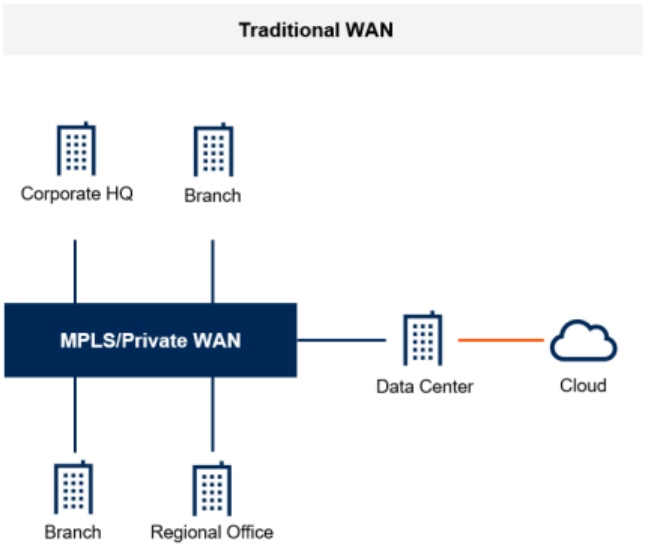


Figura 4. WAN tradicional. [6]

2.2 Red de la empresa actualmente

La red MPLS suele ser entonces un servicio subcontratado, gestionado por proveedores de servicios que garantizan el rendimiento, la calidad y la disponibilidad de la red. El mantenimiento de esta red y todas sus ventajas vistas anteriormente, conllevan un gran gasto económico para las empresas. Y este es el caso de la empresa en la que está basado este trabajo, cuya arquitectura de red veremos a continuación. Podemos observar en la figura 5, cómo las diferentes sedes son capaces de conectarse a dos centros de datos "on Premise" a partir de una red MPLS y mediante túneles VPN. Confirmamos entonces que se implementa la MPLS como una solución IP sobre FastEthernet para conectividad con uno de los centros de datos y sobre GigabitEthernet para el otro, cuya gestión y mantenimiento depende de un proveedor de servicios de Internet.

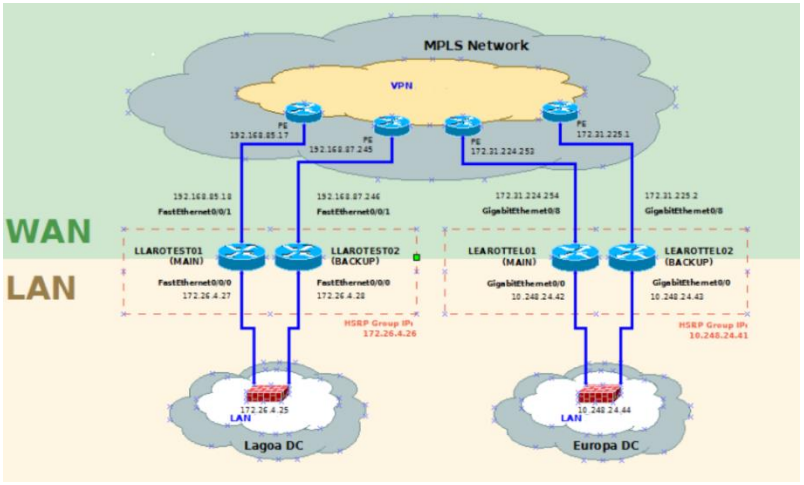


Figura 5. Arquitectura de conexión de la empresa con sus centros de datos.

Con esta tipología de red, la empresa ha podido garantizar una conectividad fiable y segura entre sus sedes en los últimos 15 años. Pero, a día de hoy, los escenarios y necesidades de conectividad en la multinacional han cambiado notablemente:

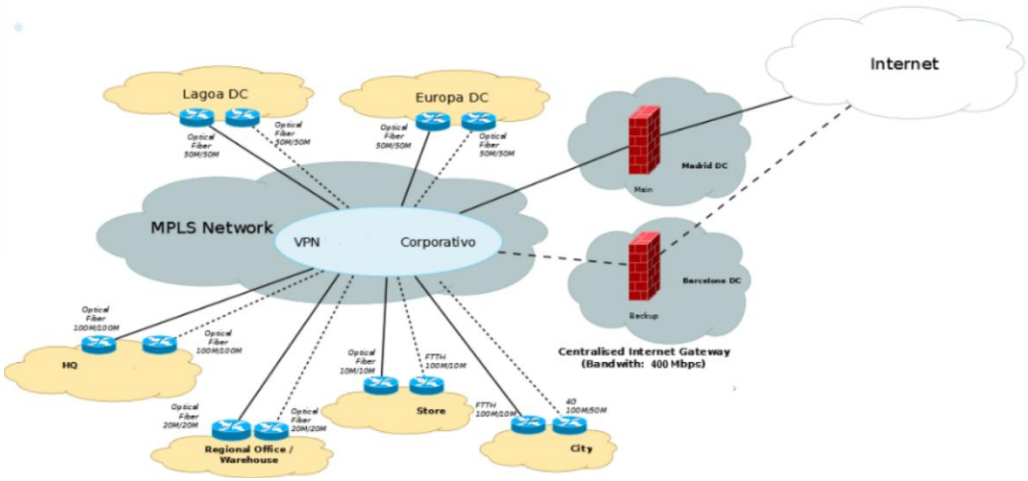


Figura 6. Arquitectura de red de la multinacional en España.

La realidad es que el auge de la computación en la nube o "cloud computing" ha roto los paradigmas tradicionales para los que se diseñó la MPLS. Comunicaciones con el entorno cloud requieren del mencionado backhauling de tráfico vinculado a Internet, y considerando que en un principio la MPLS fue diseñada para conectividad site-to-site dentro de la misma empresa, el desempeño de la red puede verse afectado negativamente con aplicaciones de tipo Saas (Software-as-service) como lo son Google Workspace u Office 365 y que hoy representan grandes volúmenes de tráfico en el entorno empresarial. Con lo cual, nos encontramos con una tipología de red que hoy presenta un bajo rendimiento y una mala experiencia de usuario con la conectividad al entorno de la nube. Esto lo ha empezado a notar la empresa en alguna de sus sedes, ya que comprobando el uso que se hace de la red, más del 80% del tráfico que sale actualmente de sus sedes está destinado a Internet. Teniendo en cuenta que, debido a la arquitectura presentada, el encaminamiento se hace de forma tal que la salida a Internet pasa por un punto centralizado, las sedes han comenzado a sufrir una mala experiencia de conectividad debido a saturación como consecuencia del ancho de banda limitado a través de la MPLS. Produciéndose lo que se conoce coloquialmente como un "cuello de botella".

Por otro lado, y como consecuencia de estas mismas limitaciones que presenta la MPLS con respecto al tráfico cursado hoy en las sedes, la empresa se vería obligada a contratar una conectividad MPLS con un ancho de banda pensado para el peor caso de volumen de tráfico que pueda experimentar. Lo que significa que, en muy buena parte del tiempo, hay un ancho de banda (económicamente costoso) que no se está utilizando. La falta de visibilidad y capacidad de entendimiento del tipo de tráfico cursado, le imposibilitan el hecho de poder modificar dinámicamente ajustes en la red de forma adecuada. Este hecho perjudica a las sedes de la empresa, ya que se hace un gran uso de la red para aplicaciones de voz y de video, y mientras que todo el tráfico cursado por la red necesita de ancho de banda para funcionar, estas dos aplicaciones tienen requerimientos de latencia que necesitan ser monitorizados de forma constante para garantizar una QoE (calidad de la experiencia) conforme a los estándares actuales. Sin embargo, la realidad es que cuando múltiples aplicaciones son encaminadas bajo el mismo caudal, el tráfico que requiere baja latencia se verá afectado si la red no es capaz de priorizarlo.

