

Redes definidas por software para mejorar la disponibilidad en RedUNAM

Información del reporte:

Licencia Creative Commons



El contenido de los textos es responsabilidad de los autores y no refleja forzosamente el punto de vista de los dictaminadores, o de los miembros del Comité Editorial, o la postura del editor y la editorial de la publicación.

Para citar este reporte técnico:

Rivera Martínez, H. (2024). Redes definidas por software para mejorar la disponibilidad en RedUNAM. *Cuadernos Técnicos Universitarios de la DGTIC*, 2 (1), páginas (37 - 54).

<https://doi.org/10.22201/dgtic.ctud.2024.2.1.32>

Hugo Rivera Martínez

Dirección General de Cómputo y de
Tecnologías de Información y Comunicación
Universidad Nacional Autónoma de México

hugo.rivera@unam.mx

ORCID: 0009-0007-1248-9412

Resumen:

La innovación se presenta como la adopción de nuevas tecnologías o soluciones a problemas existentes en la RedUNAM, uno de ellos es mejorar la disponibilidad de los servicios de acceso a Internet y recursos de la UNAM por parte de las entidades remotas ubicadas fuera de Ciudad Universitaria. y que son parte de la Universidad. Como parte del proceso de adopción de tecnologías se realizan pruebas de las mismas; en este documento se describen los escenarios de prueba y los resultados obtenidos de la tecnología SD WAN dentro de infraestructuras de red de RedUNAM.

Palabras clave:

Redes definidas por software (SDN), redes avanzadas, virtualización de red, gestión de servicios de TIC

1. INTRODUCCIÓN

La disponibilidad es una de las características de cualquier servicio, que impulsa el ser confiable para los usuarios, por lo que es importante incrementar, dentro de costos razonables, esta disponibilidad, ya que cada vez son más importantes los servicios, aplicaciones, sistemas e información que la comunidad universitaria utiliza en su día a día, desde un punto de vista académico, de investigación, administrativo e inclusive financiero. Los servicios de TIC tienen un alto impacto en la vida universitaria y por ello se proponen soluciones tecnológicas que promuevan la mejora de esta disponibilidad, proporcionando mayor confianza al usuario.

Una propuesta para dar solución a esta y otras necesidades de gestión y operación es el paradigma de Redes Definidas por Software (SDN, Software Defined Networks), ya que proporciona mejoras en la gestión centralizada de los elementos activos de una red (ruteadores, switches), al separar el plano de control del de operación, visibilidad del tráfico y aplicaciones que circulan por la misma, etiquetar las diferentes aplicaciones para que sean tratadas de diferente manera (calidad de servicio), así como funciones de automatización y adaptación a cambios en el estado de los enlaces (saturación, retardo y pérdida de paquetes) agregando funciones de seguridad que ayudan a salvaguardar los servicios, información y aplicaciones que se utilizan.

Dentro de las funcionalidades que proporciona la solución SDN y que nos ayudan a mejorar la disponibilidad, es construir túneles seguros a través de los enlaces con que cuente la entidad remota, independientemente del proveedor, lo que da la oportunidad de utilizar los enlaces de Internet público con que contamos, para llevar a cabo comunicaciones seguras a través de Internet, lo cual anteriormente solo se lograba con enlaces dedicados.

El despliegue de esta tecnología es diversa, y actualmente el mercado no cuenta con protocolos estándares que apoyen a la integración de diversos fabricantes en la implementación dentro de una red, además, no permiten que el despliegue y operación sea homogéneo haciendo uso de equipamiento de diferentes fabricantes, por lo que para su implementación se recomienda la evaluación de las necesidades a cubrir y la forma en que cada fabricante pueda aportar a la solución de estas necesidades, y así seleccionar a quien pueda dar una mejor solución en relación costo - beneficio.

Con base en las prácticas que la gestión de servicios de ITIL (Information Technology Infrastructure Library) recomienda para la generación de servicios que aporten valor a las organizaciones, se realizaron pruebas con el fin de mejorar la disponibilidad del servicio de Internet para la comunidad universitaria ubicada en las entidades foráneas al Campus Ciudad Universitaria y que son parte de la RedUNAM.

2. OBJETIVO

El presente documento busca mostrar la aplicación de la tecnología SDN (SD WAN) para mejorar la disponibilidad del acceso a Internet y a los recursos digitales que se encuentran tanto en Ciudad Universitaria como en Internet, por parte de las diferentes entidades que integran la RedUNAM a nivel nacional y metropolitano.

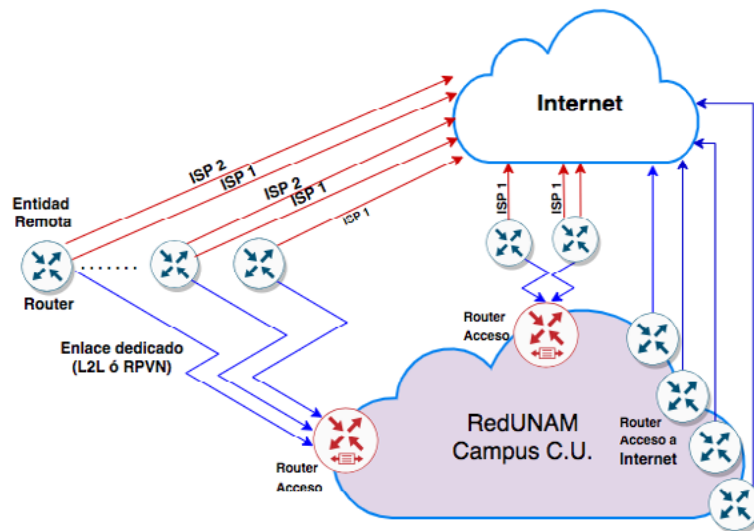
3. DESARROLLO

INFRAESTRUCTURA ACTUAL DE REDUNAM

La arquitectura actual es de estrella en donde Ciudad Universitaria es el punto Central, ya que cuenta con sistemas y aplicaciones que son utilizadas por toda la Universidad. Las diferentes entidades se conectan a través de enlaces dedicados, los cuales son simétricos en el ancho de banda contratado, incluyendo el ruteador que hace la segmentación física (diferentes puertos) y lógica (direccionamiento IPv4 e IPv6), utilizando diferentes protocolos de enrutamiento (OSPF¹ y BGP²) para el intercambio de redes dentro de RedUNAM y hacia los diferentes proveedores de servicio de Internet (ISP, Internet Service Provider) para su propagación a Internet.

