# DISEÑO DE RED PARA LA INTEGRACIÓN DE SEDES TIPO MARKET DE UNA EMPRESA DE PRODUCCIÓN Y COMERCIALIZACIÓN DE ALIMENTOS BASADO EN CONECTIVIDAD SDWAN

PRESENTADO POR:
ÁLVARO JAVIER CARRILLO HERNANDEZ
IVONNE ANDREA RONCANCIO CASTILLO

ASESOR TÉCNICO DE PROYECTO:
IVAN ENRIQUE PERNETT PINILLA

UNIVERSIDAD EL BOSQUE
FACULTAD DE INGENIERÍA ELECTRÓNICA
ESPECIALIZACIÓN EN DISEÑO DE REDES TELEMÁTICAS
BOGOTÁ, COLOMBIA
JUNIO 22 de 2020

Contenido

## RESUMEN

Este documento contiene el diseño propuesto para una red basada en la conectividad definida por software (SDN) para una empresa de producción y comercialización de alimentos y plantea un modelo de implementación aplicando SD-WAN que es como tal la virtualización de las redes definidas por software para mejorar la necesidad de conectividad que tiene dicha empresa.



## PALABRAS CLAVE

SD-WAN, SDN, WAN, LAN, CONTROLADOR, VIRTUALIZACIÓN, MPLS, QoS



## ABSTRACT

This document contains the proposed design for a network based on software-defined connectivity (SDN) for a food production and marketing company and proposes an implementation model applying SD-WAN that is as such the virtualization of software-defined networks to improve the need for connectivity that company has.



## KEYWORDS

SD-WAN, SDN, WAN, LAN, CONTROLLER, VIRTUALIZATION, MPLS, QoS

## 1. Título.

Diseño de red para la integración de sedes tipo market de una empresa de producción y comercialización de alimentos basado en conectividad SDWAN.

## 2. Introducción.

La necesidad de acceder a una red de comunicaciones que permita el flujo de información actualizada, confiable, integra y disponible en cualquier momento hace que para muchas empresas y entidades sea necesario rediseñar y estructurar su red de comunicaciones ajustándola a las características de conectividad que tiene cada una de sus sedes y usuarios particulares con el fin que interactúen con los aplicativos, bases de datos, servidores y demás recursos compartidos.

En este proyecto presentará una propuesta en la que se rediseña la manera con la que actualmente tienen conectividad y acceso a la red las sedes tipo market de una empresa productora y comercializadora de alimentos a la cual llamaremos el CLIENTE las cuales actualmente tienen implementada una solución de conectividad tipo MPLS, con el fin de hacer una integración a un modelo de virtualización más conocido como SDWAN.

## 3. Descripción general del proyecto.

### 3.1. Definición del problema.

La empresa objeto de este diseño se dedica a la fabricación y comercialización al mayor y al detal de productos alimenticios a nivel nacional, para ello cuenta con varias plantas de producción, sedes administrativas, centros de acopio de mercancía y tiendas denominadas Markets para la venta directa de sus productos a los consumidores finales. La empresa cuenta con más de 6500 empleados, 100 sedes distribuidas en el país y categorizadas así:

- 7 plantas de Producción
- 8 sedes administrativas
- 40 centros de acopio y Distribución de Mercancía
- 45 Markets

El cliente tiene una necesidad inherente de conectividad entre todas sus sedes para realizar sus labores productivas y de core de negocio, con lo cual tienen implementada una solución de conectividad MPLS a nivel nacional con redundancia en las sedes que denomina como críticas que son las plantas de producción y los servicios alojados en 2 Datacenter que funcionan uno como contingencia del otro. También tiene implementada redundancia para los centros de acopio y las sedes administrativas ya que el funcionamiento de estas sedes son determinantes en su cadena de producción, pero no de carácter critico como lo son sus plantas de fabricación y los Datacenter que alojan los servidores de Correo electrónico, ERP, telefonía y el aplicativo de facturación.

La conectividad de los market se realiza a través de un único enlace fibra punto a punto sin redundancia, esta situación se explica en que el escenario de caída de un solo market no impactara gravemente en la operación de la compañía y tener un canal de contingencia de características similares al principal generan un gasto que aumentan considerablemente los costos de operación.

Actualmente estas sedes representan el 45% del total de sedes de la compañía y se basan estrategia de acercamiento hacia los clientes finales con el fin de ofrecerles una experiencia completa y personalizada en la compra de sus productos. Esto se traduce en que los markets busquen instalarse donde un posible nicho de mercado surja lo que impulsaran un mayor crecimiento en este tipo de sedes, claramente estas nuevas implementaciones están tomando importancia dentro de la organización.

El diseño de conectividad que tienen actualmente las sedes Criticas y principales está muy bien contenido y ofrecen estabilidad, redundancia y alta disponibilidad al ser base del objeto de operación de la empresa, aunque los markets cuentan con un único enlace de conectividad que se amolda a las necesidades de disponibilidad del cliente, se evidencia que no contar con un enlace de backup aumenta el riesgo de cese de operación del market, individualmente estas caídas no son criticas pero el número de sedes y el crecimiento que están teniendo si podrían ser determinantes en los reportes de ventas.

La empresa se decanta por que los enlaces de conectividad de los markets sean siempre fibra punto a punto confiando plenamente en las redes metropolitanas y en los SLA que ofrecen los diferentes ISP, pero este tipo de enlaces son los más costosos del mercado y presentan tiempos de instalación elevados debido a ejecución de obras civiles, radicación de permisos o memorias y equipos capa 1 costosos. Adicionalmente estos enlaces no son móviles, es decir no pueden ser trasladados fácilmente y su implementación en tiempo generalmente no es inferior a los 40 días calendario.

Los markets actualmente presentan 2 grandes falencias en cuanto a conectividad:

- Enlaces de Fibra punto a punto que limitan la movilidad e implementación de estas sedes, condicionando las aperturas de futuros enlaces a los tiempos de entrega de los ISP y no a las necesidades del negocio.
- Falta de un enlace de backup que genere una redundancia y evite una indisponibilidad de la sede, afectando las ventas del establecimiento y sometiendo a la sede a la espera de la solución de la falla para poder retomar su operatividad, el Cliente manifiesta que en promedio los últimos 6 meses sufrió al menos de 5 fallas que superaban las 4 horas de solución haciendo que la las sedes afectadas quede sin servicio prácticamente medio día, impactado seriamente las ventas.

Actualmente los market representan el casi el 50% de las sedes instaladas y es evidente que irán aumentando, ya que el cliente está buscando instalarse cerca a los consumidores y ser lo más flexibles posibles es decir que puedan instalarse de donde el mercado lo requiriera y de manera fácil y rápida. Esta flexibilidad está lejos de las ofertas de conectividad que ofrecen los grandes operadores que administran la red de transporte ya que las contrataciones estándar están sujetas a cobertura, obras civiles, cláusulas de permanencia y demás, lo que conlleva a una planificación no solo de negocio sino de la disponibilidad para implementar estos enlaces por parte del operador en donde el cliente lo necesita.

Por otra parte, entre más markets este instalados las fallas de estos van a representar un valor más significativo en las ganancias de la empresa debido al volumen de sitios y a su peso al momento de sumarse en los libros contables.

### 3.2. Aspectos a solucionar.

Los markets actualmente presentan 2 grandes falencias en cuanto a conectividad:

- Enlaces de Fibra punto a punto que limitan la movilidad e implementación de estas sedes, condicionando las aperturas de futuros enlaces a los tiempos de entrega de los ISP y no a las necesidades del negocio.
- Falta de un enlace de backup que genere una redundancia y evitar una indisponibilidad de la sede, afectando las ventas del establecimiento y sometiendo la reanudación del servicio a la solución de una falla que se condiciona en tiempos de resolución al origen de esta.

### 3.3. Solución propuesta.

El cliente necesita una solución en la que pueda usar canales de comunicación de fácil instalación, que sean móviles y a un menor costo que la actual solución implementada además que según necesidad pueda tener backup donde los necesite sin elevar los costos, permitiendo que pueda implantar rápidamente un market en donde los necesite sin necesidad de preocuparse por la cobertura del proveedor actual, gasto y tiempos de instalación elevados. Para logar esto es mejor usa canales de Internet que al no estar atados a la MPLS de un proveedor le da una mayor flexibilidad a la red, que junto a servicios como FTTH (Fiber To The Home) e Internet Celular de 4G y 5G se puede lograr tener conectividad con redundancia done el cliente lo necesite sin elevar los costó y con SLA igualmente buenos comparados con la solución de fibra punto a punto actual. Para poder unificar la propuesta de diseño usaremos la tecnología de SDWAN que permite convertir la conectividad WAN en parámetros configurables mediante software logrando que canales de internet de múltiples proveedores y medios de acceso distintos se integren de manera sencilla, rápida y segura a la red MPLS dando como resultado que la indisponibilidad de los markets sean menor, se desplieguen más rápido, en más lugares y que los costos sean menores.

Algo a tener en cuenta en el desarrollo de la solución es que actualmente todos los equipos comunicaciones esta basados en equipos CISCO SYSTEMS® por lo que espera que cualquier cambio en su red sea propuesta desde el portafolio de servicio CISCO y teniendo en cuenta que el plan a mediano plazo y dependido de los resultados de este proyecto es tener todas su sedes funcionado en un ambiente SDWAN y único.

## 4. Estado del arte.

### 4.1. Marco de referencia teórico.

Teniendo en cuenta que por especificación del cliente nuestro diseño debe estar soportado en equipos y plataformas CISCO SYSTEMS® toda nuestra investigación estará enfocada en dicho fabricante y sus desarrollos e implementaciones en las redes SDWAN.

#### 4.1.1. Introducción a SDWAN

En primer lugar, mencionaremos que las redes definidas por software SDN (Software Defined Network) son una arquitectura permite a la red ser controlada de manera inteligente y central, o "programada", utilizando aplicaciones de software. Esto ayuda a que toda la gestión la red sea de manera constante e integral, independientemente del acceso o medio que cada punto remoto tenga.

SD-WAN es la aplicación de soluciones de SDN orientadas al uso más eficiente y controlado de las conexiones WAN. Ya que, mientras que las redes definidas por software están destinado a centros de datos internos en una sede, SD-WAN toma esos conceptos definidos por software similares y el desacoplamiento del plano de control del plano de datos a la WAN. Muchas empresas cuentan con infraestructura compleja en sus sucursales, consistentes en routers, controladores de rutas WAN, optimizadores de WAN, firewalls y otros componentes que son costosos en cuanto a adquisición y mantenimiento a como tienen una administración compleja y especializada.

El principal propósito de SD-WAN es brindar la posibilidad que los servicios de conectividad sean más baratos usando el crecimiento que ha tenido Internet en la actualidad tanto a nivel de conectividad, debido a los bajos costo que tienen los servicios de internet de Ancha sumado con el crecimiento y los bajos costos que se está dando en el mercado en los servicios en la Nube. Las soluciones MPLS han dominado el mercado empresarial desde hace varias décadas proveyendo redes Privadas dedicadas en donde si era necesario que estos puntos remotos tuvieran conectividad a internet se necesitaba grandes concentradores donde se concretara el tráfico sumado con grandes puntos de acceso a internet y equipos muy robustos que dieran soporte al tráfico y seguridad a la red.

Presentado 2 problemas fundamentales, uno el tráfico de internet sea usado por los enlaces de MPLS que son más caros que un internet normal y debido al gran crecimiento que está teniendo el tráfico de internet las aplicaciones corporativas esta quedado relegadas tendrá que aplicar cada vez más filtrados y reglas para tener control sobre el tráfico. SDWAN está en la capacidad de ofrecer una opción segura que se integre con las costosas soluciones MPLS con canales de menor costo y diversos como los son los canales de banda Ancha y cuando se está implementando correctamente está en capacidad de encaminar el tráfico empresarial de manera simplificada a pensar de utilizar múltiples fuentes de canales de una manera segura y centrado en la calidad de servicio que el cliente experimenta en sus servicios.

### 4.1.2. Ventajas de SDWAN

- Simplicidad: en las redes definidas por software un aspecto básico es que el control de las rutas es manejado por alguien más, generalmente por dispositivos en la nube diseñado como interfaces de manejo muy sencillo y que permite tener control detallado con una alta granularidad de todas las políticas de manera remota desde una sola locación pudiendo aplicar cambios a nivel de aplicaciones es toda la red con un par de clicks

- Seguridad: es más que solo hablar de IPSEC, está más relacionada a 3 dimisiones que van de la mano encriptación autenticación e integridad. Realizar la conexión de un nuevo punto de red es fácil, pero para poder realizar esta nueva conexión se deben pasar por un proceso de autenticación contra el sitio central que precede a cualquier flujo de tráfico entre las sedes determinadas y debido a la flexibilidad que se tiene se puede optar por que las conexiones cifrada responda a las necesidades que se presente y tener el equilibrio entre rendimiento y seguridad hasta en conexiones complicadas de administrar y manejar como lo era las Full-mesh

- Calidad de la experiencia: Internet no es lo mismo que una red privada. Sin embargo, hay bastantes cosas que ahora se pueden hacer para mejorar los niveles de seguridad. La conectividad de red híbrida, combinada con controles granulares, debería permitir políticas que puedan dictar las condiciones bajo las cuales se podría elegir una ruta MPLS. Esta es una nueva opción de término medio que anteriormente no existía. La idea es que su implementación de SD-WAN debería permitirle reducir el tamaño de los circuitos MPLS (lo que

reduce los costos operativos) porque tiene políticas que dicen que ciertas aplicaciones pueden funcionar bien en Internet 'la mayor parte del tiempo' y lo que desea es una medición en tiempo real que pueda elegir esa ruta MPLS para una conversación específica en un momento específico porque la red es lo suficientemente inteligente como para llevarla a cabo.

### 4.1.3. Arquitectura SDWAN

Para dar una explicación más aterrizada se empelarán gráficos, en la siguiente imagen se muestran las siglas e iconos que vamos a utilizar:

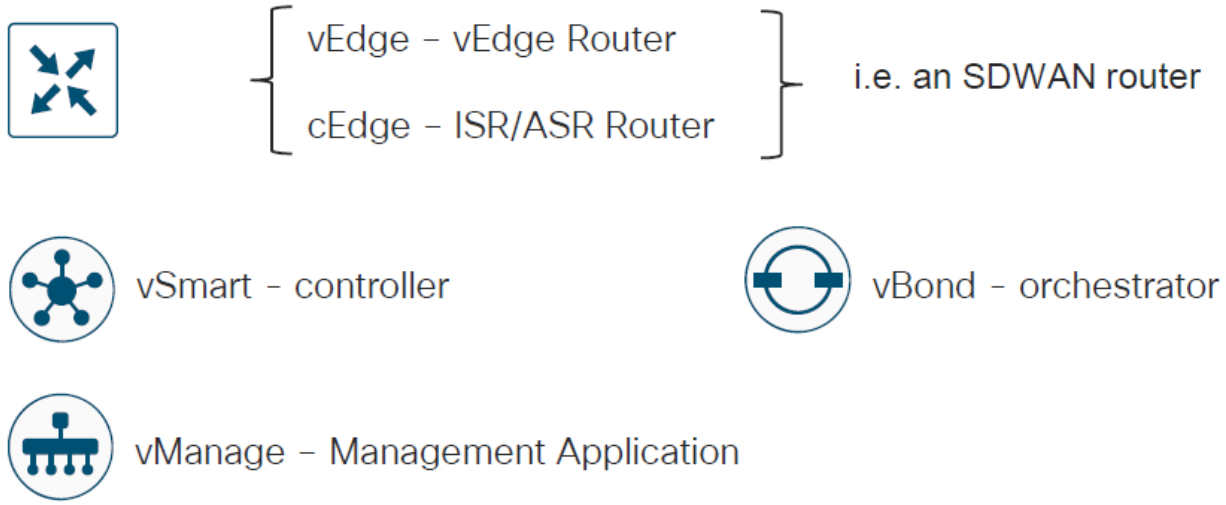




Figura 1. Siglas e iconos.

La arquitectura de SD-WAN está dividida en 4 planos: Plano de control (Control plane), plano de datos (Data plane), plano de orquestación (Orchestration plane) y plano de administración (Management plane). Los componentes que hacen parte de la solución son:

- vBond (Orchestration Plane)
- vManage (Management Plane)
- vSmart (Control Plane)
- vEdge (Data Plane)

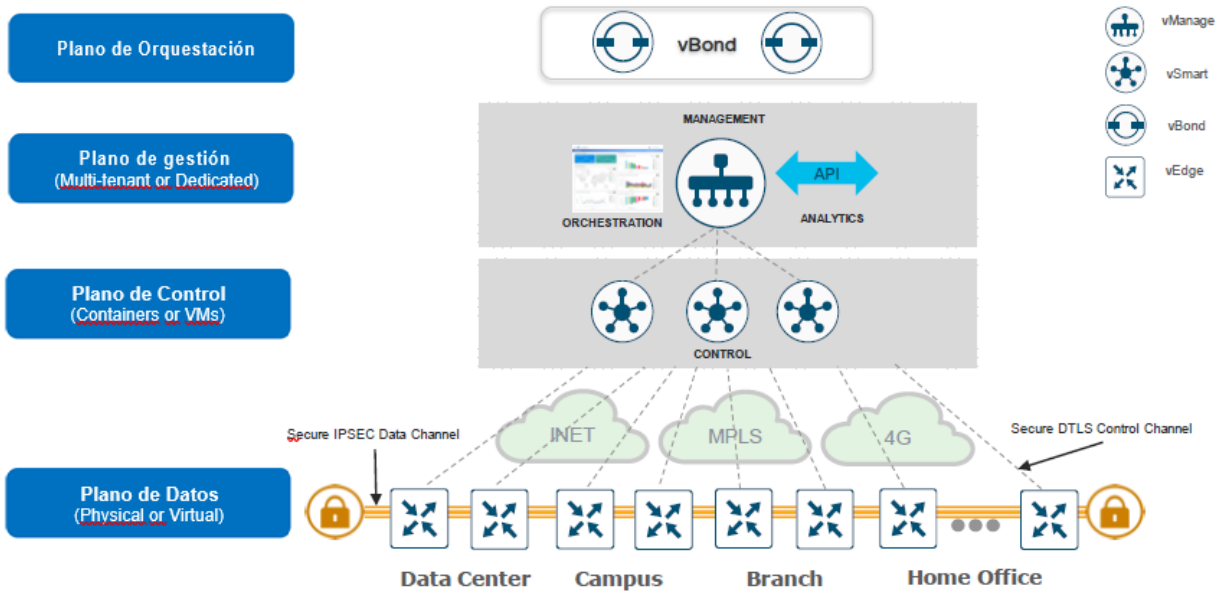




Figura 2. Arquitectura general de una red SDWAN

- Plano de orquestación: vBond

Este componente basado en software realiza la autenticación inicial de los dispositivos vEdge y organiza la conectividad entre vSmart y vEdge. También tiene un papel importante en permitir la comunicación de dispositivos que se encuentran detrás de NATs. Siempre se le debe asignar una IP pública fija.

- Plano de gestión: vManage

Este sistema de administración de red centralizada proporciona una interfaz GUI para monitorear, configurar y mantener fácilmente todos los dispositivos y enlaces SD-WAN en la red.

- Plano de Control: vSmart

Este componente basado en software es responsable del plano de control centralizado de la red SD-WAN. Establece una conexión segura a cada cpe o vEdge y distribuye rutas e información de políticas a través del Protocolo de administración de superposición (OMP), que actúa como un reflector de ruta. También organiza la conectividad segura del plano de datos entre los cpe vEdge mediante la distribución de información de clave criptográfica, lo que permite una arquitectura muy escalable.

- Plano de Datos: vEdge/cEdge

Estos dispositivos, disponibles como dispositivo de hardware o software, se ubican en un sitio físico o en la nube y proporcionan conectividad segura del plano de datos entre los sitios a través de uno o más transportes WAN. Son responsables del reenvío de tráfico, la seguridad, el cifrado, la Calidad de servicio (QoS), los protocolos de enrutamiento como BGP y OSPF, ETC.

### 4.1.4. Topología Lógica SDWAN

La topología lógica de SDWAN se basa en realizar enrutamientos y enrutamientos de anuncios para establecer y mantener el flujo de tráfico en toda la red mediante una segmentación de Capa 3 (VRF) Su conectividad está basada en conceptos punto a punto para configurar y mantener conexiones bidireccionales entre pares de protocolos entidades. Así mismo de manera mandatoria implementa la autenticación y encriptación junto con Políticas de enrutamiento y tráfico de datos.

La red de transporte se encarga de transportar paquetes de un equipo de red a otro y por lo tanto debe conocer solo las rutas a seguir para llegar al siguiente router, salto o destino. Separar el transporte de red del lado del servicio de la red permite al administrador de la red influir comunicación de router a router independientemente de la comunicación entre usuarios o entre hosts.

Cada router en el borde de una red tiene dos lados para el enrutamiento: uno a la red de transporte y otro al servicio lado de la red. Para tener una comunicación entre todos los routers, todos los routers deben aprender todos los prefijos. Tradicionalmente, los routers aprenden estos prefijos utilizando IGP / BGP de malla completa o habilitando el enrutamiento en un túnel superpuesto (por ejemplo, BGP o IGP sobre MPLS o GRE). Varias técnicas permiten mitigar o eliminar los problemas de escala asociados con full-mesh por sus adyacencias de enrutamiento, como por ejemplo utilizar un reflector de ruta para BGP. SDWAN se basa el modelo de reflector de ruta centralizando para la inteligencia de enrutamiento. Esencialmente, todos los prefijos aprendidos desde el lado del servicio en un router se anuncian a un controlador centralizado, que luego refleja la información a otros routers a través del plano de control de la red. Los controladores no manejan el tráfico de datos; son involucrados solo en la comunicación del plano de control.