Por lo tanto, hoy vemos que las conexiones de tipo MPLS resultan ser rígidas o fijas y que no se pueden adaptar tan fácilmente al tipo de interconectividad dinámica que las redes de las sedes de la empresa hoy requieren. Tampoco están capacitadas para proveer a la red de reconocimiento de tráfico según las aplicaciones ni de un manejo sofisticado del ancho de banda para priorizar tráfico o aplicaciones con requerimiento de baja latencia. Pero, más aún, no responden a un principio básico en el uso que se les da a las redes hoy en la empresa, y es que enviar tráfico de tipo "cloud" desde una sede (que está destinado a Internet) de vuelta a los HQ, no tiene sentido: añade retardo, deteriora el rendimiento de la aplicación y consume mucho ancho de banda de la línea dedicada. La pregunta que nos planteamos en este trabajo a partir de aquí es la siguiente: ¿Por qué no utilizar Internet directamente para llegar a aplicaciones que están alojadas en Internet? Sabiendo que hoy las aplicaciones están siendo alojadas en múltiples entornos "cloud"

distribuidos en lugar de en un centro de datos centralizado. Para ello, necesitamos de un modelo dotado con “inteligencia” de software, y esa es la respuesta que buscamos conseguir en este trabajo.

3. Solución SD-WAN

Software-Defined WAN o SD-WAN es una tecnología que distribuye el tráfico por redes de área amplia (WAN) y que utiliza conceptos de redes definidas por software (SDN) para determinar la manera más efectiva de enrutar dicho tráfico. Las SDN "representan un enfoque en el que las redes utilizan controladores basados en software o interfaces de programación de aplicaciones (API) para dirigir el tráfico en la red y comunicarse con la infraestructura de hardware subyacente." [7] Esta tecnología surge como consecuencia de aplicar las ventajas de la virtualización en las redes locales de los centros de datos, trasladándose ahora a la WAN. A partir de esta definición, podemos decir que el principio de funcionamiento de la SD-WAN consiste en separar los procesos de administración y control de la red del hardware subyacente (o underlay) y los pone a disposición como software que puede configurarse e implementarse fácilmente en redes WAN. Se puede decir que es una arquitectura virtual de WAN formada a partir del despliegue de túneles encriptados (que forman el overlay) entre sedes o "branches". Esto conlleva múltiples ventajas que veremos con más detalle a continuación.

3.1 Combinación de servicios de transporte

SD-WAN llega como una solución capaz de beneficiar a organizaciones y empresas que buscan más flexibilidad para conectar sedes y redes remotas. Una de las características más destacables de esta solución es que administra múltiples tipos de conexiones, incluidas MPLS, banda ancha y evolución a largo plazo (LTE), con la capacidad de enrutar el tráfico por la mejor ruta en tiempo real. Al poder enrutar el tráfico a través de diferentes rutas de red según las prioridades de tráfico, es posible optimizar el rendimiento de las aplicaciones y minimizar las interrupciones del servicio.

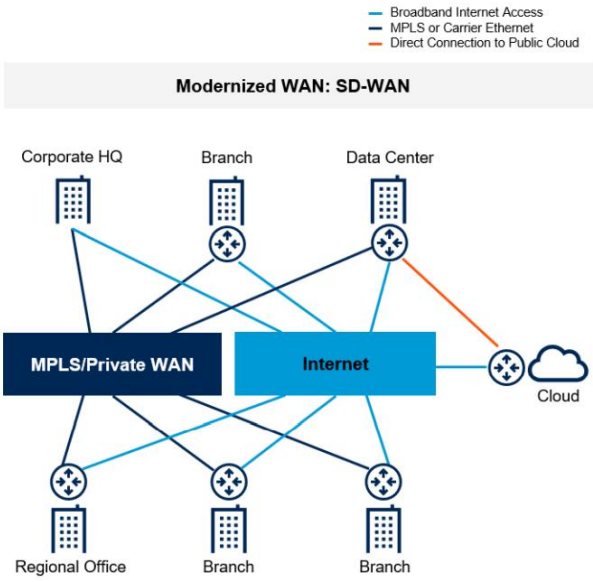


Figura 7. WAN moderna. [6]

Esto supone un cambio de paradigma, ya que hasta ahora el tráfico en las organizaciones se enrutaba desde origen a destino basado en direcciones TCP/IP, tablas de ACL (Access Control List o lista de accesos) y protocolos de enrutado. SD-WAN separa la gestión del plano de control de dispositivos de red (controladores que tienen visibilidad sobre toda la red) del plano de datos que reenvía el tráfico (underlay), eliminando el procesado de enrutamiento en los routers como se hacía en WAN tradicionales. Estos controladores son capaces de programar los dispositivos de la red que, en este caso, conforman el plano de datos. Las rutas del underlay son importadas al overlay de la SD-WAN a través de los dispositivos en el borde de la red (tecnología que permite SD-WAN) y a partir de protocolos de enrutamiento estándares como, por ejemplo: Border Gateway Protocol (BGP) u Open Shortest Path First (OSPF). Dichos dispositivos en el borde de la red luego intercambian la información con los controladores de la SD-WAN. Al tener una visión global de la red y el poder gestionarla a través de algoritmos basados en software, resuelve las limitaciones en cuanto a flexibilidad de la red y de aplicación de políticas sobre múltiples enlaces WAN hoy existente en muchos entornos empresariales.

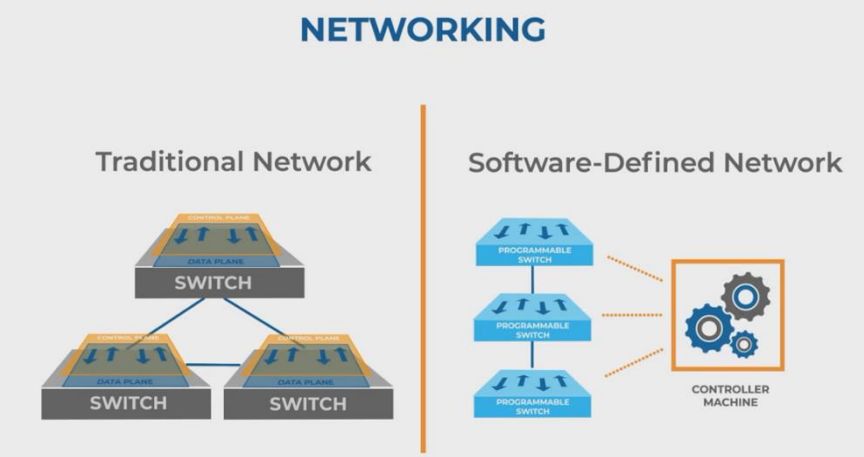


Figura 8. Plano de datos y control en WAN tradicionales vs SDN. [8]

3.2 Encaminamiento “application aware”

La calidad del servicio (QoS) y las políticas de tráfico y seguridad que definen cómo una aplicación debe ser llevada a un usuario se establecen de forma centralizada y se programan automáticamente para miles de dispositivos en sedes o ubicaciones “branch”. A esto se hace referencia cuando se dice que la SD-WAN es capaz de hacer enrutamiento de tipo “application aware”. Ya que, lo que permite es que el tráfico pueda salir por diferentes rutas de conectividad dependiendo del perfil de la aplicación. Esto mejora el rendimiento de la red notablemente, ya que se estaría enrutando el tráfico a nivel de capa 7 del conocido modelo OSI, es decir, la capa de aplicación. Por ejemplo, una sede puede ser capaz de utilizar este tipo de enrutamiento para priorizar el tráfico de Microsoft Office 365 o Google localmente. En este caso concreto, el encaminamiento basado en aplicaciones utilizando políticas de tráfico es capaz de definir optimización de rutas,

proxies y ACLs en local. De esta forma, sería posible enviar dicho tráfico sobre la conexión que presente menor latencia al punto de presencia más cercano (POP).

En la misma línea de la idea anterior, la configuración programática de la infraestructura de red puede mejorar en gran medida el rendimiento, la agilidad y las capacidades de supervisión sobre la red. Para controlar el tráfico, es necesario saber el tráfico cursado y su tipología. SD-WAN, a través de la inspección de paquetes, permite una profunda visibilidad de la red. De forma activa, monitoriza pérdidas de paquetes, métricas de latencia y el jitter (o fluctuación del retardo), y a su vez, nos da información en un nivel granular de los flujos de las aplicaciones. Así, esta nueva tipología nos ofrece una visibilidad de la red desde la perspectiva de las aplicaciones a partir de parámetros como: cantidad de tráfico cursado, consumo del ancho de banda y en ocasiones, calidad de la experiencia (QoE) dependiendo del proveedor de la tecnología. Esto trae un mejor desempeño, mayor fiabilidad y visibilidad sobre la conectividad entre las sedes y los centros de datos o entornos cloud según la arquitectura de red.

