Migración del monitoreo y gestión de la red tarjeta tuya por medio de redes definidas por software para una red WAN (SDWAN)

SANTIAGO ALEJANDRO SEPÚLVEDA PALACIO

Trabajo de semestre de industria presentado para para optar al título de:
Ingeniero de Telecomunicaciones

Asesor Interno:
Jaime Alberto Vergara Tejada - Profesor Facultad de Ingeniería

Asesor Externo:
Andrea del Pilar Garay Buitrago - Ingeniera de Sistemas

Universidad de Antioquia

Facultad de Ingeniería

Departamento de Ingeniería Electrónica y Telecomunicaciones

Medellín, Colombia

2021

Cita	(Sepúlveda Palacio, 2021)
Referencia **Estilo IEEE (2020)**	Sepúlveda Palacio, S. (2021). Migración del monitoreo y gestión de la red tarjeta tuya por medio de redes definidas por software para una red WAN (SDWAN) [Trabajo de semestre de industria]. Universidad de Antioquia, Medellín, Colombia.

Tabla de contenido

Resumen

Con la globalización la digitalización ha traído muchísimos cambios y consigo nuevos modelos de negocio, es por esto que las empresas tienen el desafío de incrementar su productividad, lo que las empuja a mejorar sus soluciones de conectividad remota para incrementar el ancho de banda, por esto necesitan hoy en día de nuevas tecnologías que le permitan tener una interconexión confiable entre todas sus sedes por medio de una red WAN pero que esa interconexión pueda ser centrado en la nube y en servidores en centros de datos; para esto es necesario una nueva tecnología, una red definida por software SD-WAN que ofrezca lo que la red WAN tradicional no puede ofrecer, interconexión de las sedes con dos diferentes enlaces aprovechando en este caso la red MPLS de claro permitiendo que las sedes tengan un respaldo en caso de que uno de los dos enlaces se vea afectado en su operación y ofreciendo resolución de incidentes con mayor escalabilidad sin ver afectada la operación de las sedes completamente ya que se cuenta con la conmutación de paquetes permitiendo la interconexión y salida a internet superando la limitación física de la wan tradicional que es usada en tuya que solo cuenta con un enlace MPLS lo que produce afectación total de la sede en caso de ocurrir la caída del enlace.

Siguiendo este orden de ideas se quiere aprovechar estas nuevas tecnologías para implementar SD-WAN en la red corporativa de la empresa TUYA usando la red existente MPLS de claro, routers PE y switches de acceso para conectar las sedes de la entidad financiera por medio de dos enlaces, uno principal (MPLS) y otro de respaldo (banda ancha). Esta implementación solo requiere cambiar los equipos físicos de la sede agregándolos de manera sencilla a través de vmanage ahorrando costos en desplazamientos de ingenieros a la sede para su integración a SDWAN. Con esta adición de tuya a sdwan se va a mejorar la escalabilidad y gestión en la resolución de caídas de enlaces permitiendo que las sedes se beneficien del balanceo de cargas que ofrece esta nueva tecnología evitando saturación de los canales y conmutando el tráfico en caso de afectación de uno de los dos enlaces.

1. Introducción

Las redes WAN actualmente permiten conectar diferentes sedes de una empresa y a su vez a centros de datos permitiendo extender las redes de estas empresas a grandes distancias. Entregando servicios y aplicaciones necesarias para poder funcionar, pero debido a las limitaciones físicas impuestas por el tiempo de propagación de datos y paquetes a grandes distancias las redes WAN se enfrentan a varios problemas operativos. Los cuales son: congestión en la red, retardos y pérdidas de paquetes. Además, se requiere de baja latencia para las aplicaciones actuales, por ejemplo, las videoconferencias, telefonía por voz IP y máquinas virtuales, hacen que la demanda de banda ancha crezca rápidamente por lo que es posible pensar en ampliar la capacidad de la red WAN.

El escenario anterior implica dificultades en la resolución de problemas y la gestión de la red además de que puede incrementar los costos significativamente en los presupuestos de las operaciones. SDWAN está diseñado para abordar estos problemas de red al mejorar o reemplazar los routers de sedes de alguna empresa con dispositivos de virtualización que pueden controlar las políticas de nivel de aplicación y ofrecer una superposición de red.

SDWAN tiene varias ventajas entre ellas la capacidad de admitir múltiples tipos de conexión de red de fibra óptica de última milla, MPLS, o redes inalámbricas como 4G LTE y 5G, puede admitir VPN y servicios de terceros como firewalls y puertas de enlace web, e implementa el balanceo de cargas que realiza una selección de ruta dinámica y una interfaz simple de configurar y administrar.

En este trabajo se propone que la red Corporativa de la Empresa Tuya haga la migración a la tecnología SDWAN para que pueda tener estas ventajas de conectividad y de mejor ancho de banda, la posibilidad de tener un enlace backup en todas sus sedes para garantizar una conectividad con alta disponibilidad y con mejor performance en las aplicaciones. A su vez permite que la administración y monitoreo de la red sea proactiva.

2. Marco Teórico

Para proponer la implementación de la tecnología SDWAN es necesario contextualizar la forma en que las empresas desde hace varios años vienen interconectándose por medio de una red llamada WAN (RED DE ÁREA AMPLIA). Estas redes se extienden por grandes áreas geográficas y conectan redes más pequeñas como redes LAN (Local Area Networks) o MAN (Metropolitan Area Networks). Por esto, solo se utilizan en el sector profesional. Las WAN públicas son operadas por proveedores de servicios de Internet para permitir a sus clientes el acceso a este. Las redes privadas de área amplia son utilizadas principalmente por empresas, por ejemplo, para permitir servicios en la nube y para conectar las redes de las diferentes sedes de la empresa.

Como una red WAN no conecta ordenadores individuales, sino redes enteras, la tecnología utilizada difiere de los otros tipos de red (por ejemplo, la red LAN o MAN). Emplea otros protocolos de transmisión y conceptos de dirección. Las redes WAN utilizan técnicas y protocolos de transmisión de las capas uno a tres del modelo de referencia OSI. De este modo, una WAN funciona en la capa física (capa 1), la capa de enlace (capa 2) y la capa de red (capa 3). Ya sea un PC, un teléfono inteligente, un televisor, sistemas intermedios o nodos de red, como conmutadores, puentes y enrutadores garantizan que los paquetes de datos enviados se reenvían a la dirección correcta. Mediante el hardware y software, los paquetes de datos se envían de una subred a la otra y se entregan al participante de red con un refrigerador. La tecnología básica de esto es la pila de protocolos TCP/IP. Los distintos protocolos de esta familia de protocolos garantizan, por ejemplo, que los datos se procesen correctamente y que los paquetes lleguen a su destino, aunque haya dificultades en la transmisión. [1]

Los medios de transmisión físicos utilizados son los cables de cobre y fibra óptica, así como los enlaces inalámbricos. Los cables de fibra óptica son especialmente adecuados para conexiones a larga distancia sobre tierra y agua. En la práctica, se suele utilizar una combinación de varios medios de transmisión distintos. Con los llamados convertidores de medios, se pueden interconectar distintos tipos de cables. En los grandes nodos de Internet hay puntos de intercambio especiales interconectados, donde a menudo hay más de cien redes interconectadas para permitir un intercambio de datos eficiente. Los repetidores se encargan de que los paquetes de datos no pierdan información, incluso a grandes distancias.

El mundo empresarial actualmente demanda estar conectados muchas más horas y con mayor estabilidad para obtener mejor y mayor alcance, de esta manera los negocios se reinventan hacia lo digital y se mantienen en el mercado. Para ello las empresas se valen de la tecnología y hacen que trabaje para su beneficio y el de las personas. Entre infinidad de tecnologías, nace SD-WAN, diseñado especialmente para las necesidades corporativas, de oficina y empresariales que necesitan estar conectados 7 días 24 horas sin interrupciones, con una estabilidad impenetrable y a un costo atractivo. Sus siglas SDWAN significan Software Defined Networking Wide Area Network y se traduce al español como redes definidas por software en una red de área amplia, los elementos que la conforman no son nuevos en las telecomunicaciones, pero

al unirlos resultan una solución dirigida a apoyar a las empresas.

La gestión de la WAN siempre ha sido uno de los elementos más caros e inflexibles en la operación de una red empresarial, sin embargo, las nuevas características presentes en la tecnología SD-WAN han simplificado la administración con la aplicación de dispositivos de red programables, que permiten a los analistas ajustes de forma remota. Además, el sistema ejecuta automáticamente la elección de la mejor ruta de enrutamiento, disminuyendo costos y mejorando el rendimiento de las redes.

Lo que hace que este servicio sea tan eficiente, es precisamente su capa de software (SD, que significa Software Defined), que garantiza la calidad del servicio y la protección de datos de los enlaces de Internet, independientemente de su tipo.

SDWAN, por lo tanto, permite que el tráfico se envíe automáticamente a través del camino más adecuado de la WAN, respetando las condiciones de seguridad, el costo de los circuitos y las exigencias de la calidad de los servicios. Esta calidad está garantizada por la toma de decisión inteligente del software, que utiliza métricas de calidad de los enlaces, como el tiempo de respuesta, evitando que el encaminamiento se base sólo en el protocolo dinámico, como su predecesor. [2]

La tecnología SDWAN respalda la calidad del servicio al tener conocimiento del nivel de aplicación, dando prioridad de ancho de banda a las aplicaciones más críticas. Esto puede incluir la selección de rutas dinámicas, enviar una aplicación en un enlace más rápido o incluso dividir una aplicación en dos rutas para mejorar el rendimiento entregándose más rápido. Las SDWAN pueden mejorar la entrega de aplicaciones mediante el almacenamiento en caché, almacenando información a la que se ha accedido recientemente en la memoria para acelerar el acceso futuro. [3]

Existen algunas similitudes entre SD-WAN y el mejoramiento de la WAN. El objetivo de cada uno es acelerar la entrega de aplicaciones entre las sucursales y los centros de datos, pero la tecnología SD-WAN se enfoca adicionalmente en el ahorro de costos y la eficiencia, específicamente al permitir enlaces de red de menor costo para realizar el trabajo de líneas arrendadas más costosas, mientras que el mejoramiento WAN se enfoca directamente en afinar la entrega de paquetes. Una SDWAN que utiliza técnicas de virtualización asistidas con el control de tráfico de mejoramiento WAN permite que el ancho de banda de la red crezca o se reduzca dinámicamente según sea necesario.

La tecnología SDWAN y el mejoramiento WAN se pueden usar por separado o juntas, y algunos proveedores de SDWAN están agregando funciones de mejoramiento de la red WAN a sus productos. [3] SDWAN basado en la nube ofrece funciones avanzadas, como seguridad mejorada, nube transparente y soporte para usuarios móviles, que resultan naturalmente del uso de la infraestructura en la nube. Como resultado, SDWAN basada en la nube puede reemplazar MPLS, lo que permite a las organizaciones liberar recursos una vez vinculados a inversiones WAN y crear nuevas capacidades.

3. Objetivos

3.1 Objetivo General

Objetivo General

Implementar una prueba piloto para la migración de la infraestructura de red asociada al servicio de tarjeta tuya a la tecnología SDWAN, donde se van a medir métricas (que son disponibilidad del servicio y latencia de los paquetes) de la nueva tecnología para mostrar la eficiencia del servicio con el fin de mejorar el monitoreo, gestión y calidad del mismo.

Se va a medir la disponibilidad del servicio sobre el 98% y se toma en cuenta con la instalación del enlace principal y enlace backup, es decir, se afecta disponibilidad cuando se caen ambos enlaces simultáneamente. La latencia en el servicio debe ser menos del 1% en pérdida de paquetes independiente del tamaño del paquete.

3.2 Objetivos Específicos

- Realizar el levantamiento de requerimientos para la migración, teniendo en cuenta el número de sedes y equipos en los cuales se implementará la tecnología SDWAN, con el fin de preparar la separación de los planos de administración, control y datos.

- Implementar la migración sobre algunas sedes de la infraestructura de red actual, virtualizando los planos de control y administración, buscando reducir costos.

- Evaluar el desempeño de la migración, comparando los resultados a través de las métricas definidas en la infraestructura antes desplegada, examinando el desempeño de red y la atención de fallas y degradación de enlaces WAN.

4. Metodología

A continuación, se presentan las actividades desarrolladas con las cuales se cumplieron cada uno de los objetivos del proyecto.

Objetivo Específico	Metodología	Actividad
Realizar el levantamiento de requerimientos para la migración, teniendo en cuenta el número de sedes y equipos en los cuales se implementará la tecnología SDWAN, con el fin de preparar la separación de los planos de administración, control y datos.	Se consultó y estudió documentación sobre SD-WAN para conocer las ventajas que tiene sobre la WAN tradicional y como se puede implementar. Ver actividad 1.	1. Recolección de información acerca de la tecnología SDWAN.
	Se averiguó y consultó documentación con los ingenieros encargados de la operación acerca del proyecto TUYA para saber cómo es la topología de la red implementada para la conexión en las sedes. Ver actividad 2.	2. Análisis y estudio de la red WAN implementada en tuya con el fin de utilizar los equipos de la red ya existentes.
	Se identificaron equipos, marca, y especificaciones. Ver actividad 3.	3. Identificar equipos físicos de las sedes los cuales se pueden usar en la implementación.
	Se analizaron datos de casos de negocios de implementaciones de SD-WAN que ha habido en el mercado. Ver actividad 4.	4. realizar inventario para saber que costos tiene la implementación.

	Se obtuvo una data con información de tiempos de resolución de los incidentes de los enlaces del éxito (SD-WAN) y tuya (WAN). Ver actividad 5.	5. recolectar información para tener una estadística de tiempos de resolución de inconvenientes con WAN y SDWAN.
Implementar la migración sobre la infraestructura de red actual, virtualizando los planos de control y administración, buscando reducir costos.	Se analizó qué equipos son necesarios para la implementación del plano de datos de SDWAN en tuya. Ver actividad 6.	6. Preparar la infraestructura física para la implementación del plano de datos.
	Se muestra como configurar los routers CPE C1111-4P desde VMANAGE para separar el plano de datos del plano de control y administración. Ver actividad 7.	7. separar estos dos planos del plano de datos para una mejor gestión y escalabilidad de la caída de los enlaces.
	Se usa la red MPLS de claro que conecta los routers PE y estos a su vez a los routers CPE. Ver actividad 8.	8. usar la red MPLS existente para usarlo como fabric o nube para interconectar las sedes y darles conectividad y salida a internet.

	Se escoge una sede en la ciudad de Medellín para implementar la prueba. Ver actividad 9.	9. Se va a implementar la prueba piloto para la migración en una sede en la ciudad de Medellín para poder tener una cercanía física de la sede en la cual se van a realizar las pruebas.
Evaluar el desempeño de la migración realizando comparativas con la anterior tecnología en la gestión para examinar el desempeño de la escalabilidad de las caídas o degradación de los enlaces WAN.	Se analiza la información recolectada de tiempos de resolución en almacenes éxitos y tuya y se almacenan en una gráfica. Ver actividad 10.	10. hacer estudios de tiempos de resolución de inconvenientes como caídas de enlaces o degradaciones de los mismos

	Se hacen pruebas de última milla a sede el éxito y a tuya para analizar resultados. Ver actividad 11.	11. Analizar los resultados en cuanto a la mejora de ancho de banda, velocidad de enlaces y conexión garantizada agregando un enlace backup.
	Se comparan los tiempos de resoluciones entre tuya y almacenes éxito. Ver actividad 12.	12. comparar tiempos de resoluciones de inconvenientes de caída y degradación de enlaces, con la tecnología anterior WAN y con la nueva tecnología SDWAN
	Se muestran ventajas de sdwan. Ver actividad 13.	13. Analizar y mostrar ventajas de gestión y monitoreo de la red por medio de la descentralización de los planos de administración y de control.

Actividades

1. Viptela como solución para SDWAN.

2. Infraestructura general de la red WAN de tuya

3. Equipos implementados en la red WAN de tuya.

4. Datos de casos de negocios de implementaciones de SD-WAN que ha habido en el mercado

5. Data con información de tiempos de resolución de los incidentes de los enlaces del éxito (SD-WAN) y tuya (WAN).
6. Equipos necesarios para la implementación del plano de datos de SDWAN en tuya.
7. Configuración de los routers CPE C1111-4P desde VMANAGE para separar el plano de datos del plano de control y administración.
8. Se usa la red MPLS de claro que conecta los routers PE y estos a su vez a los routers CPE.
9. Elección de una sede en la ciudad de Medellín para implementar la prueba.
10. Gráfica de tiempos de resolución de tuya y almacenes éxito.
11. Pruebas de última milla a sede el éxito y a tuya para analizar resultados.
12. Comparación entre los tiempos de resoluciones entre tuya y almacenes éxito.
13. Ventajas de sdwan.

Actividad 1. Viptela como solución para SDWAN.

La tecnología que implementa Cisco para SD-WAN es la tecnología Viptela que es una arquitectura segura a escala de nube, que es abierta, programable y escalable. A través de la consola de Cisco vmanage, se puede establecer rápidamente una estructura de superposición SD-WAN. Es usada para conectar centros de datos, sucursales, campus e instalaciones de colocación para mejorar la velocidad, la seguridad y la eficiencia de la red.