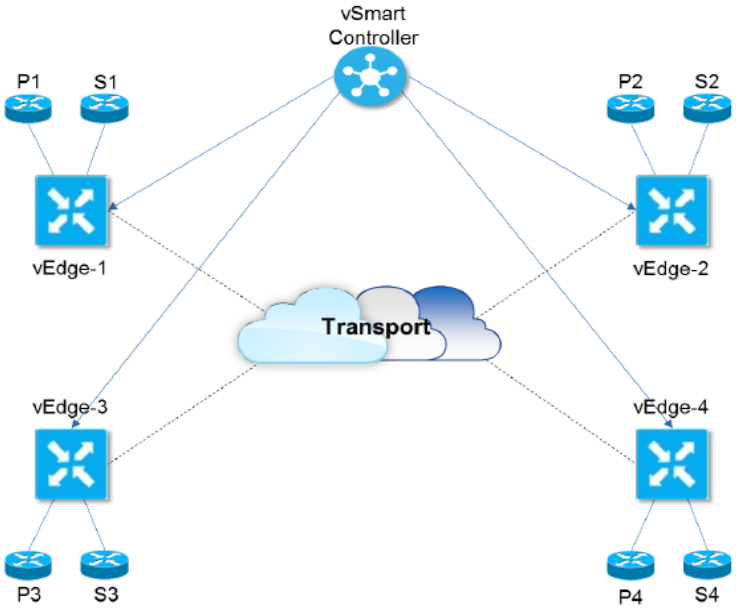




Figura 3. Transporte y enrutamiento

SDWAN permite la identificación de los enlaces del lado del transporte y cifra automáticamente el tráfico entre sitios. Las claves de cifrado asociadas se intercambian a través de una sesión segura con el controlador centralizado (Ipsec Tunnel) Las sesiones seguras con el controlador se configuran automáticamente, utilizando RSA e infraestructura de certificados (DTLS/TLS tunnel)

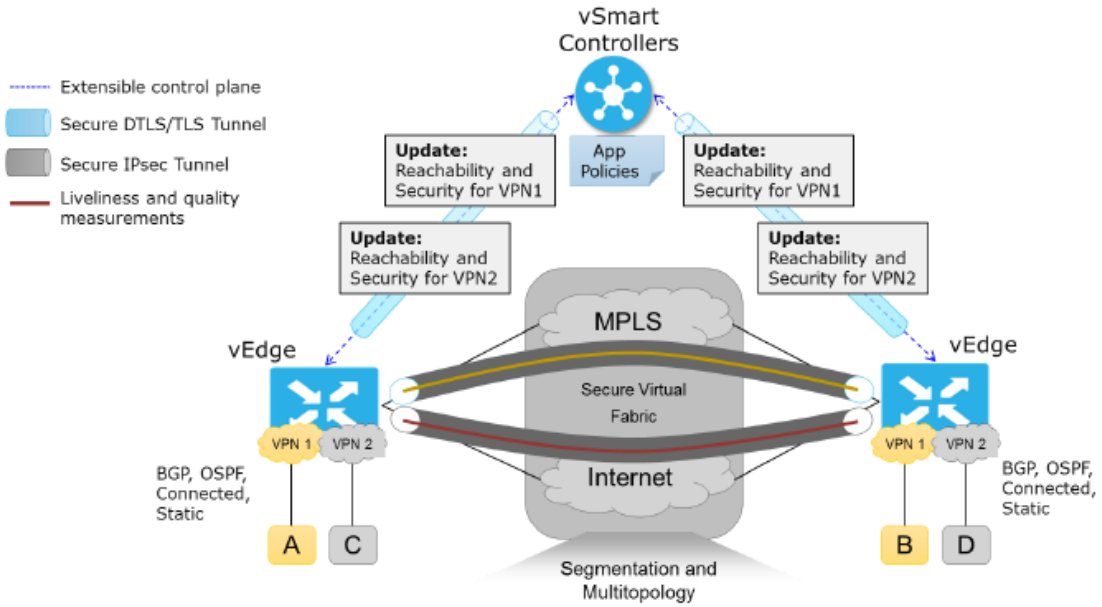




Figura 4. Tipos de enlaces

La centralización de la conectividad permite que se administren de manera más asertiva los prefijos de comunicación dentro de una misma VPN, permitiendo que se pueda asignar cual será el enlace para hacer la comunicación, así como la implementación de políticas de QoS con el fin de mejorar el transporte y la percepción de las aplicaciones a nivel de usuario.

Otro de los grandes beneficios de SDWAN es que centraliza y simplifica significativamente el aprovisionamiento y la administración a través del Sistema de administración de red (NMS) vManage. El VManage NMS proporciona un panel de control gráfico fácil de usar desde el cual puede monitorear, configurar y mantener todos los dispositivos y enlaces en la red. Por ejemplo, desde panel de control proporciona una vista con plantillas de varias configuraciones para facilitar el aprovisionamiento de un servicio, de modo que todos los elementos comunes, como AAA y servidores específicos de la empresa, se pueden enviar a múltiples dispositivos con un solo clic.

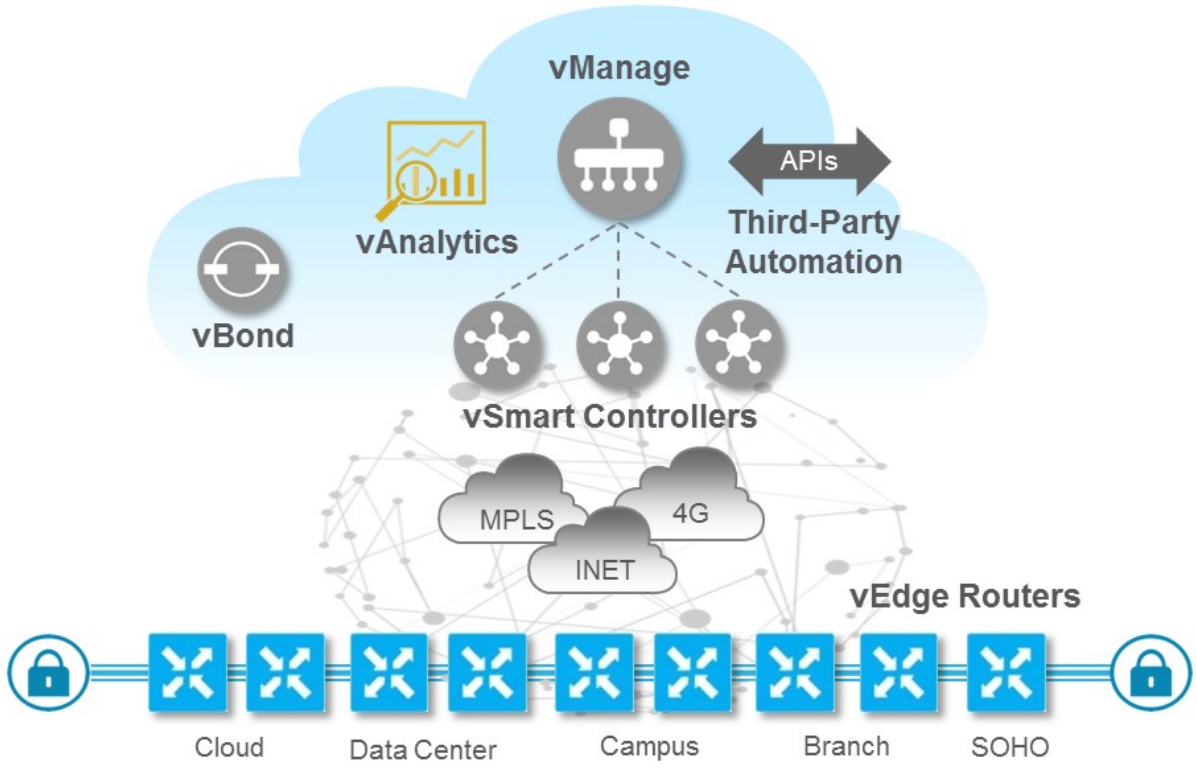




Figura 5. vManage

### 4.1.5. Modelo de autenticación SDWAN

Para proporcionar el nivel más alto de seguridad, solo los dispositivos autenticados y autorizados pueden acceder y participar en la red de superposición SD-WAN. Para su fin, el vSmart realiza una autenticación automática en todos los routers vEdge antes de que puedan enviar tráfico de datos a través de la red.

A medida que los Routers SD-WAN se unen a la red, se validan y autentican automáticamente, y establecen canales de comunicación seguros entre ellos. Para los vBond y los vSmart, un administrador de red debe descargar los archivos relacionados con la autenticación necesarios de vManage, y luego estos dispositivos reciben automáticamente sus configuraciones de vManage. Para los routers de hardware vEdge, después de que se inician, se autentican en la red y reciben sus configuraciones automáticamente desde vManage a través de un proceso llamado aprovisionamiento cero al tacto (ZTP).

Este proceso automático está dirigido por el vBond. Bajo la dirección del software vBond, los dispositivos SDWAN configuraron canales de comunicación encriptados entre ellos. A través de estos canales, los dispositivos se validan y autentican automáticamente entre sí, un proceso que establece una red de superposición operativa. Cuando se ejecuta la red, los dispositivos SD-WAN reciben y activan automáticamente sus configuraciones completas desde el servidor vManage.

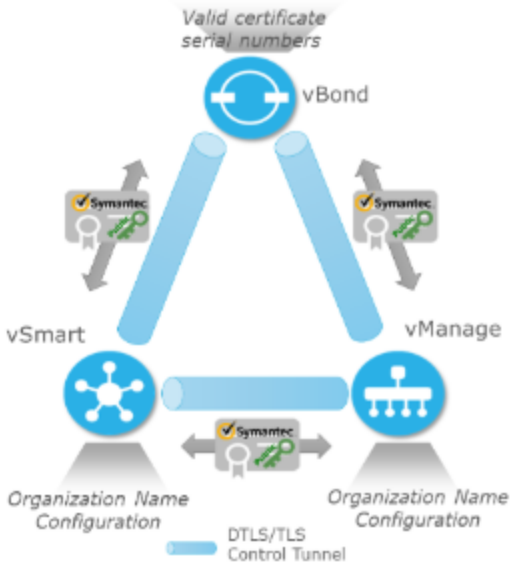




Figura 6. Autenticación en SDWAN

La validación y autenticación automáticas de los dispositivos SD-WAN durante el proceso de actualización solo se produce si los vSmart y los vBond conocen los números de serie y de chasís de los dispositivos que están permitidos en la red.

- Número de serie: cada dispositivo SD-WAN tiene un número de serie; que es un número de 40 bytes que se incluye en el certificado del dispositivo. Para el vBond y el vSmart, el certificado puede ser proporcionado por Symantec. Para los routers vEdge; el certificado se proporciona en el hardware de confianza chip de identificación de la placa.
- Número de chasis: además de un número de serie, cada router vEdge se identifica mediante un número de chasis. Hay un mapeo uno a uno entre el número de serie de un router vEdge y su número de chasís.

Los vSmart y los vBond aprenden los números de serie y chasis durante la configuración inicial de estos dispositivos.

- Números de serie autorizados de vSmart: vManage aprende los números de serie de todos los vSmart que pueden estar en la red mientras crea un CSR e instala el certificado firmado. Descarga estos números de serie al vBond orchestrator; y el vBond los empuja al vSmart durante el proceso de autenticación automática.

- Archivo de número de serie autorizado de vEdge: este archivo contiene los números de serie y chasis de todos los routers vEdge que pueden estar en la red. Este archivo debe ser cargado en el vBond y el vSmart.

Además de los números de serie y chasis del dispositivo; El procedimiento de validación y autenticación automática depende de que cada dispositivo esté configurado con el mismo nombre de organización. Este nombre se configura en el vManage y se incluye en el archivo de configuración en todos los dispositivos. El nombre de la organización debe ser idéntico en todos los dispositivos que pertenecen a una sola organización (el nombre distingue entre mayúsculas y minúsculas)

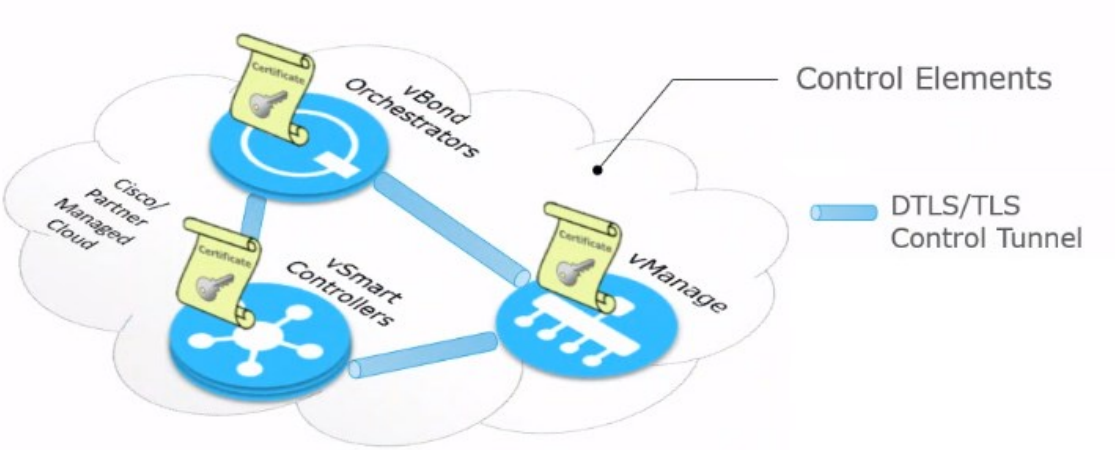




Figura 7. Autenticación entre los elementos de control

Para iniciar una sesión entre el vSmart y el vBond, el vSmart inicia una conexión DTLS encriptada con el vBond. El cifrado es proporcionado por RSA. Cada dispositivo genera automáticamente un par de claves públicas de clave privada RSA cuando se inicia. Sobre este canal encriptado, el vSmart y el vBond se autentican entre sí.

Una vez que se completa la autenticación bidireccional entre los dos dispositivos, la conexión DTLS entre el vBond y el vSmart pasa de ser una conexión temporal a ser una conexión permanente, y los dos dispositivos establecen una sesión OMP sobre la conexión.

Un orquestador vBond tiene solo tantas conexiones DTLS permanentes como el mismo número de vSmart haya en la topología de la red. Estas conexiones DTLS son parte del plano de control

de la red; no fluye tráfico de datos sobre ellos. Después de que todos los vSmart se hayan registrado con el vBond están listos para validar y autenticar los routers vEdge en la red.

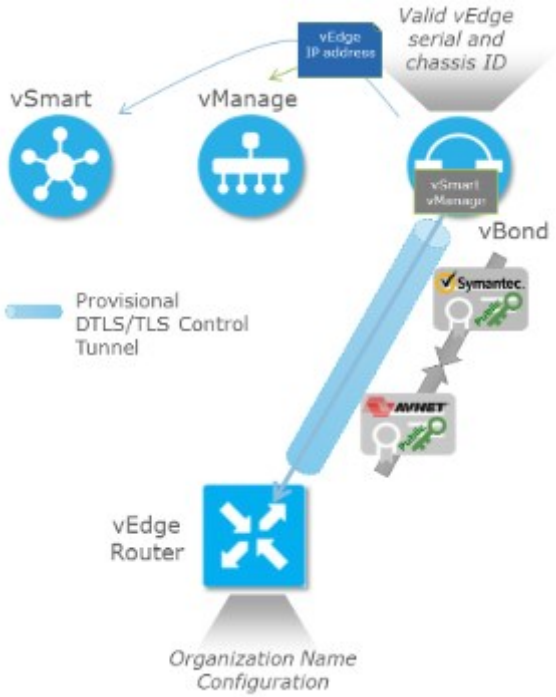




Figura 8. Autenticación de los vEdge con el vBond

El hardware de los vEdge Routers incluye un chip Trusted Board ID, que es un criptoprocesador seguro que contiene la clave privada y la clave pública del router; junto con un certificado firmado. Las claves públicas y privadas y los certificados se administran automáticamente; Cuando los routers vEdge se inician y se unen a la red, intercambian los certificados (incluyendo la clave pública y el número de serie del dispositivo) con otros dispositivos SD-WAN como parte del proceso de autenticación del dispositivo.

Cuando aparece un dispositivo vEdge, descubre automáticamente vManage, el vSmart y establece conexiones con ellos con la ayuda del vBond. La configuración inicial en el router vEdge contiene la dirección IP (o nombre DNS) del sistema vBond. Con esta información, el vEdge establece una conexión DTLS con el vBond, y los 2 dispositivos se autentican entre sí para confirmar que son dispositivos válidos. Los certificados se intercambian y se produce una autenticación mutua entre vBond y vEdge a través del túnel encriptado.

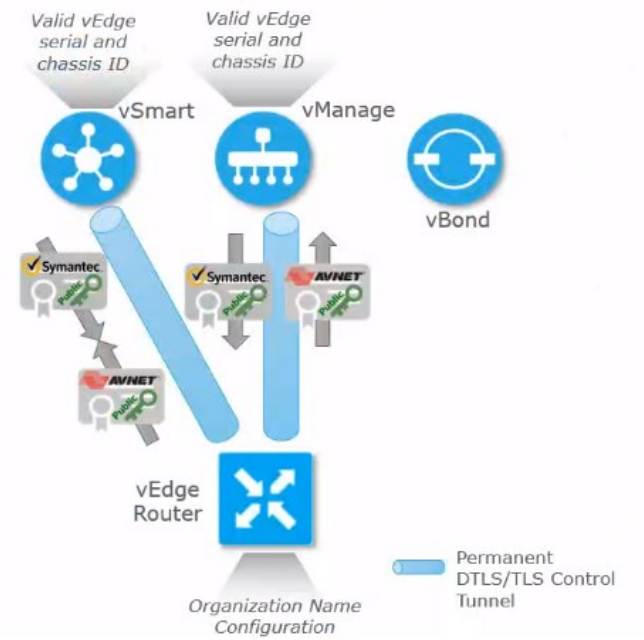




Figura 9. Autenticación de los vEdge con vSmart y vManage

Después de que el router vEdge y el vBond se hayan autenticado entre sí, el vEdge recibe su configuración completa a través de una conexión DTLS con vManage. Se intercambian certificados y se produce una autenticación mutua entre vSmart, vManage y vEdge.

### 4.1.6. Overlay Routing SDWAN

El enrutamiento de superposición u Overlay crea una topología enrutable de capa 3 lógica que se utiliza para interconectar virtualmente los dispositivos y se construye sobre una topología física subyacente que está siendo abstraída por la superposición. La superposición está diseñada para proporcionar VPN a petición escalables y proporciona distribución de rutas entre todos los sitios dentro de una VPN.

La red Overlay está controlada por el Protocolo de administración de superposición SD-WAN (OMP), que es la parte más importante del enrutamiento de superposición SD-WAN. Esta solución permite la creación de VPN escalables, dinámicas, bajo demanda y seguras. La solución SD-WAN utiliza un controlador centralizado para una fácil orquestación, con control de políticas completo que incluye control de acceso y un plano de datos escalable y seguro entre todos los nodos de borde.

El Protocolo de administración de superposición SD-WAN (OMP) es el protocolo responsable de establecer y mantener el plano de control SD-WAN. Brinda los siguientes servicios:

- Orquestación de comunicación de red overlay, incluida la conectividad entre sitios de red, encadenamiento de servicios y topologías VPN
- Distribución de información de enrutamiento a nivel de servicio y mapeos de ubicación relacionados
- Distribución de los parámetros de seguridad del plano de datos.
- Control central y distribución de la política de enrutamiento

OMP interactúa con el enrutamiento tradicional en sitios locales en la red overlay. Importa información de protocolos de enrutamiento tradicionales, como OSPF y BGP, y esta información de enrutamiento proporciona accesibilidad dentro del sitio local. La importación de información de enrutamiento de los protocolos de enrutamiento tradicionales está sujeta a políticas definidas por el usuario.

Overlay Management Protocol (OMP) es un protocolo de plano de control extensible basado en TCP. Se ejecuta dentro de las conexiones TLS / DTLS entre los routers vEdge y vSmart. OMP utiliza familias de direcciones para anunciar la accesibilidad para TLOC, destinos de unidifusión y multidifusión que son rutas del lado del servicio aprendidas estática o dinámicamente y rutas de servicio para los servicios de Capa 4 a Capa 7. Estadísticas de BFD, incluyendo Traffic Engineering (TE) y Hierarchical SD-WAN (H-SDWAN) y Cloud onRamp para estadísticas de sonda SaaS, también son transportadas por OMP utilizando atributos. OMP también distribuye claves de cifrado IPsec y políticas de datos y aplicaciones al usar NETCONF incorporado.

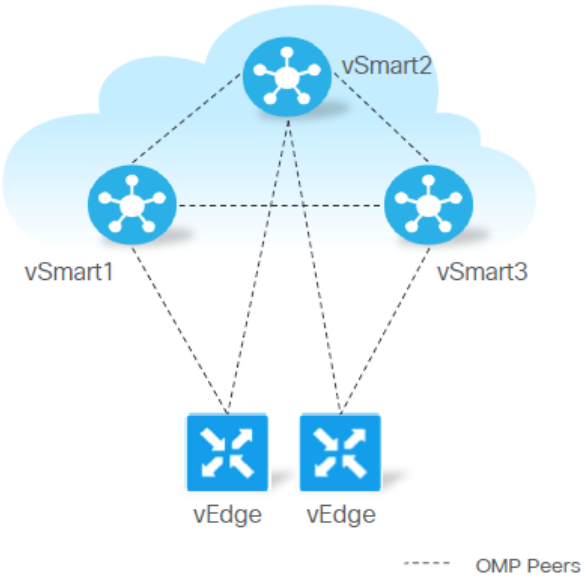




Figura 10. Adyacencias de OMP

OMP es el protocolo de control que se utiliza para intercambiar información de enrutamiento, políticas y administración entre los vSmart y los routers vEdge en la red overlay de manera predeterminada, por lo tanto, después de iniciar los vSmart y los vEdge, no es necesario configurar o habilitar explícitamente OMP.
Estos dispositivos inician automáticamente sesiones de emparejamiento OMP entre ellos, y los dos puntos finales IP de la sesión OMP son las direcciones IP del sistema de los dos dispositivos (System-IP).

En los vSmart y vEdge, OMP anuncia a sus pares las rutas y servicios que ha aprendido de su sitio local, junto con sus correspondientes asignaciones de ubicación de transporte, que se denominan TLOC. Estas rutas se denominan rutas OMP o vRoutes, para distinguirlas de las rutas IP estándar. Los vSmart aprenden a través de las rutas OMP que la topología de la red overlay y los servicios disponibles en la red.

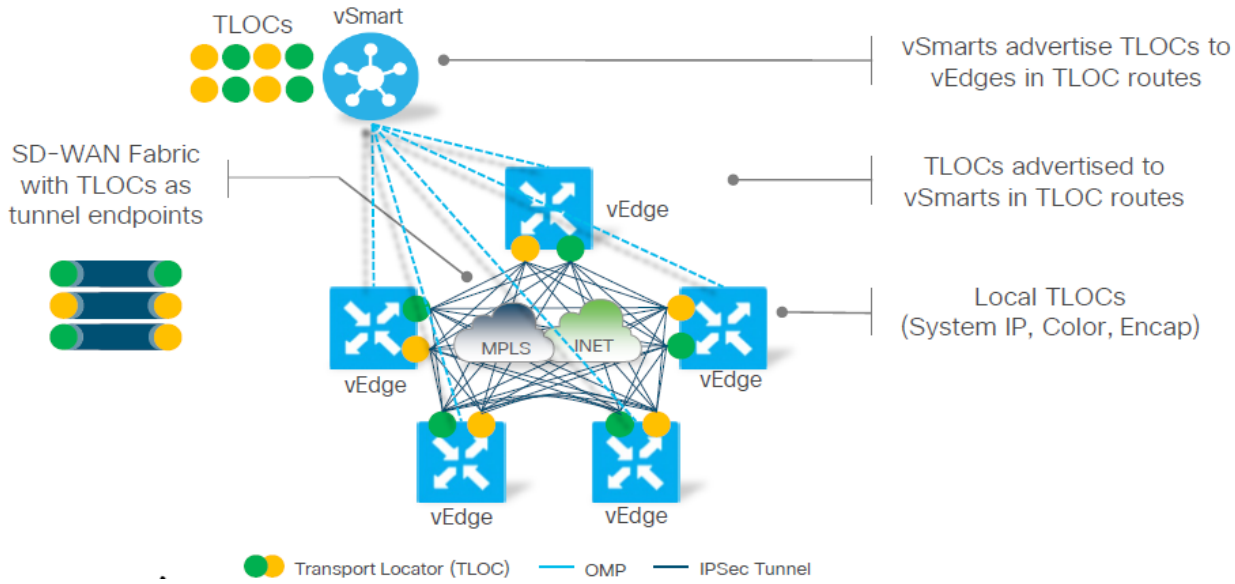




Figura 11. Ejemplo de Overlay Routing

OMP anuncia los siguientes tipos de rutas:

- **Rutas OMP (también llamadas vRoutes):** prefijos que establecen el alcance entre puntos finales que usan la red de transporte orquestada por OMP. Las rutas OMP pueden representar servicios en un centro de datos central, servicios en una sucursal o colecciones de hosts y otros puntos finales en cualquier ubicación de la red superpuesta. Las rutas OMP requieren y se resuelven en TLOC para el reenvío funcional. En una comparación con BGP, una ruta OMP es el equivalente de un prefijo transportado en cualquiera de los campos BGP AFI / SAFI.