En el caso de la conectividad con la nube o entorno cloud, SD-WAN permite reenviar el tráfico de Internet directamente a la sede sin backhauling, ya que da la posibilidad de acceso directo a Internet desde las sedes sin necesidad de centralizar el tráfico en una ubicación antes de salir a Internet. Con esto, no sólo se mejora la experiencia del usuario en las sedes al sufrir menos latencia, sino que también se reserva ancho de banda para aplicaciones más críticas y necesidades de acceso a los centros de datos.

3.3 Aprovisionamiento

Un indicador importante que toda organización debe tener en cuenta antes de hacer un despliegue de red es el tiempo de ahorro que en este caso le habilitaría la solución de red a escoger. Recordemos que una WAN tradicional unifica toda la información de control y aprovisionamiento a nivel de hardware, lo que implica que cada dispositivo de la red se debe configurar de forma manual e independiente. SD-WAN como hemos mencionado, centraliza los datos de configuración y aprovisionamiento en un repositorio, para luego orquestar las funciones de red a todos los dispositivos en el borde de la WAN de manera simultánea. Estamos hablando de lo que se conoce como “Aprovisionamiento de cero toque” (ZTP - Zero Touch Provisioning): “es una función de conmutador que permite que los dispositivos se aprovisionen y configuren automáticamente, eliminando la mayor parte del trabajo manual que implica agregarlos a una red. Cuando se enciende, el conmutador envía una solicitud a través de DHCP (Dynamic Host Configuration Protocol) o TFTP (Trivial File Transfer Protocol) para obtener la ubicación de su imagen y configuración almacenadas centralmente, que descarga y ejecuta” [9]. En este caso, la SD-WAN supone también un incremento de la agilidad de despliegue de red.

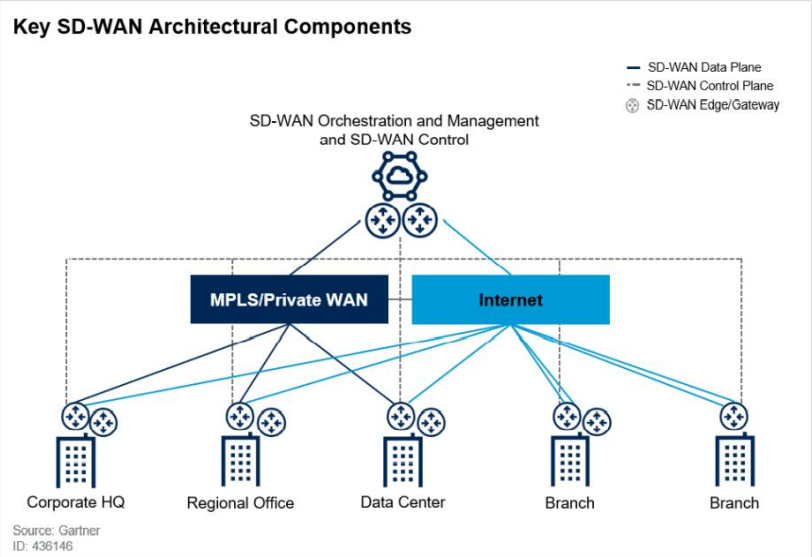


Figura 9. Componentes de arquitectura SD-WAN. [6]

Otro evaluador importante en este sentido es el coste de la solución. Un aprovisionamiento de SD-WAN con enlaces públicos de Internet puede ser significativamente rápido, ya que estamos hablando de cuestión de minutos. Este tipo de enlaces resulta mucho más económico de mantener que una macro LAN basada en MPLS. Es decir, SD-WAN permite a sus usuarios el aprovechar el ancho de banda asequible de Internet sin sacrificar del todo la fiabilidad de la red, ya que se pueden configurar métodos de respaldo o "failover" entre múltiples enlaces de conectividad.

De la mano con la idea anterior, un aspecto a resaltar en las redes de hoy en día es la necesidad de securización de las mismas, y más aún, a nivel corporativo. En este sentido, SD-WAN aborda la seguridad a dos niveles: Por un lado, es capaz de securizar el tráfico localmente, de forma centralizada (mediante un servicio cloud) o de forma híbrida según las necesidades del usuario en cuestión. Y, por otro lado, automatiza el proceso manual y tedioso de crear VPNs (Redes privadas virtuales) encriptadas. Siendo también capaz de ofrecer tipologías de VPN hub-and-spoke o any-to-any.

4. Meraki SD-WAN

Hemos analizado anteriormente una de las limitaciones más destacables que sufre la empresa con su arquitectura de red actual: Las aplicaciones están migrando a entornos cloud, incrementando la necesidad de las sedes o branches de conectarse directamente a Internet para mejorar la experiencia de usuario, sabiendo que hoy se produce un "cuello de botella" debido al punto centralizado de salida a Internet. Considerando este escenario, la empresa ha decidido cambiar a una tipología de red que, entre otras cosas, brinde mejores prestaciones y se adapte de mejor manera a los entornos cloud.

Toda solución SD-WAN incluye entonces dispositivos en el borde de la red (entre los que se establecen los túneles del overlay) y dispositivos de control. Hemos visto también que en el centro de toda solución SD-WAN está el controlador, que no es más que software que corre en un servidor, que mantiene toda la configuración, aprovisionamiento y políticas de tráfico para manejar las diferentes conexiones WAN.

Sabiendo esto, la realidad del mercado hoy es que existen muchos vendedores con diferentes modelos de despliegue aunado al hecho de que no existen estándares industriales para la SD-WAN. La mayoría de los trabajos relacionados a SD-WAN en el mercado se centran en reducir la dependencia de la MPLS en vez de discutir los beneficios propios de esta tecnología. La decisión de escoger a quien comprar la tecnología necesaria impacta directamente en nuestro equipo de trabajo en la empresa, pues es el encargado de todo lo relacionado con la red corporativa. Luego de evaluar las opciones de mercado, finalmente se decide optar por la solución SD-WAN Meraki del proveedor Cisco [10].

Figura 10. Meraki Security SD-WAN. [10]

Esta solución conlleva los siguientes conceptos y hardware:

- Conexión de tipo hub-spoke donde todas las sedes (spokes) se interconectan vía VPN a través de un hub centralizado.

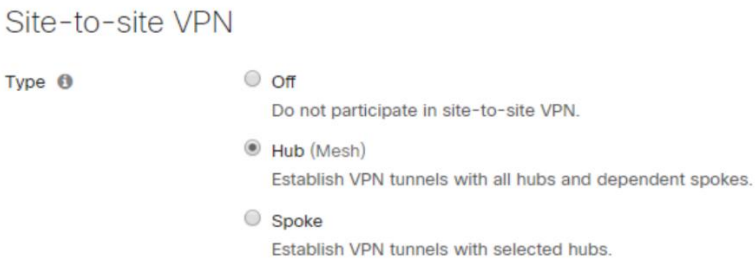


Figura 11. Configuración de VPN entre sedes. [10]

- Las sedes requieren de dispositivos Firewall Cisco Meraki MX que "incluyen funcionalidades de SD-WAN, firewall basado en aplicaciones, filtrado de contenido, filtrado de búsqueda web, detección y prevención de intrusiones basadas en SNORT, protección avanzada contra malware (AMP), almacenamiento en caché web y conmutación por falla de red celular 4 G, entre muchos otros. Las características de SD-WAN y VPN automática están disponibles en nuestros dispositivos virtuales y componentes de hardware". [10]

- "Group policies" como capacidad de aplicar reglas de Firewall en el MX a nivel de la capa de aplicación, en este caso clasificando las políticas de securización por grupos que están directamente relacionados con las direcciones web:

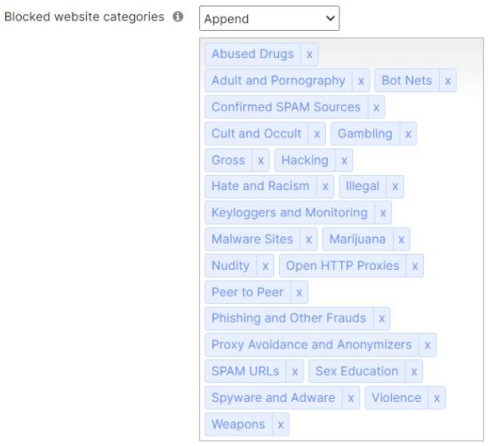


Figura 12. Group policies. [10]

- "Split tunnel", en otras palabras, la configuración que permite que las sedes envíen tráfico vía VPN sólo si está destinada a una subred específica que esté siendo anunciada por otro dispositivo MX.