Descripción general

Con el panel de Cisco SD-WAN (Figura 1), puede conectar rápidamente todos los centros de datos de la empresa, ubicaciones centrales y de campus, sucursales WAN, instalaciones de colocación, infraestructura en la nube y trabajadores remotos. Para habilitar esto, Cisco SD-WAN aplica el Protocolo de administración de superposición (OMP) a toda su red. Cisco SD-WAN simplifica las operaciones de TI con aprovisionamiento automatizado, políticas unificadas y administración optimizada, realizando cambios, actualizaciones y resoluciones en un tiempo récord. Obtiene funcionalidad, confiabilidad y seguridad de red avanzadas. [4]

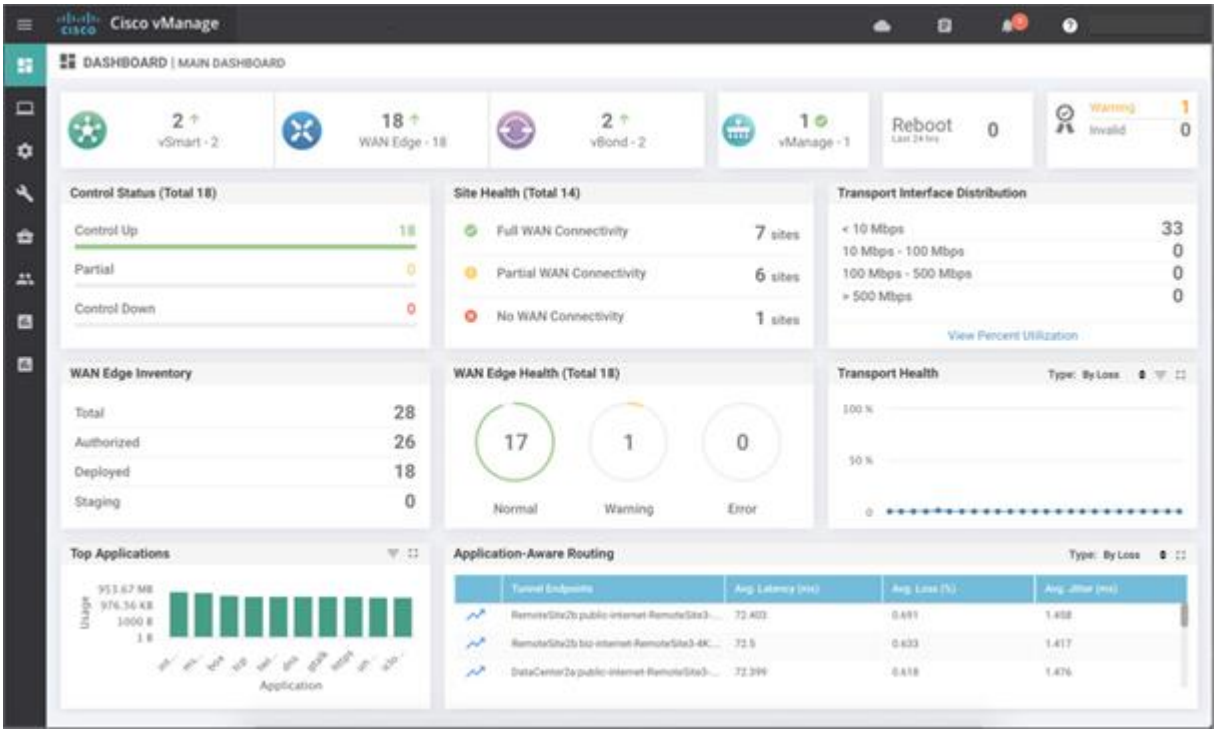


Figura 1. *El panel de Cisco SDWAN, vmanage****. [4]***

Cisco proporciona una arquitectura flexible para extender SD-WAN a cualquier entorno (Figura 2). Ya sea que implemente su producto en la nube o en las instalaciones, Cisco SD-WAN detecta, autentica y aprovisiona automáticamente dispositivos nuevos y existentes.

Después de conectarse a Cisco SD-WAN, cada dispositivo de red puede encontrar la mejor ruta a las aplicaciones que sus usuarios necesitan. Cisco SD-WAN puede utilizar cualquier método de transporte (satélite, banda ancha, MPLS, 5G / LTE) desde cualquier ubicación (núcleo, borde, nube) para cualquier servicio de red (seguridad, calidad de experiencia de la aplicación, voz). A través de OMP, Cisco SD-WAN admite protocolos de enrutamiento comunes y avanzados que son necesarios para administrar redes a través de la WAN y la nube, como BGP, EIGRP, OSPF, VRRP e IPv6. Cisco SD-WAN proporciona esta flexibilidad en entregas cifradas de malla total y parcial, lo que permite la máxima personalización en función de sus necesidades. [4]

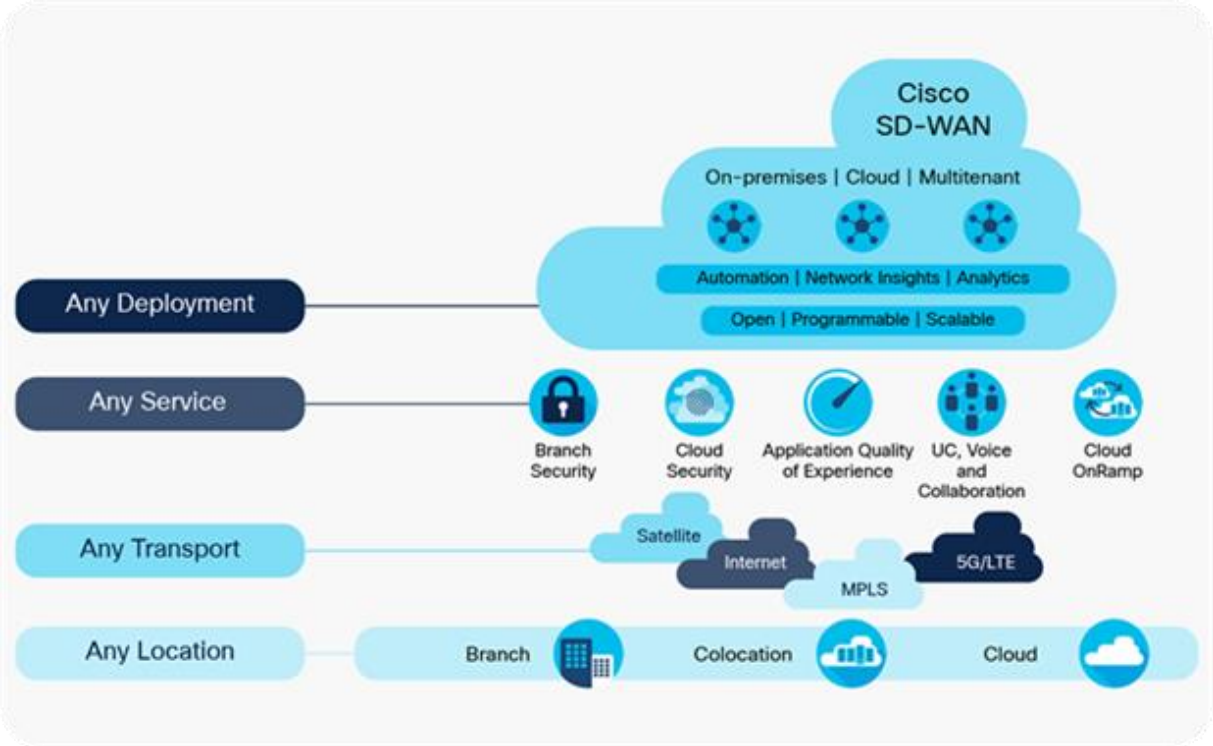


Figura 2. *La arquitectura segura a escala de nube de Cisco SD-WAN [4].*

Actividad 2. Infraestructura general de la red WAN de tuya.

La infraestructura de la red WAN implementada en TUYA consta de un enlace MPLS entre la nube del proveedor de servicios (que en este caso es CLARO telecomunicaciones) y la sede del éxito donde está la red corporativa de la empresa TUYA. Este enlace forma una red de acceso que va desde un router PE (proveedor) hasta un router CPE (cliente).

A. Infraestructura general del enlace entre el proveedor y el cliente (red de acceso)

El enlace entre el router PE (proveedor) y el router CPE (cliente) consta de una red de acceso con switches de acceso distribuidos a lo largo de la línea del enlace entre los routers conectados mediante fibra óptica, estos switches de acceso sirven para conectar otras sedes geográficamente cerca y dependiendo de las necesidades pueden ser de 3 marcas específicas, Huawei, Alcatel o ZTE los cuales se identifican con las siglas HAC, AAC Y ZAC respectivamente. Estos switches de acceso van conectados a los router mediante transceiver o demarcadores (depende de las tasas de bits) para hacer el paso de fibra óptica a cable UTP que es el que finalmente va conectado a los puertos de los routers.

Todas las sedes de la red corporativa de la empresa TUYA están conectadas de esta forma con un enlace MPLS. Estas sedes son algunas tiendas del éxito a nivel nacional, tiendas de alkosto en algunas ciudades del país y sedes administrativas ubicadas en las ciudades de Bello, Medellín y Bogotá.

B. Enlace MPLS

Todas las sedes de la red corporativa TUYA están conectados con intranet mediante MPLS, este enlace es identificado mediante un código el cual identifica el servicio para poder saber desde que router PE e interfaz sale el mismo. Este enlace es monitoreado con una plataforma la cual constantemente realiza pruebas de última milla para conocer el estado del enlace.

Nota: por seguridad y confidencialidad la nomenclatura de los códigos de identificación del servicio y la plataforma de monitoreo usada son omitidos.

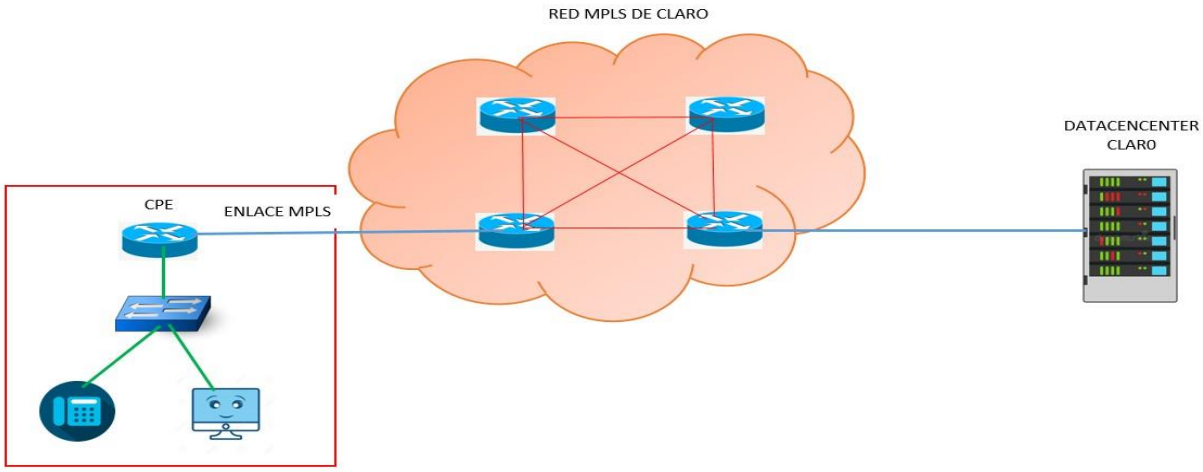


Figura 3. *Diagrama de la red WAN de tuya.*

Actividad 3. Equipos implementados en la red WAN de tuya.

Las sedes de la entidad financiera tarjeta tuya están divididas en sedes administrativas, tiendas del éxito y tiendas alkosto en diferentes zonas del país. Cada una de estas sedes tiene un router CISCO de diferentes modelos que van a ser descritos a continuación.

Sedes administrativas

Las sedes administrativas tienen los siguientes modelos, cisco 881, cisco 4331, cisco 2921.

Modelo cisco 881

Descripción del producto

Los enrutadores de servicios integrados de la serie Cisco 880 son enrutadores de configuración fija que brindan soluciones comerciales colaborativas para la comunicación segura de voz y datos para pequeñas empresas y teletrabajadores empresariales. Ofrecen servicios de banda ancha concurrentes sobre tercera generación (3G), Metro Ethernet y múltiples tecnologías DSL para brindar continuidad comercial. Wireless 802.11ny 3G ofrece movilidad LAN y WAN. Los enrutadores brindan el rendimiento requerido para servicios concurrentes, incluidos firewall, prevención de intrusiones, filtrado de contenido y encriptación para VPN; 802.11g / n opcional para movilidad; y características de calidad de servicio (QoS) para optimizar las aplicaciones de voz y video. Además, la herramienta de configuración Cisco Configuración Profesional basada en la web simplifica la instalación y la implementación. [5]

Models	WAN Interface	LAN Interfaces	802.11g/n Option	Embedded 3G	Integrated ISDN Dial Backup
C881	10/100-Mbps Fast Ethernet	4-port 10/100-Mbps managed switch	No	No	No
Cisco 881	10-/100-Mbps Fast Ethernet	4-port 10-/100-Mbps managed switch	Yes (Cisco 881W)	Yes (Cisco 881G)	No
C886VA	Multimode VDSL2/ADSL2/2+ over ISDN	4-port 10-/100-Mbps managed switch	No	No	Yes
C886VAJ	Multimode VDSL/ADSL Annex J over ISDN	4-port 10-/100-Mbps managed switch	No	No	Yes

Tabla 1. *Modelos de datos de la serie Cisco 880 [5].*

Figura 4. *Enrutador de servicios integrados Cisco 881 con punto de acceso 802.11n integrado [6]*

Feature	Description
Default and maximum flash memory	• 128 MB on Cisco 880 Series data, embedded 3G Wireless WAN (WWAN), and Cisco Unified Border Element models • 256 MB on Cisco 880 Series Voice and SRST models • 256 MB on newer C881-K9, C886VA-K9, C886VAJ-K9, C887VA-K9, C887VAM-K9 and C888-K9 models
WAN	• Fast Ethernet • Multimode VDSL2 and ADSI2/2+ over ISDN with ISDN backup • Multimode VDSL2 and ADSI2/2+ over basic telephone service • ADSL2/2+ over ISDN with ISDN backup • ADSL2/2+ over basic telephone service with ISDN backup • VDSL2 over basic telephone service with ISDN backup • Multimode G.SHDSL (2- and 4-wire support) with ISDN backup • Fast Ethernet and 3G WAN for Code Division Multiple Access (CDMA) and High-Speed Downlink Packet Access (HSDPA)

Tabla 2*. Especificaciones del sistema [6].*

Modelo cisco 4331

Descripción del producto

Los enrutadores de servicios integrados de la serie Cisco ® 4000 (ISR 4000) revolucionan las comunicaciones WAN en la rama empresarial. Con nuevos niveles de convergencia y capacidades de red inteligente integradas, abordan específicamente la creciente necesidad de redes con reconocimiento de aplicaciones en sitios empresariales distribuidos. Estas ubicaciones tienden a tener recursos de TI ajustados. Pero a menudo también tienen una creciente necesidad de comunicación directa con centros de datos privados y nubes públicas a través de diversos enlaces, incluidas las VPN de conmutación de etiquetas multiprotocolo (MPLS) e Internet. La serie ISR 4000 contiene las siguientes plataformas: los ISR 4461, 4451, 4431, 4351, 4331, 4321 y 4221. [7]

Figura 5. *Routers de servicios integrados de la serie Cisco 4000 [7]*

Technical specifications	ISR 4461	ISR 4451	ISR 4431	ISR 4351	ISR 4331	ISR 4321	ISR 4221
Aggregate throughput (default)	1.5 Gbps	1 Gbps	500 Mbps	200 Mbps	100 Mbps	50 Mbps	35 Mbps
Aggregate throughput (Performance license)	3 Gbps	2 Gbps	1 Gbps	400 Mbps	300 Mbps	100 Mbps	75 Mbps
Aggregate Cisco Express Forwarding only[1] throughput (Boost license)	Over 7 Gbps	Over 4 Gbps	Over 4 Gbps	Over 2 Gbps	Over 2 Gbps	1.5 Gbps	1.2 Gbps
Total onboard WAN or LAN 10/100/1000 ports	4	4	4	3	3	2	2
Total onboard WAN or LAN 10-Gbps ports	2	–	–	–	–	–	–
RJ45-based ports	4	4	4	3	2	2	2
SFP-based ports	4	4	4	3	2	1	1
Enhanced service-module slots	3	2	0	2	1	0	0
Double-wide service-module slots	2	1 (assumes no single-wide SM-X modules installed)	0	1 (assumes no single-wide SM-X modules installed)	0	0	0
NIM slots	3	3	3	3	2	2	2
OIR (all I/O modules)	Yes	Yes	Yes	Yes	Yes	Yes	No

Tabla 3. *Enumera las especificaciones generales del producto para la serie ISR 4000. [7]*

Modelo cisco 2921

Descripción del producto

La serie Cisco 2900 se basa en la mejor oferta de su clase de los enrutadores de servicios integrados de la serie Cisco 2800 existentes al ofrecer cuatro plataformas (Figura 1): los enrutadores de servicios integrados Cisco 2901, 2911, 2921 y 2951.

Todos los enrutadores de servicios integrados de la serie 2900 de Cisco ofrecen aceleración de cifrado de hardware integrado, ranuras de procesador de señal digital (DSP) con capacidad de voz y video, firewall opcional, prevención de intrusiones, procesamiento de llamadas, correo de voz y servicios de aplicaciones. Además, las plataformas son compatibles con la gama más amplia de opciones de conectividad inalámbrica y por cable de la industria, como T1 / E1, T3 / E3, xDSL, cobre y fibra GE. [8]

Figura 6. *Routers de servicios integrados de la serie Cisco 2900 [8].*

Feature	Support
Protocols	IPv4, IPv6, Static Routes, Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol (IGMPv3) Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), Distance Vector Multicast Routing Protocol (DVMRP), IPSec, Generic Routing Encapsulation (GRE), Bi-Directional Forwarding Detection (BVD), IPv4-to-IPv6 Multicast, MPLS, L2TPv3, 802.1ag, 802.3ah, L2 and L3 VPN.
Encapsulation	Ethernet, 802.1q VLAN, Point-to-Point Protocol (PPP), Multilink Point-to-Point Protocol (MLPPP), Frame Relay, Multilink Frame Relay (MLFR) (FR.15 and FR.16), High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, X.21, V.35, and EIA-530), Point-to-Point Protocol over Ethernet (PPPoE), and ATM.
Traffic Management	QoS, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Hierarchical QoS, Policy-Based Routing (PBR), Performance Routing (PfR), and Network-Based Advanced Routing (NBAR).

Tabla 4. *Compatibilidad con protocolos y funciones del software IOS de la serie Cisco 2900 ISR G2 [9].*

Sedes de alkosto.

Las sedes de alkosto tienen los router cisco modelo 881-K9 que pertenecen a la familia de la serie Cisco 880 descrito anteriormente.

Sedes de tiendas Éxito.

Las sedes de las tiendas éxito tienen los router cisco modelo 881-K9 que pertenecen a la familia de la serie Cisco 880 descrita anteriormente.

Actividad 4. Datos de casos de negocios de implementaciones deSD-WAN que ha habido en el mercado.

Nota: La siguiente información fue consultada con el duty manager encargado del proyecto de la administración de la red WAN de la entidad financiera tarjeta tuya por eso no se tiene referenciada esta información porque toda esta documentación es de carácter confidencial.

La solución SD-WAN tiene un valor de 44 mil dólares mensuales por 60 meses, que incluye servicio de operación por 5 años, es decir, los agentes de mesa

encargados de la parte de monitoreo y gestión de casos y el personal N1 y N2 (administrador y gerente de proyectos), todas las UM (ÚLTIMAS MILLAS) que incluye la solución con anchos de banda entre 20 y 50 megas de canal dedicado sin reúso. Adicionalmente la solución trae todo el personal ingeniero experto en soluciones SD-WAN, ingenieros de implementación en SD-WAN, desplazamiento a la sede para configuración de los equipos y lo que se relaciona con la parte de direccionamiento y estructuración del proyecto.