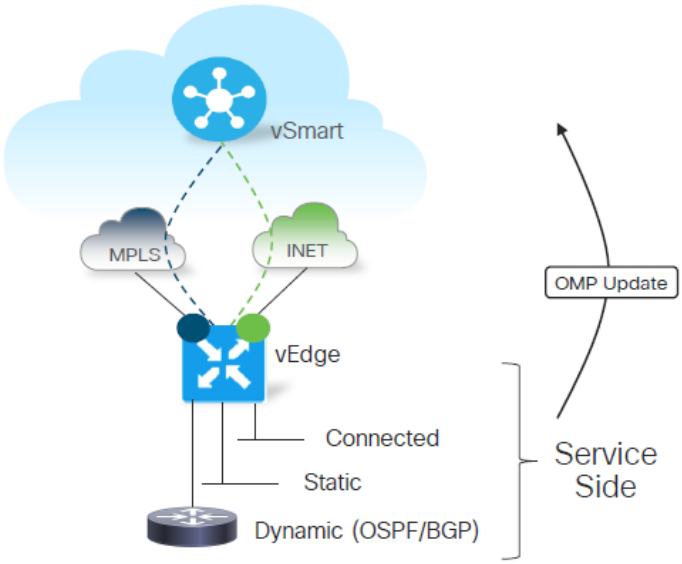




Figura 12. Ejemplo de ruta OMP

- **Transport Locations (TLOC):** identificadores que vinculan una ruta OMP a una ubicación física. El TLOC es la única entidad del dominio de enrutamiento OMP que es visible para la red subyacente y debe ser accesible a través del enrutamiento en la red subyacente. Se puede acceder directamente a un TLOC a través de una entrada en la tabla de enrutamiento de la red física. En una comparación con BGP, el TLOC actúa como el próximo salto para las rutas OMP.

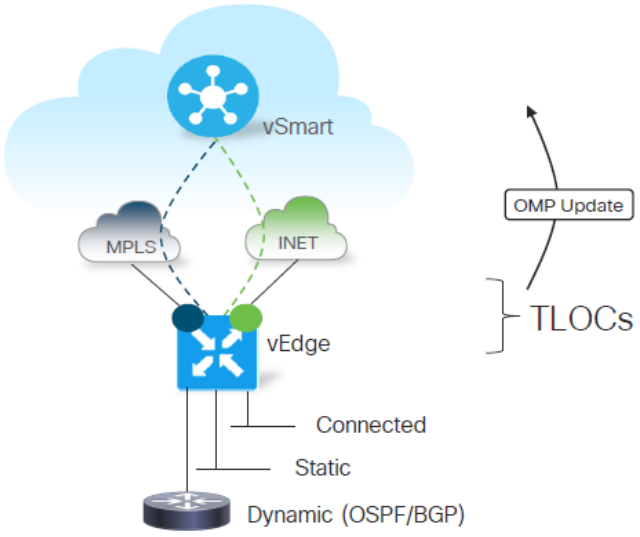




Figura 13. Ejemplo de ruta TLOC

- **Rutas de servicio:** identificadores que vinculan una ruta OMP a un servicio en la red, especificando la ubicación del servicio en la red. Los servicios incluyen firewalls, sistemas de detección de intrusiones (IDP) y equilibradores de carga. La información de la ruta de servicio se transporta tanto en las rutas de servicio como en las de OMP.

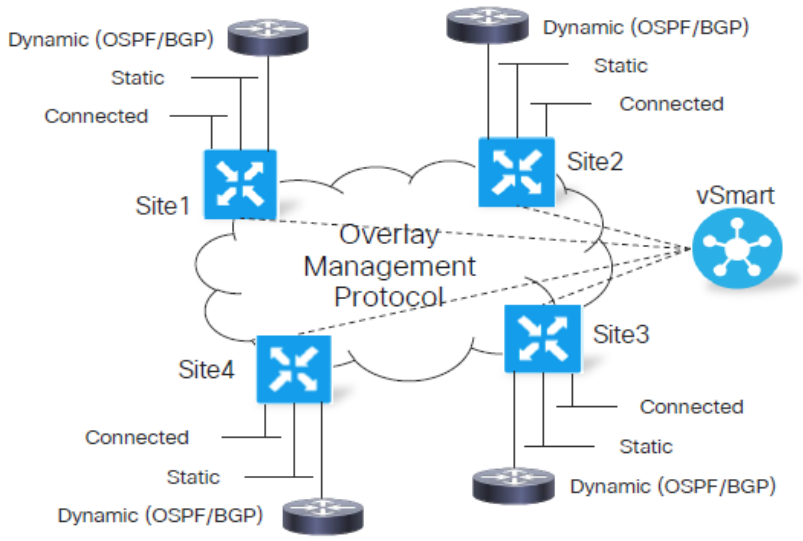




Figura 13. Ejemplo de ruta de servicio

### 4.1.7. Data Plane en SDWAN

La independencia del transporte es una de las piedras angulares de la solución SD-WAN utilizando el poder de la abstracción, puede construir una estructura overlay segura sobre cualquier transporte público o privado como MPLS, Internet, satélite 4G LTE, circuitos punto a punto, etc. a través del cifrado IPsec. Los Transport Locators (TLOC) son quienes definen los puntos finales del túnel Ipsec porque el direccionamiento IP no es determinista y puede cambiar; especialmente en los circuitos de banda ancha habilitados para DHCP, la red SD-WAN utiliza el color y la encapsulación IP del sistema para definir los puntos de terminación de túnel IPsec. Esto permite la independencia de la dirección IP de transporte individual.

Los TLOC se anuncian como rutas TLOC en los mensajes OMP entre los vEdge y los vSmart así mismo los vSmart reflejan la accesibilidad de TLOC entre los vEdge a través de la red. En caso de que no se definan políticas de control en los vSmart, estos anuncian todas las rutas TLOC en todos los routers vEdge. Los vEdge pueden construir túneles IPsec directos entre sí por default construyendo una topología denominada full-mesh.

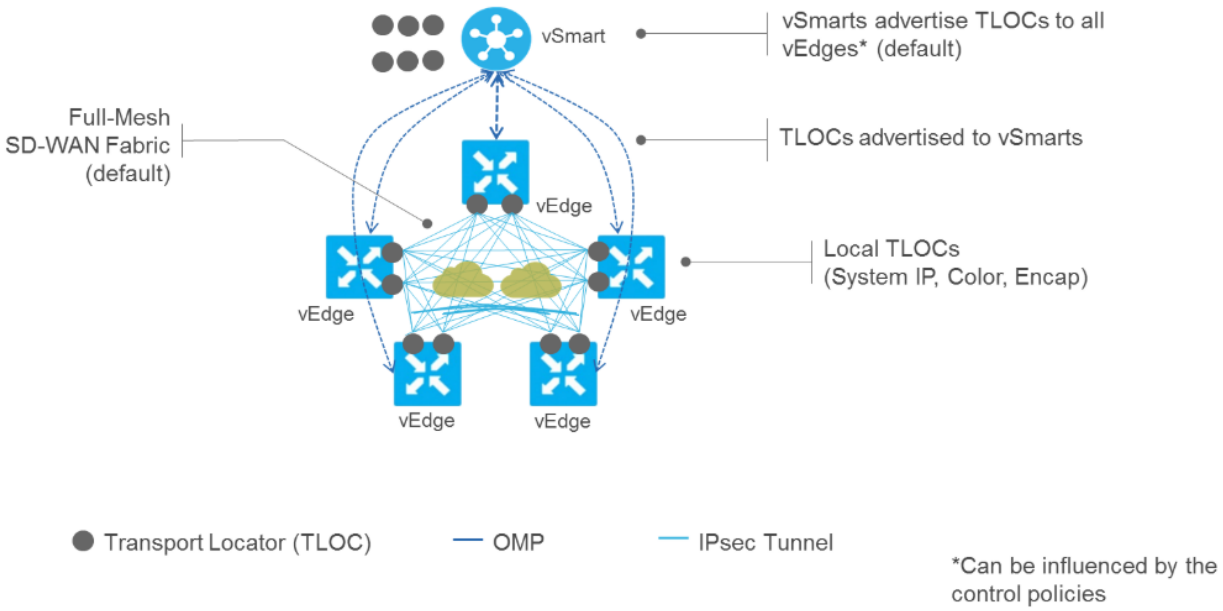




Figura 14. Ejemplo de topología Full-Mesh

Las rutas TLOC identifican las ubicaciones de los vEdge y estas ubicaciones están definidas en la red Overlay que se asocian a un transporte físico a través de la identificación de la interface WAN del dispositivo conectado. Una TLOC se caracteriza por enviar 3 identificadores de los vEdge que son únicos y relativos a cada dispositivo:

- **System-IP**: La dirección IP utilizada en las TLOC es la dirección fija del sistema configurada en el vEdge. El motivo por el que no se utiliza una dirección IP o una dirección IP de interfaz para denotar una TLOC es que las direcciones IP pueden moverse o cambiar, por ejemplo, pueden ser asignados por DHCP o pueden intercambiarse de interface, al usar la dirección IP del sistema para identificar un TLOC asegura que siempre se pueda identificar un punto final de transporte independientemente de la dirección IP.

- **Color**: identifica un túnel de transporte WAN individual asignándole un color. El color es uno de los parámetros TLOC asociados con el túnel. En un vEdge, solo se puede configurar una interfaz de túnel con el color predeterminado (default). Los colores metro-ethernet, mpls y private1-private6 son colores privados. Usan direcciones privadas para conectarse al vEdge del lado remoto en una red privada. Puede usar estos colores en una red pública, siempre que no haya ningún dispositivo que realice NAT entre los routers vEdge locales y remotos. Todos los valores de color posibles son: 3g, biz-internet, azul, bronce, custom1, custom2, custom3, default, gold, green, LTE, metro-ethernet, mpls, private1, private2, private3, private4, private5, private6, public-internet, red y silver.
- **Tipo de encapsulación:** está definida por la encapsulación del tunnel que fue implementada, SDWAN permite IPSec y GRE.

SDWAN admite la segmentación de tráfico mediante el uso de VPNs. Cada VPN tiene su propia tabla de reenvío que proporciona aislamiento dentro del vEdge. El uso de etiquetas que se intercambian como atributos de servicio a los vSmart y se encapsula en los paquetes entrantes para su identificación en el plano de datos.

Para imponer la separación entre servicios y transporte, todas las interfaces de transporte (es decir, todas las TLOC) se mantienen en la misma VPN de transporte, que se asocian internamente con su respectiva etiqueta. Esto garantiza que La red de transporte no puede alcanzar la red de servicio. Múltiples TLOCs pueden pertenecer a la misma VPN de transporte y los paquetes pueden reenviarse desde y hacia TLOCs.

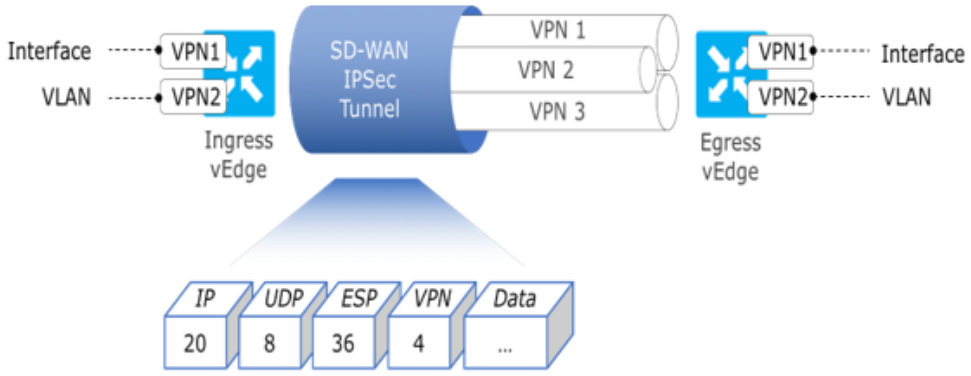




Figura 15. VPN en SDWAN

### 4.1.8. Políticas de enrutamiento en SDWAN

El objetivo principal de un diseño SDWAN es optimizar el rendimiento de las aplicaciones y la experiencia del usuario para servicios de voz, video y datos con lo cual se proporciona un conjunto de capacidades para la optimización de aplicaciones, como el control de admisión, clasificación, marcado, asignación de ancho de banda, priorización de aplicaciones, selección de rutas según los acuerdos de nivel de servicio (SLA) e ingeniería de tráfico. Estas capacidades se proporcionan mediante políticas centralizadas y localizadas.

La política centralizada se refiere a la política aprovisionada en los vSmart. Hay dos tipos:

- **Política de control (Control Policy):** afecta el enrutamiento OVERLAY de toda la red.
- Filtra o modifica la información almacenada en la tabla de enrutamiento del vSmart.
- Filtra los anuncios realizados por el controlador vSmart a los elementos del plano de datos.
- La política de control siempre está en el vSmart. Nunca es generada por los vEdge.

- **Política de datos (Data Policy):** afecta el flujo de tráfico a través de los segmentos de VPN en la red.
- Se aplica al flujo de tráfico de datos.
- Permite o restringe el acceso basado en una coincidencia de VPN.
- Estas políticas se envían a los vEdge afectados.

La política localizada se refiere a la política aprovisionada en los routers del plano de datos. Hay dos tipos:

- **Política de control local (Local Control Policy):** políticas de rutas underlay en el servicio o redes de transporte.
- Implementa los comportamientos tradicionales de enrutamiento BGP u OSPF necesarios para interactuar con el servicio o las redes de transporte en el sitio local.

- **Política de datos locales (Local Data Policy):** afecta el flujo de tráfico a través de los segmentos de VPN en la red.

- Listas de acceso aplicadas a una interfaz específica en el router vEdge.
- Las listas de acceso simples permiten y restringen el acceso en función de coincidencias.
- Listas de acceso para marcado de clase de servicio (CoS), colas, vigilancia, mapeo de rutas y SPANning.
- Controla cómo el tráfico de datos fluye desde y hacia las interfaces y las colas de interfaz del enrutador.

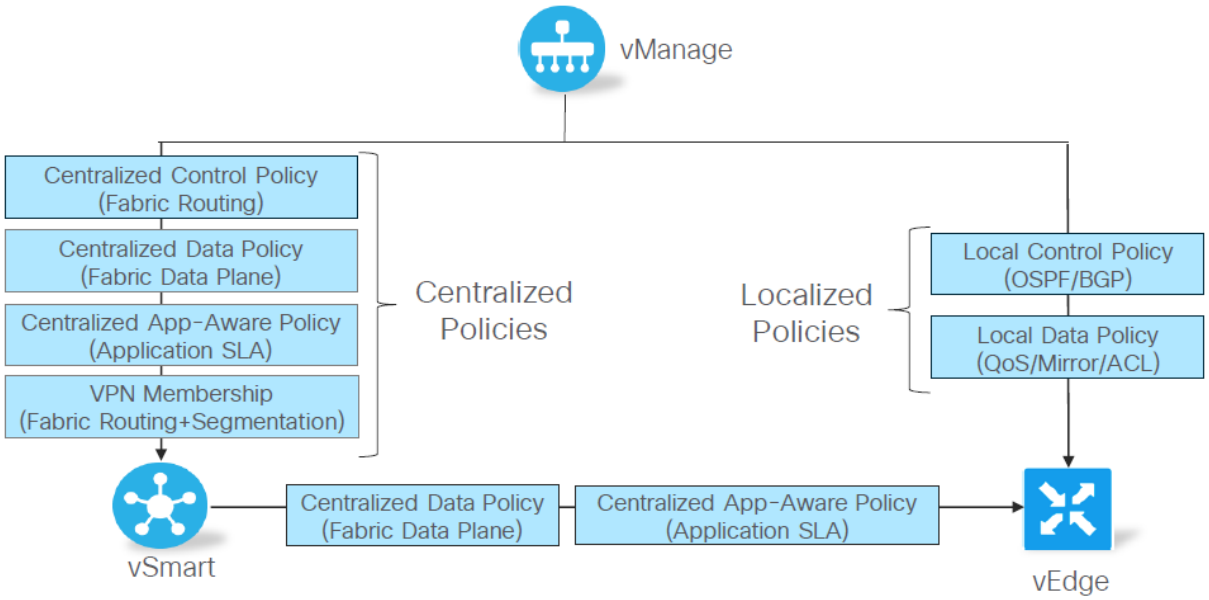




Figura 16. Esquema de aplicación de políticas en SDWAN

### 4.1.9. Alta disponibilidad y Redundancia

SDWAN permite diversas implementaciones para garantizar la disponibilidad de conectividad en cualquier plano y sobre cualquiera de los elementos de la red.

- **Site Redundancy - Routed (Redundancia del sitio – Enrutada):**

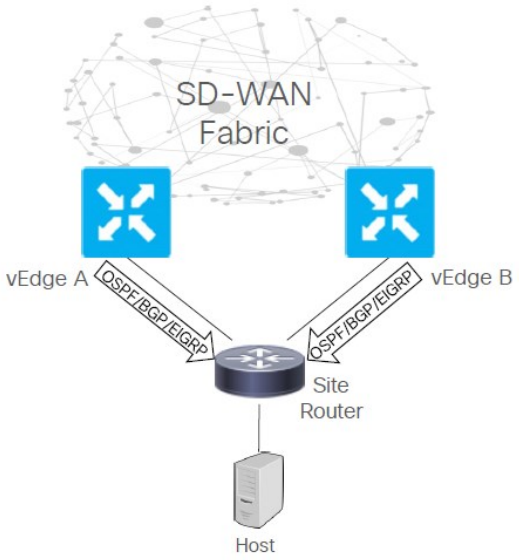




Figura 17. Site Redundancy - Routed

- 2 routers vEdge que funcionan en modo activo / activo y están a uno o más saltos de capa 3 de los hosts
- Los protocolos de enrutamiento estándar OSPF / BGP / EIGRP se ejecutan entre los vEdge de par redundante y el router del LAN
- Redistribución bidireccional entre OMP y OSPF / BGP y viceversa en los routers vEdge
- El enrutador del sitio realiza rutas múltiples de igual costo para destinos remotos en la red SDWAN (Se puede manipular OSPF / BGP para preferir un vEdge sobre el otro)

- **Site Redundancy - Bridged (Redundancia del sitio - Puenteada):**

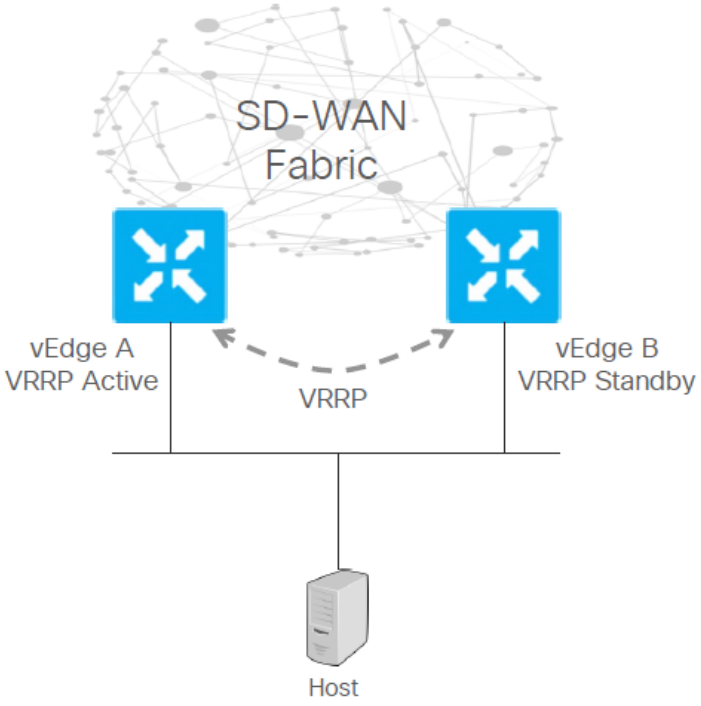




Figura 18. Site Redundancy - Bridged

- Los routers vEdge son de capa 2 adyacentes y son el Gateway predeterminado para los hosts
- Se ejecuta el Protocolo de redundancia de virtual routing (VRRP) entre los dos vEdge redundantes (Activo / activo cuando se usa grupo múltiple por VLAN)
- VRRP Active vEdge responde a las solicitudes ARP para la IP virtual con su interfaz física MAC (no se implementa una MAC virtual)
- En caso de conmutación, el nuevo vEdge activo envía ARP gratuito para actualizar la tabla ARP en los hosts y la tabla de direcciones mac en los Switches intermedios capa2

- **Transport Redundancy - Meshed (Redundancia de transporte - Malla):**

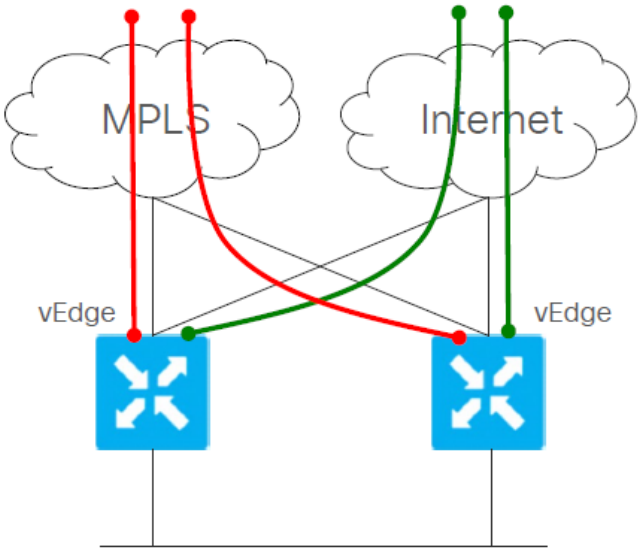




Figura 19. Transport Redundancy – Meshed

- Los routers vEdge están conectados directamente a todas las redes de transporte (No hay necesidad de Switches capa2 para conectar entre si los vEdge)
- Cuando alguna de las redes de transporte se cae, los vEdge detectan la condición y derriban los túneles construidos a través del transporte que falla
- Ambos vEdge mantienen el tráfico para los prefijos disponibles a través de la estructura SDWAN
- Si uno de los routers vEdge falla (falla doble), el segundo enrutador vEdge se hace cargo de reenviar el tráfico dentro y fuera del sitio

- **Transport Redundancy - TLOC Extension (Redundancia de transporte - TLOC Extensión)**

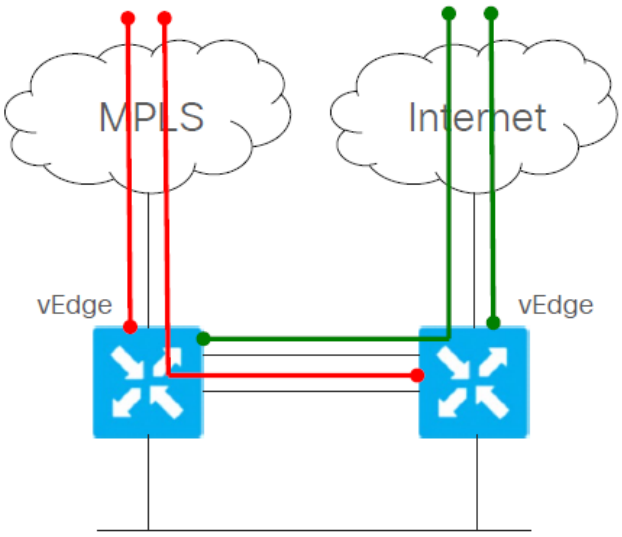




Figura 20. Transport Redundancy - TLOC Extension

- Los routers vEdge están conectados solo a su respectiva red de transporte
- Los vEdge construyen túneles IPSec a través de red de transporte conectados directamente y a través de red de transporte conectados al router vEdge vecino (El vEdge vecino actúa como un enrutador overlay para túneles iniciados desde el otro vEdge)
- Si uno de los vEdge falla (falla doble), el segundo vEdge se hace cargo de reenviar el tráfico dentro y fuera del sitio (Solo se puede utilizar el transporte conectado al vEdge restante)

- **Controllers Redundant Deployment (Despliegue redundante de controladores):**

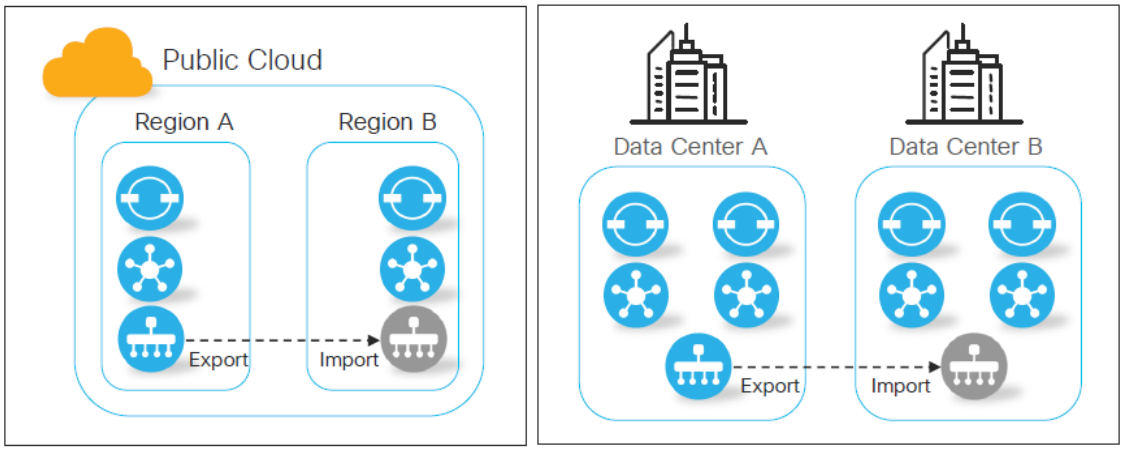




Figura 21. Controllers Redundant Deployment

- Los controladores se distribuyen en múltiples regiones de nube pública y/o data centers
- Los vManage funcionan como Activo-activo, quedando uno de los 2 en standby.