- Si se configura para "alta disponibilidad", un MX sirve como unidad máster y la otra como "spare" o de repuesto. Todo el tráfico es cursado por el MX primario mientras que el spare opera de forma redundante en caso de failover. Eventos tanto

de failover como de disponibilidad, se comunican entre los MX mediante el protocolo VRRP (Virtual Router Redundancy Protocolo).

5. Nueva solución de red planteada

Partiendo de las necesidades de arquitectura y a nivel de conectividad antes destacadas, e impulsada también por el vencimiento de las licencias de los equipos hardware de las redes a nivel país, la empresa finalmente decide plantear una nueva solución de red. De esta forma, se plantea la nueva arquitectura de red en el equipo, representada en la siguiente figura en comparación con la solución MPLS anterior:

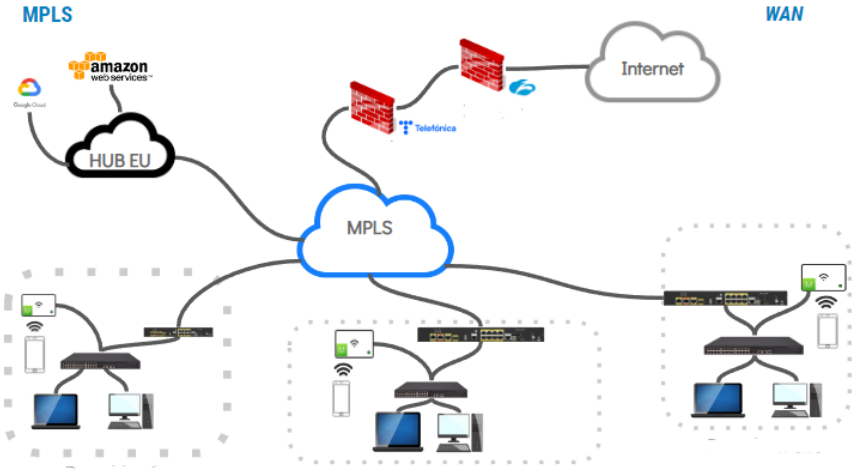


Figura 13. Arquitectura solución MPLS.

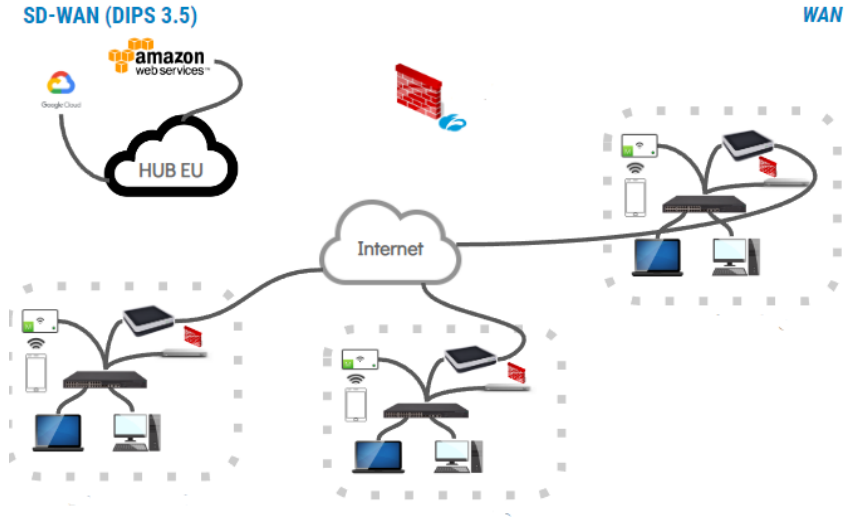


Figura 14. Arquitectura solución SD-WAN.

5.1 Nueva configuración WAN

Partiendo de esta idea, hemos pasado a configurar las conexiones a nivel WAN en las sedes:

Para que los trabajadores puedan cursar tráfico que no apunte a IPs de tipo corporativas y que no exista comunicación que comprometa la seguridad ni la fiabilidad de la red corporativa, hemos planteado la creación de subrangos que puedan permitir a varios departamentos cursar tráfico en el mismo switch. Esto lo hacemos a partir de VLANs (LANs virtuales). Cada VLAN tiene su propio dominio broadcast, reduciendo el tráfico en la red local. De la arquitectura anterior nos encontrábamos con un cuello de botella que hacía pasar todo el tráfico (tanto corporativo como no corporativo) por el mismo punto centralizado, comprometiendo tanto el rendimiento como la seguridad de la red. La manera de securizar todo el tráfico pasaba por un proxy de tipo cloud que también centralizaba el mismo y agregaba latencia. A partir de aquí, hemos planteado un tipo de configuración que Meraki nos ha permitido establecer: diferenciar el tráfico corporativo de la LAN que sale a Internet mediante VPNs del tráfico no corporativo que sale a Internet mediante reglas de Firewall. Aquellas VLANs que necesitan de una salida directa a Internet, las catalogaremos como DMZs (Zona Desmilitarizada). De esta forma, damos una solución al cuello de botella, dando salida directa a Internet a aquellas conexiones que requieren de una menor latencia y un mayor uso del ancho de banda, y las securizamos mediante las reglas aplicadas en local en cada sede en el mencionado Firewall MX. Por otro lado, el tráfico considerado como corporativo sale a Internet mediante una conexión VPN al proxy de tipo cloud, antes mencionado, de forma única y segura.

5.2 Nueva configuración LAN

Para definir la disposición y las conexiones a nivel de hardware local, hemos tenido en consideración varios aspectos que definen el contexto actual de las sedes:

- Existen sedes con 2 switches.
- Existen sedes con 1 switch.
- El equipo plantea que se haga un diseño con todas las conexiones redundadas para evitar SPOF (Punto único de fallo).

Teniendo en cuenta esto, el planteamiento presentado ha sido el de realizar una conexión en los switches de tipo anillo, de forma que se permita un envío de datos de tipo bidireccional (sabiendo que no sería posible asegurarlo en las sedes con 1 sólo switch):

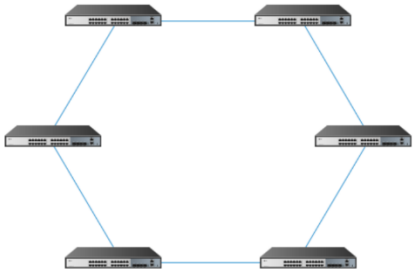


Figura 15. Tipología de tipo anillo.

Para seguir cumpliendo con las especificaciones anteriores, decidimos mantener la instalación de dos conexiones con los routers del ISP (Proveedor de Servicios de Internet) por cada sede. Con la especificación de que se tratase de conexiones de distinta tipología (Fibra dedicada, FTTH, Radioenlace, 4G LTE) para así asegurar una redundancia a nivel de tecnología de la instalación.

Una vez definido el underlay, pasamos entonces a la capa de los dispositivos overlay: los responsables de permitir las configuraciones de la SD-WAN. Siguiendo el mismo hilo de la idea anterior, se ha propuesto la conexión redundada de dos dispositivos MX-67 para las sedes.

6. Primeras pruebas (Laboratorio)

Una vez escogida la solución y los modelos a utilizar, llega la hora de hacer las primeras pruebas necesarias antes de comprometernos a hacer la compra de todos los equipos necesarios. Aquí abarcamos dos diseños: el de la instalación de los armarios informáticos y el del dimensionamiento de la instalación de los APs (Puntos de Acceso) para las sedes.

