ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELECTRÍCA Y ELECTRÓNICA

DISEÑO DE UNA iWAN

REDES iWAN

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN TELECOMUNICACIONES

PRISCILA CAROLINA FLORES CARRERA

priscila.flores@epn.edu.ec

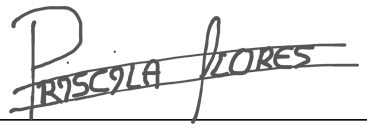
DIRECTOR: CARLOS ALFONSO HERRERA MUÑOZ

carlos.herrera@epn.edu.ec

DMQ, OCTUBRE 2022

CERTIFICACIONES

Yo, PRISCILA CAROLINA FLORES CARRERA declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.



PRISCILA CAROLINA FLORES CARRERA

Certifico que el presente trabajo de integración curricular fue desarrollado por PRISCILA CAROLINA FLORES CARRERA, bajo mi supervisión.

CARLOS ALFONSO HERRERA MUÑOZ

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

PRISCILA CAROLINA FLORES CARRERA

CARLOS ALFONSO HERRERA MUÑOZ

DEDICATORIA

Dedico este logro a mi hijo quien ha sido el motor para poder salir a delante con mis estudios, a mi esposo quien fue mi apoyo incondicional, a mis padres y hermana que siempre tuvieron una palabra de apoyo en los momentos que mas lo necesite, y a mi abuelita ya que siempre me tenía presente en cada uno de sus rezos.

AGRADECIMIENTO

En primer lugar, agradezco a Dios por haberme dado la salud y la oportunidad de haber estudiado en tan prestigiosa universidad, en segundo agradecer a mi familia por siempre ser mi apoyo, por no dejarme vencer ante cualquier situación.

De manera muy especial agradezco a mi esposo por ser mi sostén, el que a pesar de cualquier circunstancia estaba ahí para darme una palabra de aliento, también agradezco a mi hijo que aparte de ser la principal razón para luchar por mis sueños y metas, siempre entendía cuando no podía salir a jugar por quedarme haciendo deberes o estudiando para algún examen, por hacerme reír o por darme un abrazo cuando mas lo necesitaba.

También, agradezco al Ing. Carlos Herrera por brindarme su apoyo y sus consejos no solo ahora como director sino en el transcurso de toda la carrera.

Tabla de contenido

Índice de figuras

Capítulo 1

Capítulo 2

Capítulo 3

Índice de tablas

RESUMEN

En el presente trabajo de integración curricular se realiza un estudio sobre la tecnología Cisco Intelligent WAN iWAN.

En el primer capítulo se explican la evolución de las redes WAN a lo largo de los años, además se exponen las razones por las cuales existe un aumento de la demanda de las redes WAN y el por qué las redes WAN se han vuelto más críticas para las empresas en cualquier tipo de mercado.

En el segundo capítulo proporciona los conceptos básicos sobre Cisco Intelligent WAN (iWAN) y cómo es capaz de mejorar la experiencia del usuario al mismo tiempo que reduce los costos operativos. También se explican los principales modelos de implementación de la tecnología ya antes mencionada. Además, se da una introducción a los componentes de esta tecnología como son: la independencia de transporte, el control de ruta inteligente, la optimización de aplicaciones y la conexión segura.

En el tercer capítulo explica los conceptos básicos de DMVPN, su funcionamiento, los principales componentes que hacen que DMVPN sea una pieza clave al momento de implementar iWAN, también se van a detallar los modelos de implementación, sus características y beneficios.

En el cuarto y último capítulo se desarrollan las conclusiones y recomendaciones que deja el desarrollo del presente trabajo de integración curricular.

PALABRAS CLAVE: Cisco Intelligent WAN iWAN, independencia de transporte, control de ruta inteligente, optimización de aplicaciones, conexión segura, DMVPN.

ABSTRACT

In this curricular integration work, a study on Cisco Intelligent WAN iWAN technology is carried out.