- **Control Redundancy - vBond (Control de redundancia - vBond):**

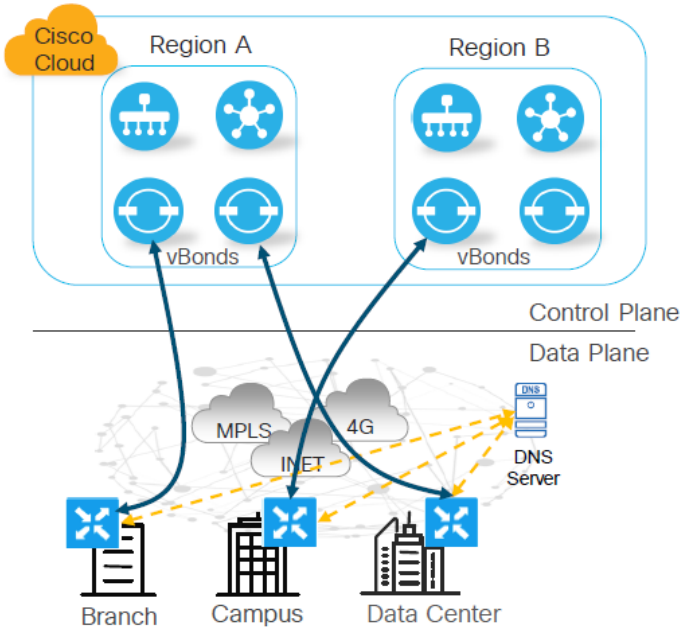




Figura 22. Control Redundancy - vBond

- Los orquestadores vBond tienen una vista completa de los dispositivos permitidos en la red
- Se pueden implementar múltiples vBonds para la función y la redundancia geográfica
- Los vEdges eligen el vBond a través de DNS configurado (Se utiliza DNS round-robin)
- La conexión vEdge a vBond puede ser Temporal o Stateless
- vBonds mantiene la vista en las cargas de los vSmarts para determinar cual deben usar

- **Control Redundancy - vSmart (Control de redundancia - vSmart):**

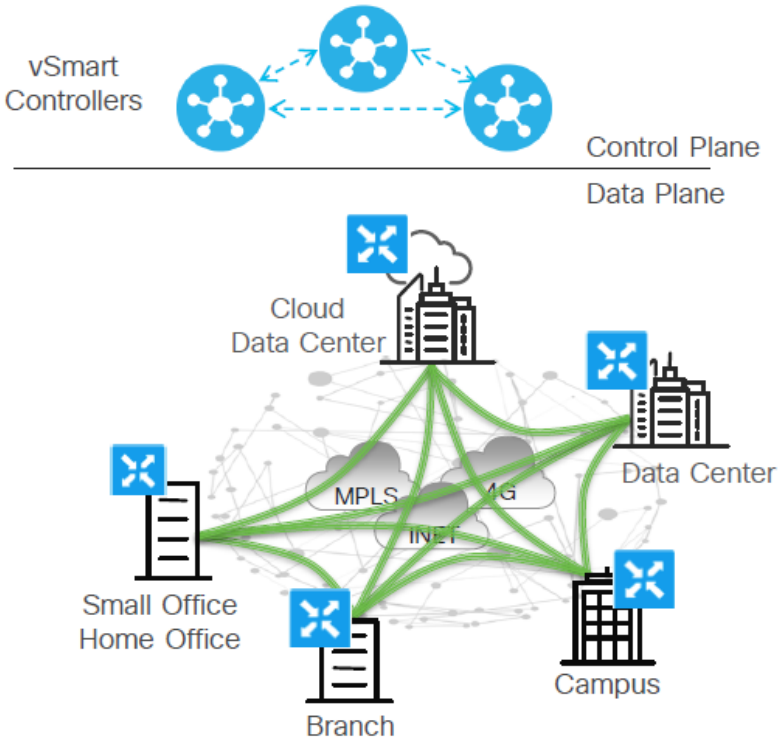




Figura 23. Control Redundancy – vSmart

- Los vSmart intercambian mensajes OMP y tienen una vista idéntica de la estructura SDWAN
- Los vEdge se pueden conectar a hasta tres vSmart para redundancia
- La falla de un solo vSmart no tiene impacto, otros vSmart registrados aún están disponibles
- Si todos los vSmart fallan o se vuelven inalcanzables, los vEdge continuarán operando durante un período de tiempo configurable (min de temporizador de reinicio de KEY y temporizador GR) En este periodo no hay actualizaciones de accesibilidad, no hay propagación de cambios de política y no se envían las KEY en los túneles IPSec

- **Control Redundancy - vManage (Control de redundancia – vManage):**

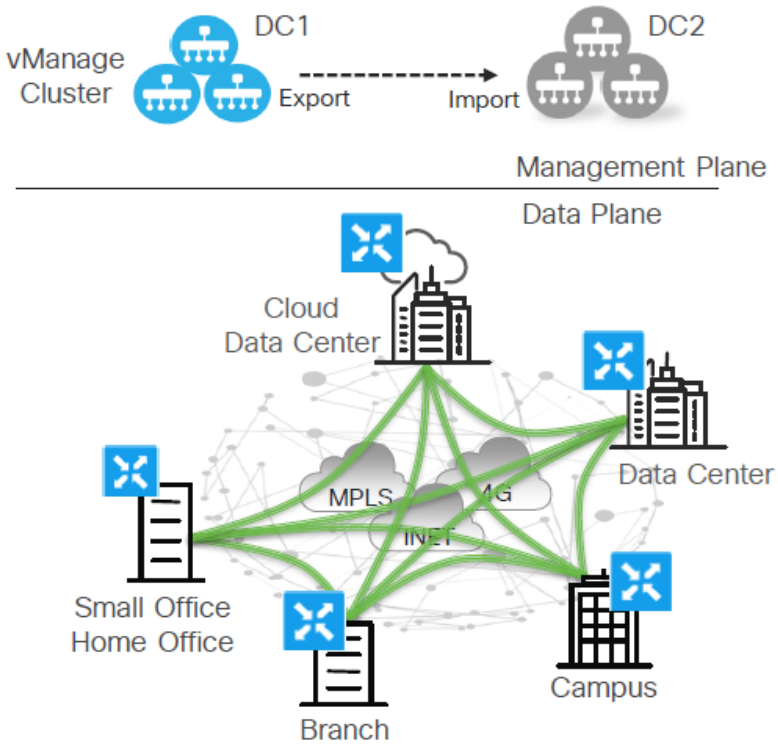




Figura 24. Control Redundancy – vManage

- Los servidores vManage forman un clúster para redundancia y alta disponibilidad.
- Todos los servidores en el clúster actúan como nodos activos / activos siempre y cuando todos los miembros del clúster estén en la misma área de DC / metro
- Para la redundancia geográfica, los servidores vManage funcionan en modo activo / en espera (Se necesita la replicación de la base de datos entre sitios)
- La pérdida de todos los servidores de vManage no tiene ningún impacto en el funcionamiento de la estructura. (En este periodo no se presentarán cambios administrativos ni recopilación de estadísticas)

### 4.2 Marco de referencia tecnológico

Continuando nuestra investigación se procede a analizar el equipamiento disponible en el mercado por el fabricante CISCO SYSTEMS® para las soluciones SDWAN en cuanto a Software y Hardware.

Inicialmente CISCO SYSTEMS® incursiona en el mundo de las redes SDWAN al adquirir en el año 2018 a la empresa Viptela Inc la cual se especializa en Software y hardware para redes SDN desde el año 2012 y quienes ya tenían un portafolio de software y hardware consolidad. Con esta compra CISCO SYSTEMS® continúa comercializando el portafolio de Viptela y a su vez desarrolla nuevos equipos para que sean compatibles y convivan en entornos SDWAN.

Dentro de las gamas de hardware CISCO SYSTEMS® agrupa sus equipos de acuerdo a series a continuación se detallan las disponibles en el mercado para equipos:

#### 4.2.1 Series ASR1000

| | **ASR 1002-HX** | **ASR 1001-X** | **ASR 1002-X** | **ASR 1001-HX** |
|---|---|---|---|---|
| |  |  |  |  |
| Height | 3.5 in/88.9 mm | 1.71 in/43.43 mm | 3.5 in/88.9 mm | 1.71 in/43.43 mm |
| Width | 17.3 in/439.42 mm | 17.3 in/439.42 mm | 17.2 in/437.4 mm | 17.3 in/439.42 mm |
| Depth | 19.25 in/489 mm (2 RU) | 18.17 in/461.5 mm (1 RU) | 18.15 in/461 mm (2 RU) | 18.38 in/466.85 mm (1 RU) |
| Weight | 34 lb/15.45 kg with dual AC power supplies | 25 lb/11.35 kg (fully loaded) | 38.25 lb/17.36 kg with dual AC power supplies | 23 lb/10.44 kg with dual AC power supplies |

Tabla 1. Comparativa Routers SDWAN ASR1000

Fuente: *https://www.cisco.com/c/en/us/products/routers/routercomparison.html?product_id=48|49|50|51*

| | ASR 1002-HX | ASR 1001-X | ASR 1002-X | ASR 1001-HX |
|---|---|---|---|---|
| **Power** | | | | |
| Power supply type | Modular | Modular | Modular | Modular |
| Redundant power supply | Yes | Yes | Yes | Yes |
| PoE support (wattage) | No | No | No | No |
| DC power | Yes | Yes | Yes | Yes |
| **Security** | | | | |
| Cisco Umbrella Branch | Yes | Yes | Yes | Yes |
| Cisco Cloud Web Security | Yes | Yes | Yes | Yes |
| Encrypted Traffic Analytics | Yes | Yes | Yes | Yes |
| Cisco TrustSec | Yes | Yes | Yes | Yes |
| MACsec | Yes | Yes | No | Yes |
| IPsec tunnels | Yes | Yes | Yes | Yes |
| GETVPN | Yes | Yes | Yes | Yes |
| Content filtering | No | No | No | No |
| NAT | Yes | Yes | Yes | Yes |
| Zone-based firewall | Yes | Yes | Yes | Yes |
| Hardware VPN acceleration | Yes | Yes | Yes | Yes |
| **LAN** | | | | |
| Built-in ports | 16 | 8 | 6 | 16 |
| 802.11 wireless | No | No | No | No |
| Layer 3 switch module | No | No | No | No |
| SFP built-in GE ports | 8 to 12 | 6 | 6 | 8 |
| SFP built-in 10GE ports | 4 to 8 | 2 | No | 8 |
| Shared port adapters | No | 1 | 3 | No |
| Ethernet port adapters | 1 | No | No | No |
| Network interface modules | 1 | 1 | No | No |
| Enhanced services modules | No | No | No | No |

| **WAN** | **ASR 1002-HX** | **ASR 1001-X** | **ASR 1002-X** | **ASR 1001-HX** |
|---|---|---|---|---|
| ATM interfaces | No | No | Yes | No |
| Network interface modules | Yes | Yes | No | No |
| Ethernet | Yes | Yes | Yes | Yes |
| Fiber | Yes | Yes | Yes | Yes |
| 3G/4G LTE | No | No | No | No |
| Legacy TDM interfaces | Yes | Yes | Yes | Yes |
| **Network Services** | | | | |
| SD-WAN | Cisco SD-WAN | Cisco SD-WAN | Cisco SD-WAN | Cisco SD-WAN |
| Module online insertion and removal (OIR) | Yes | Yes | Yes | No |
| SD-Access | Yes | Yes | Yes | Yes |
| AppNAV | Yes | Yes | Yes | Yes |
| Application Visibility and Control | Yes | Yes | Yes | Yes |
| IOS high availability | Software | Software | Software | Software |
| Segment routing | Yes | Yes | Yes | Yes |
| Multicast routing protocols | Yes | Yes | Yes | Yes |
| Overlay Transport Virtualization (OTV) | Yes | Yes | Yes | Yes |
| Ethernet VPN (EVPN) | Yes | Yes | Yes | Yes |
| IPv6 support | Yes | Yes | Yes | Yes |
| **Key Features** | | | | |
| Target deployments | High-end enterprise branch, high-performance WAN, MSP, WAN aggregation | Enterprises, MSP, WAN aggregation | Enterprise, MSP, WAN aggregation | High-end enterprise branch, high-performance WAN, MSP, WAN aggregation |

| | ASR 1002-HX | ASR 1001-X | ASR 1002-X | ASR 1001-HX |
|---|---|---|---|---|
| Encryption throughput (Internet MIX) | 24 Gbps | 6 Gbps | 4 Gbps | 15 Gbps |
| SD-WAN software | Cisco SD-WAN | Cisco SD-WAN | Cisco SD-WAN | Cisco SD-WAN |
| **PRICE (USD)** | **$134,674** | **$17,000** | **$38,500** | **$95,000** |

Tabla 2. Comparativa Routers SDWAN ASR1000

Fuente: *https://www.cisco.com/c/en/us/products/routers/routercomparison.html?product_id=48|49|50|51*

### 4.2.1 Series ISR4000

| | ISR 4451 | ISR 4431 | ISR 4351 | ISR 4331 |
|---|---|---|---|---|
| |  |  |  |  |
| Height | 3.5 in/43.9 mm | 1.73 in/43.9 mm | 3.5 in/88.9 mm | 1.75 in/ 44.45 mm |
| Width | 17.25 in/438.15 mm | 17.25 in/438.15 mm | 17.25 in/438.15 mm | 17.25 in/438.15 mm |
| Depth | 18.5 in/469.9 mm | 19.97 in/507.2 mm | 18.5 in/469.9 mm | 17.25 in/438.15 mm |
| Weight | 42.7 lb/19.4 kg | 22.4 lb/10.2 kg | 37.7 lb/17.1 kg | 16.1 lb/7.3 kg |
| **Power** | | | | |
| Power supply type | Internal | Internal | Internal | Internal |
| Redundant power supply | Yes | Yes | No | No |
| PoE support (wattage) | 1000W | 500W | 950W | 500W |
| DC power | Yes | Yes | Yes | Yes |
| **Security** | | | | |
| Cisco Umbrella Branch | Yes | Yes | Yes | Yes |

| | ISR 4451 | ISR 4431 | ISR 4351 | ISR 4331 |
|---|---|---|---|---|
| Cisco Cloud Web Security | Yes | Yes | Yes | Yes |
| Encrypted Traffic Analytics | Yes | Yes | Yes | Yes |
| Cisco TrustSec | Yes | Yes | Yes | Yes |
| MACsec | Yes | Yes | Yes | Yes |
| IPsec tunnels | Yes | Yes | Yes | Yes |
| GETVPN | Yes | Yes | Yes | Yes |
| Content filtering | Yes | Yes | Yes | Yes |
| NAT | Yes | Yes | Yes | Yes |
| Zone-based firewall | Yes | Yes | Yes | Yes |
| Hardware VPN acceleration | Yes | Yes | Yes | Yes |
| Intrusion prevention | Yes | Yes | Yes | Yes |
| **LAN** | | | | |
| Built-in ports | Yes | Yes | No | No |
| Layer 3 switch module | Yes | No | 16 and 24 port | 16 and 24 port |
| Maximum switched Ethernet ports | 72 | 24 | 24 | 40 |
| Maximum switched Ethernet LAN ports with POE | 72 | 24 | 24 | 24 |
| SFP built-in GE ports | 4 | 4 | 2 | 1 |

| | ISR 4451 | ISR 4431 | ISR 4351 | ISR 4331 |
|---|---|---|---|---|
| Network interface modules | 3 | 3 | 3 | 2 |
| Enhanced services modules | 2 | No | 2 | 1 |
| **WAN** | | | | |
| Network interface modules | Yes | Yes | Yes | Yes |
| Enhanced services modules | Yes | Yes | Yes | Yes |
| Ethernet | Yes | Yes | Yes | Yes |
| VDSL2/ADSL2+ | Yes | Yes | Yes | Yes |
| SHDSL | Yes | Yes | Yes | Yes |
| Fiber | Yes | Yes | Yes | Yes |
| **Network Services** | | | | |
| SD-WAN | Cisco SD-WAN | Cisco SD-WAN | Cisco SD-WAN | Cisco SD-WAN |
| Module online insertion and removal (OIR) | Yes | Yes | Yes | Yes |
| SD-Access | Yes | Yes | Yes | Yes |
| WAN optimization | Yes | Yes | Yes | Yes |
| AppNAV | Yes | Yes | Yes | Yes |
| Application Visibility and Control | Yes | Yes | Yes | Yes |
| | | | | |

| | ISR 4451 | ISR 4431 | ISR 4351 | ISR 4331 |
|---|---|---|---|---|
| Segment routing | Yes | Yes | Yes | Yes |
| Multicast routing protocols | Yes | Yes | Yes | Yes |
| Overlay Transport **Virtualization (OTV)** | Yes | No | No | No |
| Ethernet VPN (EVPN) | Yes | No | No | No |
| IPv6 support | Yes | Yes | Yes | Yes |
| **Key Features** | | | | |
| Target deployments | Large branch | Large branch | Medium branch | Medium branch |
| Encryption throughput (Internet MIX) | Up to 2 Gbps | Up to 1 Gbps | 400 Mbps | 300 Mbps |
| SD-WAN software | Cisco SD-WAN | Cisco SD-WAN | Cisco SD-WAN | Cisco SD-WAN |
| **PRICE (USD)** | **$23,350** | **$15,717** | **$10,500** | **$6,111** |

Tabla 3. Comparativa Routers SDWAN ISR4000

Fuente: *https://www.cisco.com/c/en/us/products/routers/router-comparison.html?product_id=43|44|45|46*

### 4.2.2 Series C1000

| | C1111X-8P | C1100-8P | C1100-4P | C1101-4P | C1109-4P | C1109-2P |
|---|---|---|---|---|---|---|
| Typical number of users | 100 | 100 | 75 | 75 | 75 | 75 |
| Performance positioning | 350 Mbps | 350 Mbps | 250 Mbps | 250 Mbps | 200 Mbps | 200 Mbps |
| **WAN** | | | | | | |
| Ethernet | 2 GE | 2 GE | 2 GE | 1 GE | 1 GE | 1 GE |
| VDSL2, ADSL2+ | - | Yes | Yes | - | - | - |
| VDSL2 35b / G.fast | - | Yes | - | - | - | - |
| SHDSL | - | Yes | - | - | - | - |
| Fiber | SFP | SFP | SFP | - | - | - |
| **Wireless WAN** | | | | | | |
| 3G/4G LTE cellular | - | Yes | Yes | Yes | Yes | Yes |
| LTE Advanced | - | Yes | Yes | Yes | Yes | - |
| Active GPS support | - | Yes | Yes | Yes | Yes | Yes |
| Multiband dipole antenna (x2) | - | TNC | TNC | SMA | SMA | SMA |
| Dual SIM | - | Yes | Yes | Yes | Yes | Yes |
| Carrier Aggregation | - | Yes | Yes | Yes | Yes | - |
| **LAN** | | | | | | |
| Ethernet | 8 GE | 8 GE | 4 GE | 4 GE | 4 GE | 2 GE |
| VLAN | 32 VLANs | 32 VLANs | 32 VLANs | 32 VLANs | 32 VLANs | 32 VLANs |
| PoE power budget | 80W | 80W | 60W | - | - | - |
| PoE ports | 4 x PoE or 2 x PoE+ | 4 x PoE or 2 x PoE+ | 2 x PoE or 1 x PoE+ | - | - | - |
| **Wireless LAN** | | | | | | |
| 802.11ac Wave 2 | - | Yes | Yes | Yes | Yes | - |
| | | | | | | |

| | **C1111X-8P** | **C1100-8P** | **C1100-4P** | **C1101-4P** | **C1109-4P** | **C1109-2P** |
|---|---|---|---|---|---|---|
| Unified mode | - | Yes | Yes | Yes | Yes | - |
| Mobility Express | - | Yes | Yes | Yes | Yes | - |
| **Software Features** | | | | | | |
| Routing protocols | RIPv1, RIPv2, BGP, OSPF, EIGRP, PBR, PfR | RIPv1, RIPv2, BGP, OSPF, EIGRP, PBR, PfR | RIPv1, RIPv2, BGP, OSPF, EIGRP, PBR, PfR | RIPv1, RIPv2, BGP, OSPF, EIGRP, PBR, PfR | RIPv1, RIPv2, BGP, OSPF, EIGRP, PBR, PfR | RIPv1, RIPv2, BGP, OSPF, EIGRP, PBR, PfR |
| Multicast | PIM-SM, mroute (static route), MLD | PIM-SM, Mroute (static route), MLD | PIM-SM, Mroute (static route), MLD | PIM-SM, Mroute (static route), MLD | PIM-SM, mroute (static route), MLD | PIM-SM, mroute (static route), MLD |
| IPv6 | Yes | Yes | Yes | Yes | Yes | Yes |
| AppX licensing | Yes | Yes | Yes | Yes | Yes | Yes |
| **Security** | | | | | | |
| IPsec VPN | FlexVPN, DMVPN, GET VPN | FlexVPN, DMVPN, GET VPN | FlexVPN, DMVPN, GET VPN | FlexVPN, DMVPN, GET VPN | FlexVPN, DMVPN, GET VPN | FlexVPN, DMVPN, GET VPN |
| Zone-based firewall | Yes | Yes | Yes | Yes | Yes | Yes |
| IPsec tunnels | Yes | Yes | Yes | Yes | Yes | Yes |
| Encrypted Traffic Analytics | Yes | Yes | Yes | Yes | Yes | Yes |
| Umbrella Connector | Yes | Yes | Yes | Yes | Yes | Yes |
| **Application Experience** | | | | | | |
| Trustworthy Systems | Yes | Yes | Yes | Yes | Yes | Yes |

| | **C1111X-8P** | **C1100-8P** | **C1100-4P** | **C1101-4P** | **C1109-4P** | **C1109-2P** |
|---|---|---|---|---|---|---|
| Application Visibility and Control | Yes | Yes | Yes | Yes | Yes | Yes |
| Intelligent path control | PfR | PfR | PfR | PfR | PfR | PfR |
| **Physical Attributes** | | | | | | |
| Maximum dimensions | 44 mm (height) x 323 mm (width) x 244 mm (depth) | 44 mm (height) x 323 mm (width) x 244 mm (depth) | 44 mm (height) x 323 mm (width) x 244 mm (depth) | 44 mm (height) x 247 mm (width) x 167 mm (depth) | 43 mm (height) x 248 mm (width) x 279 mm (depth) | 29 mm (height) x 193 mm (width) x 160 mm (depth) |
| Maximum weight | 2.45 kg | 2.22 kg | 2.22 kg | 1.7 kg | 2.8 kg | 1.02 kg |
| Fanless | Yes | Yes | Yes | Yes | Yes | Yes |
| DRAM/Flash | 8 GB/8 GB | 4 GB/4 GB | 4 GB/4 GB | 4 GB/4 GB | 4 GB/4 GB | 4 GB/4 GB |
| **PRICE (USD)** | **$1,930** | **$1,743** | **$1,493** | **$1,292** | **$1,695** | **$1,495** |