Figura 1

Diagrama Topológico de la RedUNAM y sus conexiones WAN hacia entidades remotas e Internet



Se cuenta con 241 enlaces (dedicados, RPVN, Red Privada Virtual Nacional e Internet) que interconectan a 135 entidades a nivel nacional y metropolitano, así como al Campus de Ciudad Universitaria; de éstos, 104 son enlaces dedicados hacia Ciudad Universitaria y 123 hacia Internet, los restantes 14 son de RPVN topológicamente formando una estrella distribuida teniendo como objetivo que las entidades universitarias cuenten con un enlace hacia Ciudad Universitaria y con ello utilizar aplicaciones y acceso a recursos digitales que se encuentran en servidores dentro del campus principal.

1 OSPF, Open Shortest Path First, protocolo de enrutamiento de compuerta interna utilizado para intercambiar segmentos de red (IPv4 e IPv6) dentro de una red, definido en el RFC 2328.

 2 BGP, Border Gateway Protocol, protocolo de enrutamiento de compuerta externa utilizado para el intercambio de anuncios de red entre diferentes redes que tienen su propio sistema autónomo, es el protocolo utilizado en Internet para propagar a través de aplicación de políticas de enrutamiento las redes que integran Internet (definido en el RFC 4271).

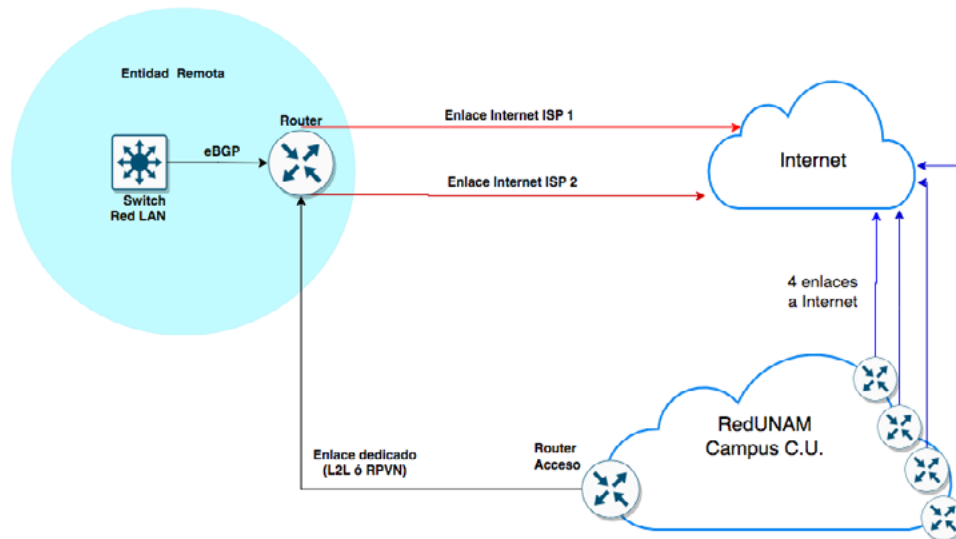
De estas 135 entidades, hay 75 que además del enlace dedicado también cuentan con por lo menos un enlace de Internet, con las siguientes características:

1. 75 de estas entidades cuentan con por lo menos un enlace de Internet que permite el intercambio de tráfico a Internet de manera local, no tienen que utilizar el enlace dedicado (ED) hacia Ciudad Universitaria para transportar el tráfico de Internet. Este enlace puede funcionar como respaldo para intercambiar tráfico a Ciudad Universitaria.
2. Cuentan con su propio direccionamiento IPv4 e IPv6 (asignada por el NIC UNAM) para poder utilizar este enlace de Internet. Tienen asignadas redes con máscara /24 en IPv4 y /48 en IPv6, que son anunciadas por el protocolo estándar BGP a Internet.
3. Ofrecen servicios públicos (sitios web, sistemas propios) y privados (estaciones de trabajo de su personal) a los cuales los usuarios pueden acceder desde fuera de la entidad, utilizando el direccionamiento público con que cuentan.
4. En algunos casos cuentan con direccionamiento IPv4 con máscaras mayores a /24, lo cual no puede ser anunciado por el enlace de Internet, lo que ocasiona que su acceso a Internet sólo sea por el enlace dedicado a Ciudad Universitaria, y el tráfico de Internet se intercambia por los enlaces del campus principal. En estos casos la entidad universitaria no cuenta con enlace de Internet local.

En la siguiente figura 2 se muestra la arquitectura de estos servicios.

Figura 2

Interconexión entre Ciudad Universitaria y una entidad remota, modelo de conexión



Estos enlaces se rentan a través de concursos de licitación, dado que este tipo de infraestructura es costosa y difícil de mantener, por lo que se adquieren con proveedores de acceso a Internet quienes cuentan con una amplia red de telecomunicaciones, por ello tampoco es fácil contratar grandes anchos de banda o múltiples enlaces para proporcionar ancho de banda ilimitado o diferentes accesos a las entidades remotas, por lo que se trata de eficientar el uso y proponer soluciones tecnológicas y lógicas que puedan apoyar en proporcionar una mayor disponibilidad en la red.

Como se aprecia en la figura, existen puntos de falla que podrían afectar el servicio de acceso a Internet y/o a Ciudad Universitaria. A continuación, se describen los escenarios:

1. Falla de enlace de Internet. En el caso de falla de uno o dos enlaces de Internet, según sea el caso, la entidad remota (ER) utiliza el enlace dedicado (ED) para pasar el tráfico hacia Ciudad Universitaria como enlace de respaldo, no de redundancia, ya que estos ED no cuentan con la misma cantidad de ancho de banda que se tiene a Internet, por lo que la comunidad usuaria de los servicios de Internet y RedUNAM de la ER experimentarán lentitud para utilizar sus aplicaciones de datos o imágenes, en tanto que las comunicaciones en tiempo real (voz, y video), como es el caso de telefonía, pueden verse afectadas al no ser coherentes por causa de pérdida de paquetes; en tanto que el video se puede ver afectado al congelarse la imagen (video asíncrono: YouTube) o en congelarse o cortarse la comunicación (conferencias en tiempo real). Se pueden mantener los servicios, pero pueden afectarse por la pérdida de paquetes debido a la saturación de ancho de banda. **Solución temporal.** Se podría configurar cierta calidad de servicio (QoS) para el tráfico que pase por el enlace dedicado hacia Ciudad Universitaria que permita que tengan mayor prioridad los paquetes de tráfico que requieran comunicaciones de tiempo real (voz y video), pero las demás comunicaciones podrían verse afectadas en caso de que el incidente en los enlaces hacia Internet se prolongara. Asimismo, al ser un enlace con menor ancho de banda, éste pudiera verse saturado por el tráfico con mayor prioridad en caso de presentarse una alta demanda por parte de los usuarios de la ER.