6.1 Diseño conectividad LAN

Para el primer diseño, la idea es simular la propuesta de conexiones que se pretende desplegar en todas las sedes. Para ello, contamos con 2 switches, 2 routers de ISP, 2 MX67 y la creación de una red en el dashboard cloud de Meraki que simula la creación de una de las sedes. Configuramos entonces las VLANs correspondientes:

VLAN name	Subnet	MX IP	Group policy	VPN mode
LAN	10.95.86.0/24	10.95.86.5	None	Enabled
DMZ_FREEWIFI	192.168.88.0/23	192.168.88.1	GP_DMZ	Disabled
DMZ_OPS	192.168.5.0/24	192.168.5.1	GP_DMZ	Disabled
DMZ_DKTMOBILITY	192.168.108.0/22	192.168.108.1	GP_DMZ	Disabled
DMZ_RFID	192.168.10.0/24	192.168.10.1	GP_DMZ	Disabled

Figura 16. VLANs Laboratorio.

Vemos en la figura 16, cómo seguimos la configuración antes planteada: La LAN es la única que tiene habilitada una VPN para comunicarse con el servidor proxy antes de salir a Internet y que no requiere de aplicación de políticas de securización de tráfico a nivel local, mientras que las DMZs tienen una salida directa a Internet con la aplicación de Group Policies para securizar dicho tráfico a nive local.

También era importante conocer de antemano el comportamiento de los MX en caso de la caída de una de las 2 salidas a Internet o en caso de perder conectividad a nivel LAN:

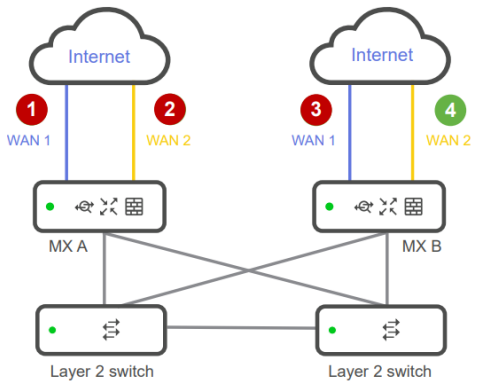


Figura 17. Failover de los MX.

Así, si el MX1 pierde su interfaz con la WAN1, cambiará a WAN2. Si el MX1 pierde la conectividad con la WAN1 y la WAN2, éste bascula todo el tráfico al MX2 que, a su vez, priorizará el tráfico saliente por la WAN1.

De manera que el diseño planteado resultante es el siguiente:

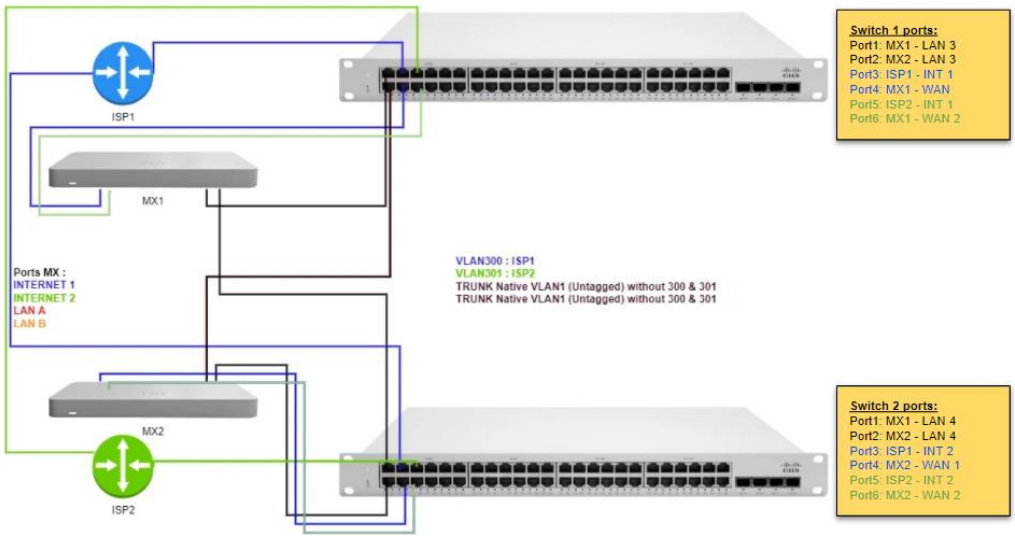


Figura 18. Diseño de conexiones LAN.

De esta forma, aseguramos siempre una conexión activa en caso de que falle alguno de los equipos. Los MX son capaces de cursar tráfico entre ellos a nivel LAN tanto por el switch 1 como por el switch 2, mientras que también tienen conexión a internet tanto por el ISP 1 como por el ISP 2. Esta era la teoría del diseño, pero había que realizar todas las pruebas necesarias antes de validar la configuración.

6.1.1 Resultados

- Lo primero que hemos aprendido a la hora de realizar estas conexiones es que, para aplicar la conexión redundada de los switches, es importante tener en cuenta que los switches crearían congestión de la red debido a los bucles que se forman por la conexión redundada. Cuando los switches empiezan a enviar paquetes de tipo broadcast, resulta que uno de ellos recibe paquetes por puertos diferentes con la misma dirección MAC de origen. Esto forma un bucle y los paquetes broadcast se siguen enviando continuamente sin encontrar destinatario, con lo cual, finalmente acaban “inundando” la red. Para resolverlo, hemos aplicado el protocolo que se conoce como Spanning Tree Protocol (STP) para bloquear uno de los puertos y así no generar el loop o bucle.
- Este mismo comportamiento de tipo bucle que acaba por inundar la red se produce cuando los routers de ISP se conectan de forma redundada. Esto ha sido crucial

para tener en cuenta (en caso de aprobar esta tipología de conexión) a la hora de pedir al proveedor la correcta configuración de los routers.

- Realizamos todas las pruebas para comprobar el funcionamiento de las conexiones redundadas:

1) Pérdida de conectividad LAN de MX1 con Switch 1: Se pierde sólo 1 paquete al bascular al Switch 2

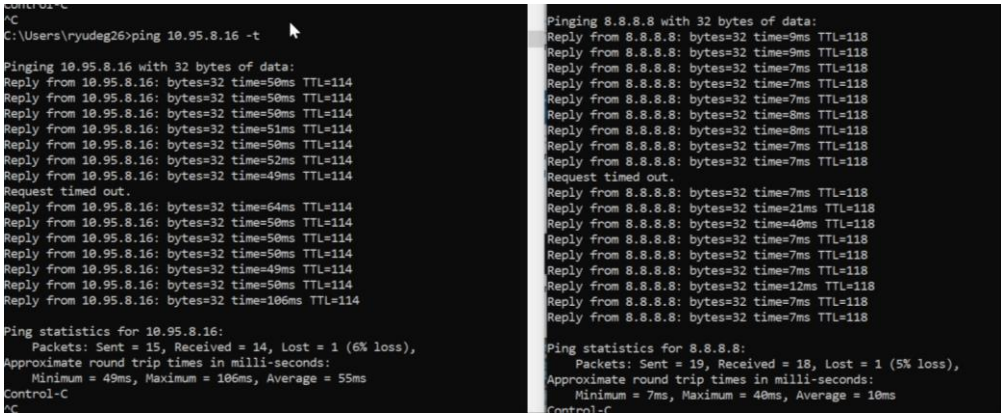


Figura 19. Mensajes ICMP en paquetes IP a direcciones privadas y públicas.