Tabla 4. Comparativa Routers SDWAN C1000

Fuente: *https://www.cisco.com/c/en/us/products/routers/1000-series-integrated-services-routers-isr/compare-model.html*

### 4.2.2 Serie vEdge

Dentro de la Gama Viptela OS el catálogo incluye:

- vEdge-100: cinco puertos fijos de 10/100/1000 Mbps. Viene en tres variedades diferentes:
  - vEdge 100b: solo Ethernet
  - vEdge 100m: Ethernet y módem 2G / 3G / 4G integrado
  - vEdge 100wm: Ethernet y módem 2G / 3G / 4G integrado + LAN inalámbrica

- vEdge-1000: 8 puertos de GE SFP fijo
- vEdge-2000: 2 módulos de interfaz conectables
- vEdge-5000: 4 módulos de interfaz de red



Figura 25. Serie vEdge Viptela OS

| | **vEdge-100** | **vEdge-1000** | **vEdge-2000** | **vEdge-5000** |
|---|---|---|---|---|
| **Servicios y densidad de ranuras** | | | | |
| Puertos de tráfico | 5 x puertos RJ-45 10/100/1000 Mbps | 8 x 1 Gbps SFP | 4 x 1 Gbps SFP, 2 ranuras de módulo de interfaz conectable (PIM).<br>Opciones de PIM: 2 x 10 Gbps SFP, 8 x 1 Gbps SFP | 4 ranuras del módulo de interfaz de red (NIM): opciones de NIM: 8 x 1 Gbps de cobre, 8 x 1 Gbps SFP y 4 x 10 Gbps |
| Memoria DDR3 ECC | 2 GB | 2 GB | 8 GB | 32 GB DDR4 |
| Ranura para tarjeta SD (externa) | N / A | Capacidad máxima admitida 32 GB | Capacidad máxima admitida 32 GB | N / A |

| | **vEdge-100** | **vEdge-1000** | **vEdge-2000** | **vEdge-5000** |
|---|---|---|---|---|
| Almacenamiento NAND (interno) | 4 GB | 8 GB | 8 GB | 120GB |
| USB externo | 100b: N / A | 2 (USB 3.0 tipo A) | 2 (USB 3.0 tipo A) | 2 (USB 2.0 tipo A) |
| Puerto host | 100m y 100wm: 1 (USB 3.0 Tipo A) | | | |
| Alimentación por Ethernet (PoE) | 100b: N / A | N / A | N / A | N / A |
| | 100m y 100wm: 1 puerto, 15.4W (802.3af) | | | |
| 4G LTE | 100b: N / A | N / A | N / A | N / A |
| | 100m y 100wm: 1 integrado | | | |
| Sistema de posicionamiento global (GPS) | Integrado con antena externa | N / A | N / A | N / A |
| Puerto de consola USB | 1, Mini Tipo B (115.2 Kbps) | 1, tipo B | 1, tipo B | N / A |
| | | (115,2 Kbps) | (115,2 Kbps) | |
| Puerto serie de consola | N / A | 1, RJ-45 (115,2 Kbps) | 1, RJ-45 (115,2 Kbps) | 1, RJ-45 (115,2 Kbps) |

| | **vEdge-100** | **vEdge-1000** | **vEdge-2000** | **vEdge-5000** |
|---|---|---|---|---|
| Puerto Ethernet de administración (RJ-45 10/100 / 1000Mbps) | N / A | 1, RJ-45 10/100/1000 | 1, RJ-45 10/100/1000 | 1, RJ-45 10/100/1000 |
| Opción de fuente de alimentación | 100b: adaptador de corriente externo AC-DC<br>100m: adaptador de corriente alterna fijo interno | Adaptador de corriente AC-DC externo | Unidades de fuente de alimentación intercambiables en caliente (PSU) | Unidades de fuente de alimentación intercambiables en caliente (PSU) |
| Soporte de fuente de alimentación redundante | N / A | si | 1 + 1 redundancia activo-activo | si |
| Aficionados | 100b: N / A (sin ventilador)<br>100m y 100wm: 1 ventilador, fijo | 2 | 2, intercambiables en caliente | 4, intercambiables en caliente |

| **Especificaciones de potencia** | | | | |
|---|---|---|---|---|
| | **vEdge-100** | **vEdge-1000** | **vEdge-2000** | **vEdge-5000** |
| Voltaje de entrada de CA | 90-264 Vrms | 90-264 Vrms | 90-264 Vrms | 90-264 Vrms |
| | (100-240V) | (100-240V) | (100-240V) | (100-240V) |
| Frecuencia de línea de entrada de CA | 47-63 Hz | 47-63 Hz | 47-63 Hz | 47-63 Hz |
| Consumo de energía típico | 100b: 15W | 28W | 125W | Consumo máximo de energía 285W |
| | 100m y 100wm: 35W con PoE, 20W sin PoE | | | |
| **Especificaciones físicas** | | | | |
| Altura del estante | 100b: 1 RU | 1 RU | 1 RU | 1 RU |
| | 100m y 100wm: 1RU Plus | | | |
| Altura del chasis | 100b: 1,75 | 1,75 | 1,75 | 1,75 |
| | pulg . (4,4 cm) | pulg . (4,4 cm) | pulg . (4,4 cm) | pulg . (4,4 cm) |
| | 100 my 100 wm: | | | |
| | 1,8 pulg . (4,6 cm) | | | |

| | **vEdge-100** | **vEdge-1000** | **vEdge-2000** | **vEdge-5000** |
|---|---|---|---|---|
| Ancho del chasis | 100b: 6,75 pulgadas (17 cm)<br>100 my 100 wm: 9,25 pulg. (23,5 cm) | 7,5 pulgadas (19 cm) | Solo chasis: 17.25 pulg. (43.82 cm)<br>Chasis con soportes de montaje unidos: 19 pulg. (48.2 cm) | Solo chasis: 438 mm<br>Chasis con soportes de montaje unidos: 19 pulg. (482 mm) |
| Profundidad del chasis | 100b: 5.5 pulg. (14 cm)<br>100 my 100 wm: 5,75 pulg. (14,6 cm) | 10 pulg. (25,4 cm) | 18,5 pulgadas (47 cm) | 580mm |
| Peso del chasis | 1,75 lb (0,79 kg) | 3,55 libras (1,6 kg) | Solo chasis: 11 lb (5 kg)<br>Chasis con dos fuentes de alimentación.<br>Instalado: 15 lb (6.8 kg) | Chasis con ventiladores y fuentes de alimentación instaladas: 37 lbs. |
| Flujo de aire | 100b: N / A (noventilador)<br>100 my 100 wm: superior | Desde el frente hacia atrás | Desde el frente hacia atrás | Desde el frente hacia atrás |

| | vEdge-100 | vEdge-1000 | vEdge-2000 | vEdge-5000 |
|---|---|---|---|---|
| Kit de accesorios para montaje en bastidor EIA de 19 pulgadas (48,3 cm) | 100b: suministrado con la unidad 100m y 100wm: disponible y vendido por separado | Disponible y vendido por separado | Proporcionado con la unidad | Proporcionado con la unidad |
| **Condición de uso** | | | | |
| Temperatura | 0 a 40 ° C (32 a 104 ° F) al nivel del mar (disminución de la temperatura de 1.5 grados C por 1000 pies de altitud aplicable hasta un máximo de 10000 pies o 3000 m) | 0 a 40 ° C (32 a 104 ° F) al nivel del mar (disminución de la temperatura de 1.5 grados C por 1000 pies de altitud aplicable hasta un máximo de 10000 pies o 3000 m) | 0 a 40 ° C (32 a 104 ° F) al nivel del mar (disminución de la temperatura de 1.5 grados C por 1000 pies de altitud aplicable hasta un máximo de 10000 pies o 3000 m) | 0 a 40 ° C (32 a 104 ° F) al nivel del mar (disminución de la temperatura de 1.5 grados C por 1000 pies de altitud aplicable hasta un máximo de 10000 pies o 3000 m) |
| Altitud | Máx.3000 m (10000 pies) | Máx.3000 m (10000 pies) | Máx.3000 m (10000 pies) | Máx.3000 m (10000 pies) |
| Humedad | 10 a 85% | 10 a 85% | 10 a 85% | 10 a 85% |

| | vEdge-100 | vEdge-1000 | vEdge-2000 | vEdge-5000 |
|---|---|---|---|---|
| **Condición de transporte / almacenamiento** | | | | |
| Temperatura | -40 a 70 ° C | -40 a 70 ° C | -40 a 70 ° C | -40 a 70 ° C |
| | (-40 a 158 ° F) | (-40 a 158 ° F) | (-40 a 158 ° F) | (-40 a 158 ° F) |
| Humedad | 5 a 95% HR | 5 a 95% HR | 5 a 95% HR | 5 a 95% HR |
| Altitud | 4570 m (15000 pies) | 4570 m (15000 pies) | 4570 m (15000 pies) | 4570 m (15000 pies) |
| **Fiabilidad** | | | | |
| MTBF | 104 mil horas | 80 mil horas | 420 mil horas | 178 mil horas |
| **Cumplimiento normativo** | | | | |
| La seguridad | AS / NZS 60950-1 | AS / NZS 60950-1 | AS / NZS 60950-1 | AS / NZS 60950-1 |
| | CAN / CSA 60950-1 | CAN / CSA 60950-1 | CAN / CSA 60950-1 | CAN / CSA 60950-1 |
| | CB-IEC60950-1 | CB-IEC60950-1 | CB-IEC60950-1 | CB-IEC60950-1 |
| | Marcado CE | Marcado CE | Marcado CE | Marcado CE |
| | EN 60950-1 | EN 60950-1 | EN 60950-1 | EN 60950-1 |
| | UL60950-1 | UL60950-1 | UL60950-1 | UL60950-1 |

| | **vEdge-100** | **vEdge-1000** | **vEdge-2000** | **vEdge-5000** |
|---|---|---|---|---|
| EMC | 100b: AS / NZS CISPR22 Clase A | AS / NZS CISPR22 Clase A | AS / NZS CISPR22 Clase A | EN 550332: 2012 + AC: 2013 Clase A |
| | 100m: AS / NZS CISPR22 Clase B | | | AS / NZS CISPR 32: 2015 |
| | | | | CISPR32: 2015 |
| | | | | EN55024: 2010 + A1: 2015 |
| | | | | EN 61000-3-2: 2014 CLASE A |
| | | | | EN 61000-3-3: 2013 |
| | EN 300 386 | EN 300 386 | EN 300 386 | |
| | 100b: EN 55022 Clase A | EN 55022 Clase A | EN 55022 Clase A | FCC PARTE 15, SUBPARTE B |
| | 100m: EN 55022 Clase B | | | ANSI C63, 4-2014 |
| | | | | ICES-003 NÚMERO 6: 2016 |
| | | | | CISPR 22: |

| | | | | |
|---|---|---|---|---|
| | | | | 2008<br>CAN / CSA-CISPR 22-10 |
| | 100b: FCC Clase A<br>100m: FCC Clase B | FCC Clase A | FCC Clase A | FCC Clase A |
| | 100b: ICES Clase A<br>100m: ICES Clase B | CIEM clase A | CIEM clase A | CIEM clase A |
| | 100b: VCCI Clase A<br>100m: VCCI Clase B | VCCI clase A | VCCI clase A | VCCI clase A |
| Ambiental | ROHS 6/6 | ROHS | ROHS | ROHS |
| **PRICE (USD)** | **$1,050** | **$2,995** | **$11,000** | **$32,055** |

Tabla 5.Comparativa Routers SDWAN vEdge

Fuente: *https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-07-vedge-routers-data-sheet-cte-en.html*

## 5. Glosario de términos.

- (ANS) Es un acuerdo negociado entre dos partes donde una de ellas es el cliente y la otra un proveedor de servicios, cada área de servicio debe tener un ANS definido, que comprenda los niveles de disponibilidad, servicio, rendimiento u otros atributos del servicio.
- (ATP) Documento de Protocolo de Aceptación.
- (BACKUP) Se refiere a la copia y archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.
- (COLOR) etiqueta de plano de control utilizada para la lógica de establecimiento del túnel IPSec.
- (DC) (Data Center) Centro de Datos.
- (FIREWALLS) Un firewall o cortafuegos es un Programa Informático (Software) o un Hardware que brinda protección a una computadora (ordenador) o a una red frente a intrusos. También en software o sistema informático cuya función es bloquear el acceso no permitido al equipo o a la infraestructura de red en cuestión.
- (HA) Estado de programa de protección en una red computadora o (ordenador) llamado Firewall.
- (HARDWARE) Es la parte física de un ordenador o sistema informático. Está formado por los componentes eléctricos, electrónicos, electromecánicos y mecánicos, tales como circuitos de cables y luz, placas, memorias, discos duros, dispositivos periféricos y cualquier otro material en estado físico que sea necesario para hacer que el equipo funcione.
- (HOST) Un host o anfitrión es un ordenador que funciona como el punto de inicio y final de las transferencias de datos. Más comúnmente descrito como el lugar donde reside un sitio web.
- (LAN) (Local Área Network), Red de área local.
- (ORGANIZATION NAME) identificador de overlay común a todos los elementos de la estructura.
- (PING) (Packet Internet Groper). Este comando se utiliza para comprobar si una determinada interfaz de red, de nuestra computadora o de otra, se encuentra activa.
- (PROTOCOLO DE ADMINISTRACIÓN DE SUPERPOSICIÓN OMP) protocolo de plano de control que distribuye accesibilidad, seguridad y políticas en todo el tejido de red.

- (ROUTER) Es un dispositivo de hardware que permite la interconexión de ordenadores en red. El router es un dispositivo que opera en capa tres de nivel de 3. Así, permite que varias redes u ordenadores se conecten entre sí y, por ejemplo, compartan una misma conexión de Internet.
- (SD-WAN) (Software Defined Wide Área Network), Red de área amplia definida por Software.
- (SITE ID) identificador numérico único por sitio utilizado en la aplicación de políticas.
- (SOFTWARE) Es un término informático que hace referencia a un programa o conjunto de programas de cómputo, así como datos, procedimientos y pautas que permiten realizar distintas tareas en un sistema informático.
- (SWITCH) Es un dispositivo que permite que la conexión de computadoras y periféricos a la red para que puedan comunicarse entre sí y con otras redes. Switch es una palabra en inglés usada en el área de informática para referirse al controlador de interconexión entre varios dispositivos.
- (SYSTEM IP) identificador de notación IPv4 único por dispositivo (vEdge y vSmart). También se utiliza como ID de Router para BGP y OSPF.
- (TRANSPORT LOCATOR TLOC): punto de conexión de transporte y atributo de ruta del siguiente salto.
- (TOPOLOGIA) La topología de red se define como el mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico.
- (VEDGE o CEDGE) Nombre que se suministra a un Router.
- (VPN) (Virtual Privarte Network) VPN, es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.
- (WAN) (Es la sigla de Wide Área Network) Red de Área Amplia el concepto se utiliza para nombrar a la red de computadoras que se extiende en una gran franja de territorio, ya sea a través de una ciudad, un país o, incluso, a nivel mundial.

## 6. Justificación

Las redes virtualizadas ya son una realidad para hacer la conectividad de las empresas ofreciendo muchos más beneficios que las redes convencionales; la implementación de esta tecnología en las compañías representa una modernización e innovación en sus comunicaciones y dadas las características de crecimiento de nuestro cliente, se presenta como la alternativa más escalable. El Core de negocio de nuestro cliente claramente no son la implementación de enlaces de comunicación y el área de TI debe ajustarse a las necesidades reales de la empresa que es la expansión y conquiste de nuevos mercados, para ello necesitaran disponer de canales de comunicación de instalación rápida, confiable y móviles para llegar a donde sus potenciales clientes se encuentran.

Esta propuesta ofrece al cliente la flexibilidad de implementación de un nuevo canal en el momento que lo requiera, no sujeto a la disponibilidad técnica de instalación por parte de un ISP ya que se propone la implementación de 2 enlaces en sus sedes tipo market con una disponibilidad de servicio de 99.9% al tener una redundancia por red móvil Celular y sin incrementar los costos actuales; si bien los enlaces de fibra tienen una buena estabilidad sus costos son bastante elevados y por el precio de uno se pueden implementar 2 enlaces que ofrezcan la misma disponibilidad de conectividad que necesita la sede y así tener continuidad del negocio.

Por otra parte, este diseño le permite tener una red completamente escalable y de fácil administración gracias al uso de SDWAN ya que para su utilización solo necesita de acceso a Internet y todo su funcionamiento interno está orientado a las aplicaciones que usa el cliente y así poder usar todo el potencial de los canales que se instalan sin elevar los costos.

# 7. Objetivos

## 7.1. General.

Diseñar una red para realizar la integración de conectividad de las sedes tipo market de una empresa de producción y comercialización de alimentos basado en el principio de virtualización más conocido como SDWAN

## 7.2. Específicos.

- Analizar las necesidades y requerimientos de conectividad de las sedes tipo market de una empresa de producción y comercialización de alimentos
- Diseñar una propuesta de conectividad para las sedes tipo market de una empresa de producción y comercialización de alimentos que permita la integración de conectividad a la red actual de la compañía soportada en tecnología SDWAN usando equipos Cisco
- Realizar los diseños específicos de conectividad de una sede Piloto
- Verificar mediante simulación el diseño de conectividad de la sede piloto para su comprobación.

# 8. Requerimientos

## 8.1. Requerimientos funcionales

Por medio de una simulación practica en la que se incluirá el diseño de conectividad las sedes del cliente se procederá a evaluar el diseño usando un software de simulación, en dicha herramienta se ejecutaran test de control de tráfico, verificación de ancho de banda consumido por la red, así como verificación de los diferentes protocolos y aplicaciones definidas en la solución de conectividad , cuyo entregable será el archivo propio de la simulación funcionando junto con un documento descriptivo de la simulación.

## 8.2. Requerimientos no funcionales

Con el fin de hacer la documentación y correspondiente entrega de la solución se establecerá un Documento de Protocolo de Aceptación de Implementación (ATP) que recopilará el protocolo de pruebas de verificación de conectividad de la solución sobre SDWAN y será complemento del archivo de simulación.

## 9. Metodología

La metodología que se va a implementar es de investigación documental y práctica. Documental porque en una primera instancia se realizará una compilación de todo el material bibliográfico que se tenga disponible ya que estamos hablando de la implementación de una nueva tecnología, con lo cual es necesario realizar un estudio y comprensión del funcionamiento y arquitectura del modelo SDN en su implementación final SD-WAN, con el fin de adquirir los conocimientos que permitan desarrollar y plantear el diseño de red que supla el problema definido.

Una vez finalizada la etapa anteriormente mencionada, continuaremos con la metodología práctica en la que se definirá y planteará el diseño de la red del objeto de este proyecto, aplicando las técnicas de diseño que optimicen la necesidad de conectividad requerida y que integren la tecnología y funcionamiento del modelo SD-WAN. Seguidamente se planteará la simulación o implementación del diseño bajo un ambiente de virtual bajo software libre que permita realizar un testeo de la red con el fin de obtener pruebas que permitan verificar que la solución propuesta se ajusta de manera óptima a la necesidad planteada inicialmente ofreciendo mejoras considerables y garantizando que su implementación es apta para el funcionamiento de la empresa.

# 10. Desarrollo

## 10.1 Discriminación de la red Actual

### 10.1.1 Servicios Prestados

Todo Market Tiene 4 elementos fundamentales para poder funcionar adecuadamente

- Un PC para la facturación, el correo, el manejo de inventario y acceso a Internet
- Un teléfono IP para comunicarse
- Cámaras IP para seguridad
- Un datafono para recibir los pagos por medios electrónicos

Por lo que se adelantó la discriminación de los servicios que cada dispositivo en la sede accede para poder tener aclarar

**PC**

- Acceso al ERP
- Acceso a Archivos compartidos con promociones e informacion
- Acceso al aplicativo de facturacion
- Acceso al correo electronico
- Acceso a Internet

**Telefono IP**

- Llamadas codificacion G711

**Camaras IP**

- Streaming de Video para Backup MPEG-4

**Datafono**

- Acceso al aplicativo de pagos en linea

**Servicios alojados en el Datacenter Principal**

- Facturación
- Llamadas IP
- Backup de Video cámaras IP
- ERP
- FTP MARKET

**Servicios en la nube**

- Correo electrónico
- Acceso Internet

En la sede market según lo indicado por el cliente, los servicios críticos son los de pagos en línea, de facturación junto con el manejo de Stock ya que son lo que se usa al momento de que los clientes realizan compras en el local.

Como servicios de importancia alta para el cliente encantamos la Voz, los correos electrónicos y el repositorio FTP de información.

De prioridad baja el tráfico de Video que se genera de las cámaras la cual se respalda en el Datacenter del cliente junto con la navegación web que genera el operador en el computador.

### 10.1.2 Trafico Actual

El Cliente actualmente tiene un solo canal de MPLS con una capacidad de 5Mb/s simétricos, Se tomaron 5 canales al azar para analizar el comportamiento del tráfico de los canales, tomando muestras del tráfico que cursa la interface WAN cada 5 minutos durante todo el mes alimentado
una serie de 5 tablas que se encuentra adjunta en los Anexos

Esta información la analizamos para conocer la media de consumo durante un mes y para conocer el comportamiento genera del canal en busca de problemas que se pueda corregir en el diseño o factores a mejorar en tal caso.

Lo primero que realizamos es un análisis estadístico simple donde revisamos los Puntos clave como mínimos, máximos, la media y la correlación entre si para poder validar esta información como una muestra promedio real o se presentó algún enveto en el monitoreo que afecto esta muestra ya que si encontramos Mínimos en valores de 0 nos mostraría la caída del servicio y si encontramos máximo iguales al el contratado serian puntos de saturación

| | **Subida** | **Bajada** |
|---|---|---|
| Promedio | 400463,1615 | 48897,05632 |
| Máximo | 2514000 | 3290000 |
| Mínimo | 1000 | 1000 |

Tabla 6 Datos Market 1

En el Market 1 no encontramos muestras de valor 0 por lo que no se presentó caídas de más de 5 minutos durante periodo de tiempo analizado, se observa que los valores máximo no alcanzaron el valor límite de 5Mb

| | **Subida** | **Bajada** |
|---|---|---|
| Promedio | 56137,25823 | 87973,53241 |
| Máximo | 3944000 | 5094000 |
| Mínimo | 2000 | 1000 |

Tabla 7 Datos Market 2

En el Market 2 no encontramos muestras de valor 0 por lo que no se presentó caídas de más de 5 minutos durante periodo de tiempo analizado, se observa que el canal de bajada alcanzo el lumbar de saturación, pero el promedio general no está entre los más altos y en el análisis individual de la información esta saturación no duro más de 1 hora en el mes

| | **Subida** | **Bajada** |
|---|---|---|
| Promedio | 142713,5661 | 11136,12933 |
| Máximo | 4994000 | 2585000 |
| Mínimo | 0 | 0 |

Tabla 8 Datos Market 3

En el Market 3 encontramos muestras de valor 0 por lo que se presentó caídas en el servicio, analizando los datos individuales encontramos que este servicio estuvo caído por 4970 Minutos, siendo un valor bastante alto, el cliente nos indica que esta fue una caída de su proveedor actual, se observa que los valores máximo alcanzaron el valor límite de 5Mb en el aspecto de subida y corresponde a picos de no más de 5 minutos continuos y no por más de 30 m al mes

| | **Subida** | **Bajada** |
|---|---|---|
| Promedio | 647198,502 | 44237,5936 |
| Máximo | 4903000 | 4721000 |
| Mínimo | 0 | 0 |

Tabla 9 Datos Market 4

En el Market 4 encontramos muestras de valor 0 por lo que se presentó caídas en el servicio, analizando los datos individuales encontramos que este servicio estuvo caído por 120 Minutos, el cliente nos indica que esta fue una caída de su proveedor actual, presenta un picos de subida y lato trafico sol por 30 m en el mes

| | Subida | Bajada |
|---|---|---|
| Promedio | 504572,4761 | 160920,7026 |
| Máximo | 2548000 | 4997000 |
| Mínimo | 1000 | 1000 |

Tabla 10 Datos Market 5

En el Market 5 no encontramos muestras de valor 0 por lo que no se presentó caídas de más de 5 minutos durante el mes analizado, Se observa que de valores máximo alcanza el punto de saturación pero solo fue un valor puntual y los valores cercanos está en una duración de 30 minutos en el mes

Profundizando en los puntos de datos con consumo alto de descarga se encontró que el destino de los picos corresponde a actualizaciones de Windows y los puntos altos corresponden a un proceso de backup automatizado que corre en la sede una vez al mes.