2. Falla del enlace dedicado (ED) hacia Ciudad Universitaria. Solo se presenta la falla en el enlace hacia C.U., en tanto que el enlace o enlaces de Internet se mantienen en operación. En este escenario se presentan dos problemáticas:

- Las peticiones al DNS (ubicado en Ciudad Universitaria) no se pueden procesar puesto que del lado de los ruteadores de acceso a Internet en Ciudad Universitaria no conocen una entrada en la tabla de ruteo para responder a las solicitudes hechas por los enlaces de Internet de la entidad remota. Con esto no puede haber resolución inversa de nombres y se tiene la percepción de que no hay acceso a Internet y el servicio se ve interrumpido, a pesar de que no se presentan fallas en el o los enlaces de Internet locales.
- Si la entidad cuenta con un DNS local o utiliza el DNS externo (por ejemplo, DNS de Google), pueden continuar con el acceso a Internet, pero el acceso a recursos en Ciudad Universitaria no puede llevarse a cabo por la misma situación, en los ruteadores de acceso a Internet en Ciudad Universitaria no tienen cómo llegar a la red de la entidad remota, pues en su tabla de enrutamiento no cuenta con ella.

Solución temporal. Para solucionar ambas problemáticas al momento de presentarse el incidente en el enlace dedicado se puede configurar manualmente una ruta estática en los ruteadores de acceso a Internet del lado de Ciudad Universitaria con la red IP de la entidad remota, con ello se ingresa

una ruta para poder llegar a la entidad universitaria y la comunicación se puede llevar a cabo entre las aplicaciones y sistemas en Ciudad Universitaria (incluido el DNS) y hacia la entidad universitaria que lo requiera, pero se agrega una problemática al poder llevar a cabo esta comunicación: la seguridad.

Tanto del lado de la entidad remota como de Ciudad Universitaria se utilizan los enlaces de Internet, estos enlaces son públicos pues ISPs integran estos enlaces a su infraestructura de red, en donde el tráfico de todos sus clientes (incluyendo los de la UNAM) y las comunicaciones que se llevan a cabo entre los servicios y los usuarios se transportan por esta misma infraestructura por lo que el tráfico puede ser susceptible a ser interceptado e intervenido para ser conocido o modificado por personas diferentes al usuario o destinatario, vulnerando la seguridad y poniendo en riesgo la información. Por lo que es necesario contar con un mecanismo de seguridad que evite que esta información pueda ser interceptada y manipulada en la red pública de Internet, y para ello se proponen las soluciones de SDN (SD WAN).

TECNOLOGÍA SD WAN

La tecnología conocida como Redes Definidas por Software en Redes de Área Amplia (Software Defined – Wide Area Network, SD WAN) ofrece solventar nuevas necesidades de las organizaciones, entre las cuales se mencionan:

- 1. Seguridad de comunicaciones.** Al construir un túnel seguro a través de enlaces de Internet, se logra una comunicación cifrada entre un punto remoto y un punto central (u otro punto remoto). Este túnel se construye entre los dispositivos de red involucrados y no en el usuario final o servicio al cual quiere acceder, lo cual permite concentrar la inteligencia en los dispositivos SD WAN y no en los dispositivos del usuario.
- 2. Alta disponibilidad.** Puesto que estos túneles se pueden construir entre los dispositivos remotos y centrales de SD WAN, siempre que haya 2 o más enlaces de Internet, estos túneles podrán mantenerse en operación, a pesar de que uno de los enlaces quede fuera de operación, lo que permite mantener la comunicación a través de los enlaces que se mantengan en funcionamiento.
- 3. Independencia del proveedor.** Esta tecnología no depende de quién sea el proveedor de los enlaces, ni el tipo de tecnología que se utilice para la entrega de los mismos; los túneles SD WAN pueden construirse siempre y cuando se cumpla la condición de que exista conectividad de capa 3 entre el dispositivo de SD WAN del campus central y el dispositivo remoto. A esta conectividad, previa a establecer el túnel, se denomina *underlay*, y al establecimiento de los túneles se le llama *overlay*.
- 4. Gestión centralizada.** La arquitectura de SD WAN define un plano de control, el cual es un punto central en el que se registran los dispositivos involucrados, este controlador se encarga de la gestión de cada uno de ellos, con lo cual se ofrece una administración y operación centralizada, no importando la complejidad de la red que se tenga; otras funciones que ofrece este plano de control es el monitoreo de los dispositivos, visibilidad de las aplicaciones que se transportan, todo esto ayuda a simplificar la operación y monitoreo de la infraestructura y servicios de red. Esta controladora por lo regular se tiene instalada en la nube de los fabricantes para proporcionar disponibilidad y operación a sus clientes.

5. Comunicación a nubes de redes de entrega de contenido. Dado que la migración de servicios de las organizaciones hacia la nube se va incrementando poco a poco, se requiere tener una mayor seguridad y velocidad en las comunicaciones a estas nubes, por lo que al utilizar SD WAN puede establecerse esta comunicación segura y rápida a las diferentes redes de entrega de contenido (CDN) como son Azure, AWS, Cloudflare, Google.

Cabe mencionar que esta tecnología SD WAN es la aplicación del paradigma de redes definidas por software (SDN) hecha por el fabricante de los equipos.

MEJORES PRÁCTICAS PARA LA GESTIÓN DE SERVICIOS DE TIC

Dentro del equipo de trabajo de la Dirección de Telecomunicaciones de la DGTIC, en el Departamento de Monitoreo de la Red (NOC RedUNAM), se ha permeado la forma de trabajo basada en las mejores prácticas internacionales para llevar a cabo la gestión de servicios de TIC (ITIL (s.f.)) por lo que la propuesta de mejora se desarrolla bajo las recomendaciones del ciclo de vida del servicio de TIC que ofrece este modelo.