In the first chapter, the evolution of WAN networks over the years is explained and the reasons why there is an increase in the demand for WAN networks and why WAN networks have become more critical for companies in any type of market.

The second chapter provides the basics of Cisco Intelligent WAN (iWAN) and how it can improve the user experience while reducing operating costs. The main implementation models of the aforementioned technology are also explained. In addition, an introduction to the components of this technology is given, such as transport independence, intelligent route control, application optimization, and secure connection.

The third chapter, explains the basic concepts of DMVPN, its operation, the main components that make DMVPN a key piece when implementing iWAN, it will also detail the implementation models, their characteristics, and benefits.

In the fourth and last chapter, the conclusions and recommendations that leave the development of the present work of curricular integration are developed.

KEYWORDS: Cisco Intelligent WAN iWAN, Transport Independence, Intelligent Path Control, Application Optimization, Secure Connection, DMVPN

1 INTRODUCCIÓN

El mundo está en un proceso de cambio permanente y más aún las telecomunicaciones. Ahora más que nunca las empresas están buscando tecnologías que les permita proporcionar velocidad, flexibilidad e información de manera rentable en todos sus sistemas y procesos. Algunas redes WAN utilizan el servicio MPLS, pero lamentablemente no siempre está disponible o es rentable para que pueda ser utilizado exclusivamente para la creación de una WAN robusta, segura y rentable, otros servicios que utiliza WAN son las VPN MPLS, Internet y Carrier Ethernet. Si bien las redes VPN IP de internet posees una opción atractiva para una conectividad WAN efectiva, cada que se envían datos a través de la red pública va a existir el riesgo de que los datos se vean comprometidos[1]. En la mayoría de las implementaciones WAN tradicionales tanto clientes, vendedores, proveedores y empleados que se encuentran en las sucursales, no tienen la capacidad de recibir un servicio óptimo, además de que tienen limitaciones en sus capacidades. La tecnología Cisco Intelligent WAN (iWAN) permite eliminar esas limitaciones, gracias a la adaptación de inteligencia en la WAN. Con esta adaptación la tecnología iWAN va a tener la capacidad de simplificar las VPN para así poder tener un mayor control sobre el tráfico de internet interno y externo, los servicios de la nuble pública, etc. La tecnología iWAN es capaz de proporcionar una conectividad segura con un servicio y rendimiento mejorado[2].

Cisco Intelligent WAN (iWAN) brinda ayuda para que las empresas de cualquier segmento del mercado se puedan conectar las sucursales con el valor comercial ubicado en cualquier lugar de la red. Es decir que, ya sea que la empresa sea una clínica, una tienda minorista o una oficina remota, un componente fundamental de estas empresas son las sucursales. En estos lugares se tiene la interacción con los clientes además aquí es donde la mayoría del personal de la empresa trabaja[2].

La tecnología Cisco Intelligent WAN (iWAN) brinda una orientación en el diseño e implementación para organizaciones que desean llevar a cabo un transporte de red de área amplia (WAN) con independencia de transporte, control de ruta inteligente, optimización de aplicaciones y lo más importante es que hace las comunicaciones más seguras gracias a que están encriptadas, logrando que su costo se reduzca. En las redes iWAN los servicios de transporte logran ser aprovechados al máximo y así se puede aumentar la capacidad de ancho de banda sin que el rendimiento, confiabilidad o seguridad se vean afectadas[3].

1.1 OBJETIVO GENERAL

Estudiar la tecnología Cisco Intelligent WAN (iWAN)

1.2 OBJETIVOS ESPECÍFICOS

- Estudiar los conceptos y generalidades necesarias para comprender la solución que la empresa CISCO propone a través de la tecnología Cisco Intelligent WAN (iWAN).
- Describir la arquitectura y componentes de la tecnología Cisco Intelligent WAN (iWAN) utiliza para poder cumplir con las necesidades de los usuarios.
- Estudiar la independencia de transporte que está basado en Dynamic Multipoint VPN (DMVPN) para redes iWAN

1.3 ALCANCE

Las redes WAN han evolucionado desde la década de 1990, al inicio la mayor cantidad de tráfico permanecía en un ambiente LAN; mientras que en los enlaces WAN permitían la transferencia de datos entre servidores de correo electrónico o para usuarios que ingresaban a la intranet corporativa. Actualmente estos enlaces WAN han experimentado un aumento del tráfico, es por esto que la empresa CISCO presenta la solución Cisco Intelligent WAN (iWAN) [2].