Actividad 5. Datos con información de tiempos de resolución de los incidentes de los enlaces del éxito (SD-WAN) y tuya (WAN).

Para realizar el análisis de los tiempos de resolución de los incidentes que se presentan en el éxito (red implementada con SD-WAN) y la entidad financiera tuya (red implementada con WAN tradicional) se deben tener en cuenta dos puntos. El primero es que se van a escoger sedes en la ciudad de Medellín o en su defecto en el área metropolitana dado que la prueba piloto para la migración se quiere implementar en una sede dentro de esta área para poder tener una cercanía física de la sede en la cual se van a realizar las pruebas. El segundo punto es que se debe hacer una aclaración de los tipos de incidentes ya que dependiendo del tipo se van a definir los tiempos de plazo para la solución de estos incidentes.

Las sedes que se van a escoger para tener una estadística de tiempos de resolución de WAN y SD-WAN son las siguientes:

ALMACENES ÉXITO:

AEXI662 - MEDELLIN EXITO JUNIN PPAL – 276
AEXI473 - MEDELLÍN CARULLA LAURELES – 729
XITO357 - MEDELLÍN SURTIMAX BELLO PPAL- 342--SD-WAN
AEXI661-GRUPO ÉXITO_SDWAN_EXITO ITAGUI PPAL – 040
AEXI595_XITO133_EXI_BELLO_2030
AEXI198_XITO056 - MEDELLÍN SURTIMAX SANTA FE DE ANTIOQUIA PORTACHUELO - 453-SDWAN

ENTIDAD FINANCIERA TUYA S.A:

CDM0595 - MEDELLÍN TUYA S.A
CDM0207 - MEDELLÍN COMPANIA DE FINANCIAMIENTO TUYA S.A
CDM0711 - BARRANCABERMEJA TUYA S. A.
CDM0705- IPIALES TUYA S.A CDM0851
CDM0615 - NEIVA TUYA S.A
CDM0592 - MEDELLIN PUNTO CENTRAL TUYA DC NIQUIA

Para los almacenes éxito existen tres tipos de incidentes: incidentes de prioridad 1 (P1), incidentes de prioridad 2 (P2) e incidentes de prioridad 3 (P3). Los incidentes P1 son los que se presentan cuando hay afectación total del enlace, es decir, cuando se presenta simultáneamente afectación del enlace principal y enlace backup. Los incidentes P2 son los que se presentan cuando hay afectación o en el enlace principal o en el enlace backup y por último los incidentes P3 son los que se presentan cuando hay afectación en la red LAN de los almacenes; para

nuestros casos solo nos interesan los incidentes tipo P1 y P2 que son los que conciernen a la red SD-WAN. Para la entidad financiera tuya existe un tipo de incidente de prioridad P1 y se presenta cuando hay afectación en el enlace MPLS que a su vez es el único enlace que tienen las sedes de tuya para conectarse. Los tiempos de resolución de los incidentes tienen un tiempo máximo para ser solucionados y con base en éste se tiene un tiempo de referencia para saber si los incidentes son solucionados a tiempo; estos tiempos de referencia se dan con base en SLA (Service Level Agrement) por sus siglas en inglés acuerdo de nivel de servicio que es el tiempo que se acuerda entre el cliente y proveedor para levantar un servicio (dar solución a un servicio) o cambiar un equipo. De acuerdo al nivel de prioridad de los incidentes se acuerdan los tiempos máximos para que se levante un servicio. Ver tabla 5, 6 y 7.

*Ver Tabla Ciudades TIPO (A, B y C)		TIPO A		
		Tiempo de resolución cuando es falla lógica		Tiempo de resolución cuando es falla física
Tabla 1	Sedes	Configuraciones en el CPE y/o primer Salto	Configuraciones en la red MPLS	
Prioridad Alta	*Caida de los servicios de manera Total o Parcial en un sitio o sede * Perdida de conexión desde los equipos CORE de la Solución, hacia los equipos de la sede o sitio , sin que esta sea atribuible a fallas sobre las F.O o equipos CORE de la sede. * Degradación de los servicios hasta el punto que no puedan ser utilizados. Cuando se presente una pérdida de paquetes superior al 5%, se considera como caida total del servicio así como tiempos de respuesta superiores a los 120 ms.	1 H	2 h	4hr
Prioridad Media	* Falla en puertos de acceso * Degradación de los servicios. Cuando se presente una pérdida de paquetes entre el 5% y el 10% * Intermitencias con intervalos superiores a 20 minutos en el mismo dia.	2 H	3 h	6h
Prioridad Baja	* Degradación de los servicios. Cuando se presenta una pérdida de paquetes inferior al 5% con la cual se perciba una lentitud en la Sede * Intermitencias con intervalos superiores a un día.	4hr	5 h	12h

Tabla 5. *SLA. Tiempos de resolución de inconvenientes.*

*Ver Tabla Ciudades TIPO (A, B y C)		ANS SOLUCIÓN DE INCIDENTES		
		TIPO B		
		Tiempo de resolución cuando es falla lógica		Tiempo de resolución cuando es falla física
Tabla 1	Sedes	Configuraciones en el CPE y/o primer Salto	Configuraciones en la red MPLS	
Prioridad Alta	*Caida de los servicios de manera Total o Parcial en ur sitio o sede * Perdida de conexión desde los equipos CORE de la Solución, hacia los equipos de la sede o sitio , sin que esta sea atribuible a fallas sobre las F.O o equipos CORE de la sede. * Degradación de los servicios hasta el punto que no puedan ser utilizados. Cuando se presente una pérdida de paquetes superior al 5%, se considera como caida total del servicio así como tiempos de respuesta superiores a los 120 ms.	1 H	2 h	6h
Prioridad Media	* Falla en puertos de acceso * Degradación de los servicios. Cuando se presente una pérdida de paquetes entre el 5% y el 10% * Intermitencias con intervalos superiores a 20 minutos en el mismo dia.	2 H	3 h	9h
Prioridad Baja	* Degradación de los servicios. Cuando se presenta una pérdida de paquetes inferior al 5% con la cual se perciba una lentitud en la Sede * Intermitencias con intervalos superiores a un día.	4hr	5 h	15h

Tabla 6. *SLA. Tiempos de resolución de inconvenientes.*

*Ver Tabla Ciudades TIPO (A, B y C)		TIPO C		
		Tiempo de resolución cuando es falla lógica		Tiempo de resolución cuando es falla física
Tabla 1	Sedes	Configuraciones en el CPE y/o primer Salto	Configuraciones en la red MPLS	
Prioridad Alta	*Caida de los servicios de manera Total o Parcial en ur sitio o sede * Perdida de conexión desde los equipos CORE de la Solución, hacia los equipos de la sede o sitio , sin que esta sea atribuible a fallas sobre las F.O o equipos CORE de la sede. * Degradación de los servicios hasta el punto que no puedan ser utilizados. Cuando se presente una pérdida de paquetes superior al 5%, se considera como caida total del servicio así como tiempos de respuesta superiores a los 120 ms.	1,5h	2 h	8h
Prioridad Media	* Falla en puertos de acceso * Degradación de los servicios. Cuando se presente una pérdida de paquetes entre el 5% y el 10% * Intermitencias con intervalos superiores a 20 minutos en el mismo dia.	2,5hr	3 h	10h
Prioridad Baja	* Degradación de los servicios. Cuando se presenta una pérdida de paquetes inferior al 5% con la cual se perciba una lentitud en la Sede * Intermitencias con intervalos superiores a un día.	4hr	5 h	16h

Tabla 7. *SLA. Tiempos de resolución de inconvenientes.*

SERVICIOS DE TUYA

PRIORIDAD_ATENCION	DESCRIPCION	FECHA_CREACION	FECHA_INGRESO_ESTADO	SLA_Calc	Reclasificacion_atencion_Calc	Tiempo_Horas_SLA_Calc	Cumplimiento_Calc
1 - Critical	CDM0595 - MEDELLIN TUYA S.A || Afectación enlace WAN	16/04/2021	17/04/2021	4	Incidente	1,1375	Cumple
1 - Critical	CDM0595 - MEDELLIN TUYA S.A// SIN AFECTACION	19/04/2021	19/04/2021	4	Incidente	0,15805556	Cumple
1 - Critical	CDM0207 - MEDELLIN COMPANIA DE FINANCIAMIENTO TUYA S.A	4/04/2021	6/04/2021	4	Incidente	0,01305556	Cumple
1 - Critical	CDM0705 - IPIALES TUYA S.A || Afectación enlace WAN, Telefonía	1/04/2021 18:35	14/04/2021 19:24	4	Incidente	0,06027778	Cumple
1 - Critical	CDM0705- IPIALES TUYA S.A CDM0851 //Se asocia a falla masiva IM126672	5/04/2021 19:55	6/04/2021 19:55	4	Incidente	0,00972222	Cumple
1 - Critical	CDM0615 - NEIVA TUYA S.A	7/04/2021 20:28	7/04/2021 21:56	4	Incidente	0,0475	Cumple
1 - Critical	CDM0711 - BARRANCABERMEJA TUYA S. A. || Afectación enlace WAN	1/04/2021 21:00	2/04/2021 7:47	4	Incidente	0,04138889	Cumple
1 - Critical	CDM0711 - BARRANCABERMEJA TUYA S. A. || Afectación enlace WAN	3/04/2021 23:36	4/04/2021 6:07	4	Incidente	0,052222	Cumple
1 - Critical	CDM0578 - TUYA S.A - MEDELLIN	13/04/2021 5:28	13/04/2021 7:47	4	Incidente	0,09555556	Cumple
1 - Critical	CDM0716 - MEDELLIN - Calle 41c # 54 - 17	16/04/2021 1:48	16/04/2021 6:52	4	Incidente	0,08027778	Cumple
1 - Critical	CDM0716 - MEDELLIN - Calle 41c # 54 - 17	17/04/2021 9:22	17/04/2021 13:37	4	Incidente	0,10333333	Cumple
1 - Critical	CDM0592 - MEDELLIN PUNTO CENTRAL TUYA DC NIQUIA - BKP-EXITO || Afectación enlace WAN	18/04/2021 23:45	18/04/2021 23:45	4	Incidente	1,96083333	Cumple

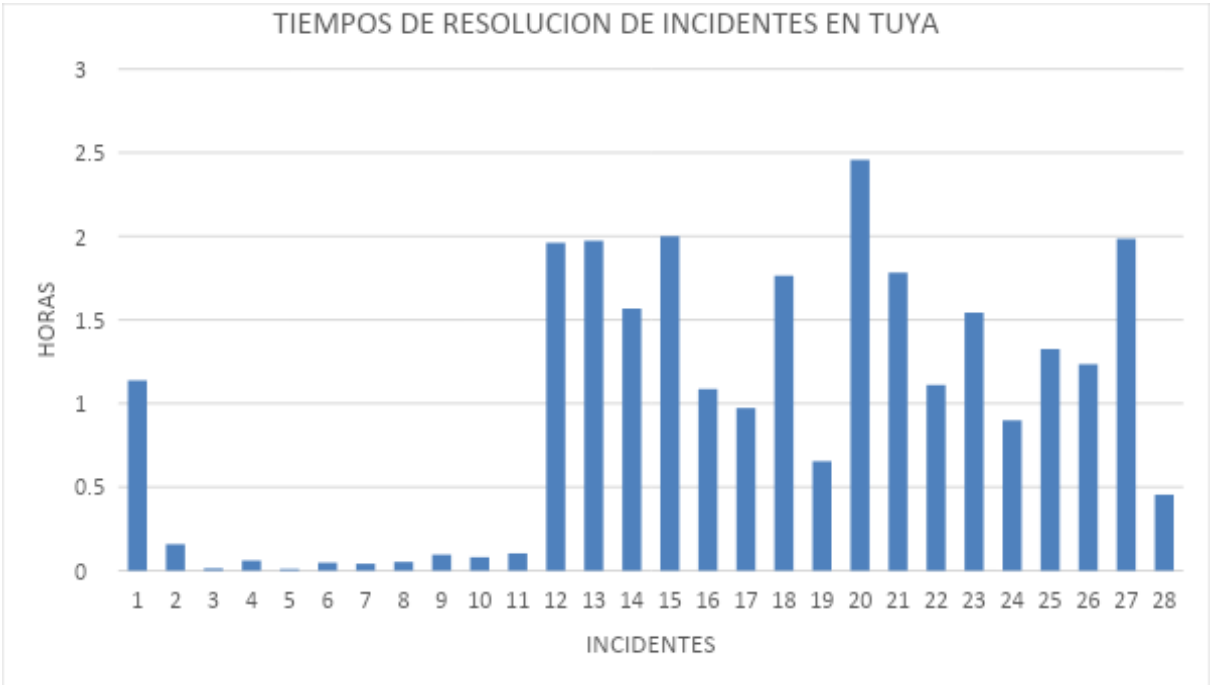
***Tabla 8**. Tiempos de solución de servicios afectados.*

SERVICIOS DE ALMACENES ÉXITO.

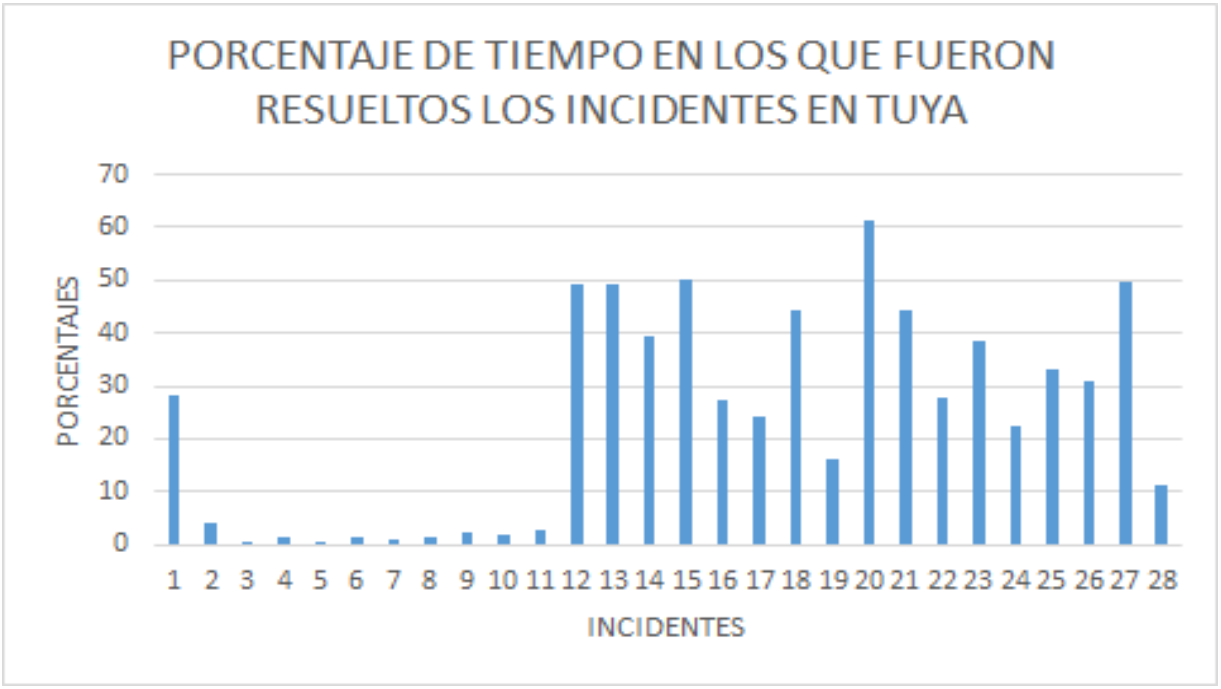
PRIORIDAD_ATENCION	DESCRIPCION	FECHA_CREACION	FECHA_INGRESO_ESTADO	SLA_Calc	Reclasificacion_atencion_Calc	Tiempo_Horas_SLA_Calc	Cumplimiento_Calc
1 - Critical	AEXI662 - MEDELLIN EXITO JUNIN PPAL - 276 || Afectación enlaces WAN	13/04/2021 7:05	13/04/2021 7:31	4	Evento	0,03694444	Cumple
1 - Critical	AEXI662_XITO054_EXITO_JUNIN_2276 // BKP	30/04/2021 8:55	30/04/2021 13:40	6	Incidente	0,78305556	Cumple
2 - High	AEXI473 - MEDELLIN CARULLA LAURELES - 729 || Operativo * B	29/04/2021 23:35	30/04/2021 10:54	6	Incidente	1,69	Cumple
2 - High	XITO357 - MEDELLIN SURTIMAX BELLO PPAL-342--SD-WAN || Afectación enlace WAN PPAL operativo por BKP || RUPTURA DE FIBRA POR VANDALISMO	19/04/2021 2:13	19/04/2021 15:22	6	evento	5,58611111	Cumple
1 - Critical	AEXI661-GRUPO ÉXITO_SDWAN_EXITO ITAGUI PPAL - 040_MPLS_PRIMARIO	13/04/2021 16:36	13/04/2021 17:33	4	Incidente	0,05083333	Cumple
2 - High	AEXI595_XITO133_EXI_BELLO_2030 || RUPTURA DE FIBRA POR VANDALISMO	19/04/2021 11:08	19/04/2021 15:48	6	Incidente	0,025	Cumple

1 - Critical	AEXI595_XITO133_EXI_BELLO_2030	29/04/2021 23:18	30/04/2021 4:58	4	Incidente	0,01111111	Cumple
1 - Critical	AEXI198_XITO056 - MEDELLIN SURTIMAX SANTA FE DE ANTIOQUIA PORTACHUELO - 453-SDWAN || CON AFECTACION// MASIVA SD1378154	29/04/2021 8:08	29/04/2021 11:39	4	Incidente	1,76666667	Cumple