En la publicación de ITIL (s.f), *Continual Service Improvement* (2022, pp. 31), nos brinda un modelo de fases, procesos y prácticas definido como Ciclo de vida para la gestión de servicios de TIC, en el cual se definen 5 diferentes fases cuyo objetivo es gestionar y brindar servicios de tecnologías de la información y comunicación (TIC) que ayuden a la organización y sus usuarios a lograr sus objetivos a través del desarrollo y uso de servicios TIC. La definición de cada una de estas fases se presenta en ITIL (s.f.), *Service Strategy* (2011) y son las siguientes:

- 1. Estrategia del servicio.** Define la perspectiva, posición, planes y patrones que el proveedor de servicio necesita ejecutar para alcanzar los resultados de la organización. Los procesos que se incluyen son: gestión de la estrategia, gestión del portafolio de servicios, gestión financiera de los servicios, gestión de la demanda y gestión de las relaciones con la organización.
- 2. Diseño del servicio.** Incluye el diseño de los servicios de TIC, prácticas de gobierno, procesos y políticas que se requieren para llevar a cabo la estrategia del proveedor del servicio, y para facilitar la introducción de servicios dentro ambientes de producción.
- 3. Liberación del servicio.** Se asegura que los servicios nuevos, modificados o retirados cumplan las expectativas de la organización de acuerdo con lo definido en las fases del ciclo de vida de estrategia y diseño.
- 4. Operación del servicio.** Coordina y lleva a cabo las actividades y procesos que se requieren para entregar y gestionar servicios de acuerdo con los niveles de servicio de clientes, usuarios y la organización. También se encarga de gestionar la tecnología que es utilizada para estos servicios.
- 5. Mejora continua.** Esta fase asegura que los servicios se encuentren alineados con los cambios de la organización, identificando e implementando mejoras a los servicios de TIC para soportar los procesos de la organización.

PROPUESTA DE MEJORA

Dentro de cada una de las fases del ciclo de vida de ITIL (s.f.), se recomienda una serie de procesos que interactúan con el fin de entregar y brindar servicios de TIC que ofrezcan valor a la organización. A continuación, se presenta una tabla en donde se enuncian los procesos, actividades y resultados que se utilizaron para poder lograr con éxito las pruebas en sedes foráneas:

Tabla 1

Actividades y resultados obtenidos dentro del Ciclo de Vida de ITIL

Fase del ciclo de vida	Actividad	Resultado
Estrategia	Revisión del Plan de Desarrollo Institucional	Se atiende el objetivo
Diseño	Análisis de tecnologías que puedan apoyar la mejora de la disponibilidad	Definición de pruebas de la tecnología SD WAN
	Revisión de las topologías, configuraciones y capacidades tecnológicas de la infraestructura actual	Inventario de ruteadores con versiones de sistema operativo, lista de necesidades para implementar
	Diseño de pruebas de las diferentes tecnologías	Redacción de las pruebas para SDWAN
Liberación	Llevar a cabo pruebas con SDN (SD WAN)	Se llevaron a cabo pruebas de SD WAN en las entidades PIIT Monterrey y Campus Juriquilla
Operación	Puesta en operación de SD WAN	Se llevaron a cabo pruebas en conjunto con proveedores y fabricantes en los Campus PIIT Monterrey y Juriquilla
Mejora continua	Detección y atención de incidentes	

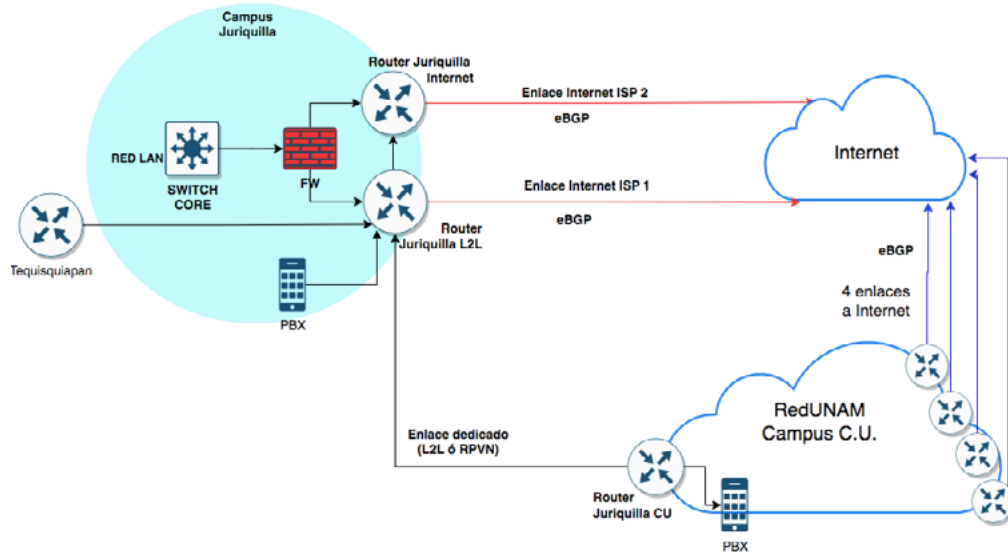
Parte muy importante para el despliegue de una nueva tecnología es conocerla y realizar pruebas sobre sus capacidades. Las pruebas realizadas no se hicieron sobre maquetas, sino con infraestructura en operación, por lo que se tuvo que cuidar que no impactaran en la operación de la red. Para ello se establecieron ventanas específicas para realizar la instalación, configuración, migración de enlaces y pruebas, validando que los servicios se mantuvieran en operación, en común acuerdo con los responsables de TIC de los campus participantes, con el fabricante de los equipos y con el proveedor de Internet.

PRUEBAS SD WAN CAMPUS JURIQULLA

El Campus Juriquilla de la UNAM cuenta con un enlace dedicado hacia Ciudad Universitaria y dos enlaces de Internet, con diferentes ISP's, en dos diferentes ruteadores, que proporcionan cierto nivel de redundancia en caso de falla de uno de estos servicios de Internet. La figura 3 muestra estas conexiones.

Figura 3

Interconexiones WAN del Campus Juriquilla hacia Ciudad Universitaria e Internet



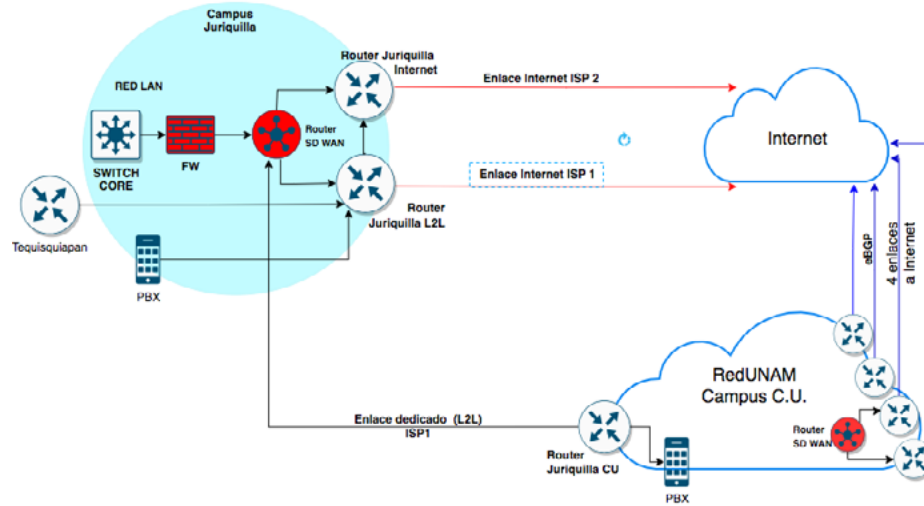
La infraestructura con la que se cuenta para llevar a cabo estas conexiones son tres ruteadores del fabricante distribuidos de la siguiente manera:

1. a. **Ruteador Juriquilla Ciudad Universitaria.** Este ruteador interconecta a RedUNAM y Juriquilla; adicional a estas conexiones también se cuenta con una conexión hacia uno de los conmutadores telefónicos (PBX) de Zona Cultural (ZC), con esta interconexión el ruteador hace la conversión del tráfico de voz de analógico a paquetes entre los equipos conmutadores (PBX) y ruteador para que este último pueda transportar la voz a través del enlace dedicado de 200 Mbps hacia Juriquilla.
2. b. **Ruteador Juriquilla L2L.** Al igual que el de Juriquilla, Ciudad Universitaria tiene una interfaz para conectar el conmutador del Campus Juriquilla, con ello el servicio de voz puede establecerse entre el Campus y Ciudad Universitaria a través del enlace L2L. Este ruteador también conecta a la otra dependencia universitaria en Tequisquiapan con un enlace dedicado, y se interconecta al otro ruteador de acceso a Internet llamado Juriquilla Internet. También tiene un enlace a la LAN del campus, entre estos equipos hay intercambios de redes IP a través del protocolo OSPF. Para el acceso a Internet se cuenta con un enlace de 500 Mbps.
3. c. **Ruteador Juriquilla Internet.** Este ruteador conecta el otro enlace a Internet que tiene un ancho de banda de 700 Mbps y otro enlace redundante hacia la LAN del Campus. También intercambia los anuncios de enrutamiento utilizando el protocolo OSPF y la ruta de default para proporcionar una redundancia en el acceso a Internet.

La prueba de SD WAN se realiza a través de la incorporación de dos ruteadores, en color rojo, uno en Campus Juriquilla y otro en CU., estos a su vez interconectados a los ruteadores que dan acceso a Internet en cada uno de los Campus. Esta interconexión se muestra en la figura 4.

Figura 4

Interconexión de equipos de prueba SD WAN en el Campus Juriquilla y Ciudad Universitaria



Tanto en el campus como en Ciudad Universitaria se instala un ruteador con capacidades de manejo de SD WAN, estos se interconectan en la red con direccionamiento IPv4 el cual pueda ser alcanzado entre ambos ruteadores: del lado de Juriquilla se configura una IP con máscara /24 y del lado de Ciudad Universitaria una con máscara /30, una vez que ambos equipos pueden alcanzarse se procede a continuar con la prueba.

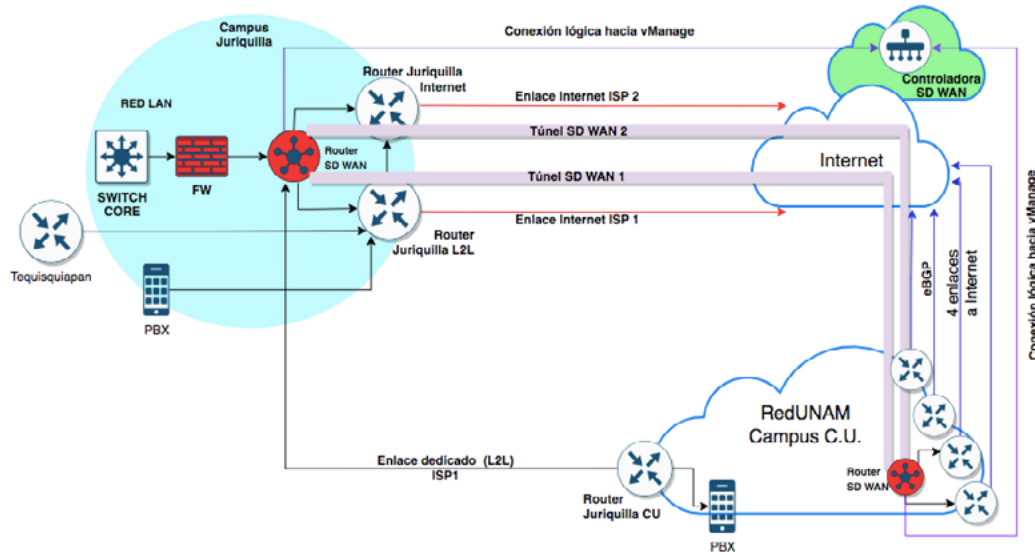
SD WAN EN JURIQUELLA

La puesta en operación de los túneles de SD WAN (1 y 2) entre los ruteadores SD WAN de Campus Juriquilla y Ciudad Universitaria se lleva a cabo dando de alta estos ruteadores en una controladora SD WAN (plano de control de redes SDN) ubicada en la nube (en color verde) del fabricante, esto se puede lograr porque de ambos campus se anuncian a Internet las redes IPv4 con máscara /24 a las que pertenece el direccionamiento que utilizan estos ruteadores, que son alcanzables por la controladora (vManage) para poder operarlos y configurarlos a partir de este registro.

Una vez establecido este registro de los ruteadores a la controladora SD WAN, los routers pueden tomar la configuración que se realiza en dicha controladora, con ello gestionamos de manera central cada uno de los ruteadores que se registren, dentro de esta configuración se establece que entre ambos ruteadores SD WAN (Juriquilla y C.U.) se construyan dos túneles para transportar dentro de ellos la información que intercambian los usuarios y aplicaciones de ambos Campus, entre ellas las solicitudes de resolución del DNS y con ello poder acceder a Internet. Se establecen dos túneles para proporcionar una redundancia en caso de que falle alguno de los dos enlaces de Internet de Juriquilla. La figura 5. Muestra estos elementos de registro hacia el vManage (controladora) y los dos túneles de SD WAN.