### 10.1.3 Análisis de las fallas en el servicio

El cliente nos compartió una tabla con la información relevante sobre las fallas que se presentaron en promedio los últimos 6 meses, donde evalúa la duración de los Mismos para aplicar las penalidad al proveedor de servicio.

| Tipo de falla | 2-4 Horas | 4-6 Horas | + 6 Horas | Total |
|---|---|---|---|---|
| Caída | 1 | 2 | 3 | 6 |

Tabla 11 Datos Caída promedio Últimos 6 meses

Encontrado que cuando presenta una caída el servicio normalmente la resolución de las falla está por encima de las 2 horas y que en genera las resorción de una falla esta rondado las 6 horas, pero en caso extraordinarios como el visto en el análisis del Market 4 encontramos que duro más de 3 días caídos y afectado el negocio fuertemente por lo que el cliente quiere poder contar con un medio de contingencia pero sin elevar los costó operativos actuales que implicaría implantar otro canal de backup MPLS

### 10.1.4 Topología Física

- **Market**

En el levantamiento de la información con el cliente encontramos que el equipamiento básico de una sede está dado por 6 equipos, inicialmente el router que ofrece el operador, un Switch, una cámara IP, un teléfono IP un y un Datafono, el acceso a Internet se hace a través de enlaces de UM de los ISP contratados:

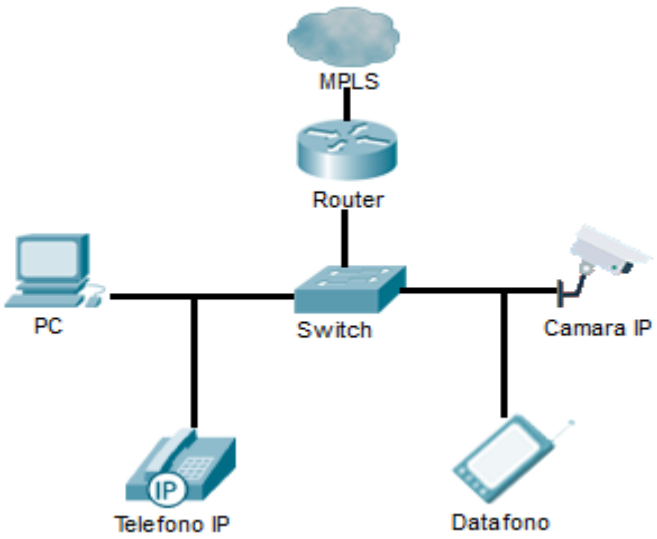


Figura 26 Esquemático Market

- **Datacenter Central**

El cliente cuenta con 2 datacenter en dos lugares Geográficos distintos uno es Bogotá y otro en Medellín, el primero es el datacenter Principal y el Segundo el DRP

El datacenter principal cuenta con esquemas de conectividad en alta disponibilidad, a nivel de enlaces, a nivel de equipos tanto WAN como LAN

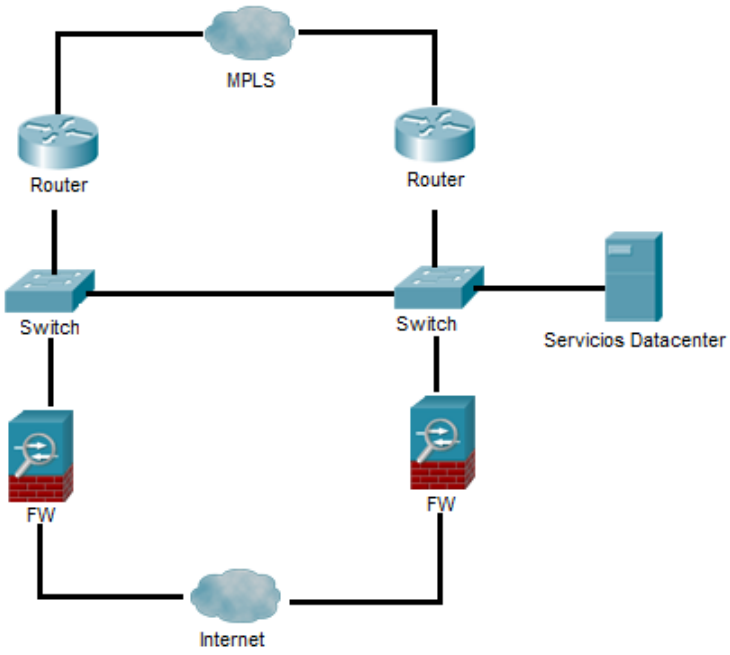


Figura 27 Esquemático Datacenter Principal

- **Datacenter DRP**

El datacenter que Funciona como DRP no cuenta con esquema de alta disponibilidad y esté operando en estado de espera a que se presente una falla en el principal

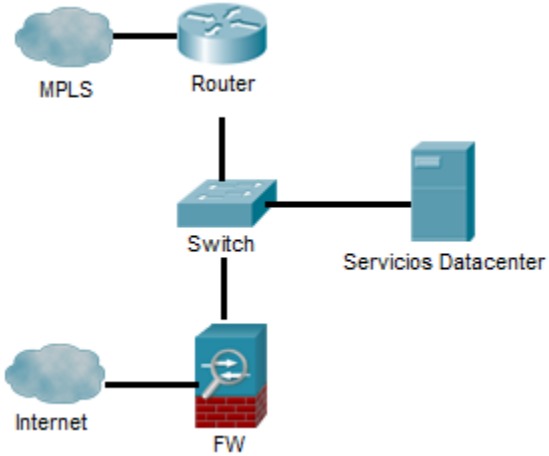


Figura 28 Esquemático Datacenter DRP

Nuestra propuesta busca que el cambio en cuanto a la topología y estructura de red interna del cliente se modifique lo menos posible remarcando así la flexibilidad que presenta las soluciones de conectividad WAN que actualmente no tiene usando solo MPLS, además busca mantener los esquemas de alta disponibilidad que ya cuenta.

### 10.2 Red SDWAN

Junto con el levantamiento de la información de la información del funcionamiento actual de la red, también se tomaron los requerimientos específicos del cliente que el cliente quiere sobre el diseño que se está realizando, en este caso fueron los siguientes:

Actualmente la red se basa en equipos Cisco, tiene Router en todas sus sedes, Firewall, Switches, AP y Telefonía IP Cisco por lo que nos pide que la solución de SDWAN sea también de Cisco porque a futuro y dependiendo de los resultados de este proyecto se migrara el resto de su sedes Criticas también a SDWAN y quiere que esta transición sea lo más fácil posible y manejando todo desde el mismo orquestador.

#### 10.2.1 Tipificación de sedes SDWAN

Bajo los parámetros de diseño de SD WAN se deben tipificar la sede que se van a implementar para poder agruparlas según sus funcionalidades y poder manejar el proceso de aprovisionamiento y configuración de una manera más ordenada y limpia.
Por lo que en el análisis realizado a la red en funcionamiento encontramos tres tipos de sedes y para cumplir las expectativas que se tienen como objetivo en este proyecto tenemos una cuarta que su conectividad se basa en solo soluciones móviles.

- **Datacenter**

Esta es la sede principal, en la cual se van a concentra las sedes para conectarse con los servicios de datacenter y debe conservar los parámetros de alta disponibilidad que tiene actualmente el modelo instalado también será el punto donde se interconectará con la red MPLS de las demás sedes.

- **Datacenter DRP**

Esta sede debe servir como punto de conexión de contingencia en caso de fallo de los servicios alojados en el datacenter principal, y al igual que en el modelo actual está en estado de espera ante la falla en el datacenter principal.

- **Market**

La sede remota debe cumplir los parámetros de conectividad actuales, donde tiene un canal terrestre, además poder darle también protección al servicio con un canal que sirva de contingencia en caso de falla del canal principal y también poder implantar un nuevo tipo de sede que sea totalmente móvil todo esto sin elevar los costos que se tiene actualmente

### 10.2.2 Tipificación de canales

Las rede SDWAN esta diseñadas para poder separar el plano de control del plano de datos, en este caso el control se realizara desde la nube por lo que usar Internet como red de comunicación para el plano de datos de toda la solución nos da la versatilidad que no ofrece la solución MPLS actual mente en operación.

Internet al ser un servicio público, y por la regulación de la legislación Colombiana día a día estay creciendo en capacidad, calidad y tenido mayor alcance a los usuarios, por lo que es proveído a través de múltiples medios por todo el país, y más fuertemente en las zonas urbanas donde se tiene instalados actualmente los marquetas y donde a futuro se instalara más

- **Datacenter**

El cliente contrata hosting en dos datacenters comerciales en donde se presta todas las garantías de estabilidad de energía y seguridad por lo que los canales necesarios para estas sedes criticas debe contar con las mismas características que los actuales por lo que se debe usar 2 Canales de Internet completamente diversos para tener protección frente a fallas en uno de los servicios

- **Market**

Para brinda la conectividad que requiere en las sedes remotas se debe implementar un canal de internet Banda Ancha que según la definición de Resolución 5161 de junio de 2017 de la CRC tiene una capacidad mínima de 25 Mbps de descarga y de 5 Mbps por segundo en capacidad se carga en el cual. En el análisis realizado del tráfico que cursa actualmente por la red, se observa que no está tenido problemas de capacidad, ya que uso del canal más fuerte se da en el tema del backup de video usando el canal de subida en un 50% y este tráfico no se plantea crecimiento ya que el sistema de video vigilancia no está en proyectos de cambio a mediano ni a largo plazo, en cambio la capacidad de descarga se crese en porcentaje de 500%.

Además de esto se contará con conectividad móvil 4G como canales de respaldo los cuales cuenta con taza variables de trafico de hasta 100 Mbit/s de bajada y 50 Mbit/s, y que para el tráfico crítico de la sede que según el análisis es solo trasnacional como lo son los aplicativos de pagos en línea la base de datos ERP, los aplicativos de facturación.

Para hacer un análisis del costo del internet en modalidad banda Ancha terrestre y móvil Celular se hizo una cotización de estos canales en los operadores más comunes en don el cliente tiene actualmente sus servicios, a la fecha de Mayo de 2020 dando como resultado las siguiente tablas con los siguiente valores

| Proveedor | Capacidad Up/ Down | Valor en Peso / Dólares |
|---|---|---|
| Claro | 50 Mb /10 Mb | 81900 /22 |
| Movistar | 80 Mb /80 Mb | 82900 /22 |
| Tigo | 30 Mb/5 Mb | 80000 /22 |
| ETB | 30 Mb/ 10 Mb | 79000 / 22 |
| EMCALI | 25Mb /12.5 Mb | 90000/ 23 |
| Promedio | - | 83000 / 22 |

Tabla 12 Comparativa precio vs capacidad internet Banda Ancha

| Proveedor | Cantidad Plan | Valor en Peso / Dólares |
|---|---|---|
| Claro | 18GB | 69000 /19 |
| Movistar | 19 GB | 85990 /23 |
| Tigo | 15 GB | 63900 /17 |
| ETB | 30 GB | 57900 / 16 |
| Avantel | 30 GB | 50400 / 15 |
| Promedio | 22 GB | 66600 / 18 |

Tabla 13 Comparativa precio vs capacidad internet LTE

EL costo actual para el canal del cliente está en es $135 dólares por mes, y donde un canal banda ancha en Colombia está costando según sondeo $22 dólares y un plan de datos LTE de 22 GB un promedio de $18 dólares estarías frente a una disminución del cargo de renta fijo ménsula de más del 70% y tendiendo un canal e backup completamente protegido

### 10.2.3 Tipificación Colores SDWAN

Par poder prestar los servicios que queremos prestar debemos tener dos colores para poder tener los servicios protegidos y segmentadas según las necesidad, para estos se usara el color BIZ-Internet para los canales terrestres y el color 3G para los canales que use la red Móvil, debido a que este color está configurado para disminuir el consumo de tráfico sobre todo en temas de señalización, así mejorando el desempeño de estos canales que se contratan con límite de tráfico y está pensado para servicio de contingencia o por pedidos determinados.

### 10.2.4 Topología Sedes

En este punto teniendo claro el funcionamiento de la red actual y de los requisitos necesario podemos proponer un diseño de topología para cada una de las sedes que hemos identificado en el proceso

- **Datacenter Principal**

En el datacenter principal al igual que con la red implantada actualmente es necesario no tener puntos únicos de falla, por lo que la solución propuesta se propone una topología de doble equipo cada uno conectado a de manera independiente a dos canales de Internet nivel WAN, A nivel LAN cada equipo se conecta a distintos SW del datacenter para que caso de que se presente una falla en cualquier punto del diseño no se presente afectación en el servicio

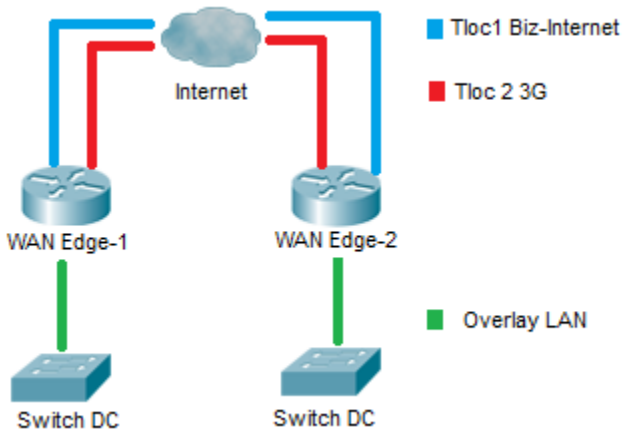


Figura 29 Esquemático Datacenter Principal SDWAN

- **Datacenter DRP**

En el datacenter DRP a nivel WAN se debe disponer un canal de internet que va a permitir conectar el equipos a los 2 colores definidos en la solución ya que este datacenter funciona solo en caso de falla catastrófica del principal no requiere de ningún tipo de protección adicional a nivel de equipos o de Canal como el diseño actualmente implementado.

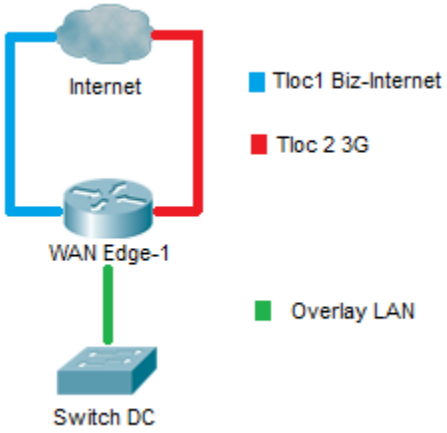


Figura 30 Esquemático Datacenter DRP SDWAN

- **Market Fijo**

En una sede de Market Fijo a nivel WAN se necesitaría 2 canales independientes uno de Internet banda ancha y otro de internet móvil con conexión 4G

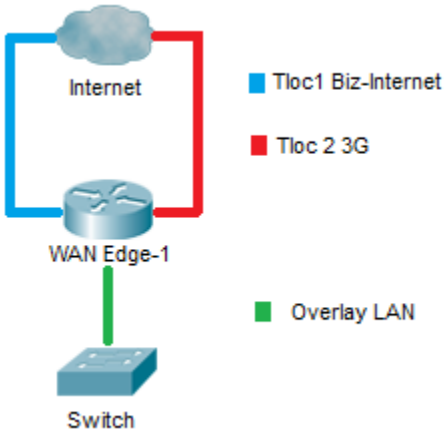


Figura 31 Esquemático Market Fijo

- **Market Móvil**

En una sede de Market Móvil a Nivel WAN se necesita 2 conexiones independiste de Internet Móvil 4G y al ser de fácil implementación para el cliente se busca que tenga la suficiente densidad de puerto para poder conectar directamente todos los equipos a Nivel LAN.

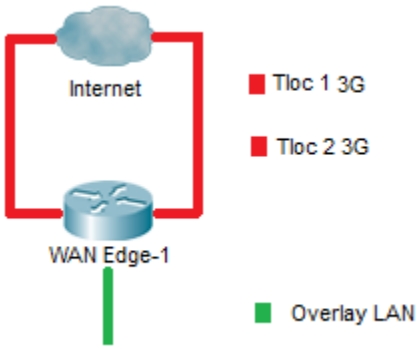


Figura 32 Esquemático Market móvil

### 10.2.5 Definición de equipos

De acuerdo al diseño propuesto y a la cantidad de markets que serán habilitados se define que para los sitios centrales serán equipos CISCO ASR 1001X-DNA:

| Sede | Ciudad | Servicio | BW Mbps | Tipo Conectividad SDWAN | Modelo (WAN-edge) |
|---|---|---|---|---|---|
| Datacenter | Bogotá | Internet | 250 | L3 Service LAN | ASR1001X-DNA |
| Datacenter | Bogotá | Internet | 250 | L3 Service LAN | ASR1001X-DNA |
| Datacenter | Medellín | Internet | 250 | L3 Service LAN (DRP) | ASR1001X-DNA |

Tabla 14 Equipos de Datacenter

Como se puede constatar en nuestro marco teórico para nuestra solución actual bien bastaría con implementar equipos ISR 4431, pero al implementar equipos 1001X se garantiza la implementación y crecimiento de la red en los próximos 5 años, evitando que se tenga que hacer cambios en los equipos concentradores siendo los más delicados de la red y cuya

modificación impactaría toda la operación del cliente; además de que permitirá que se pueda integrar el resto de las sedes al contar un performance que soporta una mayor carga de tráfico LAN del cliente. A nivel de costo estamos hablando de una diferencia de $2000 US que al sopesar resulta mucho más conveniente una inversión ahora y no un cambio en medio de una operación.

Para las sedes tipo market y de acuerdo a las características de nuestro diseño junto con el análisis de los modelos actuales en el mercado se define la implementación de routers Cisco C1117-4PLTELA - ISR 1100 4P DSL Annex A w/ LTE Adv SMS/GPS 802.11ac -Z WiFi. Ya que es el equipo que se ajusta a correctamente a las necesidades de conectividad de las sedes, no solo porque permite la implementación de UM Banda Ancha, Internet Fibra y LTE sino porque tiene incluido WIFI lo cual permitirá una conexión LAN mucho más rápida y no sujeta a implementaciones de cableados estructurados para casos en los que el tiempo o las características del market no lo permitan será una gran alternativa.

### 10.2.6 Asignación de recursos lógicos para las sedes tipo market

Dentro de los recursos lógicos que se asignaran en nuestro diseño a las sedes tipo market encontramos SITE ID, System IP, Direccionamiento LAN y QoS.

Teniendo en cuenta las recomendaciones de CISCO SYSTEMS® para la construcción de los **SITE ID** de las sedes, asignaremos un numero de 9 dígitos que estará compuesto así:

| SITE ID | | | |
|---|---|---|---|
| Country | Type | Zone | Store |
| **00** | **000** | **0** | **000** |

Tabla 15 Codificación Site ID

Dónde:

- Country: País Colombia = **57**
- Type: Tipo de sede Market Fijo = **011**
  Market Móvil = **021**

- Zona: Corresponderá al código de área asignados por departamentos:

| Departamento | Area Code / Indicativo | Departamento | Area Code / Indicativo |
|---|---|---|---|
| AMAZONAS | **8** | GUAVIARE | **8** |
| ANTIOQUIA | **4** | HUILA | **8** |
| ARAUCA | **7** | MAGDALENA | **5** |
| ATLANTICO | **5** | META | **8** |
| BOLIVAR | **5** | NARIÑO | **2** |
| BOYACA | **8** | N SANTANDER | **7** |
| CALDAS | **6** | PUTUMAYO | **8** |
| CAQUETA | **8** | QUINDIO | **6** |
| CASANARE | **8** | RISARALDA | **6** |
| CAUCA | **2** | SAN ANDRES Y PROVIDENCIA | **8** |
| CESAR | **5** | SANTANDER | **7** |
| CHOCO | **4** | SUCRE | **5** |
| CORDOBA | **4** | TOLIMA | **8** |
| CUNDINAMARCA | **1** | VALLE | **2** |
| GUAINIA | **8** | VAUPES | **8** |
| GUAJIRA | **5** | VICHADA | **8** |

Tabla 16 Códigos de Área de Colombia

- Store: Tienda = Corresponde a la asignación que tiene el cliente para cada uno de los markets en este caso se definirá desde la **001 hasta la 045**

El SYSTEM IP es la IP de identificación de cada router la cual comenzará con 10.10 y seguirá asociada con el rango LAN que le corresponderá a cada sede.