***Tabla 9**. Tiempos de solución de servicios afectados.*

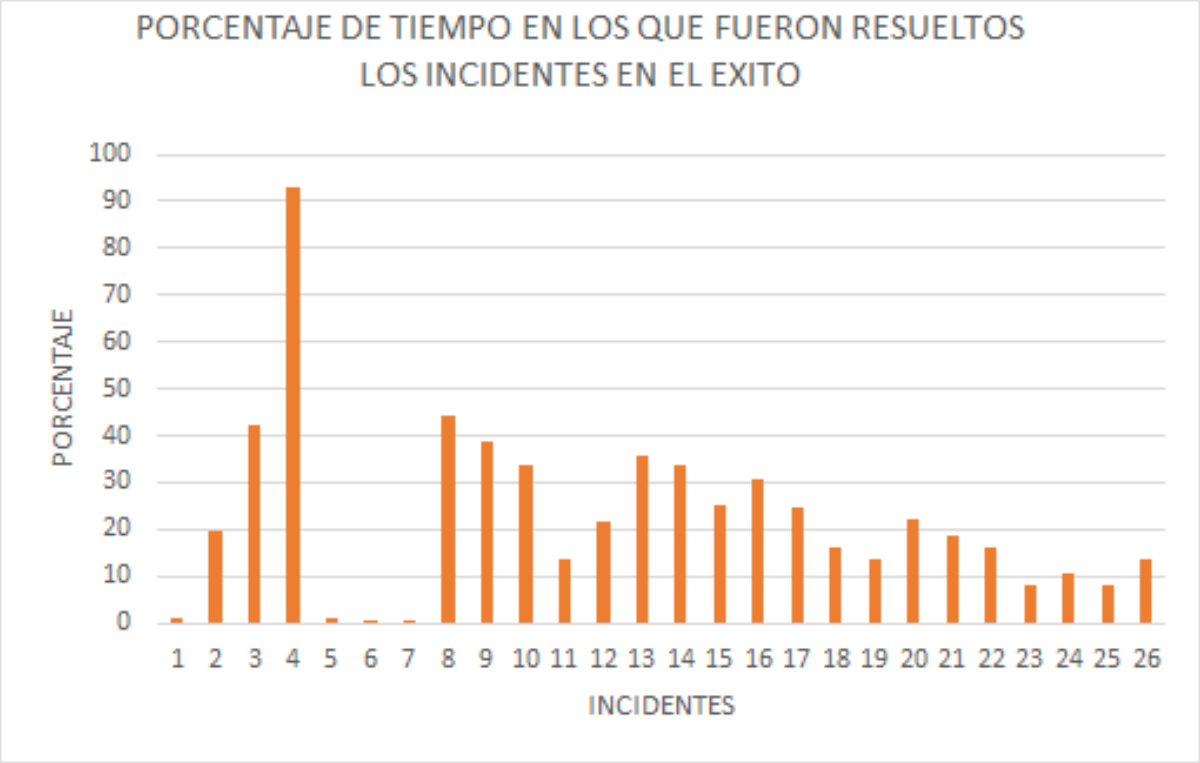


***Gráfica 1**. Tiempos de solución de incidentes de tuya.*



***Gráfica 2**. Porcentaje de tiempo en los que fueron resueltos los incidentes de tuya dentro de los SLA.*

***Gráfica 3**. Tiempos de solución de incidentes de almacenes éxito.*



***Gráfica 4**. Porcentaje de tiempo en los que fueron resueltos los incidentes del éxito dentro de los SLA.*

En la gráfica 1 se puede ver que para la sede de tuya en cuestión no se sobrepasó el tiempo máximo de 4 horas para dar solución al incidente y en la gráfica 2 los tiempos de resolución de los incidentes en tuya no superan el 62% en tiempo de resolución dado a que si se afecta el enlace la sede queda incomunicada y se le debe dar prioridad inmediata a la solución del problema este porcentaje se calcula como el número de horas en que tardó en ser solucionado el problema por 100% sobre el tiempo acordado en SLA para resolver ese tipo de inconveniente (100*#horas/tiempo SLA). También podemos observar en la gráfica 3 los tiempos de resolución de los incidentes en los almacenes éxitos tampoco sobrepasan los tiempos de acuerdo a los SLA y pero se diferencia en que a pesar de que se presente alguna afectación la sede no va a tener afectación total en su operación, en la gráfica 4 existen incidentes que son resueltos cerca del tiempo límite en los SLA dado a que son incidentes críticos como ruptura de fibra o afectación de equipos como routers o switches, sin embargo mientras solucionan estos problemas críticos las sedes siguieron operando por el otro enlace disponible.

Actividad 6. Equipos necesarios para la implementación del plano de datos de SDWAN en tuya.

Para la implementación del plano de datos hay que tener en cuenta que los equipos físicos (routers) ubicados en las sedes deben ser cambiados por routers que soporten SDWAN, estos routers son los modelos C1111-4P y C1111-4PLTEEA el primero es para usar un enlace MPLS y otro enlace banda ancha, el segundo es para usar un enlace banda ancha y otro enlace 4G. Para este caso se va a usar el modelo C1111-4P

Model	C1111-4P
WAN GE	1
WAN GE/SFP combo	1
ADSL2/VDSL2+	N/A
LTE Advanced (CAT6)	N/A
802.11ac	N/A
LAN GE	4
PoE	2
PoE+	1
Integrated USB 3.0 AUX/console	Yes
Dimensions (H x W x D)	1.75 x 12.7 x 9.03 in. (42 x 323 x 230mm) (includes rubber feet)
Weight with AC PS (w/o modules)	5.5 Lbs. (2.5 kg) maximum

***Tabla 10**. Especificaciones router cisco modelo C1111-4P. [10]*

Actividad 7. Configuración de los routers CPE C1111-4P desde VMANAGE para separar el plano de datos del plano de control y administración.

Una vez instalados físicamente los routers cisco modelo C1111-4P en la sede tuya se debe proceder a migrarlos a la tecnología SDWAN separando el plano de datos que son los routers C1111-4P del plano de administración y control. Se debe aclarar que el plano de control ya está separado ya que se van a hacer uso de los routers PE de la red de claro, lo que significa que solo hay que separar el plano de administración. Esto se logra agregando los routers CPE a los templates configurados en vmanage de una forma muy sencilla que va a ser descrita a continuación.

Ubicados en vmanage vamos a la configuración y se elige la opción templates como se ilustra a continuación.

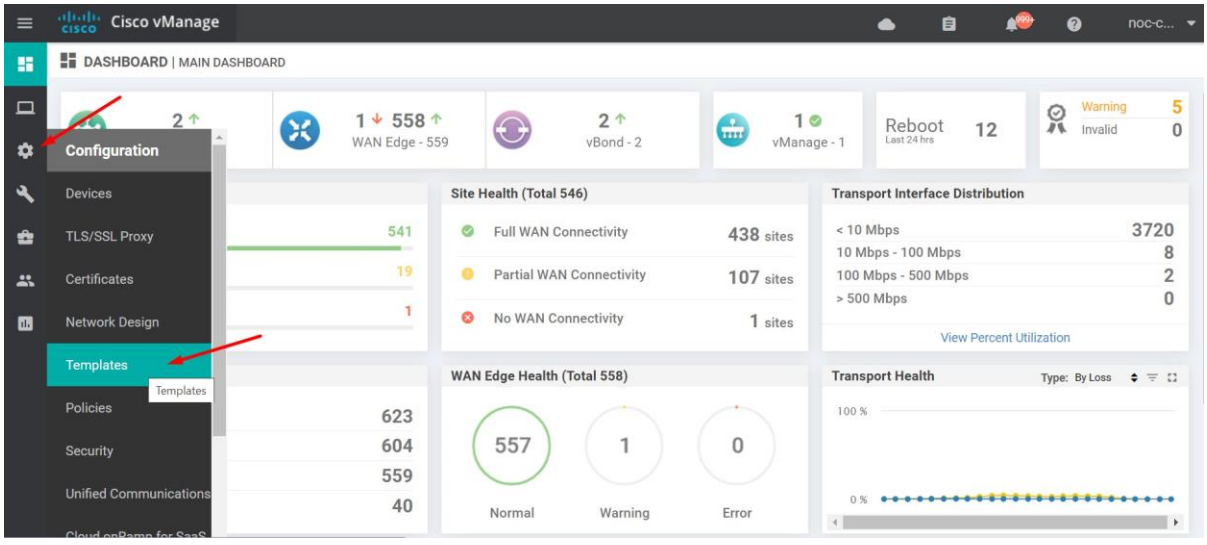


***Figura 7**. Plataforma de monitoreo vmanage.*

Luego se elige el templates, al final se encuentran 3 puntos de forma horizontal, se da clic y se selecciona la opción attach.

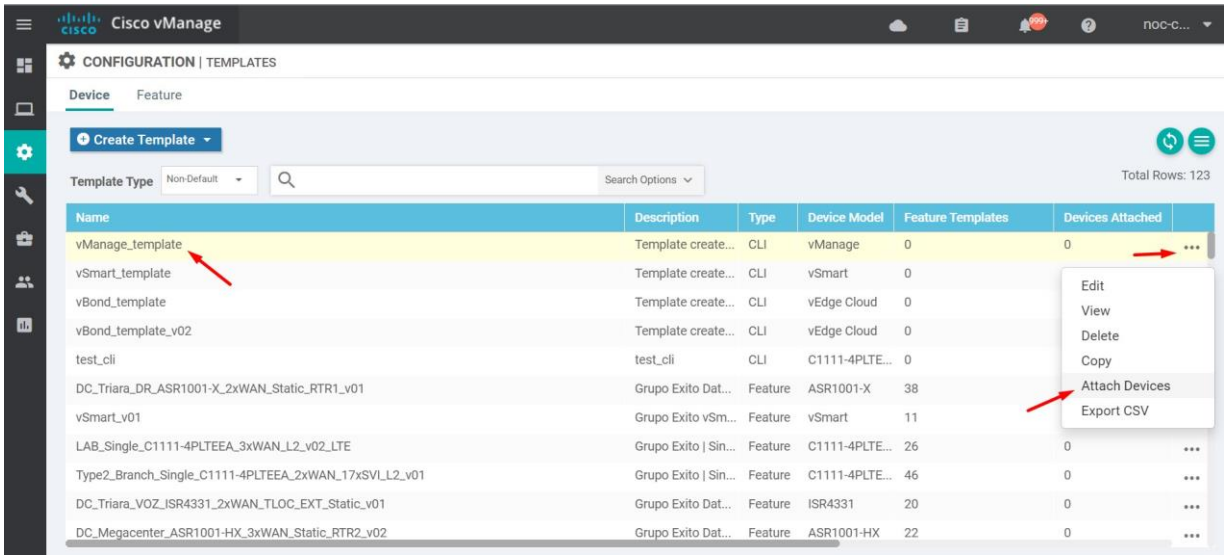


***Figura 8**. Plataforma de monitoreo vmanage.*

Luego de esto se desplegará una ventana en la cual se puede buscar el router de la sede al que se quiere adjuntar el templates.

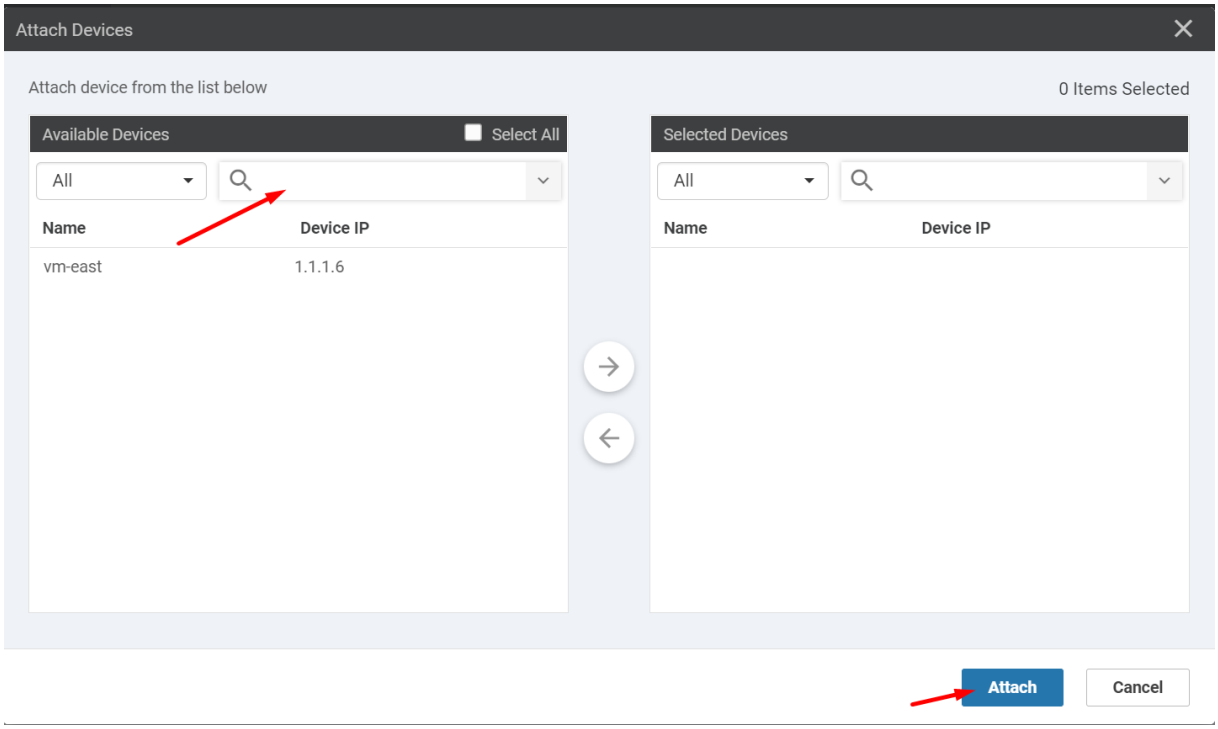


***Figura 9**. Plataforma de monitoreo vmanage.*

Una vez realizados estos pasos ya quedan separados los tres planos para una mejor escalabilidad y resolución de inconvenientes.

La instalación de equipos de oficina en redes SD-WAN puede hacerse de manera automática o a través de dispositivos preconfigurados que no requieren los servicios de ingenieros de campo. Este sistema elimina el mecanismo de instalación tradicional mediante línea de comandos y permite activar los dispositivos con solo conectarlos al cable LAN por esto los costes se reducen**,** porque los dispositivos pueden enviarse a sedes y oficinas sin necesidad de contar con ingenieros de campo.

Actividad 8. Implementación de la red MPLS de claro que conecta los routers PE y estos a su vez a los routers CPE.

Se va a aprovechar la red MPLS que conecta todos los routers PE de Claro para dar conexión a las sedes de tuya, así se le da salida por dos servicios a las sedes, uno por MPLS y otro por internet banda ancha. Esta red de claro está conectada a varios datacenters en las ciudades de Medellín y de Bogotá donde están los servidores en los cuales se almacena información que usan los almacenes éxito en el tráfico de paquetes privado que va por la red MPLS y que usan en las POS, cámaras de seguridad, registros biométricos, por ejemplo; Servidores de tacacs, radius, servidor de hendrix el cual permite acceder remotamente a cualquier router PE de la red para realizar labores de gestión y un servidor el cual tiene salida a internet en caso de que el canal internacional presente afectaciones para que las sedes puedan tener conectividad a internet.

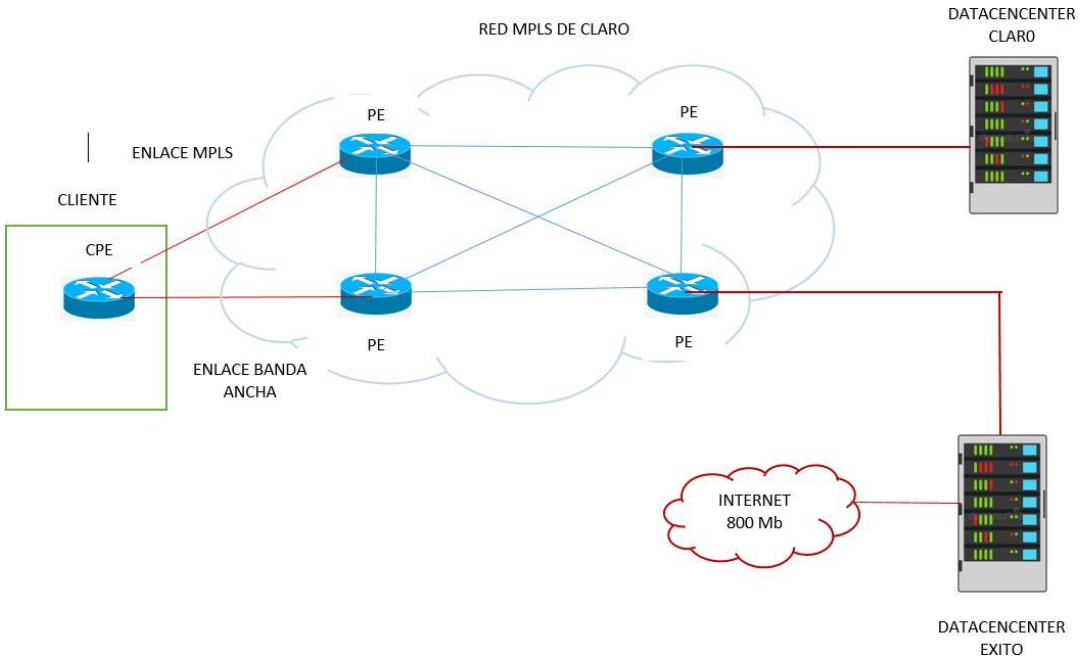


***Figura 10**. Red MPLS de claro conectada a datacenter de claro y éxito.*

Actividad 9. Elección de una sede en la ciudad de Medellín para implementar la prueba.

Como se había dicho anteriormente se va a elegir una sede en la ciudad de Medellín por cercanía y comodidad para implementar una prueba, esta sede se identifica de la siguiente manera CDM0595 - MEDELLÍN TUYA S.A. Como se va a

aprovechar la red MPLS de claro entonces se va a usar el router PE A9KESPACIOSUR (modelo cisco ASR9K Series, ver tabla 9) por el cual iba el servicio de MPLS y de telefonía para implementar el enlace principal, y adicionalmente para implementar un enlace backup se va a usar el router PE A9KSANDIEGO del mismo modelo ya que la sede se encuentra físicamente cerca de este PE. También se va a usar la misma red de acceso por lo que solo habría que habilitar subinterfaces en los routers PE para habilitar los dos servicios de MPLS y de banda ancha.