Figura 5

Comunicación SD WAN en el Campus Juriquilla- Ciudad Universitaria



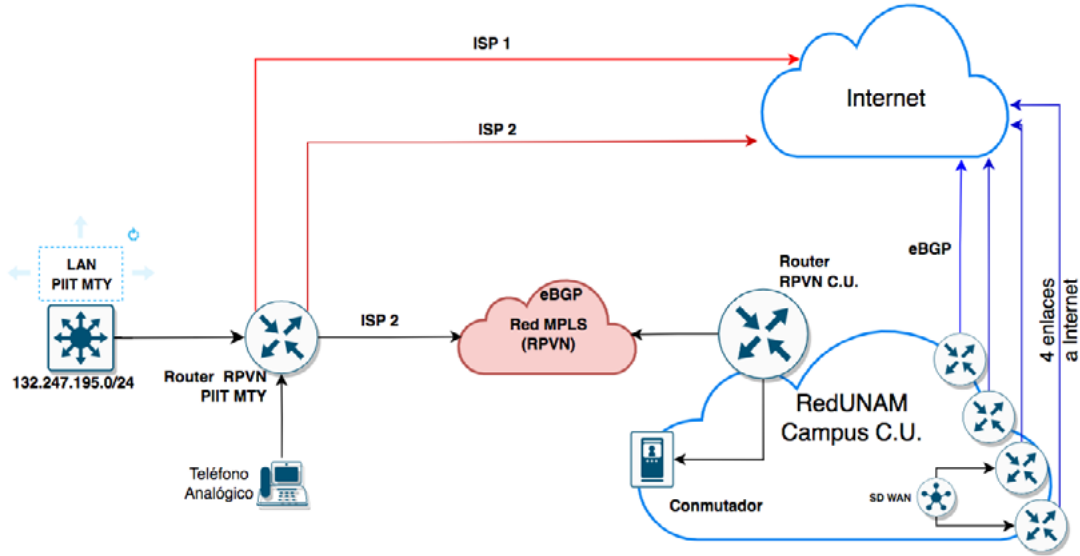
PRUEBAS SD WAN CAMPUS PIIT PARQUE DE INVESTIGACIÓN E INNOVACIÓN TECNOLÓGICA, MONTERREY (PIIT MTY)

Para considerar otro tipo de arquitectura, en esta interconexión en lugar de un enlace dedicado entre Ciudad Universitaria y la dependencia remota universitaria, se contrató un enlace MPLS (Multiprotocol Label Switching) con calidad de servicio (Red Privada Virtual) el cual tiene las características de ser un enlace hacia la red MPLS del ISP, la cual interconecta ambos campus. A diferencia de un enlace dedicado, este enlace MPLS proporciona Calidad de Servicio (QoS) para los diferentes tipos de aplicaciones que se puedan transportar en el enlace, en este caso Voz sobre IP, videoconferencias y datos, con ello se busca asegurar que dentro de la red pública (MPLS) del proveedor, se entregue dicho tráfico entre la dependencia (PIIT Monterrey) y el Campus Ciudad Universitaria, a pesar de pasar por una red pública.

Otra característica de esta dependencia universitaria es que cuenta con el servicio de voz (telefonía) a través del ruteador: en PIIT Mty el ruteador cuenta con 4 puertos FXO (analógicos) para conectar teléfonos directamente al ruteador (o a un conmutador multilíneas), y del lado de Ciudad Universitaria se cuenta con un enlace E1 (2 Mbps) que interconecta a un conmutador de la red central de telefonía de RedUNAM. Con esta arquitectura los ruteadores de ambas puntas llevan a cabo la conversión de la señal analógica generada por el sistema telefónico a paquetes IP que se transportan por el enlace MPLS, y con ello se puedan llevar a cabo las comunicaciones de voz entre ambas puntas en un ambiente “dedicado” apoyado por la QoS configurada en los ruteadores y en la nube MPLS del proveedor. En la figura 6. Se muestran los elementos de red y enlaces que integran la arquitectura de conexión WAN del Campus PIIT Monterrey.

Figura 6

Interconexiones WAN del Campus PIIT Monterrey hacia Ciudad Universitaria e Internet



Tráfico de Voz

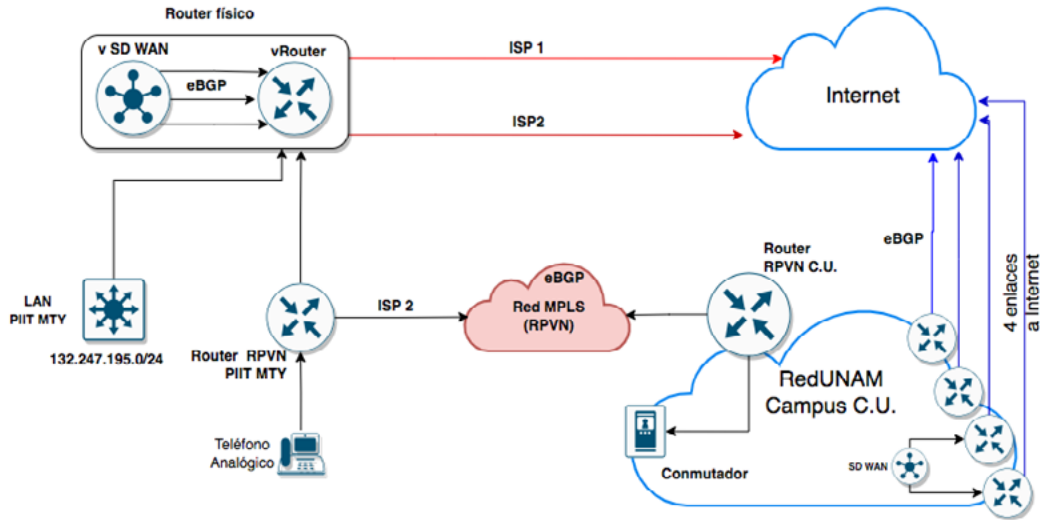
Una gran diferencia entre la prueba de Juriquilla y PIIT Monterrey es que en este último sí se realizaron pruebas transportando el tráfico de voz por los túneles SD WAN. El ruteador RPNV PIIT MTY se conectó hacia el ruteador de prueba para que el tráfico de voz se transportara por los enlaces de Internet utilizando los túneles de SD WAN. Esta conexión era necesaria pues los puertos FXO no se podían migrar al ruteador de prueba, ya que la caja blanca no tenía la capacidad para poder insertar y reconocer este tipo de tarjeta del ruteador.

PRUEBAS SD WAN PIIT MTY

Para esta prueba la arquitectura cambió en comparación con las pruebas en Juriquilla, pues en lugar de tener dos ruteadores físicos, ahora se integró un ruteador físico que hospedaba a dos ruteadores virtuales con sistema operativo IOS, un ruteador virtual vSD WAN y un vRouter; la funcionalidad SD WAN se configuró en el vSD WAN y en el vRouter con funcionamiento de ruteador tradicional.