2) Pérdida de conectividad LAN de MX1 con Switch 1 y Switch 2: Se pierden 4 paquetes de tráfico a IP privada como destino al bascular al MX2

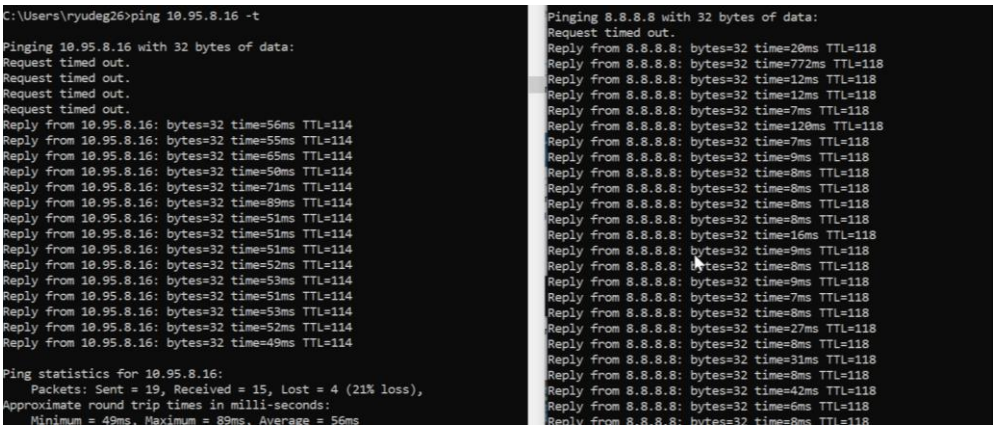
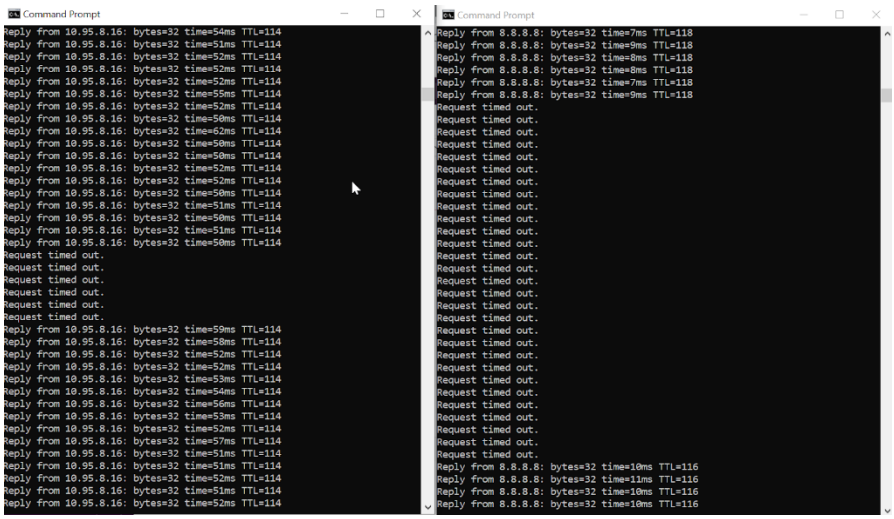


Figura 20. Mensajes ICMP en paquetes IP a direcciones privadas y públicas.

3) Pérdida de conectividad WAN de MX1 con ISP 1: Se pierden 6 paquetes de tráfico a IP privada como destino al bascular a la conexión WAN2 y se pierden 29 paquetes de tráfico a IP pública como destino (aproximadamente 2 minutos de pérdida de conectividad)


Command Prompt
Reply from 10.95.8.16: bytes=32 time=54ms TTL=114
Reply from 10.95.8.16: bytes=32 time=51ms TTL=114
Reply from 10.95.8.16: bytes=32 time=52ms TTL=114
Reply from 10.95.8.16: bytes=32 time=52ms TTL=114
Reply from 10.95.8.16: bytes=32 time=52ms TTL=114
Reply from 10.95.8.16: bytes=32 time=55ms TTL=114
Reply from 10.95.8.16: bytes=32 time=52ms TTL=114
Reply from 10.95.8.16: bytes=32 time=50ms TTL=114
Reply from 10.95.8.16: bytes=32 time=62ms TTL=114
Reply from 10.95.8.16: bytes=32 time=50ms TTL=114
Reply from 10.95.8.16: bytes=32 time=50ms TTL=114
Reply from 10.95.8.16: bytes=32 time=52ms TTL=114
Reply from 10.95.8.16: bytes=32 time=52ms TTL=114
Reply from 10.95.8.16: bytes=32 time=50ms TTL=114
Reply from 10.95.8.16: bytes=32 time=51ms TTL=114
Reply from 10.95.8.16: bytes=32 time=50ms TTL=114
Reply from 10.95.8.16: bytes=32 time=51ms TTL=114
Reply from 10.95.8.16: bytes=32 time=50ms TTL=114
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 10.95.8.16: bytes=32 time=59ms TTL=114
Reply from 10.95.8.16: bytes=32 time=58ms TTL=114
Reply from 10.95.8.16: bytes=32 time=52ms TTL=114
Reply from 10.95.8.16: bytes=32 time=52ms TTL=114
Reply from 10.95.8.16: bytes=32 time=53ms TTL=114
Reply from 10.95.8.16: bytes=32 time=54ms TTL=114
Reply from 10.95.8.16: bytes=32 time=56ms TTL=114
Reply from 10.95.8.16: bytes=32 time=53ms TTL=114
Reply from 10.95.8.16: bytes=32 time=52ms TTL=114
Reply from 10.95.8.16: bytes=32 time=57ms TTL=114
Reply from 10.95.8.16: bytes=32 time=51ms TTL=114
Reply from 10.95.8.16: bytes=32 time=51ms TTL=114
Reply from 10.95.8.16: bytes=32 time=52ms TTL=114
Reply from 10.95.8.16: bytes=32 time=51ms TTL=114
Reply from 10.95.8.16: bytes=32 time=52ms TTL=114
Command Prompt
Reply from 8.8.8.8: bytes=32 time=7ms TTL=118
Reply from 8.8.8.8: bytes=32 time=9ms TTL=118
Reply from 8.8.8.8: bytes=32 time=8ms TTL=118
Reply from 8.8.8.8: bytes=32 time=8ms TTL=118
Reply from 8.8.8.8: bytes=32 time=7ms TTL=118
Reply from 8.8.8.8: bytes=32 time=9ms TTL=118
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.

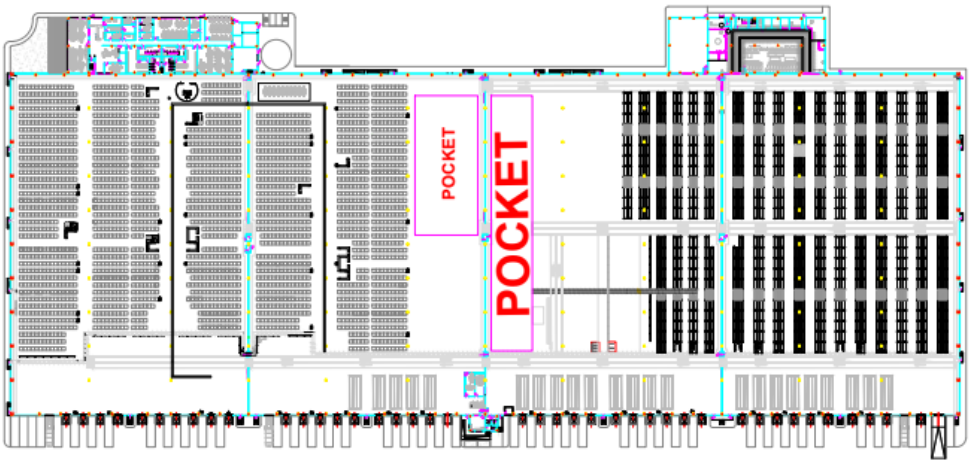


Figura 22. Almacén a realizar estudio de cobertura.

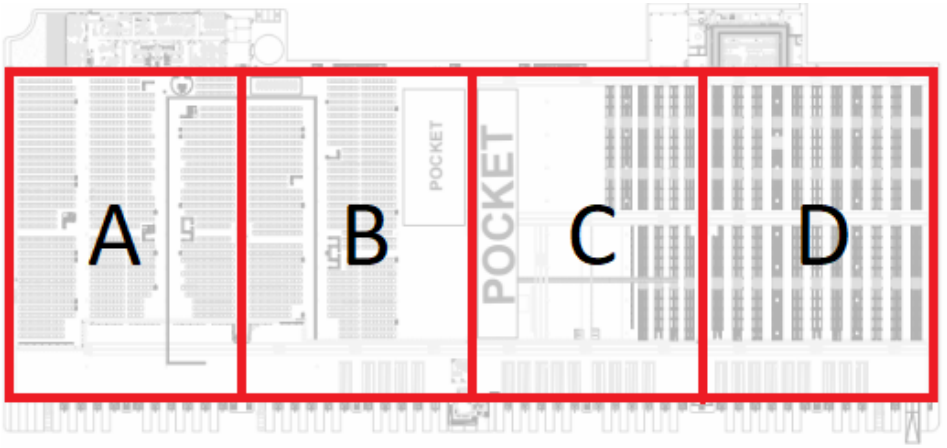


Figura 23. 4 zonas de trabajo principales del almacén.