La siguiente tabla muestra la asignación de SITE ID y SYSTEM IP para cada market:

| ZONA | | SIDE ID | | | | SYSTEM IP | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | MK Apartado | 57 | 021 | 4 | 001 | 10 | 10 | 200 | 1 |
| 2 | MK Barranquilla | 57 | 011 | 5 | 002 | 10 | 10 | 200 | 33 |
| 3 | MK Barranquilla | 57 | 011 | 5 | 003 | 10 | 10 | 200 | 65 |
| 4 | MK Bogotá | 57 | 011 | 1 | 004 | 10 | 10 | 200 | 97 |
| 5 | MK Bogotá | 57 | 011 | 1 | 005 | 10 | 10 | 200 | 129 |
| 6 | MK Bogotá | 57 | 011 | 1 | 006 | 10 | 10 | 200 | 161 |
| 7 | MK Bogotá | 57 | 011 | 1 | 007 | 10 | 10 | 200 | 193 |
| 8 | MK Bogotá | 57 | 011 | 1 | 008 | 10 | 10 | 200 | 225 |
| 9 | MK Bogotá | 57 | 011 | 1 | 009 | 10 | 10 | 201 | 1 |
| 10 | MK Bogotá | 57 | 011 | 1 | 010 | 10 | 10 | 201 | 33 |
| 11 | MK Bogotá | 57 | 011 | 1 | 011 | 10 | 10 | 201 | 65 |
| 12 | MK Bogotá | 57 | 011 | 1 | 012 | 10 | 10 | 201 | 97 |
| 13 | MK Bogotá | 57 | 011 | 1 | 013 | 10 | 10 | 201 | 129 |
| 14 | MK Bogotá | 57 | 011 | 1 | 014 | 10 | 10 | 201 | 161 |
| 15 | MK Bogotá | 57 | 021 | 1 | 015 | 10 | 10 | 201 | 193 |
| 16 | MK Bogotá | 57 | 021 | 1 | 016 | 10 | 10 | 201 | 225 |
| 17 | MK Bogotá | 57 | 021 | 1 | 017 | 10 | 10 | 202 | 1 |
| 18 | MK Bogotá | 57 | 021 | 1 | 018 | 10 | 10 | 202 | 33 |
| 19 | MK Bogotá | 57 | 021 | 1 | 019 | 10 | 10 | 202 | 65 |
| 20 | MK Bogotá | 57 | 021 | 1 | 020 | 10 | 10 | 202 | 97 |
| 21 | MK Bogotá | 57 | 021 | 1 | 021 | 10 | 10 | 202 | 129 |
| 22 | MK Bucaramanga | 57 | 011 | 7 | 022 | 10 | 10 | 202 | 161 |
| 23 | MK Bucaramanga | 57 | 021 | 7 | 023 | 10 | 10 | 202 | 193 |
| 24 | MK Cali | 57 | 011 | 2 | 024 | 10 | 10 | 202 | 225 |
| 25 | MK Cali | 57 | 011 | 2 | 025 | 10 | 10 | 203 | 1 |
| 26 | MK Cali | 57 | 011 | 2 | 026 | 10 | 10 | 203 | 33 |
| 27 | MK Cali | 57 | 011 | 2 | 027 | 10 | 10 | 203 | 65 |
| 28 | MK Cali | 57 | 011 | 2 | 028 | 10 | 10 | 203 | 97 |
| 29 | MK Cali | 57 | 011 | 2 | 029 | 10 | 10 | 203 | 129 |
| 30 | MK Cali | 57 | 021 | 2 | 030 | 10 | 10 | 203 | 161 |
| 31 | MK Cali | 57 | 021 | 2 | 031 | 10 | 10 | 203 | 193 |
| 32 | MK Cali | 57 | 021 | 2 | 032 | 10 | 10 | 203 | 225 |
| 33 | MK Envigado | 57 | 021 | 4 | 033 | 10 | 10 | 204 | 1 |
| 34 | MK Ibagué | 57 | 021 | 8 | 034 | 10 | 10 | 204 | 33 |
| 35 | MK Manizales | 57 | 011 | 6 | 035 | 10 | 10 | 204 | 65 |
| 36 | MK Manizales | 57 | 021 | 6 | 036 | 10 | 10 | 204 | 97 |
| 37 | MK Medellín | 57 | 011 | 4 | 037 | 10 | 10 | 204 | 129 |
| 38 | MK Medellín | 57 | 011 | 4 | 038 | 10 | 10 | 204 | 161 |
| 39 | MK Medellín | 57 | 011 | 4 | 039 | 10 | 10 | 204 | 193 |
| 40 | MK Medellín | 57 | 021 | 4 | 040 | 10 | 10 | 204 | 225 |

| ZONA | | SIDE ID | | | | SYSTEM IP | | | |
|---|---|---|---|---|---|---|---|---|---|
| 41 | MK Medellín | 57 | 021 | 4 | 041 | 10 | 10 | 205 | 1 |
| 42 | MK Montería | 57 | 021 | 4 | 042 | 10 | 10 | 205 | 33 |
| 43 | MK Neiva | 57 | 021 | 8 | 043 | 10 | 10 | 205 | 65 |
| 44 | MK Palmira | 57 | 021 | 2 | 044 | 10 | 10 | 205 | 97 |
| 45 | MK Santa Marta | 57 | 021 | 5 | 045 | 10 | 10 | 205 | 129 |

Tabla 17 Definición de Site ID y System IP

Con respecto a la asignación de direccionamiento LAN utilizaremos la red **192.168.200.0** y cada sede tendrá una asignación /27 la cual permite conectar hasta 30 host o dispositivos en cada market así mismo se muestra la asignación de Hostname que tendrá cada equipo:

| ZONA | | HOSTNAME | | | RED | RANGO HOSTS |
|---|---|---|---|---|---|---|
| 1 | MK Apartado | MK | 4 | 001 | 192.168.200.0/27 | 192.168.200.1 -- 192.168.200.30 |
| 2 | MK Barranquilla | MK | 5 | 002 | 192.168.200.32/27 | 192.168.200.33 -- 192.168.200.62 |
| 3 | MK Barranquilla | MK | 5 | 003 | 192.168.200.64/27 | 192.168.200.65 -- 192.168.200.94 |
| 4 | MK Bogotá | MK | 1 | 004 | 192.168.200.96/27 | 192.168.200.97 -- 192.168.200.126 |
| 5 | MK Bogotá | MK | 1 | 005 | 192.168.200.128/27 | 192.168.200.129 -- 192.168.200.158 |
| 6 | MK Bogotá | MK | 1 | 006 | 192.168.200.160/27 | 192.168.200.161 -- 192.168.200.190 |
| 7 | MK Bogotá | MK | 1 | 007 | 192.168.200.192/27 | 192.168.200.193 -- 192.168.200.222 |
| 8 | MK Bogotá | MK | 1 | 008 | 192.168.200.224/27 | 192.168.200.225 -- 192.168.200.254 |
| 9 | MK Bogotá | MK | 1 | 009 | 192.168.201.0/27 | 192.168.201.1 -- 192.168.201.30 |
| 10 | MK Bogotá | MK | 1 | 010 | 192.168.201.32/27 | 192.168.201.33 -- 192.168.201.62 |
| 11 | MK Bogotá | MK | 1 | 011 | 192.168.201.64/27 | 192.168.201.65 -- 192.168.201.94 |
| 12 | MK Bogotá | MK | 1 | 012 | 192.168.201.96/27 | 192.168.201.97 -- 192.168.201.126 |
| 13 | MK Bogotá | MK | 1 | 013 | 192.168.201.128/27 | 192.168.201.129 -- 192.168.201.158 |
| 14 | MK Bogotá | MK | 1 | 014 | 192.168.201.160/27 | 192.168.201.161 -- 192.168.201.190 |
| 15 | MK Bogotá | MK | 1 | 015 | 192.168.201.192/27 | 192.168.201.193 -- 192.168.201.222 |
| 16 | MK Bogotá | MK | 1 | 016 | 192.168.201.224/27 | 192.168.201.225 -- 192.168.201.254 |
| 17 | MK Bogotá | MK | 1 | 017 | 192.168.202.0/27 | 192.168.202.1 -- 192.168.202.30 |
| 18 | MK Bogotá | MK | 1 | 018 | 192.168.202.32/27 | 192.168.202.33 -- 192.168.202.62 |
| 19 | MK Bogotá | MK | 1 | 019 | 192.168.202.64/27 | 192.168.202.65 -- 192.168.202.94 |
| 20 | MK Bogotá | MK | 1 | 020 | 192.168.202.96/27 | 192.168.202.97 -- 192.168.202.126 |
| 21 | MK Bogotá | MK | 1 | 021 | 192.168.202.128/27 | 192.168.202.129 -- 192.168.202.158 |
| 22 | MK Bucaramanga | MK | 7 | 022 | 192.168.202.160/27 | 192.168.202.161 -- 192.168.202.190 |
| 23 | MK Bucaramanga | MK | 7 | 023 | 192.168.202.192/27 | 192.168.202.193 -- 192.168.202.222 |
| 24 | MK Cali | MK | 2 | 024 | 192.168.202.224/27 | 192.168.202.225 -- 192.168.202.254 |
| 25 | MK Cali | MK | 2 | 025 | 192.168.203.0/27 | 192.168.203.1 -- 192.168.203.30 |
| 26 | MK Cali | MK | 2 | 026 | 192.168.203.32/27 | 192.168.203.33 -- 192.168.203.62 |
| 27 | MK Cali | MK | 2 | 027 | 192.168.203.64/27 | 192.168.203.65 -- 192.168.203.94 |
| 28 | MK Cali | MK | 2 | 028 | 192.168.203.96/27 | 192.168.203.97 -- 192.168.203.126 |
| 29 | MK Cali | MK | 2 | 029 | 192.168.203.128/27 | 192.168.203.129 -- 192.168.203.158 |

| ZONA | | HOSTNAME | | | RED | RANGO HOSTS |
|---|---|---|---|---|---|---|
| 30 | MK Cali | MK | 2 | 030 | 192.168.203.160/27 | 192.168.203.161 -- 192.168.203.190 |
| 31 | MK Cali | MK | 2 | 031 | 192.168.203.192/27 | 192.168.203.193 -- 192.168.203.222 |
| 32 | MK Cali | MK | 2 | 032 | 192.168.203.224/27 | 192.168.203.225 -- 192.168.203.254 |
| 33 | MK Envigado | MK | 4 | 033 | 192.168.204.0/27 | 192.168.204.1 -- 192.168.204.30 |
| 34 | MK Ibagué | MK | 8 | 034 | 192.168.204.32/27 | 192.168.204.33 -- 192.168.204.62 |
| 35 | MK Manizales | MK | 6 | 035 | 192.168.204.64/27 | 192.168.204.65 -- 192.168.204.94 |
| 36 | MK Manizales | MK | 6 | 036 | 192.168.204.96/27 | 192.168.204.97 -- 192.168.204.126 |
| 37 | MK Medellín | MK | 4 | 037 | 192.168.204.128/27 | 192.168.204.129 -- 192.168.204.158 |
| 38 | MK Medellín | MK | 4 | 038 | 192.168.204.160/27 | 192.168.204.161 -- 192.168.204.190 |
| 39 | MK Medellín | MK | 4 | 039 | 192.168.204.192/27 | 192.168.204.193 -- 192.168.204.222 |
| 40 | MK Medellín | MK | 4 | 040 | 192.168.204.224/27 | 192.168.204.225 -- 192.168.204.254 |
| 41 | MK Medellín | MK | 4 | 041 | 192.168.205.0/27 | 192.168.205.1 -- 192.168.205.30 |
| 42 | MK Montería | MK | 4 | 042 | 192.168.205.32/27 | 192.168.205.33 -- 192.168.205.62 |
| 43 | MK Neiva | MK | 8 | 043 | 192.168.205.64/27 | 192.168.205.65 -- 192.168.205.94 |
| 44 | MK Palmira | MK | 2 | 044 | 192.168.205.96/27 | 192.168.205.97 -- 192.168.205.126 |
| 45 | MK Santa Marta | MK | 5 | 045 | 192.168.205.128/27 | 192.168.205.129 -- 192.168.205.158 |

Tabla 18 Definición de Direccionamiento y Nombre de Host

Teniendo en cuenta las mediciones realizadas sobre el tráfico de las sedes Markets la aplicación de QoS cobra una relevancia ya que por el enlace se transmitirá voz y video lo cual en un momento determinado podrían entorpecer el transporte de datos transaccionales que sin duda son importantes en la operación del cliente, por lo tanto, se define la siguiente asignación de QoS:

| QoS | | |
|---|---|---|
| Tipo de trafico | Behavior | Porcentaje |
| Datos Critico | af31 - Flash | 25% |
| Datos Prioritario | af21 - Immediate | 25% |
| Video | af41 - Flash override | 15% |
| Voz | ef - Best effort | 10% |

Tabla 19 Asignación de QoS

## 11. Resultados

Una vez realizada las investigaciones documentales sobre lo que son las redes SDWAN aplicadas en entornos CISCO SYSTEMS®, el análisis de la información y de los datos de la red actual del cliente y el correspondiente diseño de conectividad general para las sedes tipo market procederemos a realizar la correspondiente simulación del tráfico de una sede piloto, así como la definición del protocolo de aceptación de cliente ATP para las sedes.

### 11.1 Simulación

Para la simulación se usó el Software Riverbed Modeler que permite, modelar una red desde sus componentes individuales, como los son el tráfico generado por las aplicaciones, los elementos de red y las internaciones de todo  por medio de los protocolos, SDWAN es ante todo es un cambio de la visión de cómo son la redes actualmente usando herramientas tecnologías disponibles más que desarrollo puramente técnico.

#### 11.1.1 Definición de Perfiles y aplicaciones

Para la simulación se define inicialmente, las aplicaciones y los perfiles a usar en la simulación ya que son los encargados de dar forma al tráfico que va  a cursar en toda la red.

| Perfiles | Aplicaciones |
|---|---|
| Cámara | Flujo de Trafico UDP de 2 Mb/s |
| PC | • Email<br>• Navegacion HTTP<br>• Base de Datos<br>• FTP |
| Datafono | Base de datos |
| Teléfono | Voz |

Tabla 2. Asignación de Aplicaciones frente a Perfiles

#### 11.1.2 Construcción de las sedes

Luego de tener definido los perfiles se debe crear las sedes las cuales conforma la red SDWAN , según el diseño realizado en el capítulo anterior, por lo que se debe modelar el datacenter Principal el datacenter DRP y la Sede piloto.

- **Modelo datacenter principal**

El datacenter Principal en el modelo Consta de dos router los cuales van a Simular ser los cEdge, se colocan 2 switch LAN que nos permite replicar el esquema de alta disponibilidad que el cliente tiene en el datacenter y conectar en este punto los equipos cEdge y por ultimo también se conecta el Firewall de seguridad que el cliente tiene para el análisis y protección de su red como se muestra en la siguiente figura

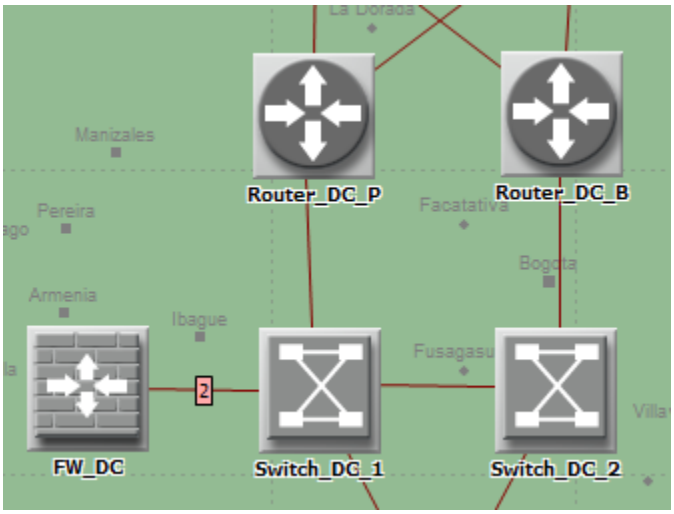


Figura 33 Diseño datacenter Principal

- **Modelo Datacenter DRP**

El datacenter DRP cuenta con los mismos elementos que el datacenter principal pero al estar en estado de espera este datacenter no tienes un esquema de alta disponibilidad y solo va a contar con un cEdge, un switch y un firewall conectados de manera sencilla según como se observa en la siguiente figura

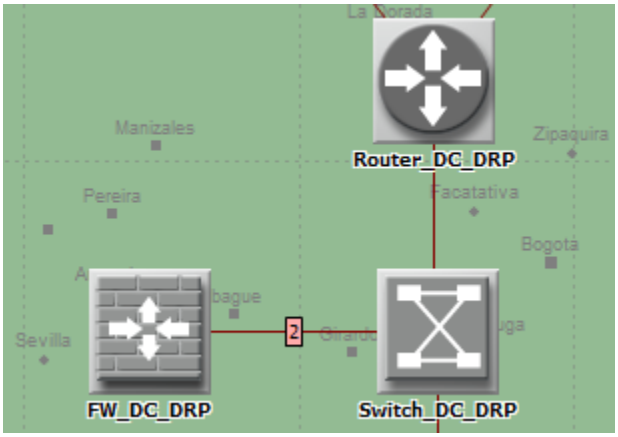


Figura 34 Diseño datacenter DRP

- **Modelo Market**

Para el market según el diseño relacionado se realizó con un solo equipo cEdge y el Switch que el cliente tiene en esta sede y donde conecta los dispositivos como se observa en la siguiente figura

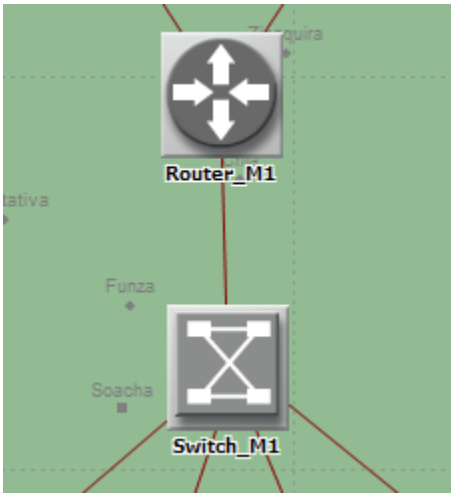


Figura 35 Diseño Market

### 11.1.3 Modelo equipos de trabajo

Según la definición de la topología de las sedes se tienen 4 estaciones de trabajo en el cliente a los cuales se les asigna su respecticos perfiles de usuario según la definición realzada al comienzo y son conectados como se observa en al siguiente figura

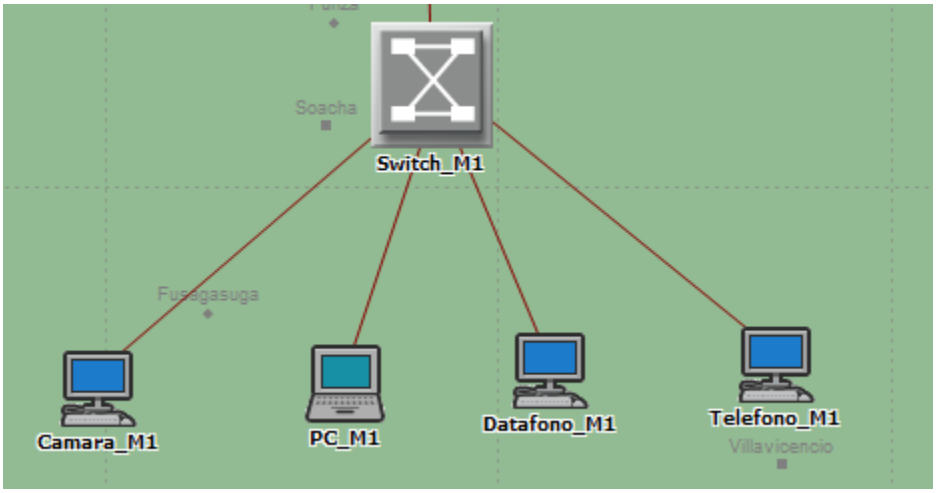


Figura 36 Diseño estaciones de trabajo market

### 11.1.4 Modelo área de Servidores

Se asigna Servidores según aplicativos 4 servidores en datacenter y un servidor para los servicios en la nube que va a ir directamente a internet gracias a la funcione internet breackdown que tiene SDWAN como se observa en las siguientes figuras

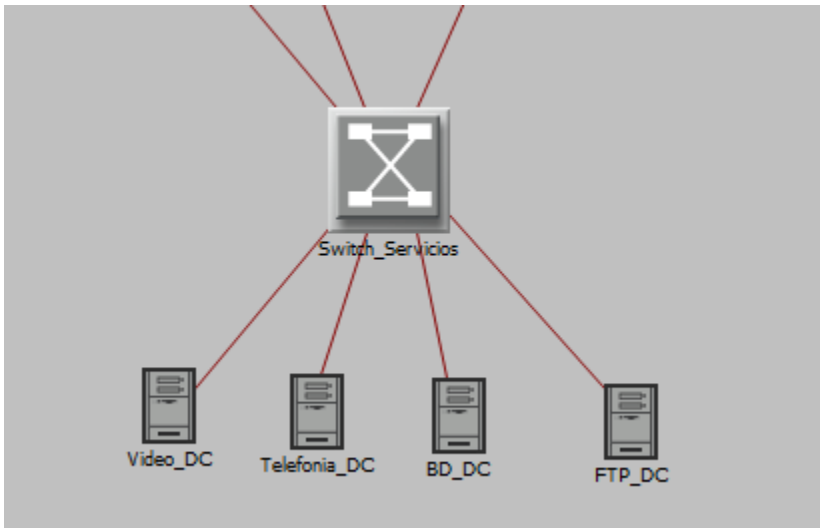


Figura 37 Diseño Servidores Datacenter

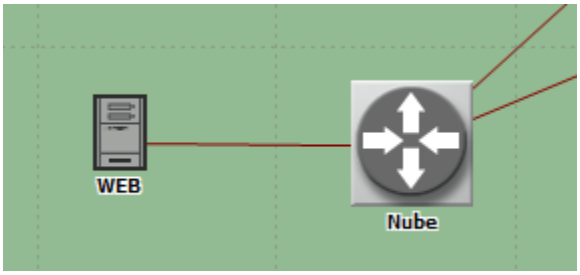


Figura 38 Diseño Servidores en la Nube

### 11.1.5 Modelo Conexión Colores

Una de las características más relevantes de las solución de SDWAN de Cisco es que las conexiones WAN son separada lógicamente en Colores y son enrutadas a través de un protocolo propietario conocido como OMP, para modelar esto se crearon dos redes apartes una para el color Internet-Biz y otra para el color 3g a la cual se concretaron de manera ordenada según los diseños los router que simulan ser los cEdge.

Se habilito el protocolo OSPF  entre los equipos para simular la función del protocolo OMP como se observa en la siguiente grafica

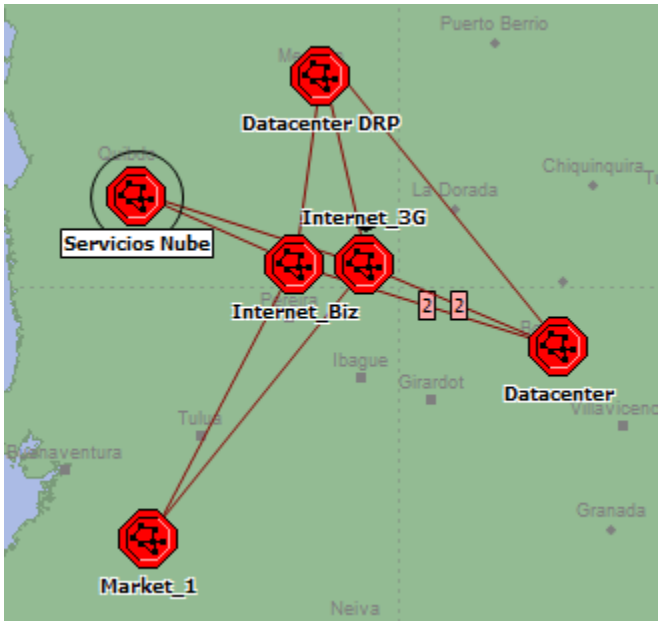


Figura 39 Diseño Conectividad WAN

### 11.1.6 Configuración de Enrutamiento WAN

Para simular el correcto funcionamiento de la red se ajustaron los costos de canales para que simulara el comportamiento de la red SDWAN Cisco

| cEdge | Color | Costo |
|---|---|---|
| Datacenter P | Internet-BIZ | 10 |
| | 3G | 40 |
| Datacenter B | Internet-BIZ | 20 |
| | 3G | 50 |
| Datacenter DRP | Internet-BIZ | 30 |
| | 3G | 60 |
| Market | Internet-BIZ | 10 |
| | 3G | 20 |

Tabla 21 Asignación de Costos de enlace

Por último se conectó el servidor de Servicios en la Nube a través de un router que para interconectar las 2 redes WAN separadas pero que cada uno tenga acceso a estos servicios.

### 11.1.7 Configuración de Enrutamiento LAN

A nivel LAN como recomienda Cisco para interconectar otras redes a la Red e SDWAN se configura también OSPF y Se interconectan los dos datacenter al área de servidores.

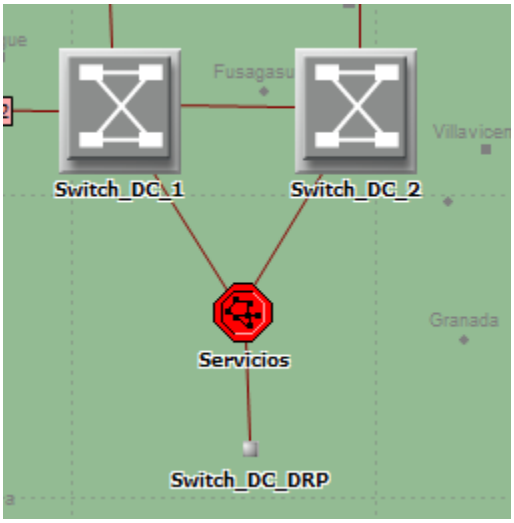


Figura 40 Diseño Conexión de datacenter a área de servidores

### 11.1.8 Configuración de Políticas

Como política especial para simular las condiciones de funcionamiento del diseño SDWAN se bloqueó el tráfico de video atreves del color 3g en la sede del market ya que el color 3g está pensado solo para ser usado de backup en caso de falla del canal principal al tráfico de Prioridad Alta y Media del cliente.