Al culminar con este proyecto se pretende que todos los conceptos relacionados con iWAN sean comprendidos. También se realizará un estudio de la arquitectura la cual proporciona a las organizaciones la capacidad de proveer mayor ancho de banda WAN a un menor costo con un mejor rendimiento, sin que la seguridad o la confiabilidad disminuyan. Cisco Intelligent WAN (iWAN) se basa en cuatro pilares que son: independencia del transporte, control de ruta inteligente, optimización de aplicaciones y conectividad segura.

1.4 MARCO TEÓRICO

1.4.1 REDES WAN

1.4.1.1 Evolución de las redes WAN

Las redes WAN iniciaron a finales de la década de los 60's con ARPANET (Advanced Research Projects Agency Network)[4] que una red de computadoras que se utilizó para la comunicación entre redes militares y también para conectar los principales grupos de investigación a través de los Estados Unidos[5].

En los años 80's fue necesario el uso de redes convergentes para poder lograr una conectividad adecuada por lo cual surgieron las redes TDM (Time Division Multiplexing). En la década de los 90's, la gran demanda que tenían los clientes de los ISP's (Internet

Service Providers) de aplicaciones multimedia con gran exigencia de ancho de banda y calidad de servicio hizo surgir a Frame Relay y ATM[6].

A comienzos de los 2000's apareció MPLS (Multiprotocol Label Switching) con el cual se logró que las LANs se puedan emplear como WAN[4].

En la figura 1.1 se puede observar la evolución de las redes WAN.

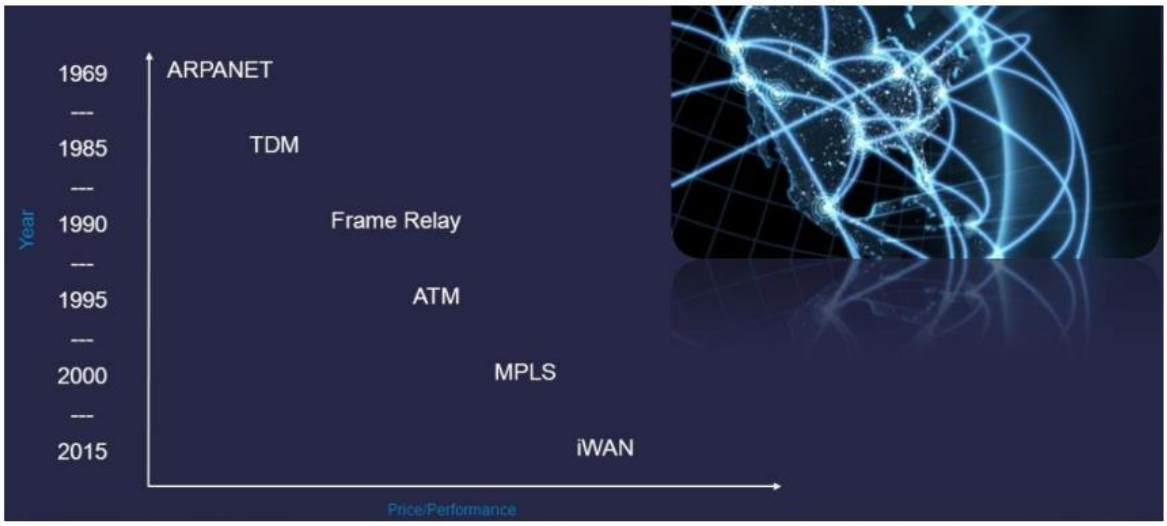


Figura 1.1 Evolución de la WAN

1.4.1.2 Problemas de las redes WAN

WAN utiliza una gran cantidad de tecnologías en cuanto a conectividad, los métodos más utilizados vienen de los proveedores de servicios (SP), estos ofrecen tres soluciones principales: circuitos arrendados, Internet y VPN de conmutación de etiquetas multiprotocolo (MPLS)[2].