Actualmente, este almacén cuenta con puntos de acceso inalámbrico que funcionan con el estándar 802.11ac (también conocido como Wi-Fi 5). Los puntos de acceso con respecto a este despliegue están cerca de su fecha de finalización de vida útil (WLC - EoL 2023). Teniendo en cuenta este contexto, queríamos tener la mejor infraestructura Wi-Fi, por eso decidimos instalar nuevos dispositivos de hardware capaces de hablar sobre el nuevo estándar 802.11ax (también conocido como Wi-Fi 6). Este estándar es capaz de brindar velocidades de rendimiento más rápidas, mayor duración de la batería de los dispositivos que se interconectan a través de ella y un uso más eficiente de la red inalámbrica en términos de ancho de banda a la hora de conectar varios dispositivos que también podrían comunicarse con este mismo estándar. Para ello, emplea tecnologías de modulación como OFDMA, además de MU-MIMO como gran novedad.

Para poder planificar y simular nuestro despliegue, la empresa ha puesto a disposición el software Ekahau Pro como nuestra herramienta de diseño de red inalámbrica. De esta manera, podíamos contar con diagnósticos Wi-Fi precisos, estudios de sitios más rápidos, análisis de espectro más rápidos y datos más precisos y confiables proporcionados con precisión 3D.

Al no tener una correcta formación en la herramienta, se ha realizado el apoyo basado en la teoría de antenas y de enlaces de radiocomunicación a compañeros que estaban capacitados para manejarla. A partir de aquí, y una vez analizados los dispositivos que tendrían que conectarse a dicha red, queríamos una infraestructura Wi-Fi preparada para todo lo que eventualmente pudiera venir en el futuro, por eso nuestros objetivos eran:

- Priorizar un nivel de señal de -67dBm en todas las áreas.
- Establecer como mínimo una SNR (relación señal-ruido) de 25 dB.

La herramienta simula escenarios de conectividad para poder prevenir posibles escenarios de interferencia cocanal y de pérdidas de señal por reflexión debido a efecto multicamino. Para ello, dispone de herramientas donde el usuario puede indicar la naturaleza de los materiales y paredes que conforman el almacén, así como sus dimensiones.

No todas las zonas del almacén son iguales. Dispone de racks (estructuras metálicas para almacenar mercancía) altos que forman pasillos a lo largo de las zonas C y D:

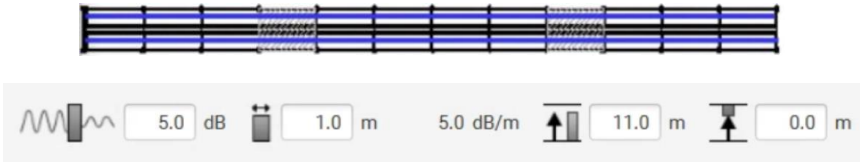


Figura 24. Atenuación debido a racks altos.

Así como también dispone de racks bajos en las zonas A y B principalmente:

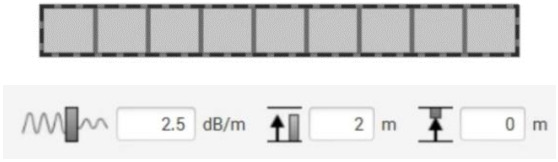


Figura 25. Atenuación debido a racks bajos.

A partir de aquí, se plantea que en zonas de racks altos lo mejor sería optar por antenas unidireccional de manera que la señal se envíe con una mejor cobertura a lo largo del pasillo, mientras que, en zonas de racks bajos, lo mejor sería optar por antenas omnidireccionales que aseguren la cobertura a lo largo de las naves A y B. Estas últimas colocadas de tal forma que comuniquen en canales pertenecientes a la banda de 5 GHz que no produzcan interferencia entre ellos.

El diseño final con la distribución de los APs y las antenas (de Meraki) queda de la siguiente manera:

Figura 26. Distribución de antenas y APs.

A continuación, la simulación de nivel de señal que proporcionarían 2 de los modelos de APs:

- MR46E + MA-ANT-3-D (Espacios abiertos y racks abajos)

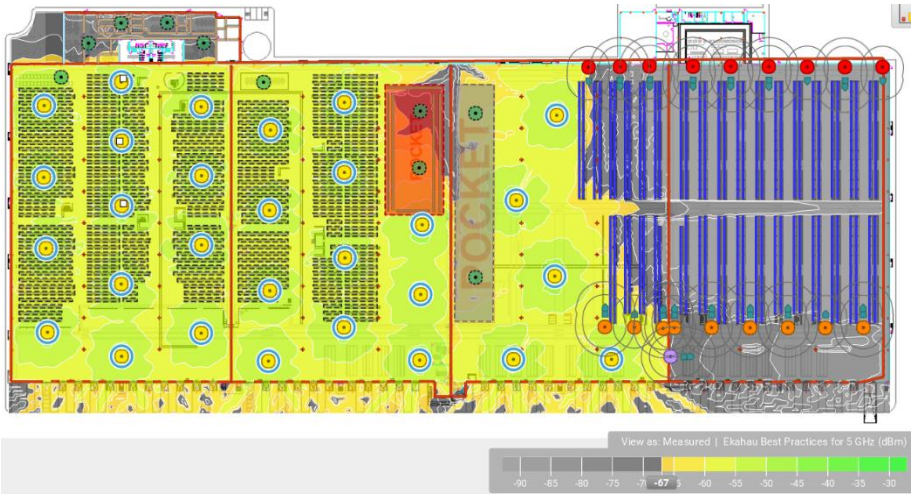


Figura 27. Nivel de señal de antenas omnidireccionales.

Figura 28. Configuración de antenas omnidireccionales.

MR46E + MA-ANT-3-E5/6 (Pared)

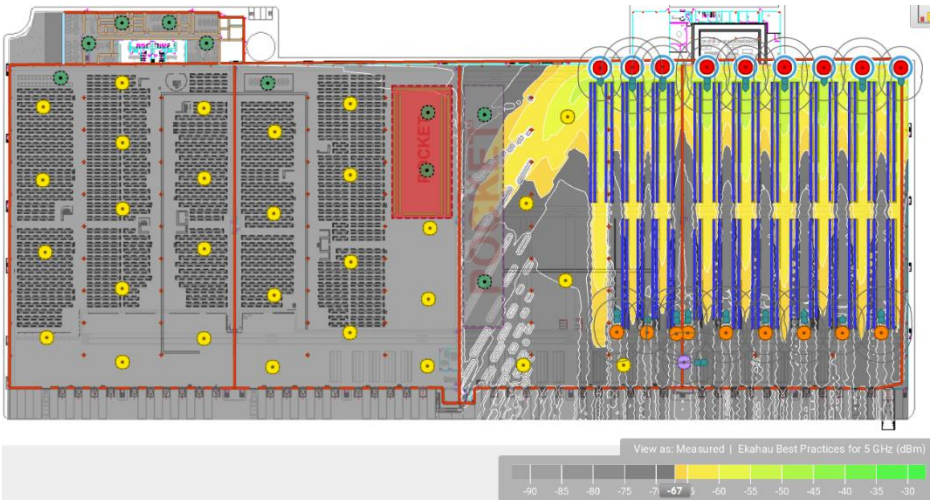


Figura 29. Nivel de señal de antenas direccionales.

Figura 30. Configuración de antenas direccionales.

En un principio, el planteamiento que se ha realizado es de 58 antena y/o APs, reduciendo notablemente la propuesta hecha por el proveedor externo. Este dimensionamiento no se puede dar como definitivo hasta que no se realicen pruebas in-situ o sobre el terreno.

7. Reuniones con proveedores y pruebas piloto

Una vez realizadas y también aprobadas las pruebas de laboratorio con la nueva solución SD-WAN llega el momento de probarla en algunas de las sedes. Para ello, se realizan varias reuniones semanales con el proveedor de acceso a Internet para planificar las instalaciones del underlay con varios requerimientos por parte de la empresa, entre los cuales están:

- Conexiones de distinta tipología (Fibra dedicada, FTTH, Radioenlace, 4G LTE) para así asegurar una redundancia a nivel de tecnología de la instalación.
- Routers que garanticen la configuración con el STP para permitir la conexión redundada.