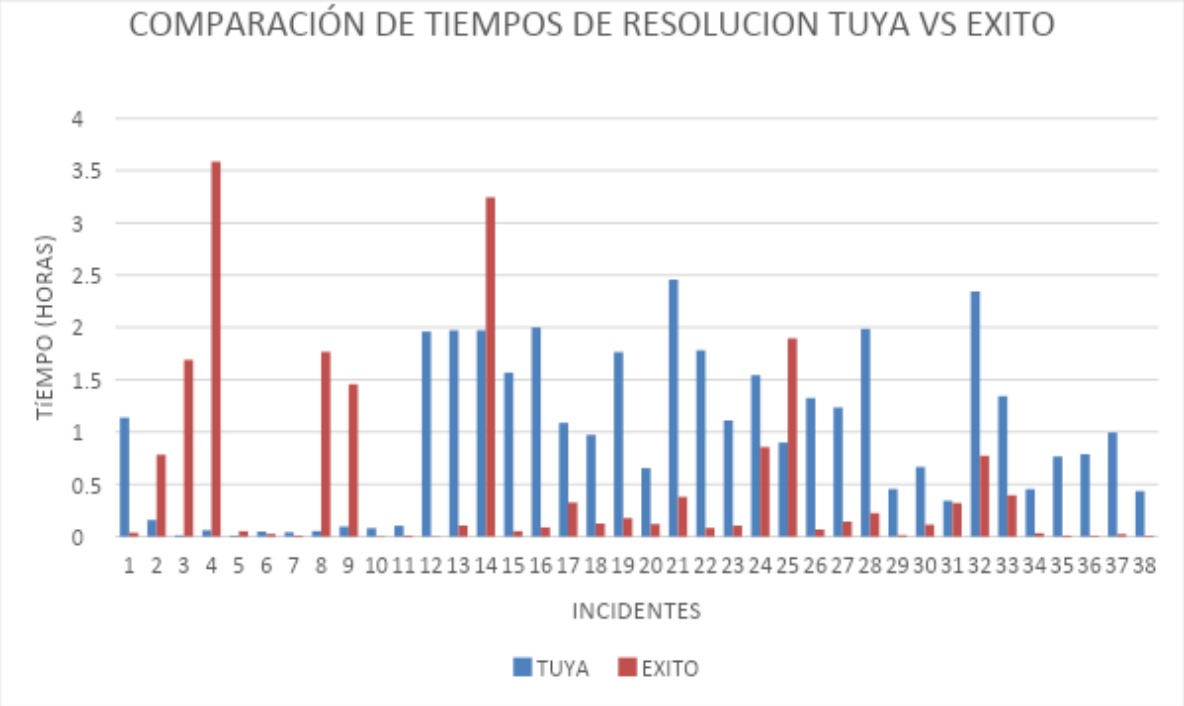
Description	Specification
Physical dimensions (includes ejector bracket/lever); (H x W x D); weight	ASR 9902 chassis (including 2 RPs, 2 PSUs, 3 FANs): H x W x D: 3.45 x 17.3 x 19 in.; 46.39 lb (87.63 x 439.74 x 482.60 mm; 21.04 kg) **Note:** Excluding ejector, the depth is 19 in./482.6 mm
Redundancy	Route processor redundancy Power supply redundancy Fan redundancy Software redundancy
Port density	ASR 9902 chassis with integrated ports: • 2 QSFP-DD ports capable of 10Gb, 40Gb, and 100Gb Ethernet • 6 QSFP28 ports capable of 10Gb, 40Gb, and 100Gb Ethernet • 16 SFP28 dual-rate ports capable of 25Gb and 10Gb Ethernet • 24 SFP+ ports capable of 10Gb Ethernet (LAN) and WAN (OTN)
RP CPU memory	SDRAM DDR4 – 32GB
Rack mounting	2-post and 4-post 19-in. and 23-in.
Airflow	Front to back

***Tabla 11**. Especificaciones router cisco modelo ASR9K Series. [11]*

Una vez identificados los dos routers PE en los cuales van a ser instalados los enlaces principal y backup se procede a configurar el router CPE de la sede como se explicó anteriormente y se usa el enlace MPLS que había como el enlace principal desde el router PE A9KESPACIOSUR y desde el router PE A9KSANDIEGO se habilita una subinterface para el enlace backup banda ancha.

Actividad 10. Gráfica de tiempos de resolución de tuya y almacenes éxito.

Se recolectó información de los tiempos de resolución de los incidentes que se presentan en tuya para la sede identificada con el código de servicio CDM0595 y en almacenes éxito en la sede MEDELLÍN ÉXITO JUNÍN PPAL en el mes de mayo donde de acuerdo a su tipo de prioridad se encontró que los inconvenientes fueron solucionados dentro de los SLA, siendo los incidentes del éxito los que fueron solucionados en el menor tiempo.



***Gráfica 5**. Tiempos de solución de incidentes de almacenes éxito (*MEDELLÍN EXITO JUNÍN PPAL*) y tuya (*CDM0595*).*

Actividad 11. Pruebas de última milla a sede el éxito (MEDELLIN EXITO JUNÍN PPAL) y a tuya para analizar resultados (CDM0595).

Se puede observar que en el enlace MPLS de la sede del éxito MEDELLIN EXITO JUNÍN en condiciones normales no tiene degradación ni pérdidas de paquetes a pesar de que el ancho de banda no es grande, de solo dos 2 megas y a pesar que el tráfico de estas sedes es congestionado, pero por el balanceo de cargas el canal no se ve saturado.

Con la WAN tradicional en la sede de MEDELLÍN-CDM0595 es común que el canal presente saturaciones o pérdidas de paquetes como en la prueba de última milla realizada por eso con SDWAN se mejora la eficiencia del ancho de banda ya que al contar con dos enlaces se divide el tráfico privado del público lo que evita saturación de los canales y pérdidas de paquetes.

Pruebas de última milla al enlace MPLS de la sede del éxito MEDELLIN EXITO JUNÍN PPAL

RP/0/RSP0/CPU0:A9KESPACIOSUR#sh int des | inc AEXI463

Thu Sep 23 11:39:02.071 COLOMBIA

Gi0/0/1/3.888147 up up IPDP ALMACENES EXITO SA GESTION_PROACTIVA PPAL - AEXI463(AEXI780)

RP/0/RSP0/CPU0: A9KESPACIOSUR #sh run int Gi0/0/1/3.888147

Thu Sep 23 11:40:09.531 COLOMBIA

interface GigabitEthernet0/0/1/3.888147

description IPDP ALMACENES EXITO SA GESTION_PROACTIVA PPAL -

```
AEXI463(AEXI780)
 service-policy input CAR-2M
 service-policy output CAR-2M
 vrf grexito-int
 ipv4 address 10.162.115.209 255.255.255.252
 encapsulation dot1q 888 second-dot1q 147
!

RP/0/RSP0/CPU0:A9KESPACIOSUR #sh run int Gi0/0/1/3
Thu Sep 23 11:40:17.575 COLOMBIA
interface GigabitEthernet0/0/1/3
 description TRUNK 8021Q AAG-CALICENTRO-C1 GE4/1/3 - TTI5301 (CERRADA FOL)
 ipv4 redirects
 Load-interval 30
!

RP/0/RSP0/CPU0:A9KESPACIOSUR #ping vrf grexito-int 10.162.115.210
Thu Sep 23 11:40:31.155 COLOMBIA
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.162.115.210, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
RP/0/RSP0/CPU0:A9KESPACIOSUR #ping vrf grexito-int 10.162.115.210 re 500 si 1500
Thu Sep 23 11:40:39.740 COLOMBIA
Type escape sequence to abort.
Sending 500, 1500-byte ICMP Echos to 10.162.115.210, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
Success rate is 100 percent (500/500), round-trip min/avg/max = 3/6/11 ms
RP/0/RSP0/CPU0:A9KCALICENTRO#
```

Pruebas de última milla al enlace banda ancha de la sede del éxito MEDELLIN EXITO JUNÍN PPAL.

RP/0/RSP0/CPU0: A9KESPACIOSUR #sh int des | inc AEXI204
Mon Sep 13 13:52:46.130 COLOMBIA
Te0/0/0/2.854 up up IPDP ALMACENES EXITO GESTION_PROACTIVA - AEXI204,XITO945
RP/0/RSP0/CPU0: A9KESPACIOSUR #sh run int Te0/0/0/2.854
Mon Sep 13 13:53:09.679 COLOMBIA
interface TenGigE0/0/0/2.854
 description IPDP ALMACENES EXITO GESTION_PROACTIVA - AEXI204,XITO945
 service-policy input CAR-12M
 service-policy output CAR-12M
 vrf internet-vip
 ipv4 address 190.145.248.57 255.255.255.252
 encapsulation dot1q 854
!

RP/0/RSP0/CPU0: A9KESPACIOSUR #sh run int Te0/0/0/2
Mon Sep 13 13:53:12.792 COLOMBIA
interface TenGigE0/0/0/2
 description TRUNK 8021Q AAG-DORADO-C1 3/2/4 - UWZ2579 (FOL MTU JUMBO)
 mtu 9216
 ipv4 unreachables disable
 flow ipv4 monitor NFMonMap-IPv4 sampler NFSamMap10GE ingress
 flow ipv4 monitor NFMonMap-IPv4 sampler NFSamMap10GE egress
!

RP/0/RSP0/CPU0: A9KESPACIOSUR #ping vrf internet-vip 190.145.248.58
Mon Sep 13 13:53:27.925 COLOMBIA
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.145.248.58, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
RP/0/RSP0/CPU0: A9KESPACIOSUR #ping vrf internet-vip 190.145.248.58 re 500 si 1500
Mon Sep 13 13:53:45.797 COLOMBIA
Type escape sequence to abort.
Sending 500, 1500-byte ICMP Echos to 190.145.248.58, timeout is 2 seconds:
!!!
!!!

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
Success rate is 100 percent (500/500), round-trip min/avg/max = 2/2/5 ms
```

Pruebas de última milla al enlace MPLS de la sede de tuya CDM0595 en Medellín

```
RP/0/RSP0/CPU0:A9KENVIGADO#sh int des | inc CDM0595
Thu Sep 23 16:38:36.375 COLOMBIA
Gi0/0/0/0.3643      up          up          IPDP TUYA S.A GESTION_PROACTIVA NIQUIA BACKUP CDM0596 - CDM0595
RP/0/RSP0/CPU0:A9KENVIGADO#sh run int Gi0/0/0/0.3643
Thu Sep 23 16:38:46.693 COLOMBIA
interface GigabitEthernet0/0/0/0.3643
 description IPDP TUYA S.A GESTION_PROACTIVA NIQUIA BACKUP CDM0596 - CDM0595
 service-policy input CAR-8M
 service-policy output CAR-8M
 vrf tuya-intranet
 ipv4 address 10.164.237.97/30
 encapsulation dot1q 3643
!

RP/0/RSP0/CPU0:A9KENVIGADO#sh run int Gi0/0/0/0
Thu Sep 23 16:38:50.170 COLOMBIA
interface GigabitEthernet0/0/0/0
 description TRUNK 8021Q AAC-ENVIGADO-C1 GE1/1/20 - TSO9029 (FOL)
 cdp
 ipv4 redirects
 negotiation auto
 load-interval 30
 mac-accounting ingress
 mac-accounting egress
 flow ipv4 monitor FNF_MONITOR_MAP sampler FNF_SAMPLER_MAP ingress
 flow ipv4 monitor FNF_MONITOR_MAP sampler FNF_SAMPLER_MAP egress
!
```