Figura 7

Interconexión de equipos de prueba SD WAN en el Campus PIIT Monterrey y Ciudad Universitaria

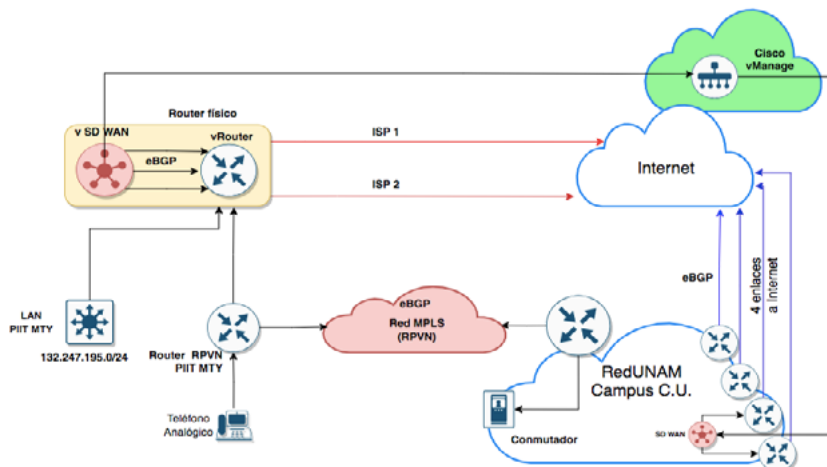


La primera fase es poder establecer el *underlay* (camino entre los dos routers con SD WAN), por lo que se realizó lo siguiente del lado de PIIT Mty:

1. En los enlaces de Internet, utilizando el protocolo BGP, el router tradicional anuncia las redes LAN que utiliza PIIT Mty, así como la red de prueba que interconecta el router tradicional y el router SD WAN, con ello este router puede ser alcanzado desde Internet. En tanto que, del lado de Ciudad Universitaria, se utiliza un direccionamiento que ya es parte de los anuncios de bloques /16 a través de los 4 enlaces de Internet.

Figura 8

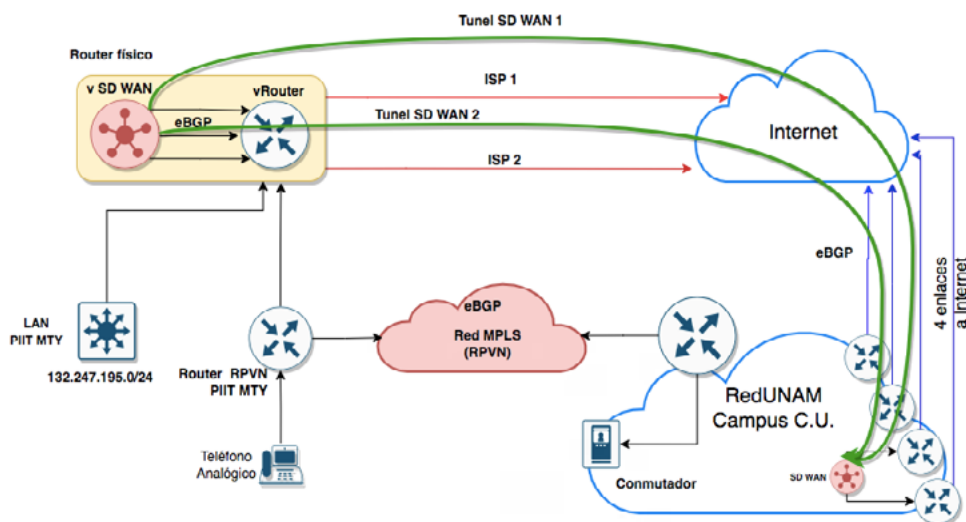
Conexiones lógicas SD WAN SD WAN para la prueba en PIIT Monterrey



- Una vez realizada esta propagación de anuncios, ambos ruteadores SD WAN podrán ser alcanzados entre ellos para poder establecer el *underlay* (la capa de transporte de ruteo tradicional) y por la controladora vManage, para poder registrarlos y configurarlos, y con ello establecer el *overlay* (la capa superior de transporte de tráfico en SD WAN).

Figura 9

Túneles SD WAN entre el campus PIIT Monterrey y Ciudad Universitaria



Esto permitió que la comunicación entre el campus y Ciudad Universitaria se realizara a través de la construcción de túneles de SD WAN, por donde se transportaba la comunicación de datos y voz que los usuarios del PIIT Mty requerían.

4. RESULTADOS

De acuerdo con las pruebas realizadas (tabla 2) con la tecnología SD WAN en conjunto con personal del fabricante de los equipos ³ y uno de los ISP, se puede concluir, en cuanto a la tecnología SD WAN:

- El paradigma de redes definidas por software (SDN) está desarrollado por múltiples fabricantes de manera independiente, sin protocolos estándar, por lo que cada fabricante propone una solución propia y no son compatibles; al no existir interoperabilidad entre marcas, su adopción debe configurarse con un solo fabricante si lo que se busca es tener una única gestión centralizada de la red.
- Los escenarios en donde SDN funciona de forma nativa es en arquitecturas en donde existe un punto central dentro de la red de la organización, y éste concentra varios servicios de TIC (centro de datos, sistemas escolares y administrativos, etc.), que son utilizados por los nodos remotos.

³ Basado en Gooley J., Yanch D., Schuemann, D., Curran, J. (2020)

A su vez estos nodos remotos (sucursales) no cuentan con direccionamiento IP público, sólo cuentan con uno no homologado (RFC 1918), y tampoco cuentan con servicios públicos a los cuales pueden acceder usuarios tales como sitios web o aplicativos, todo esto reside en el nodo central; inclusive, tampoco cuentan con acceso a Internet independiente al nodo central, por lo que su acceso a Internet también se encuentra ubicado en el nodo central de la organización.

Por lo anterior, la implementación en la arquitectura física, lógica y de aplicaciones de RedUNAM requiere de ajustes y configuraciones adicionales para que pueda operar SD WAN para que la entidad remota:

1. Mantenga el intercambio de tráfico a Internet a través del enlace local con que cuenta.
2. Mantenga el direccionamiento IPv4 público en sus servidores para poder intercambiar tráfico. En caso de tener asignado un direccionamiento IPv4 con una máscara mayor a /24, poder intercambiar tráfico por el internet utilizando un NAT.
3. La comunicación hacia Ciudad Universitaria pueda llevarse a cabo a través de los túneles SD WAN contruidos entre el ruteador remoto y el que se encuentre en Ciudad Universitaria. Estos túneles pueden ser: uno por cada uno de los enlaces de Internet con que cuente el nodo remoto.
4. Se establece una alta disponibilidad tanto para el acceso a Internet como para el acceso a Ciudad Universitaria, pues el tráfico de los DNS se mantiene por los túneles de SD WAN que permiten que el tráfico se mantenga a pesar de algún fallo. Esto último, en caso de existir dos enlaces de Internet.
5. Se tendría un nivel de control para la gestión de esta red SD WAN, pues ya no es posible la administración y operación como tradicionalmente se ha llevado a cabo.