1.4.1.2.1 Circuitos arrendados

Con el fin de obtener un mayor ancho de banda y una conectividad segura los proveedores de servicio han logrado entregar circuitos dedicados entre dos ubicaciones. Las líneas arrendadas pueden proporcionar un gran ancho de banda independientemente de la utilización del enlace, esto se puede lograr por que los circuitos están dedicados a un cliente específico. El costo que implica la instalación de estos circuitos arrendados puede llegar a representar una barrera financiera para la mayoría de las empresas[2].

1.4.1.2.2 Internet

La arquitectura de Internet consta de una red pública global que conecta varios SP, un gran beneficio que se tiene al usar Internet como transporte WAN es que no es necesario que las ubicaciones que vayan a enviar la información usen el mismo SP, es decir es posible establecer conectividad entre diferentes sitios utilizando diferentes SP. El problema con este método es que una empresa al comprar conectividad a Internet el ancho de banda que la misma contrato solo va a estar garantizado para las redes que controla el mismo SP. Esto quiere decir que, si la ruta por la cual va a transportarse la información que vamos a enviar cruza por varios SP el ancho de banda no está garantizado, por lo general el ancho de banda en los enlaces de emparejamiento poseen un menos ancho de banda que la red nativa. Por lo que en algunos casos puede existir una cierta congestión en el enlace de emparejamiento, esto genera retraso o pérdida de paquetes lo que no es conveniente para ninguna empresa[2].

En la figura 1.2 se ilustra una topología en la que puede producirse una contención de ancho de banda en los enlaces de intercambio de tráfico. Como podemos observar AS100 garantiza 1Gbps de conectividad a R1 y 10 Gbps a R3. AS200 garantiza 10 Gbps de conectividad a R4 y AS300 garantiza 1 Gbps de conectividad para R2. Supongamos que, mediante flujos normales R1 logra comunicarse con una velocidad de 1Gbps con R2. Pero, R3 está transmitiendo 10 Gbps a R4, 11 Gbps deberían viajar por un circuito que solo puede transmitir 10 Gbps hacia AS200. Debido a que los enlaces de intercambio de tráfico no están dedicados a un cliente específico, una parte del tráfico va a sufrir algún retraso o a su vez se puede caer. Es decir, que no se puede garantizar el ancho de banda o la latencia mientras que los paquetes viajen a través de enlaces de intercambio de tráfico [2].