```
RP/0/RSP0/CPU0:A9KENVIGADO#ping vrf tuya-intranet 10.164.237.98
Thu Sep 23 16:39:00.991 COLOMBIA
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.164.237.98, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
RP/0/RSP0/CPU0:A9KENVIGADO#ping vrf tuya-intranet 10.164.237.98 re 500 si
1500
Thu Sep 23 16:39:09.872 COLOMBIA
Type escape sequence to abort.
Sending 500, 1500-byte ICMP Echos to 10.164.237.98, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
Success rate is 99 percent (499/500), round-trip min/avg/max = 1/2/47 ms
RP/0/RSP0/CPU0:A9KENVIGADO#
```

Actividad 12. Comparación entre los tiempos de resoluciones entre tuya y almacenes éxito.

De acuerdo a la información recolectada en la sede del éxito y en la entidad financiera en las ciudades de Medellín se tiene que las afectaciones presentadas en la sede de tuya toman más tiempo en ser resueltas dado a que la gestión para realizar descartes de primer nivel están sometidas a respuestas vía correo electrónico, es por esto que la gestión de los descartes para hacer un diagnóstico del problema es más demorado, además por no existir un enlace backup, la sede queda incomunicada mientras solucionan el problema; se podría implementar un enlace de respaldo sin usar SDWAN pero realizar la conmutación en el tráfico tomaría tiempo dado a que se debe realizar de forma manual, por eso en el éxito los tiempos de resolución de inconvenientes son menores ya que la escalabilidad es más eficaz dado a que se cuenta con vmanage para administrar y gestionar la red SDWAN por lo que los almacenes éxito se ven beneficiados en la implementación técnica de esta tecnología que es el balanceo de cargas de forma rápida y sencilla para dividir el tráfico privado del público y conmutar este tráfico por un solo enlace en caso de verse afectado el otro. Además, otro aspecto muy importante de implementar SDWAN es que la implementación del proyecto cuenta con los agentes de mesa encargados de la parte de monitoreo y gestión de casos y el personal N1 y N2 (administrador y gerente de proyectos), todas las UM (ÚLTIMAS MILLAS) que incluye la solución con anchos de banda entre 20 y 50 megas de canal dedicado sin reúso. Adicionalmente la solución trae todo el personal ingeniero experto en soluciones SD-WAN, ingenieros de implementación

en SD-WAN, desplazamiento a la sede para configuración de los equipos y lo que se relaciona con la parte de direccionamiento y estructuración del proyecto; es por esto que los tiempos de resolución de incidentes en los almacenes éxito son menores que en las sedes de tuya ya que se cuenta con personal que se desplazan a las sedes de manera inmediata para solucionar los problemas, por el contrario para solucionar los problemas en tuya se cuenta con personal externo que de acuerdo a su disponibilidad y al tipo de incidente pueden tardarse más realizar desplazamientos para dar solución a la afectación de la sede.

Actividad 13. Ventajas de sdwan.

Al descentralizar los planos de control (PE) y de datos (CPE) del plano de administración se logra una gran reducción de costos operativos ya que el plano de administración y de control se pueden virtualizar y también se logra reducción de costos en equipos ya que si se quiere añadir una sede a la red sdwan solo habría que cambiar el equipo del cliente, usar la misma infraestructura de la red y añadir desde el plano de administración esta nueva sede de una forma sencilla. Como existe la posibilidad de dividir el tráfico se mejora la eficiencia de ancho de banda evitando saturación de los canales, además de contar con personal 24/7 para el monitoreo, gestión y escalabilidad de los incidentes está mejora en el servicio se ve reflejado en los tiempos de resolución de sdwan ya que son menores que los tiempos de tuya y permitiendo que la sede en la mayoría de los incidentes siempre cuente con conexión ya que existe la posibilidad de conmutar el tráfico por un enlace. A diferencia de lo que ocurre con las redes privadas, la tecnología SD-WAN hace que las aplicaciones ya no tengan que reenviarse a la sede central ya que ésta tecnología sigue las políticas configuradas para determinar automáticamente la forma más efectiva de enrutar el tráfico de aplicaciones entre las sucursales y los sitios del centro de datos.

5. Resultados y Análisis

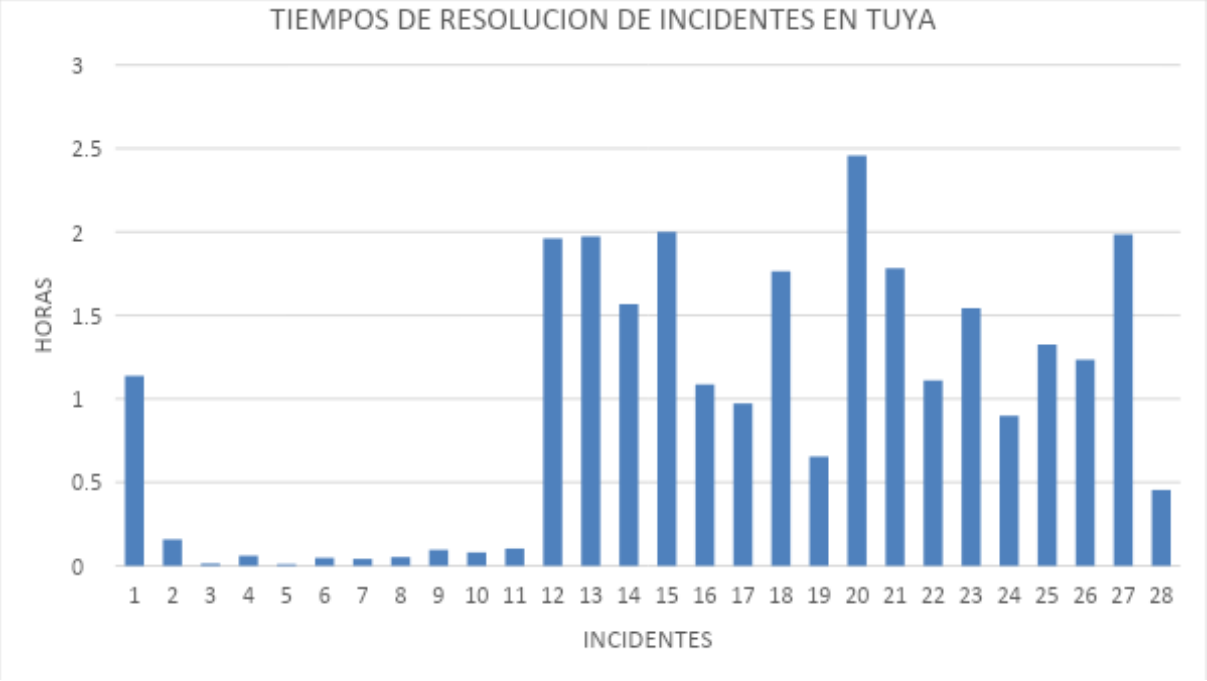
Análisis de las pruebas de última milla realizadas a las sedes MEDELLIN EXITO JUNÍN y MEDELLÍN-CDM0595.

Se puede observar en la prueba de última milla (ver anexo 11) en el enlace MPLS de la sede del éxito MEDELLIN EXITO JUNÍN que en condiciones normales no tiene degradación ni pérdidas de paquetes a pesar de que el ancho de banda no es grande, de solo dos 2 megas y a pesar que el tráfico de estas sedes es congestionado, pero por el balanceo de cargas el canal no se ve saturado.

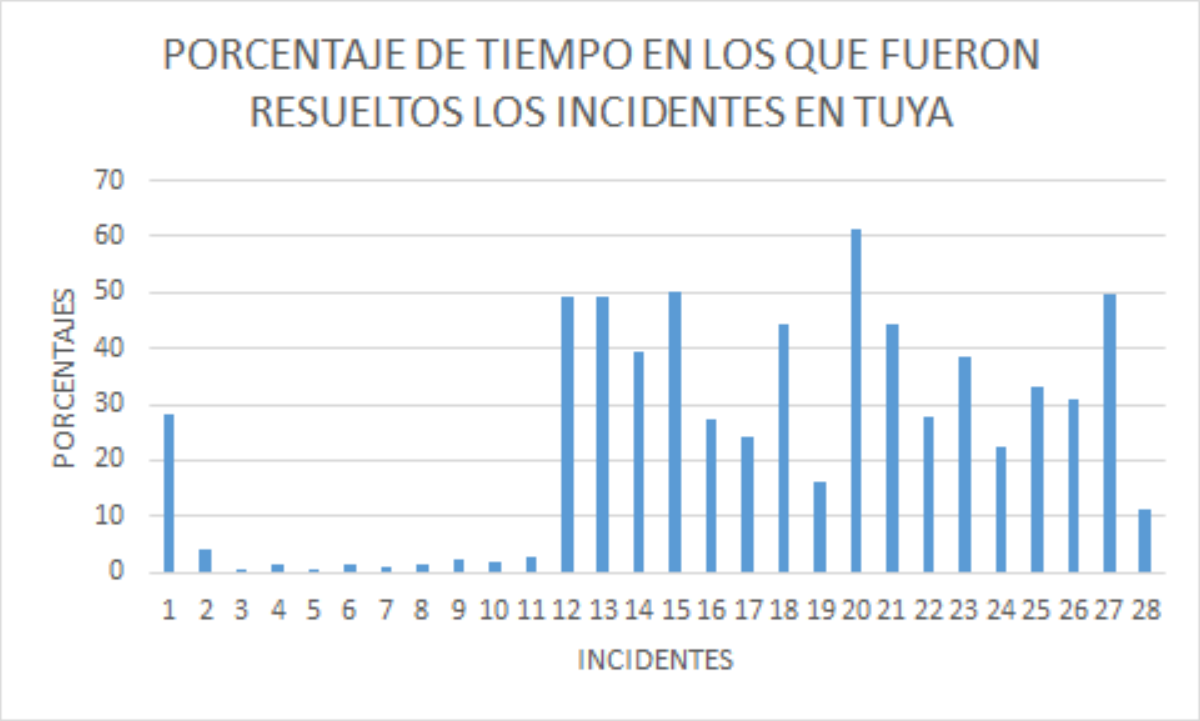
Con la WAN tradicional en la sede de MEDELLÍN-CDM0595 es común que el canal presente saturaciones o pérdidas de paquetes como en la prueba de última milla (ver anexo 11) realizada por eso con SDWAN se mejora la eficiencia del ancho de banda ya que al contar con dos enlaces se divide el tráfico privado del público de manera inmediata y sencilla realizando una conmutación a través de vmanage lo que evita saturación de los canales y pérdidas de paquetes.

Análisis de tiempos de resolución de incidentes.

Tiempos de resolución de la afectación de los enlaces MPLS en tuya en las sedes de Medellín en el mes de mayo. Se observa en la gráfica 2 que los inconvenientes fueron solucionados cumpliendo los acuerdos SLA y no superaron el 62% del tiempo disponible para la resolución. De la gráfica 1 se observa que los incidentes resueltos en menos de 0.5 horas son debido a desajustes en la fibra en los conversores de medio, bloqueo de transceiver o afectación momentánea en el fluido eléctrico; estos incidentes se resuelven de forma simple, ajustando la fibra óptica de manera manual y reiniciando el transceiver respectivamente. Hay que tener en cuenta que cuando se presenta afectación del enlace en los incidentes que toman más de una hora en ser solucionados (ver gráfica 1), la sede de tuya se ve afectada completamente y por eso se gestiona el incidente escalando al área de acuerdo al tipo de afectación ya sea fibra óptica, switch de acceso, transceiver o demarcadores. A diferencia de la implementación de SDWAN en las sedes de la empresa tuya se cuenta con personal externo (tercero) para el desplazamiento a la sede para la solución de la afectación por lo que dependiendo de la disponibilidad del personal el problema puede tomar más tiempo en ser solucionado lo que contrasta con los incidentes de los almacenes éxito que cuentan con personal para el desplazamiento inmediato por esto los tiempos en los que se solucionan los incidentes son menores (ver gráfica 3).

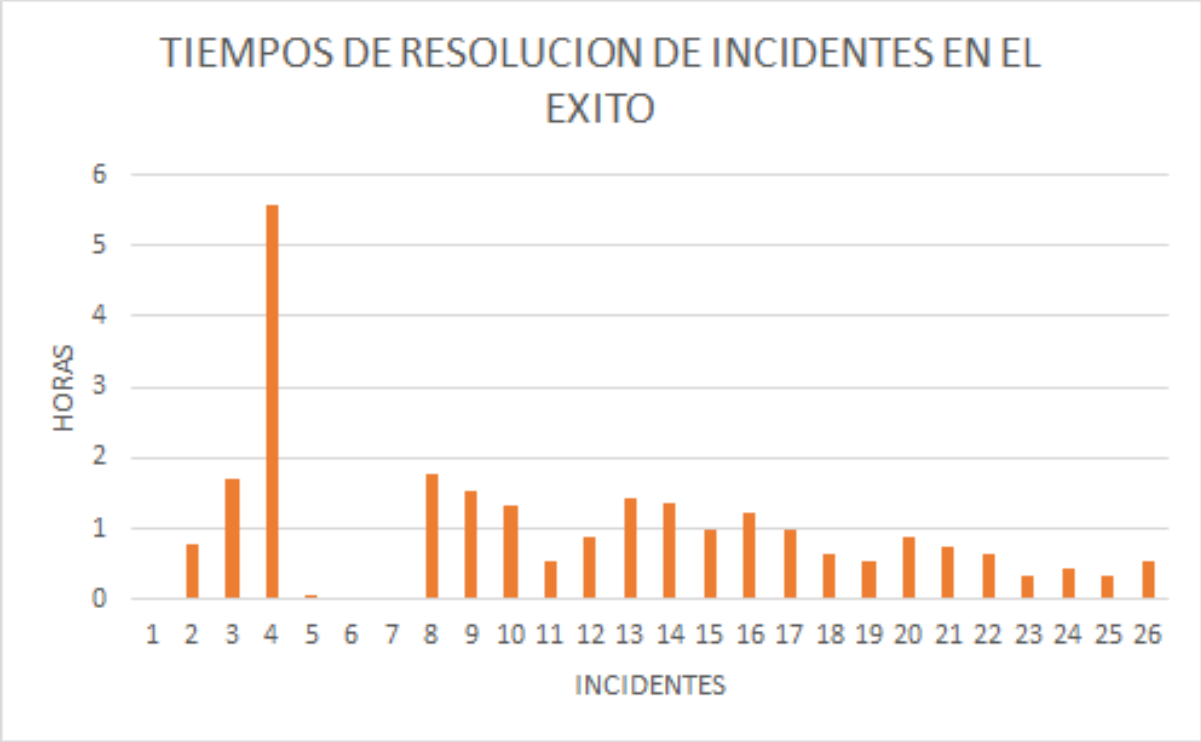


***Gráfica 1**. Tiempos de solución de incidentes de tuya donde el tiempo medio de resolución es 0,9488 horas.*

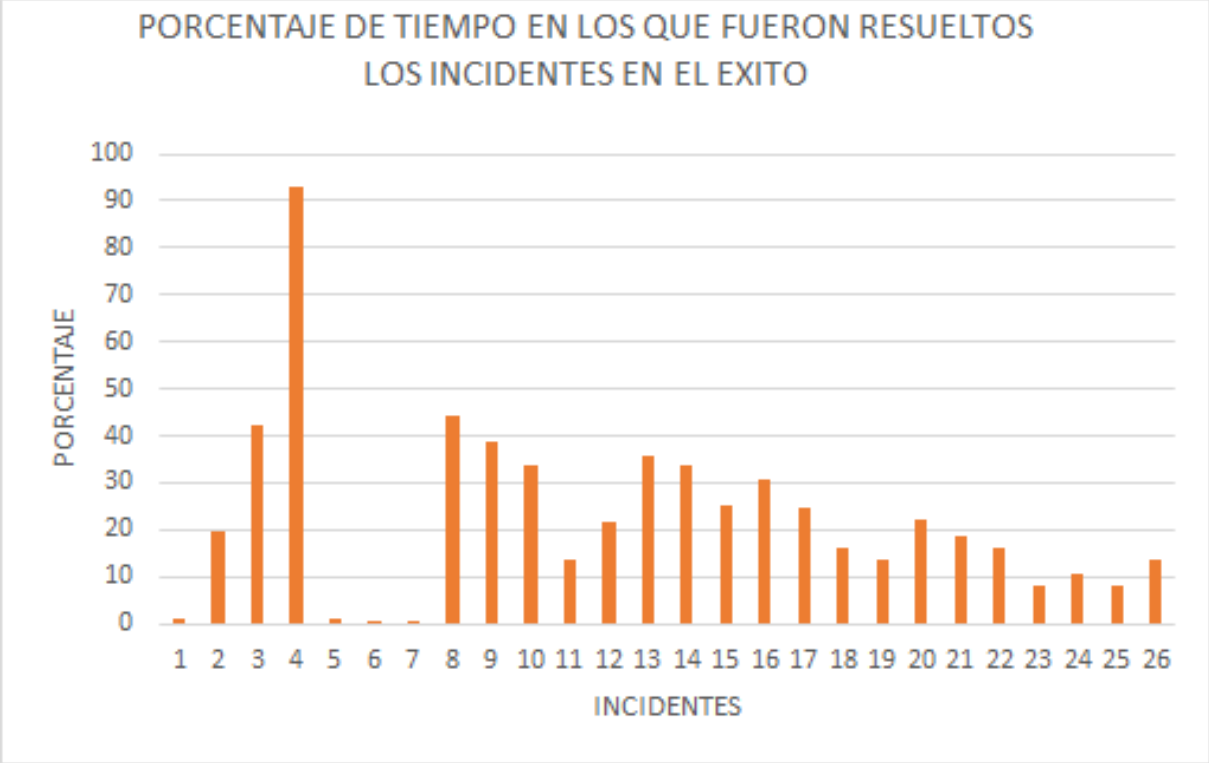


***Gráfica 2**. Porcentaje de tiempo en los que fueron resueltos los incidentes de tuya dentro de los SLA.*

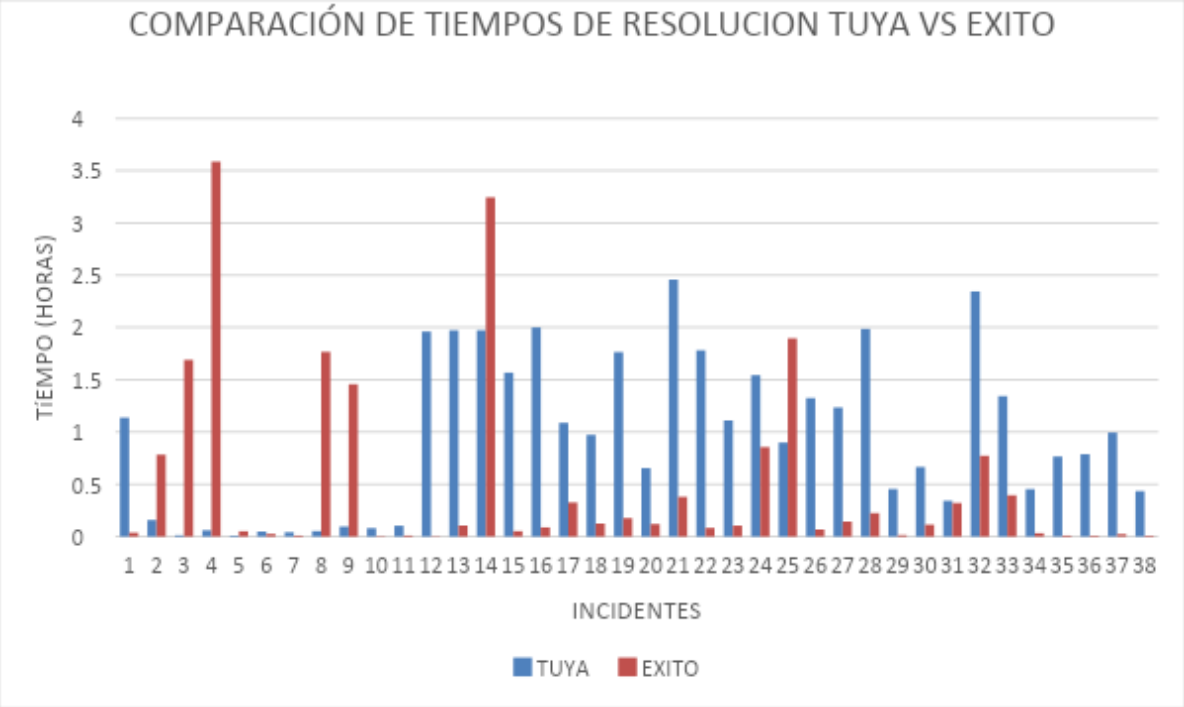
Tiempos de resolución de la afectación de los enlaces MPLS y banda ancha en almacenes éxito en las sedes de Medellín en el mes de mayo. Se observa que los inconvenientes fueron solucionados cumpliendo los acuerdos SLA y no superaron el 93% del tiempo disponible para la resolución como puede ser visto en la gráfica 4. Los inconvenientes que se demoraron más tiempo en ser solucionados (ver gráfica 3) se debe a que la afectación del enlace fue por daños en la fibra óptica o afectación de equipos de la red a acceso afectando uno de los dos enlaces, para este tipo de inconvenientes se escala a personal de claro encargados de realizar descartes y realizar reemplazo de transceiver o fusionar fibra óptica. Mientras ocurría la afectación se realizó conmutación de tráfico rápidamente gracias al balanceo de cargas que ofrece SDWAN permitiendo que los paquetes que iban por banda ancha vayan a través del enlace MPLS y viceversa. Se debe tener en cuenta si hay tiempos altos es porque la sede en ese momento no tuvo afectación completa y pudo estar conectada mientras estaba afectado el otro canal. Los demás tiempos de resolución son realmente bajos dado a que si se presenta afectación completa en una sede (se ve afectado el enlace principal y backup) se debe realizar descartes de primer nivel de forma inmediata y escalar el caso dependiendo de la afectación (como por ejemplo pérdida de alcanzabilidad hacia equipos de red de acceso, daños en conversores de medios, ruptura de fibra óptica, daños en ONT´s o routers) para dar solución lo más rápido posible y no impactar en mayor grado la operación de los almacenes por eso para SDWAN se cuenta con desplazamiento de personal de inmediato una vez se identifica el problema y se realiza el escalamiento.



***Gráfica 3**. Tiempos de solución de incidentes de almacenes éxito donde el tiempo medio de resolución es de 0,9164 horas.*



***Gráfica 4**. Porcentaje de tiempo en los que fueron resueltos los incidentes del éxito dentro de los SLA.*



Gráfica 5*. Tiempos de solución de incidentes de almacenes éxito (*MEDELLÍN ÉXITO JUNÍN PPAL*) y tuya (*CDM0595*).*

Observando la gráfica 5 donde se comparan los tiempos de resoluciones, los inconvenientes en el éxito fueron resueltos la gran mayoría en menos de una hora teniendo en cuenta que estas afectaciones se presentaron en uno de los dos enlaces permitiendo que la sede no quedara incomunicada al realizar conmutación en el tráfico de paquetes de manera inmediata a través de vmanage una vez fue identificado el tipo de afectación, esta conmutación de paquetes se mantiene activa mientras se restablece el servicio por el otro enlace de la sede. En cambio la resolución de los inconvenientes en tuya se demoran más en ser solucionados y restablecer el servicio, esto ocasiona que la sede quede incomunicada durante este periodo de tiempo ya que no está la opción de realizar el balanceo de cargas con el tráfico de paquetes porque en tuya no se puede gestionar los incidentes a través de vmanage y dado el caso de que exista un enlace backup en la sede está conmutación debe realizarse de forma manual lo que lleva más tiempo.

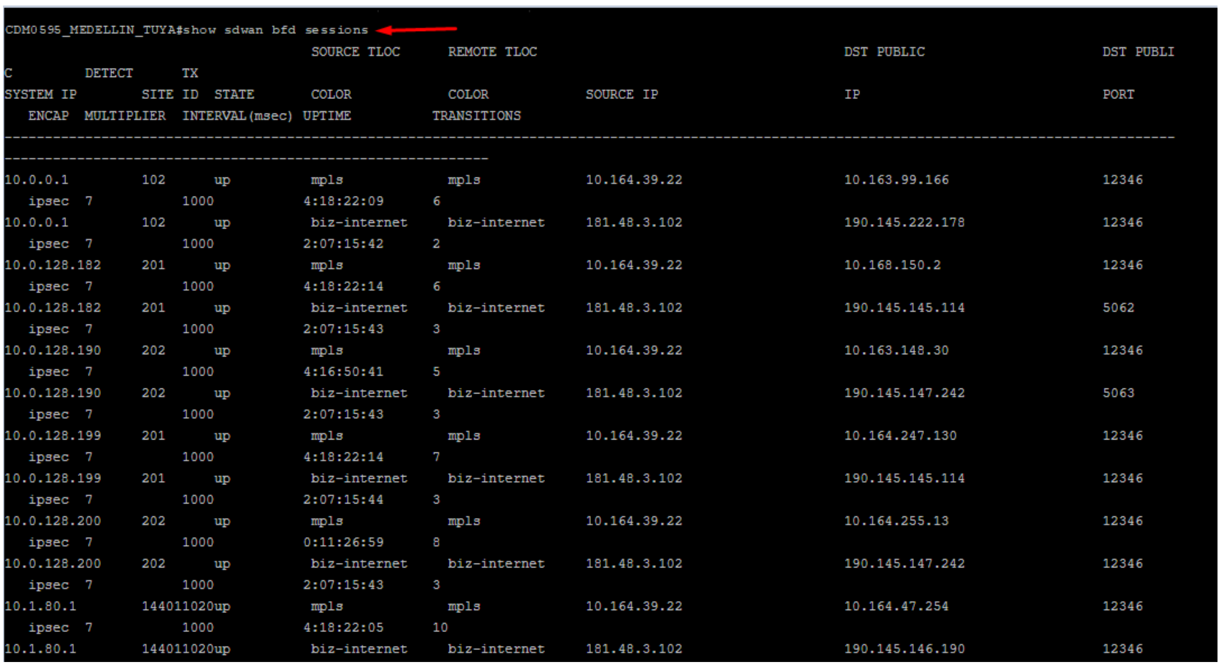
Resultados de la implementación de la sede de tuya a SDWAN.

En este orden de ideas, en la sede se puede programar de forma remota el dispositivo periférico (en este caso el router modelo C1111-4P) de la red sin intervención o con poco contacto minimizando o eliminando la necesidad de que los ingenieros de red configuren manualmente los enrutadores en las sucursales, una vez configurado este dispositivo aparecerá en la plataforma de monitoreo de vmanage permitiendo acceder al router de forma ágil y sencilla para poder realizar gestión y monitoreo como el estado de las conexiones de los dos enlaces o las sesiones bfd de sdwan (ver figura 10 y 11).