5. CONCLUSIONES

La mejora en la confiabilidad de la red y los servicios que los usuarios obtienen de ésta, se puede lograr incrementando la disponibilidad de acceso a Internet a través de la implementación de SDN en su modalidad de SD WAN.

La incorporación de esta tecnología a nivel técnico y operacional se ha probado que puede funcionar, los servicios, aplicaciones, información y contenidos digitales, tanto los alojados en Internet como en C.U. y otras entidades universitarias continuaron operando con normalidad, no se han visto afectadas, por lo que no solo las aplicaciones asíncronas (datos), sino también las síncronas (voz y video) pueden ser utilizadas por la comunidad universitaria para complementar sus tareas diarias. A nivel de operación de la red nos proporciona un control central a través de la plataforma vManage la cual me facilita la gestión de activos (ruteadores, configuraciones, información), visualización de tráfico y agrega la posibilidad de automatizar tareas de configuración e identificación de eventos (alertas) sobre lo que sucede en la RedUNAM.

El despliegue de esta tecnología se propone en el modelo de cascada o de fases, en lotes de algunos servicios y dependencias, ya que la curva de aprendizaje en la operación y atención de incidentes puede impactar negativamente en caso de un despliegue masivo dentro de la RedUNAM, por ello y para minimizar este aspecto se propone que el despliegue se acote a unos cuantos enlaces suficientes para ganar experiencias en operación y beneficio hacia los usuarios en los servicios de Internet y hacia Ciudad Universitaria.

Es importante la capacitación del personal que opere esta tecnología, ya que es una nueva forma de establecimiento de comunicaciones que requiere de práctica en la operación para generar experiencia que ayude a obtener conocimiento y sirva para el rápido despliegue de la tecnología, así como a la atención de incidentes que se presenten.

Asimismo, es importante tener un buen soporte por parte no solo del proveedor con quien se adquiera la infraestructura y tecnología, sino también del fabricante, ya que al ser una tecnología diferente se requiere de una asistencia rápida por parte de ambos actores para la atención de incidentes de segundo y tercer nivel.

El objetivo de una RedUNAM más resiliente y que responda de manera automática a los cambios que se puedan presentar en ella se podrá alcanzar con una tecnología innovadora y en constante evolución que se adapte a las necesidades universitarias; con SD WAN se puede avanzar hacia esa visión.

6. AGRADECIMIENTOS

Estas pruebas se llevaron a cabo gracias a la participación y apoyo de los responsables de TIC de los Campus Juriquilla y Campus PIIT Monterrey. Agradezco a Edgar López y a Josué Betancourt por su arduo trabajo, disposición y apoyo, así como a los equipos de ingenieros de los proveedores involucrados, quienes ayudaron a revisar y afinar los escenarios y posibles adecuaciones a las configuraciones del equipamiento.

Un especial agradecimiento a Lourdes Jiménez Ramírez y a Marcial Martínez Quinto quienes son parte del equipo de trabajo y colaboradores del NOC RedUNAM quienes también apoyaron en la elaboración de las pruebas.

REFERENCIAS BIBLIOGRÁFICAS

Best Management Practice, (2011) *ITIL Service Strategy, The Stationary Office.*

Best Management Practice, (2011) *ITIL Continual Service Improvement, The Stationary Office.*

Gooley J., Yanch D., Schuemann, D., Curran, J. (2020) *Cisco Software-Defined Wide Area Networks: Designing, Deploying and Securing Your Next Generation WAN with Cisco SD-WAN*, Cisco Press. Part of the Networking Technology series.

J.Moy (1998) Open Shortest Path First. [(OSPF) RFC 1228 consultado de <https://www.rfc-editor.org/info/rfc2328>

Rekhter. Y. (2006) a Border Gateway Protocol. RFC 4271 consultado de, <https://www.rfc-editor.org/info/rfc4271>

ANEXO 1

Tabla 2

Tabla de resultados de las pruebas de SD WAN

Prueba	Descripción	Juriquilla	PIIT Mty
Hardware			
Cisco	Modelo del equipamiento utilizado.	ASR 1001	v8000 (virtual)
Ruteador tradicional	Tipo de ruteador utilizado	Sí	v8000 (virtual)
Construcción SD WAN			
Construcción de <i>underlay</i>	Ambos ruteadores SD WAN se alcanzan por Internet	Sí	Sí
Construcción de <i>overlay</i>	Se pueden establecer túneles SD WAN entre ambas puntas	Sí	Sí
Gestión desde vManage	Se puede configurar el ruteador SD WAN desde la controladora en la nube	Sí	Sí
SD WAN			
Túneles SD WAN	Dentro del vManage se pueden configurar fácilmente las características del túnel	Sí	Sí
Intercambio de ruteo interno de la RedUNAM	Una vez establecido el túnel se puede intercambiar la tabla de ruteo de Ciudad Universitaria con la entidad remota y viceversa, sin utilizar BGP u OSPF	Sí	Sí
Intercambio a Internet por el enlace local	El tráfico de Internet que requiere la entidad remota se entrega a través de los enlaces de Internet locales, sin pasar por los túneles SD WAN	Sí	Sí
Intercambio de tráfico de aplicaciones de RedUNAM	Se puede pasar tráfico entre campus a través del o de los túneles SD WAN	Sí	Sí
Intercambio de tráfico de voz	El tráfico de voz pasa por el túnel SD WAN sin degradación	N/A	Sí
Alta disponibilidad			
Construcción de dos túneles	Se pueden construir dos túneles SD WAN independientes a los enlaces con que cuenta el campus para proporcionar alta disponibilidad por Internet	N/A	Sí
Desvío de tráfico al fallar enlace dedicado (L2L)	En caso de incidente del enlace dedicado o RPVN, el tráfico hacia Ciudad Universitaria se mantiene por el túnel SD WAN	Sí	Sí
Desvío de tráfico al fallar uno de los túneles	En caso de existir dos túneles, si uno falla el otro mantiene la comunicación hacia Ciudad Universitaria	No	Sí

Prueba	Descripción	Juriquilla	PIIT Mty
Soporte del fabricante			
Conocimiento	Alto nivel de conocimiento de la solución SD WAN	Sí	Sí
Documentación	Documentación de apoyo para implementación y solución de incidentes	Sí	Sí
Soporte	Atención rápida para la solución de incidentes	Sí	Sí
Soporte del Proveedor			
Conocimiento	Alto nivel de conocimiento de la solución SD WAN	Sí	Sí
Documentación	Documentación de apoyo para implementación y solución de incidentes	Sí	Sí
Soporte	Atención rápida para la solución de incidentes	Sí	Sí