7.1 Primera sede piloto

El operador que ha participado en las reuniones antes mencionadas, accede a hacer las primeras pruebas con sus instalaciones de underlay sobre las cuales se apoyará la solución SD-WAN:

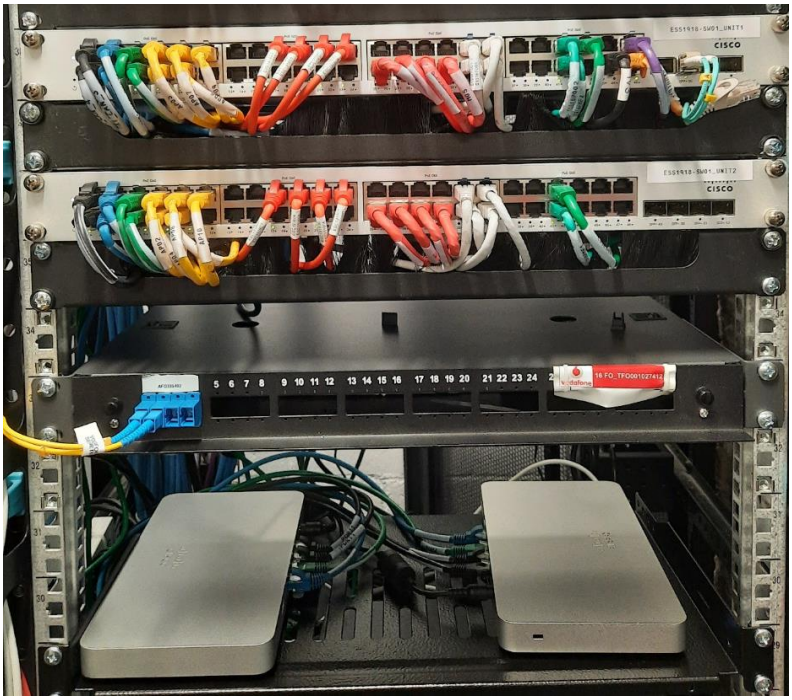


Figura 31. Armario informático de sede 1.

Se puede observar que la configuración de la red a nivel LAN sigue el mismo estándar que el testeado en el laboratorio:

LAN	10.95.83.0/24	10.95.83.5	None	Enabled
DMZ_FREEWIFI	192.168.88.0/23	192.168.88.1	GP_DMZ	Disabled
DMZ_OPS	192.168.5.0/24	192.168.5.1	GP_DMZ	Disabled
DMZ_DKTMOBILITY	192.168.108.0/22	192.168.108.1	GP_DMZ	Disabled
DMZ_RFID	192.168.10.0/24	192.168.10.1	GP_DMZ	Disabled
DMZ_DIGITAL	192.168.33.0/24	192.168.33.1	GP_DMZ	Disabled

Figura 32. VLANs Sede 1.

7.1.1 Resultados

- En esta sede se ha detectado que no estaba bien configurado el STP por parte del proveedor en uno de sus routers, lo que nos obligó a bloquear uno de los puertos que permitía la conexión redundada a nivel WAN. De lo contario la sede no tenía conexión a Internet.
- También se ha detectado la necesidad de desconectar los routers ISP que formaban parte de la red MPLS, pues a nivel público, la sede no estaba logrando conectarse a Internet debido a un conflicto de IP.
- Resultados prácticamente calcados a los realizados en las pruebas de failover en el laboratorio.
- Satisfacción de una sede que nota un mejor aprovechamiento del ancho de banda y sin cortes por saturación. Sobre todo, se resalta la baja latencia.

8. Conclusiones y próximos pasos

Se ha querido abarcar, como se marcaba en los objetivos al principio de este trabajo, todo lo que conlleva un despliegue masivo de una nueva solución de red no sólo desde el punto de vista técnico sino también desde el lado organizacional de un ingeniero.

En resumen, hemos visto y analizado que, mientras la MPLS es un circuito dedicado, SD-WAN se basa en overlay virtualizado y desacoplado de enlaces físicos. Esto, en principio, es ventajoso para la MPLS, pues la prevención de pérdida de paquetes resulta mayor, pero la empresa deberá incurrir en más gastos por cada megabit transferido. Sin embargo, la naturaleza del overlay virtualizado que propone SD-WAN trae como consecuencia un mejor aprovechamiento de conexiones como MPLS, 4G LTE o Internet, otorgando mayor flexibilidad a la red.

Por otro lado, una ventaja que trae la MPLS es el despliegue de conectividad securizada y privada entre sedes y sus centros de datos en cuestión. Conexión directa y a Internet público no es una conexión igual de segura. Pero, también es cierto, que la MPLS no brinda ningún análisis sobre los datos que cursan a través de la red, ya que es responsabilidad del propio proveedor. Esto no da visibilidad alguna a la empresa, lo cual es fundamental y más aun considerando las necesidades que existen hoy por hoy de monitorización de la red.

El tráfico cursado hoy por hoy tiene requisitos de rendimientos que pueden resultar impredecibles: el tráfico que requiere baja latencia debe ser priorizado, y esto conlleva a la necesidad de aportar inteligencia a la red para reconocer aplicaciones, un uso eficiente del ancho de banda, monitorización de pérdida de paquetes y priorización por diferentes tipos de conexiones que la MPLS simplemente no puede garantizar. También es importante recordar que la empresa tiene vistas a futuro con un entorno IoT y para ello resulta fundamental la virtualización de la red y la mejor conectividad con el entorno cloud.

No sólo se ha abarcado el diseño de conectividad LAN sino también el de la WLAN. Este último bajo revisión, ya que se deben realizar más pruebas en local para verificar que los datos que proporciona el software de Ekahau sobre la conectividad de Wi-Fi 6 bajo esas condiciones son reales. Pero es sin duda alguna, un paso significativo para el resto del despliegue a nivel económico para la empresa, y también de gran oportunidad para tener empleados preparados para realizar este tipo de despliegue sin necesidad de contratar un proveedor externo.

Después de tres sedes piloto migradas de forma satisfactoria, aunque en este trabajo sólo se ha presentado una, la empresa ahora está preparada para planificar migraciones masivas. Para ello, los próximos pasos deben ser el formar a los equipos impactados para que conozcan de primera mano la tecnología y el comportamiento de la nueva solución de red, así como las posibles incidencias que pueden surgir. Por otro lado, así como se ha realizado una animación al proveedor del underlay para las instalaciones, también resulta una posibilidad plantear la animación de otro proveedor para el overlay.

En la empresa en la que se basa este trabajo, la decisión del cambio de tipología de red se toma no sólo desde el punto de vista de modernización de la WAN y la necesidad de salida a Internet independiente de cada sede, sino también desde el punto de vista económico y de mejoría de tiempos de despliegue. Es por esto que resulta complicado sustentar con cálculos de interés técnico los resultados que suponen el llevar a cabo esta migración. El nivel de gratificación en los equipos impactados es muy alto, y esto es otro indicador de que la migración es una buena decisión. Entre ellos se encuentran equipos de soporte de incidencias, y este cambio, también resulta en un menor número de tickets por incidencias debido al rendimiento de la red.

9. Bibliografía

[1] Palo Alto Networks, "MPLS | What Is Multiprotocol Label Switching", *https://www.paloaltonetworks.com/cyberpedia/mpls-what-is-multiprotocol-label-switching*

[2] Wikipedia, "Multiprotocol Label Switching", MPLS Label, *https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching*

[3] Cloudflare, "¿Qué es el modelo OSI?", *https://www.cloudflare.com/es-es/learning/ddos/glossary/open-systems-interconnection-model-osi/*

[4] Huawei, "What is MPLS?", *https://support.huawei.com/enterprise/es/doc/EDOC1100118961*

[5] Catchpoint, "Network Admin's Guide to Synthetic Monitoring | SD-WAN vs MPLS", *https://www.catchpoint.com/network-admin-guide/sd-wan-vs-mpls*

[6] Gartner, "Technical Professional Advice | Assessing the Strengths and Weaknesses of SD-WAN Technology"

[7] Rapp, Jacob, "Evolution of Software-Defined Networking", 2019.

[8] Fungible, "Separating Data Plane and Control Plane: Why it matters?".

[9] ComputerWeekly, "Aprovisionamiento de cero toque (ZTP o zero touch provisioning)", 2018.

[10] Meraki SD-WAN, *https://meraki.cisco.com/es-co/products/security-sd-wan/*