```
10.129.240.1 login: telmexuser
telmexuser@10.129.240.1's password:
Password:
ATENCION: Este equipo es propiedad de TELMEX Colombia. El uso no autorizado esta estrictamente prohibido. Todos los usuarios son legalmente respo
nsables de sus acciones sobre el sistema y toda actividad sera registrada


CDM0595_MEDELLIN_TUYA#show sdwan control connections
                                                                                                PEER                                          PEER
                                 CONTROLLER
PEER    PEER PEER            SITE       DOMAIN PEER                                             PRIV  PEER                                    PUB
                                 GROUP
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                                       PORT  PUBLIC IP                               PORT  LOCAL
COLOR     PROXY STATE UPTIME      ID
-------------------------------------------------------------------------------------------------------------------------------------------------
---------------------------------------
vsmart  tls  1.1.1.5         4294946707 1      10.0.5.20                                        23556 52.53.98.76                             23556 mpls
          No    up     1:12:13:04  0
vsmart  tls  1.1.1.5         4294946707 1      10.0.5.20                                        23556 52.53.98.76                             23556 biz-in
ternet    No    up     1:12:13:00  0
vsmart  tls  1.1.1.4         4294946708 1      10.0.2.130                                       23556 34.230.159.72                           23556 mpls
          No    up     1:12:13:14  0
vsmart  tls  1.1.1.4         4294946708 1      10.0.2.130                                       23556 34.230.159.72                           23556 biz-in
ternet    No    up     1:12:13:02  0
vmanage dtls 1.1.1.6         4294946709 0      10.0.8.57                                        12446 3.233.9.39                              12446 mpls
```

Figura 10. *Gestión y monitoreo de los enlaces ppal y bkp de CDM0595 TUYA.*



```
CDM0595_MEDELLIN_TUYA#show sdwan bfd sessions
                                      SOURCE TLOC      REMOTE TLOC                                      DST PUBLIC                       DST PUBLI
C         DETECT      TX
SYSTEM IP        SITE ID  STATE       COLOR            COLOR            SOURCE IP                       IP                               PORT
   ENCAP  MULTIPLIER  INTERVAL(msec) UPTIME          TRANSITIONS
-------------------------------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------
10.0.0.1         102      up          mpls             mpls             10.164.39.22                    10.163.99.166                    12346
   ipsec  7           1000           4:18:22:09      6
10.0.0.1         102      up          biz-internet     biz-internet     181.48.3.102                    190.145.222.178                  12346
   ipsec  7           1000           2:07:15:42      2
10.0.128.182     201      up          mpls             mpls             10.164.39.22                    10.168.150.2                     12346
   ipsec  7           1000           4:18:22:14      6
10.0.128.182     201      up          biz-internet     biz-internet     181.48.3.102                    190.145.145.114                  5062
   ipsec  7           1000           2:07:15:43      3
10.0.128.190     202      up          mpls             mpls             10.164.39.22                    10.163.148.30                    12346
   ipsec  7           1000           4:16:50:41      5
10.0.128.190     202      up          biz-internet     biz-internet     181.48.3.102                    190.145.147.242                  5063
   ipsec  7           1000           2:07:15:43      3
10.0.128.199     201      up          mpls             mpls             10.164.39.22                    10.164.247.130                   12346
   ipsec  7           1000           4:18:22:14      7
10.0.128.199     201      up          biz-internet     biz-internet     181.48.3.102                    190.145.145.114                  12346
   ipsec  7           1000           2:07:15:44      3
10.0.128.200     202      up          mpls             mpls             10.164.39.22                    10.164.255.13                    12346
   ipsec  7           1000           0:11:26:59      8
10.0.128.200     202      up          biz-internet     biz-internet     181.48.3.102                    190.145.147.242                  12346
   ipsec  7           1000           2:07:15:43      3
10.1.80.1        144011020up          mpls             mpls             10.164.39.22                    10.164.47.254                    12346
   ipsec  7           1000           4:18:22:05      10
10.1.80.1        144011020up          biz-internet     biz-internet     181.48.3.102                    190.145.146.190                  12346
```

Figura 11. *Gestión y monitoreo de las sesiones bfd sdwan de CDM0595 TUYA.*

Una vez agregada la sede CDM0595 de tuya a vmanage automáticamente se tiene el balanceo de cargas para dividir el tráfico por los dos enlaces y así poder evitar saturaciones o degradaciones, una vez que en vmanage se detecte caída de alguno de los dos enlaces se procede a conmutar el tráfico de paquetes por el enlace que está operativo, es decir, se debe excluir a la sede de la política DIA (Direct Internet Access) para poder conmutar el tráfico por el enlace que está operativo. A continuación se muestra como realizar el procedimiento de conmutación para la sede en cuestión.

Procedimiento para excluir una sede de la política del DIA

1. Se debe ir a la opción de **policies**:

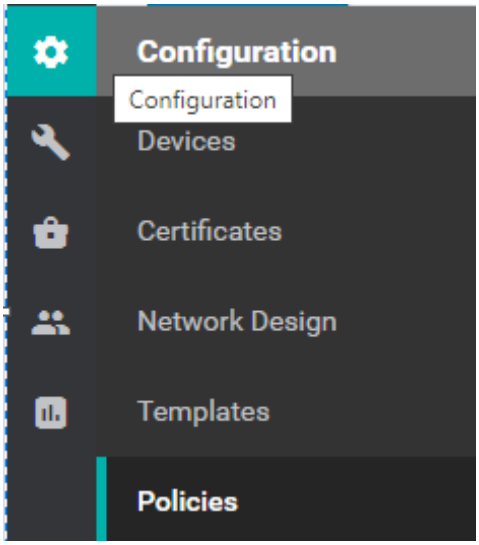


Figura 12. *Procedimiento para excluir una sede de la política del DIA.*

2. Se escoge la opción de lista dentro de la política centralizada:

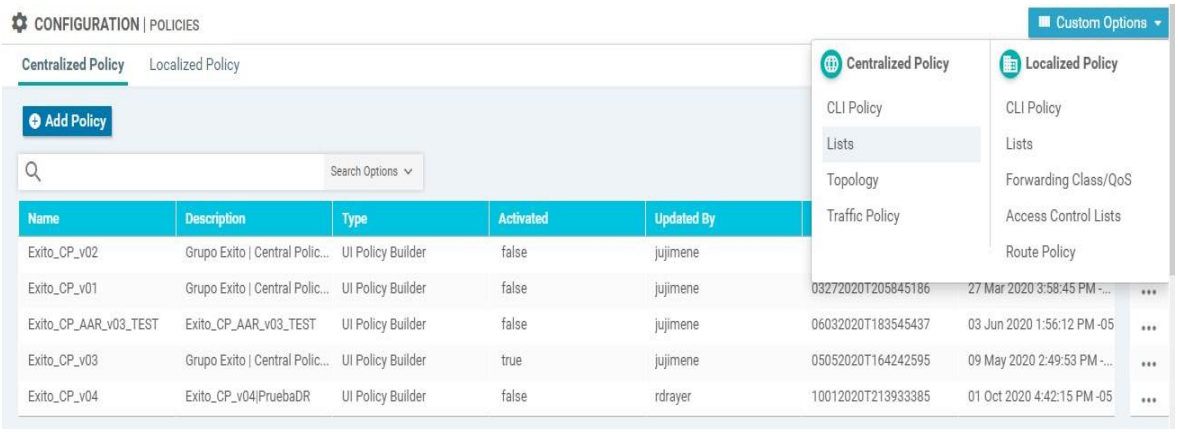


Figura 13. *Procedimiento para excluir una sede de la política del DIA.*

3. Luego dentro de las opciones se elige la opción **Site,** seguidamente se escoge el **name Branches_DIA**

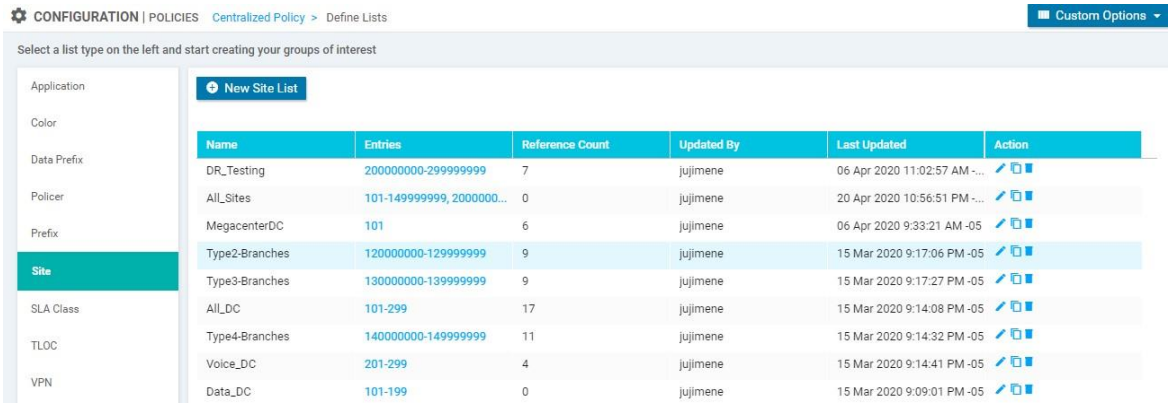


Figura 14. *Procedimiento para excluir una sede de la política del DIA.*

4. Se procede a editar el **Site List,** y al final de la lista se coloca el site que se quiere excluir de la política de DIA, se presiona el botón **save** y luego **activate**

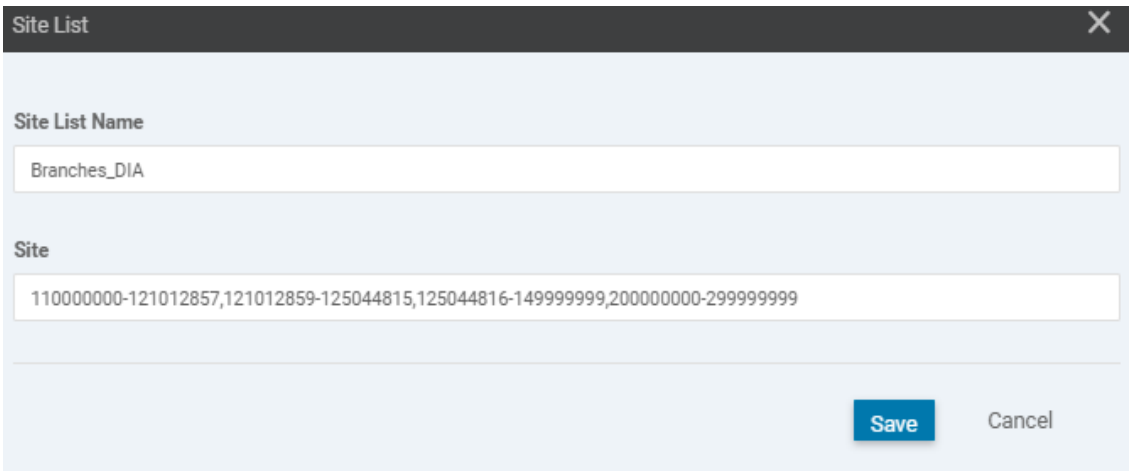


Figura 15. *Procedimiento para excluir una sede de la política del DIA.*

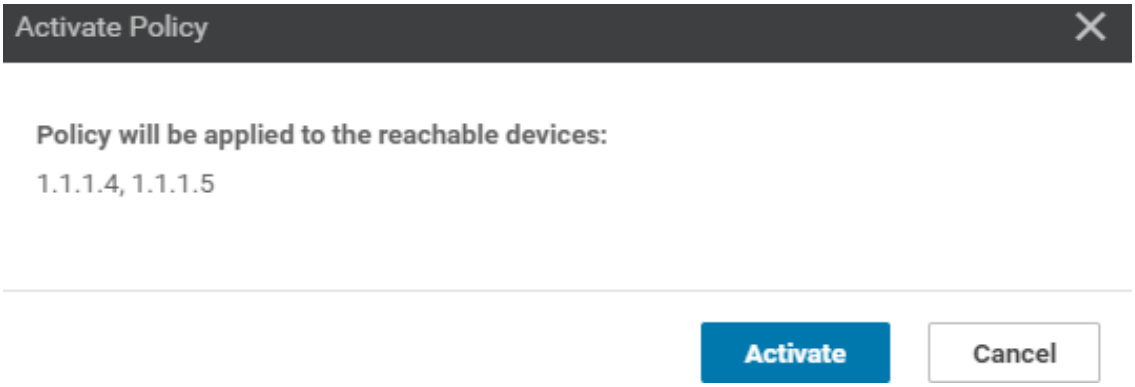


Figura 16. *Procedimiento para excluir una sede de la política del DIA.*

5. Se mostrará esta pantalla, listando los vsmart:

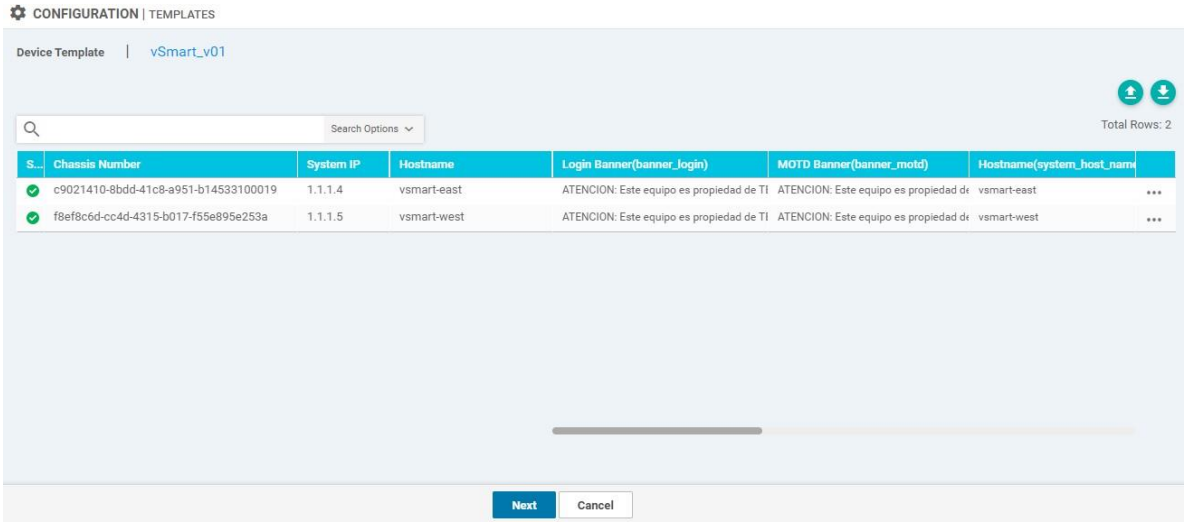


Figura 17. *Procedimiento para excluir una sede de la política del DIA.*

6. Se mostrará la siguiente imagen, se presiona el nombre del dispositivo (device list), Config Diff y luego side by side diff:

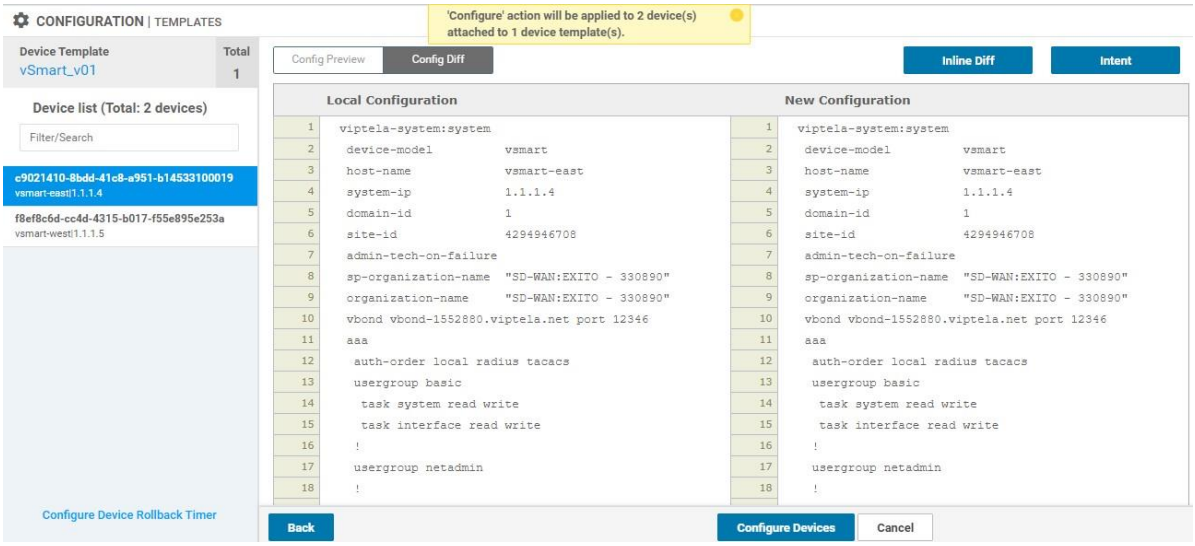


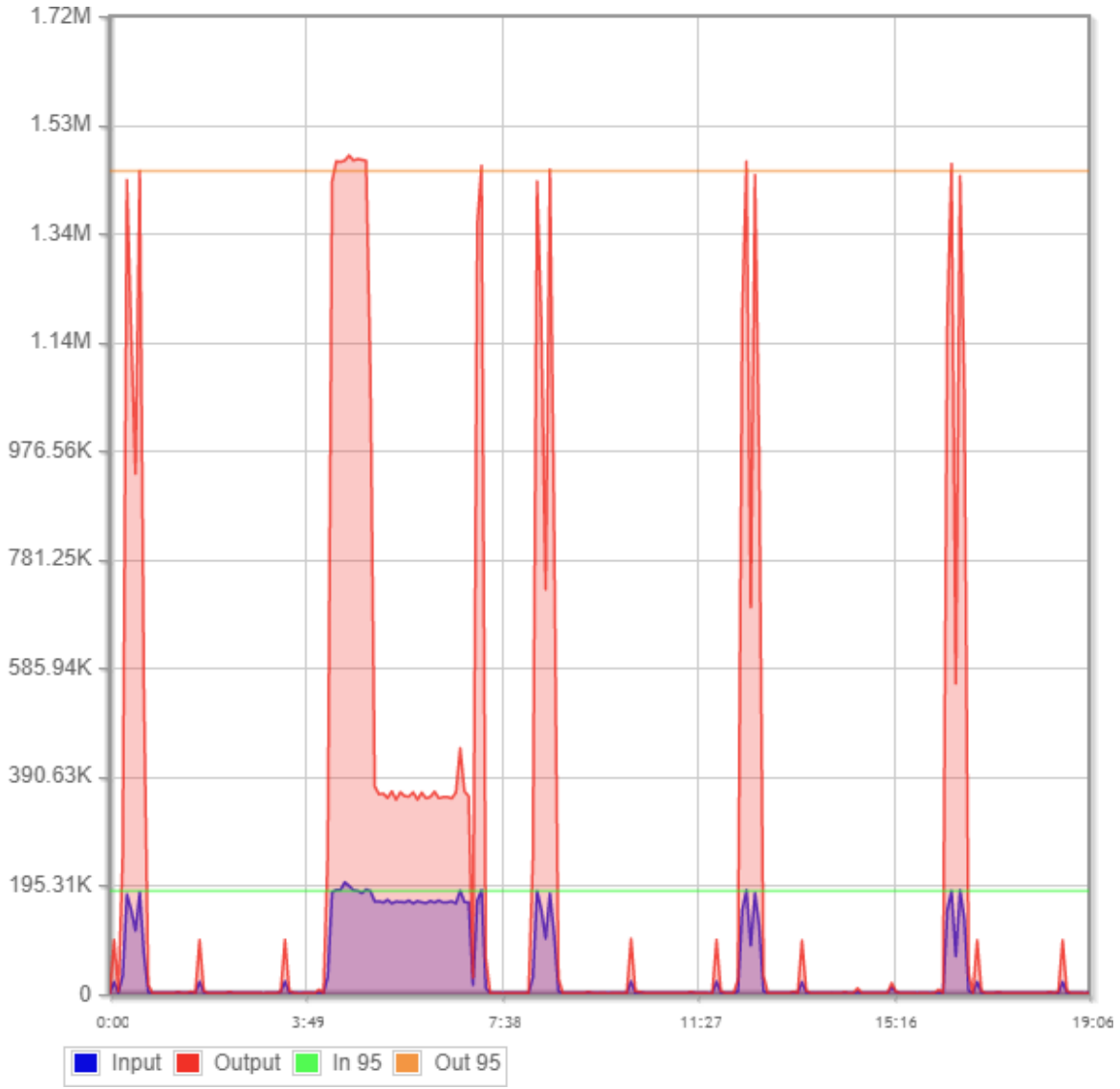
Figura 18. *Procedimiento para excluir una sede de la política del DIA.*

7. Se aplica el cambio y luego se selecciona el botón **configure devices**.

8. Luego se repite el procedimiento del punto 4 nuevamente y se incluye el site ID en la política de **Branches_No_DIA_Fallback**:

Figura 19. *Procedimiento para excluir una sede de la política del DIA.*

De esta forma se conmuta el tráfico de la sede permitiendo la operación de la misma mientras se dé solución al otro enlace afectado.



***Gráfica 6**. Tráfico enlace MPLS de la sede* CDM0595 de tuya con la WAN tradicional.

En la gráfica 6 el enlace MPLS tiene un ancho de banda de 2M se puede observar que antes de implementar SDWAN el canal presenta saturaciones (la saturación se presenta cuando el tráfico supera el 95% de la capacidad del canal) lo que produce degradación del canal y pérdidas de paquetes como se observa en la prueba de última milla realizada:

Pruebas de última milla al enlace MPLS de la sede de tuya CDM0595 en Medellín antes de implementar SDWAN

RP/0/RSP0/CPU0:A9KENVIGADO#sh int des | inc CDM0595

Thu Sep 23 16:38:36.375 COLOMBIA

Gi0/0/0/0.3643 up up IPDP TUYA S.A GESTION_PROACTIVA NIQUIA BACKUP CDM0596 - CDM0595

RP/0/RSP0/CPU0:A9KENVIGADO#sh run int Gi0/0/0/0.3643

Thu Sep 23 16:38:46.693 COLOMBIA

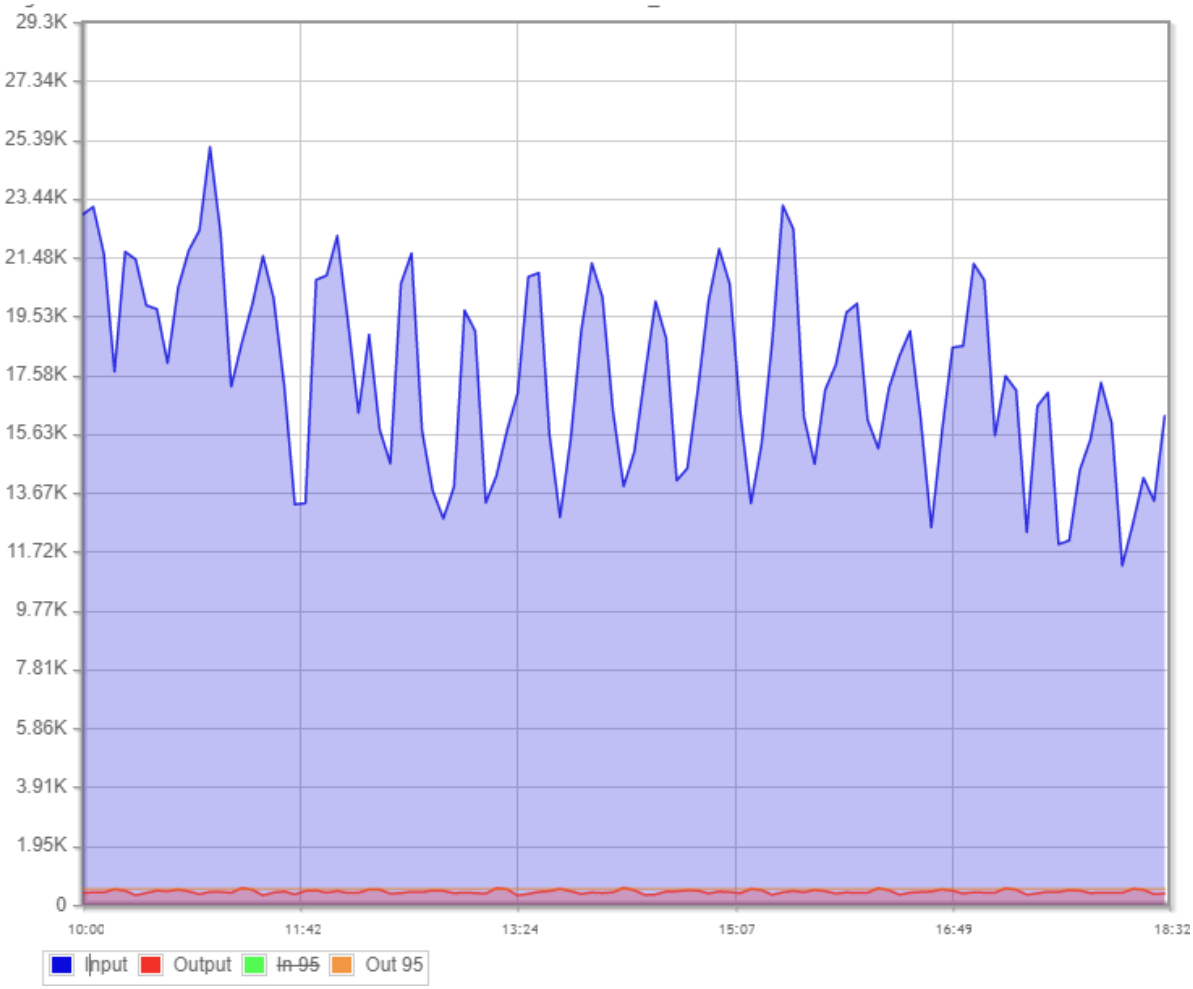
interface GigabitEthernet0/0/0/0.3643