### 11.1.9 Resultados de la simulación

Para corrobora la simulación, se corrió durante 1 hora y se compararon las grafica de tráfico obtenidas del con graficas que se realizaron con base a la información de la red actual y que se encurta en los anexos, dando como resultado un comportamiento muy similar entre sí.

Las gráficas a continuación corresponde al tráfico de entrada, la primera proviene de la simulación la segunda de la información tomada de la red actual

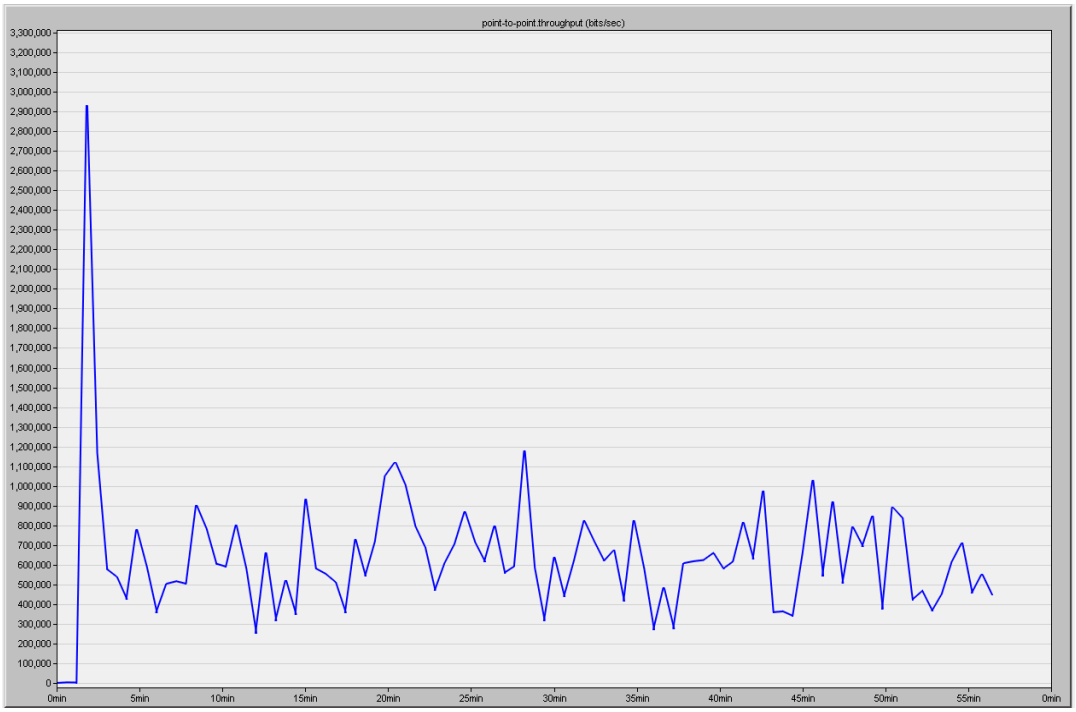


Figura 41 Grafica tráfico de entrada Simulación

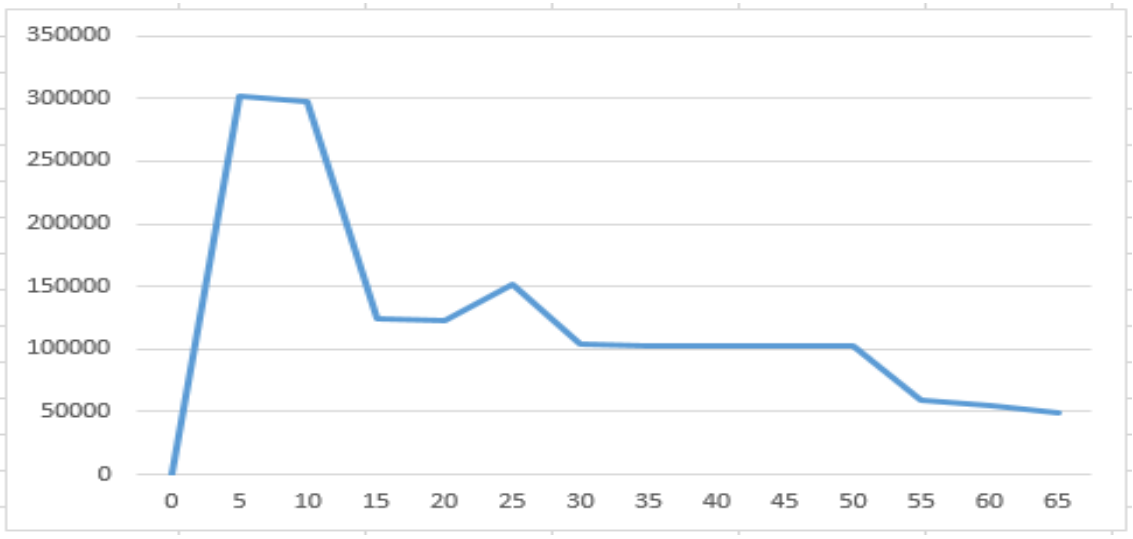


Figura 42 Grafica tráfico de entrada Real

Las gráficas a continuación corresponden al tráfico de salida, la primera proviene de la simulación la segunda de la información tomada de la red actual

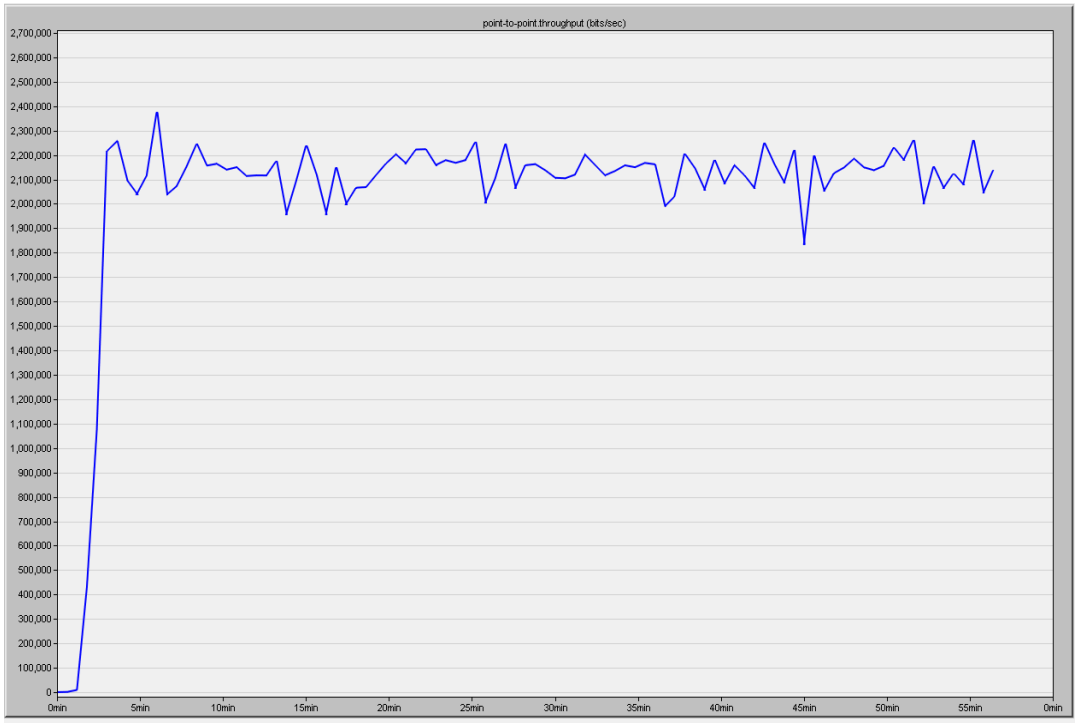


Figura 43 Grafica tráfico de salida Simulación

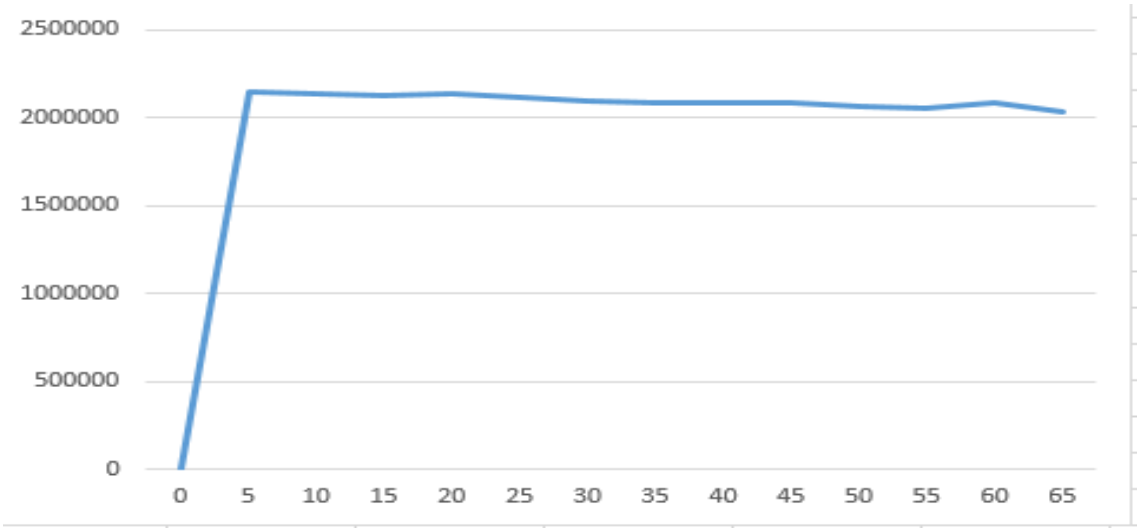


Figura 44 Grafica tráfico de salida Real

### 11.2 ATP

Las pruebas de aceptación de cliente son un documento muy importante dentro de la fase de implementación o migración de la red así como la transición de la misma hacia el área de operaciones, si bien en este proyecto no se tiene como alcance la entrega de la red a un área de operaciones que pueda tener el cliente o un ISP particular se ha diseñado un documento en el cual se consolidarán los registros fundamentales de la implementación así como de las pruebas de conectividad y de UM correspondiente en cada sede y dicho documento será una base fundamental para que tanto nuestro cliente y los ISP tenga conocimiento real de lo implementado y de las condiciones de funcionamiento que se presentaron en los primeros momentos de nuestra red.

Hemos construido 2 documentos que se adjuntaran como anexos a este documento para consulta uno para los sitos centrales y otro para las sedes tipo market

#### 11.2.1 ATP para sedes centrales

En el documento anexo llamado *ATP_Proyecto EPI-100 Sitio Central* se encontrarán los diseños específicos implementados, así como los equipos instalados (seriales y nemónicos para identificación) y su conectividad bajo un ámbito SDWAN: sincronización de túneles con el vManage, sesiones BFD bajo la última milla definida como Biz-internet y la definida como #G y las conexiones con los demás controladores (vSmart y vBond).

Complementando la información se modela un esquema de pruebas de redundancia en el cual se verificará que cada concentrador está en capacidad de ser el respaldo del otro y permitir la conectividad overlay siempre, así el cliente tendrá la certeza que en caso de algún fallo su conectividad estará protegida.

En última instancia se registrarán las pruebas de desempeño de cada última milla mostrando el tráfico que curso por cada enlace, si se presentan perdidas en la conectividad, latencia, jitter y por último la configuración con la que queda cada equipo funcionado que servirá como repositorio y consulta en el momento futuro que se requiera.

### 11.2.2 ATP para sedes tipo market

En el documento anexo llamado *ATP_Proyecto EPI-100 Sedes tipo Market* al igual que el ATP para sitios centrales contara con los diseños específicos implementados, así como los equipos instalados (seriales y nemónicos para identificación) y su conectividad bajo un ámbito SDWAN: sincronización de túneles con el vManage, sesiones BFD bajo la última milla definida como Biz-internet y la definida como LTE y las conexiones con los demás controladores (vSmart y vBond).

En cuanto al esquema de pruebas de redundancia debemos tener presente que nuestra solución para estas sedes solo contempla 1 router con lo cual las pruebas de conmutación se basan en apagados en las interfaces TLOC del router evidenciando que tanto como la última milla principal y BK quedan soportando el tráfico sin inconvenientes.

Finalmente se registrarán las pruebas de desempeño de cada última milla mostrando el tráfico que curso por cada enlace, si se presentan perdidas en la conectividad, latencia, jitter y por último la configuración con la que queda cada equipo funcionado que servirá como repositorio y consulta en el momento futuro que se requiera.

## 12. Discusión

Las redes SDN llegaron para quedarse y son sin duda el futuro en lo que respecta a la conectividad de nuestros datos, como ingenieros conocer e implementar una nueva tecnología que apenas asoma en nuestro país fue un gran reto y sobre todo un cambio en la perspectiva frente al diseño y modelación de redes y protocolos de comunicaciones. SDWAN bajo el entorno CISCO SYSTEMS® simplifica en gran medida la concepción de la red desde su inicio y permite realizar una proyección real de crecimiento futuro de la red, ya que al realizar un modelamiento estándar y centralizado básicamente solo se debe tener en cuenta la capacidad de los equipos concentradores para levantar los túneles de comunicación con cada una de las sedes, el modelo hub and spoke facilita enormemente que los tiempos de convergencia se reduzcan notablemente ya que su adyacencia siempre será un concentrador o los respectivos respaldos de este, este concentrador siempre mantendrá a toda la red informada sobre las tablas de enrutamiento y los cambios que se puedan presentar en las mismas y esto mejora notablemente el performance de la red.

Por otra parte la administración centralizada de los equipos permite que el diseño y la administración de la red sea muchísimo más controlado y coherente, en redes, la documentación es lo más importante pero sin duda es un punto de falla muy recurrente; al implementar SDWAN el vManage, se convierte en nuestro repositorio constante con información en tiempo real de lo que ocurre sobre nuestra red, así como la administración de los cambios que se quieran realizar los cuales pueden ser generalizados a todos los dispositivos remotos o relativos al que corresponda. Este control y visión de la red concentrado en un solo lugar sin duda facilita cualquier monitoreo u operación en la red, pero sobre todo permite que se tenga control sobre los eventos, sus posibles causas y soluciones, ya que permite hacer un troubleshooting de calidad y en un menor tiempo.

La solución SDWAN de CISCO viene tomado una madures muy importante luego de la adquisición de la empresa Viptela superando el intento pasado con IWAN – Meraki , dando como resultado la actual solución de SDWAN que nos presenta un gamas de equipos modernos y que soporta la solución tradicional o la Solución SDWAN solo cambiando el IOS que ejecutan, en cuanto a costos las solución SDWAN de Cisco presenta dos facetas claras a tener en cuenta, uno es el costo de los equipos , El cliente actualmente tenia router de la Cisco 881-k9 con un

costo en el mercado de 400 dólares y que actualmente está descontinuados por parte de Cisco, para las solución SDWAN se piensa integrar router Cisco C1117-4P que cuestan 3 veces más, 1200 Dólares, pero son equipos que estaría con soporte de Cisco y con la posibilidad RMA y contado que se estos equipos viene preparados para tener conectividad WifI y puertos PoE permitiendo muchas más facilidades que el equipo anterior no. Por otro lado al usar canales banda Ancha, los costos mensuales de cargo fijo por conectividad baja en un 70% esto quiere decir que en un plazo de un 1 año con este ahorro se podría cubrir los gasto del equipo nuevo permitiendo un ahorro significativo en la organización en su cargos fijos mensuales, además que al tener la flexibilidad que ofrece SDWAN, lo pone en una mejor poción par apodar negociar con los ISP ya que la Red de la compañía sería realmente del Cliente dejando tomar siempre las decisiones más ventajosa a nivel económico en un futuro

Por otro lado una simulación para poder comprobar un diseño siempre es un paso importante en todo proyecto, CISCO presenta ambiente de laboratorio en la Nube, peros son solo instancias prefabricadas que tienen más fines didácticos y demostrativos que ser un simulador de SDWAN CISCO, además estos ambientes tiene una duración finita contada en días, lo cual hace imposible guardar algún resultado, por lo que se optó por usar Riverbed Modeler una solución libre en su licencia Académica , la cual funciona modelando el funcionamiento de elementos de red como Router, Switches, junto con los canales que los interconecta y los protocolos con los que interactúan por lo que es un ambiente perfecto para poder llevar un modelo SDWAN a un ambiente de simulación virtual usando todos los conceptos de las redes traiciónales llevas a un enfoque SDWAN

## 13. Conclusiones

- Se logró elaborar y plantear el objetivo propuesto de generar un diseño de red para la integración de sedes tipo market de una empresa de producción y comercialización de alimentos basado en conectividad SDWAN, basado en todo el planteamiento teórico sobre esta tecnología en entornos CISCO SYSTEMS® y con la aplicabilidad necesaria para que exista una migración entre la red legacy actual del cliente a esta nueva tecnología planteada.

- La recolección de datos de la red legacy con la que cuenta actualmente nuestro cliente y con el respectivo análisis de dicha información se pudo concluir que para las sedes tipo market el consumo de tráfico está altamente representado por él envió de los videos de video vigilancia hacia los equipos centrales, así mismo el tráfico descarga está relacionado con actualizaciones de los sistemas operativos y datos transaccionales que son meramente ocasionales y no constantes en los canales.

- El diseño de red propuesto más allá de plantear un modelo de comunicaciones para la empresa presenta una propuesta sólida y viable para la implementación de enlaces de BK en cada uno de los market supliendo una falencia del diseño que tiene implementado actualmente, reduciendo el riesgo de que por una falla se afecte el modelo de negocio de la compañía que es básicamente vender sus productos alimenticios.

- El Modelo SDWAN con respecto a una red Legacy sin duda simplifica la labor de un diseñador u administrador de la red ya que al tener un control centralizado y en tiempo real, permitirá una gestión y optimización del performance, así como un troubleshooting más acertado.

- Modelar el funcionamiento de una red SDWAN en un simulador de redes demuestra que las redes SDWAN no está cambiando a nivel de las capas más básica del Modelo OSE sino están cambiando en el cómo se está definiendo por las persona que las diseñan y administran.

- El tener ambiente de prueba en donde se puede poner a punto un diseño y podamos probar los requerimientos de los diseños, hace que la tarea de planeación tome realmente la importancia que tiene y se pueda evaluar mejor punto de funcionamiento donde se tenga incertidumbre como picos de tráficos y saturación.

- SDWAN buscar romper el paradigma que actualmente hay entre el ISP y servicio que presta, ya que una red es diseñada para el uso del cliente sobre equipos del proveedor, y esto genera que la red nos sea del cliente sino realmente del proveedor, por lo que la definirla por software abre la puerta a que la red se pueda ser separa en los planos de control, de trasporte y de servicio, unificando el control en la Nube, permitiendo diversificar la manera en que el trasporte funciona, para prestarle los servicio de conectividad al cliente, pudiendo realizar los cambios en el área que necesite sin necesidad de que las otra área se ven afectadas.

- El costo de las solucione SDWAN frente a las tradicionales, debido a que se necesita equipos nuevos, servicio en la nube, barreras de seguridad y en la actualidad está siendo mucho más costosas, pero los beneficios que genera poco a poco está superando esta barrera de manera directa, ahorrando dinero a futuro o haciendo que los valores agregado que se están prestado justifiquen las inversiones realizada.

## 14. Referencias documentales.


[1] Cisco (2019), ENSDW - Cisco SD-WAN Operation and Deployment - Student Guide 1.0.0

[2] D. Lopez, M. Boucadair, P. Iovanna (2019) Request for Comments: 8597. Cooperating Layered Architecture for Software-Defined Networking (CLAS)

[3] Santitoro Ralph. (2017) Understanding SD-WAN Managed Services, Service Components, MEF LSO Reference Architecture and Use Cases, Metro Ethernet Forum

[4] Denazis, S. Hadi Salim, J. Meyer, D. Koufopavlou, O. (2015) Request for Comments: 7426. Software-Defined Networking (SDN): Layers and Architecture Terminology.

[5] Bellido Quintero, Enrique (2014): Equipos de interconexión y servicios de red (UF1879). Madrid, ES: IC Editorial.

[6] M. Boucadair, C. Jacquenet. (2014). Request for Comments: 7149. Software-Defined Networking: A Perspective from within a Service Provider Environment, Internet Engineering Task Force (IETF)

[7] Boronat Seguí, Fernando and Montagud Climent, Mario (2013): Direccionamiento e interconexión de redes basada en TCP/IP: IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y OSPF: IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y OSPF. Editorial de la Universidad Politécnica de Valencia.

[8] Castaño Ribes, Rafael Jesús and López Fernández, Jesús (2013): Redes locales. España: Macmillan Iberia, S.A.

[9] Hallberg, Bruce (2010): Fundamentos de redes (4a. ed.). México: McGraw-Hill Interamericana.

[10] Reyes Roig, Deborah (2010): Guía de implementación de la seguridad en redes de Núcleo Mpls. Cuba: D - Instituto Superior Politécnico José Antonio Echeverría. CUJAE.

[11] Robledo Sosa, Cornelio (2010): Redes de computadoras. Instituto Politécnico Nacional.

[12] Hillar, Gastón Carlos (2009): Redes: diseño, actualización y reparación: diseño, actualización y reparación. Editorial Hispanoamericana HASA.

[13] Cisco (2008), Academia de Networking de Cisco Systems: Guía del primer año CCNA 1 y 2". 3º Edición. Cisco Press.

[14] Cisco (2008), Academia de Networking de Cisco Systems: Guía del segundo año CCNA 3 y 4". 3º Edición. Cisco Press.

[15] J. S. Beasley (2008) Networking. 2º Edición. Pearson Education

[16] B. Forouzan (2007) Transmisión de datos y redes de comunicaciones. 4º Edición. McGraw Hill

[17] Purser, Michael (2007): Redes de telecomunicación y ordenadores. España: Ediciones Díaz de Santos.

[18] Held Gilbert, Jagannathan S. Ravi. (2004). Practical Network Design Techniques: A Complete Guide For WANs and LANs, Auerbach Publications

[19] J. F. Kurose, K.W. Ross (2004) Redes de Computadores: Un Enfoque Descendente Basado en Internet. 2º Edición. Pearson Education.

[20] W. Stallings (2004) Comunicaciones y Redes de Computadores. 7º Edición. Pearson Education.

[21] A.S. Tanenbaum (2003) Redes de Computadoras. 4º Edición. Pearson Education.

[22] Castro Lechtaler, Antonio Ricardo (2000): Comunicaciones: una introducción a las redes digitales de transmisión de datos y señales isócronas: una introducción a las redes digitales de transmisión de datos y señales isócronas. Alfaomega Grupo Editor.

[23] Íñigo Griera, Jordi and Barceló Ordinas, José María and Cerdà Alabern, Llorenç (2000): Estructura de redes de computadores. Editorial UOC.

[24] Katz, Matías David (2000): Redes y seguridad. Alfaomega Grupo Editor.

[25] Moreno Pérez, Juan Carlos and Santos González, Manuel (2000): Sistemas informáticos y redes locales. RA-MA Editorial

[26] Santos González, Manuel (2000): Diseño de redes telemáticas. RA-MA Editorial.

[27] Martin W. Murhammer, Kok-Keong Lee, Payam Motallebi, Paolo Borghi, Karl Wozabal. (1999). IP Network Design Guide; IBM Corporation, International Technical Support Organization

[28] Mccabe James D. (1999). Network Analysis, Architecture, and Design; Morgan Kaufmann

[29] Oppenheimer Priscilla. (1999). Top-Down Network Design; Cisco Press

[30] Wang, Henry Haojin. (1999). Telecommunications network management; McGraw-Hill

# 15. Anexos