```
 description IPDP TUYA S.A GESTION_PROACTIVA NIQUIA BACKUP CDM0596 - CDM0595
 service-policy input CAR-8M
 service-policy output CAR-8M
 vrf tuya-intranet
 ipv4 address 10.164.237.97/30
 encapsulation dot1q 3643
!

RP/0/RSP0/CPU0:A9KENVIGADO#sh run int Gi0/0/0/0
Thu Sep 23 16:38:50.170 COLOMBIA
interface GigabitEthernet0/0/0/0
 description TRUNK 8021Q AAC-ENVIGADO-C1 GE1/1/20 - TSO9029 (FOL)
 cdp
 ipv4 redirects
 negotiation auto
 load-interval 30
 mac-accounting ingress
 mac-accounting egress
 flow ipv4 monitor FNF_MONITOR_MAP sampler FNF_SAMPLER_MAP ingress
 flow ipv4 monitor FNF_MONITOR_MAP sampler FNF_SAMPLER_MAP egress
!

RP/0/RSP0/CPU0:A9KENVIGADO#ping vrf tuya-intranet 10.164.237.98
Thu Sep 23 16:39:00.991 COLOMBIA
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.164.237.98, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
RP/0/RSP0/CPU0:A9KENVIGADO#ping vrf tuya-intranet 10.164.237.98 re 500$
Thu Sep 23 16:39:09.872 COLOMBIA
Type escape sequence to abort.
Sending 500, 1500-byte ICMP Echos to 10.164.237.98, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
```

Success rate is 99 percent (499/500), round-trip min/avg/max = 1/2/47 ms
RP/0/RSP0/CPU0:A9KENVIGADO#



***Gráfica 7**. Tráfico enlace MPLS de la sede* CDM0595 de tuya una vez implementada la tecnología SDWAN.

En la gráfica 7 se puede ver que gracias al balanceo de cargas el tráfico del enlace MPLS de la sede de tuya no presenta saturación y está lejos de llegar al menos a la mitad de la capacidad del canal, gracias a esto la sede puede operar mejor cuando se presenten durante el día muchas transacciones bancarias (en días de promociones en el éxito, por ejemplo).

Resultados de pruebas de última milla a la sede tuya agregada a SDWAN.

las pruebas de última milla al enlace principal y backup de la sede de tuya no muestran ningún tipo de degradación del enlace o saturación de paquetes lo que muestra elgran beneficio del balanceo de cargas, en cualquier momento que se presenteuna afectación en cualquiera de estos dos enlaces, la sede no será afectadatotalmente en su operación porque una vez alarmado el enlace se activa laconmutación de paquetes directamente desde vmanage.

Prueba última milla enlace MPLS.

```
RP/0/RSP0/CPU0:A9KSANDIEGO#show int des | inc AEXI662
Fri Oct  1 21:12:51.265 COT
Gi0/1/1/0.463      up          up
 GESTION_PROACTIVA PPAL - AEXI662,ALX2064,ALEX598(XITO054)
RP/0/RSP0/CPU0:A9KSANDIEGO#show run int Gi0/1/1/0.463
Fri Oct  1 21:13:46.033 COT
interface GigabitEthernet0/1/1/0.463
description IPDP GESTION_PROACTIVA PPAL -
AEXI662,ALX2064,ALEX598(XITO054)
 service-policy input CAR-2M
 service-policy output CAR-2M
 vrf grexito-int
 ipv4 address 10.164.39.21/30
 encapsulation dot1q 463
!

RP/0/RSP0/CPU0:A9KSANDIEGO#show run int Gi0/1/1/0
Fri Oct  1 21:14:15.291 COT
interface GigabitEthernet0/1/1/0
 description TRUNK 8021Q AAG-SANDIEGO-C1 GE2/1/4 - TTU2468 (CERRADA
FOL)
 ipv4 unreachables disable
 flow ipv4 monitor NFMonMap-IPv4 sampler NFSamMapGE ingress
 flow ipv4 monitor NFMonMap-IPv4 sampler NFSamMapGE egress
!

RP/0/RSP0/CPU0:A9KSANDIEGO#ping vrf grexito-int 10.164.39.22
Fri Oct  1 21:14:24.977 COT
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.164.39.22, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
RP/0/RSP0/CPU0:A9KSANDIEGO#ping vrf grexito-int 10.164.39.22 re 100 si
1500
Fri Oct  1 21:14:45.487 COT
Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 10.164.39.22, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/5/7 ms
RP/0/RSP0/CPU0:A9KSANDIEGO#
```

Prueba última milla enlace banda ancha.

```
RP/0/RSP1/CPU0:A9KESPACIOSUR#SHOW INT DES | INC XITO054
Fri Oct  1 21:23:36.933 COLOMBIA
Te0/3/0/2.573      up          up          BACKUP
 AEXI662 - XITO054
RP/0/RSP1/CPU0:A9KESPACIOSUR#show run int Te0/3/0/2.573
Fri Oct  1 21:24:01.264 COLOMBIA
interface TenGigE0/3/0/2.573
 description IPDP BACKUP AEXI662 - XITO054
```

```
 service-policy input CAR-6M
 service-policy output CAR-12M
 vrf pymes-internet
 ipv4 address 181.48.3.101/30
 encapsulation dot1q 573
!

RP/0/RSP1/CPU0:A9KESPACIOSUR#show run int Te0/3/0/2
Fri Oct  1 21:24:03.999 COLOMBIA
interface TenGigE0/3/0/2
 description TRUNK 8021Q AAG-ESPACIOSUR-C1 3/2/6 - UWZ3843 (FOL JUMBO
MTU)
 mtu 9216
 ipv4 unreachables disable
 flow ipv4 monitor NFMonMap-IPv4 sampler NFSamMap10GE ingress
 flow ipv4 monitor NFMonMap-IPv4 sampler NFSamMap10GE egress
!

RP/0/RSP1/CPU0:A9KESPACIOSUR#ping vrf pymes-internet 181.48.3.102
Fri Oct  1 21:24:19.334 COLOMBIA
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 181.48.3.102, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
RP/0/RSP1/CPU0:A9KESPACIOSUR#ping vrf pymes-internet 181.48.3.102 re 100
si 1500
Fri Oct  1 21:24:27.213 COLOMBIA
Type escape sequence to abort.
Sending 100, 1500-byte ICMP Echos to 181.48.3.102, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/1 ms
RP/0/RSP1/CPU0:A9KESPACIOSUR#
```

Para esta implementación de SDWAN en la sede CDM0595 de tuya no hay resultados sobre los tiempos de resolución o atención de inconvenientes ya que fue una prueba que se realizó con fines académicos por lo que la sede sigue operando con la WAN tradicional, además estos tiempos son medidos cada mes con el fin de analizar si se están cumpliendo los acuerdos SLA.

6. Conclusiones

SDWAN permite que las resoluciones de los incidentes sean más escalables ya que la administración y configuración de routers se hace desde la nube esto permite que a medida que crezca la red la gestión pueda seguir siendo simple. Esta tecnología puede proporcionar un ancho de banda considerable de manera sencilla y económica esto se debe a que la red gestiona sin problemas la capa ligada al ancho de banda. Si comparamos el precio del ancho de banda (en Mbps) de una red privada, con el de una red SD-WAN, veremos que el precio de la segunda es mucho menor.

La prueba de última milla realizadas al almacén del éxito muestra menores tiempos de respuesta que en la sede tuya gracias a que el balanceo de cargas permite usar el ancho de banda más apropiado en función de la ubicación de la oficina o sucursal. También permite asignar distintos tipos de línea a tráficos diferentes y permite garantizar la disponibilidad lo que significa mayor capacidad para cubrir los picos de demanda.

Además de lo sencilla que resulta la instalación automática de los dispositivos en alguna sede, la tecnología SD-WAN permite modificar, actualizar e introducir más funcionalidades en la red desde el software del plano de control del lado (sede) central. Este método simplifica la configuración de red, la instalación y las demás funciones mencionadas. Además, la red SD-WAN puede gestionarse, en su totalidad, de manera sencilla y centralizada, esto permite que una sede nueva pueda ser agregada solo cambiando el equipo del lado del cliente y agregando desde la central este equipo desde vmanage por lo que la instalación resulta sencilla y menos costosa.

La anexión de una nueva sede a sdwan se realiza de manera rápida una vez esté instalado el equipo en la sede, esto se evidenció durante el desarrollo de este informe, igualmente se enseñó que la ejecución de la conmutación del enlace para que el tráfico de paquetes vaya por el enlace operativo, se realiza en la misma plataforma vmanage de manera sencilla. No importa si la red sigue creciendo con nuevas sedes, implementando esta tecnología la gestión y monitoreo de las sedes no se vuelve compleja gracias a los beneficios anteriormente mencionados que SDWAN ofrece.

7. Referencias bibliográficas

[1] IONOS, D. G. (02 de 03 de 2020). *www.ionos.es*. Obtenido de www.ionos.es:https://www.ionos.es/digitalguide/servidores/know-how/wan/

[2] Escandón, S. (02 de 06 de 20). *bismark*. Obtenido de bismark:https://bismark.net.co/sdwan-conceptos-y-ventajas-para-las-empresas/

[3] Foundation, W. (08 de 02 de 201). *WIKI*. Obtenido de WIKI:https://es.qaz.wiki/wiki/SD-WAN

[4] cisco. (22 de agosto de 2017). *cisco.com*. Obtenido de cisco.com: https://www.cisco.com/c/en/us/products/collateral/routers/2900-series-integrated-services-routers-isr/data_sheet_c78_553896.html

[5] cisco.com. (17 de marzo de 2017). *cisco.com*. Obtenido de cisco.com: https://www.cisco.com/c/en/us/products/collateral/routers/887-integrated-services-router-isr/data_sheet_c78_459542.pdf

[6] cisco. (22 de octubre de 2018). *cisco.com*. Obtenido de cisco.com: https://www.cisco.com/c/en/us/products/collateral/routers/887-integrated-services-router-isr/data_sheet_c78_459542.html

[7] cisco. (25 de agosto de 2021). *cisco.com*. Obtenido de cisco.com: https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/data_sheet-c78-732542.html#Productoverview

[8] cisco. (2017 de agosto de 22). *cisco.com*. Obtenido de cisco.com: https://www.cisco.com/c/en/us/products/collateral/routers/2900-series-integrated-services-routers-isr/data_sheet_c78_553896.html

[9] cisco. (2017 de agosto de 22). *cisco.com*. Obtenido de cisco.com: https://www.cisco.com/c/en/us/products/collateral/routers/2900-series-integrated-services-routers-isr/data_sheet_c78_553896.html

[10] cisco. (20 de septiembre de 2019). *cisco.com*. Obtenido de cisco.com: https://www.router-switch.com/c1111-4p-datasheet-pdf.html

[11] cisco. (20 de abril de 2021). *cisco.com*. Obtenido de cisco.com: https://www.cisco.com/c/en/us/products/collateral/routers/asr-9000-serie s-aggregation-services-routers/datasheet-c78-744663.pdf