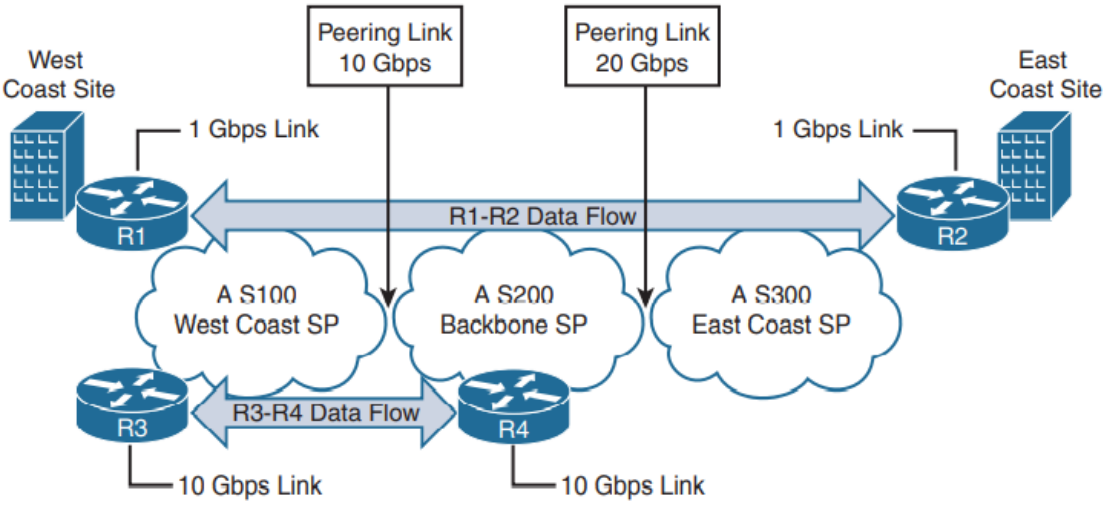


Figura 1.2. El ancho de banda no está garantizado en Internet

1.4.1.2.3 VPN de conmutación de etiquetas multiprotocolo (VPN MPLS)

Los proveedores de servicio utilizan MPLS ya que esta permite proporcionar una arquitectura peer – to – peer escalable que proporciona un método dinámico de tunelización para que los paquetes puedan ser transmitidos sin tener que mirar el contenido del mismo. Los SP pueden garantizar niveles específicos de QoS a los clientes, los mismos que son encargados de establecer los precios que van a ir en función del nivel de servicio (SLA), este va a especificar el ancho de banda, QoS, latencia de un extremo a otro, tiempo de actividad y garantías adicionales. Este precio va a ser muy alto y poco accesible para la mayoría de las empresas ya que este va a depender de las demandas en los SLA, es decir si se desea una red mucho más segura y confiable el precio va a ser alto[2].

1.4.1.3 Aumento de la demanda de las WAN empresariales

1.4.1.3.1 Consolidación y virtualización de servidores

Las CPU de los servidores cada vez son más rápidas, lo cual posibilita que los servidores logren realizar un mayor procesamiento. El personal que se encuentra a cargo del departamento de tecnología de la información pudo darse cuenta que la consolidación de servidores tanto de archivos como de correo electrónico tenía un menor consumo de recursos tales como la energía, red, servidores y personal, así mismo se tenía una disminución de los costos operativos. Cuando se logró la virtualización de servidores las empresas empezaron a virtualizar los servidores físicos en máquinas virtuales, lo cual genero un efecto no deseado, ya que la utilización de la WAN aumentó pues los servidores no se localizaban en las sucursales, sino en los centros de datos (DC). [2]

1.4.1.3.2 Servicios basados en la nube

Los encargados de asumir los costos al momento en que se realice la recuperación ante desastres son los proveedores de servicios de la nube, las licencias, el personal y el hardware brindan flexibilidad con un costo menos hacia sus clientes. Este valor puede ser distribuido a lo largo del contrato. Una ventaja de este servicio es que si se necesita cambiar de proveedor no se va a tener el mismo imparto financiero comparado con implementar una aplicación con recursos internos[2].

Para poder lograr una conectividad con los proveedores de la nube es necesario que se establezcan circuitos dedicados o también a su vez mediante portales de internet. Al momento de utilizar los circuitos dedicados se pueden gestionar los aspectos de seguridad de la aplicación en el punto de conexión, mientras que al utilizar internet se puede brindad

la misma experiencia a los empleados, ya sea que estén trabajando en la oficina o de forma remota[2].

1.4.1.3.3 Servicios de colaboración

Antiguamente las empresas utilizaban una red para voz y una red para datos informáticos. Las llamadas telefónicas que se tenían que realizar de una ciudad a otra estaban definidas como de larga distancia, las mismas que las compañías telefónicas las cobraban por minuto a la parte que iniciaba la llamada[2].

Para poder reducir los costos las empresas empezaron a usar voz sobre IP (VoIP) para poder realizar las llamadas telefónicas. Esto quiere decir que las empresas no tenían que mantener circuitos de voz y datos entre los sitios, lo que se empezó a utilizar son los circuitos WAN para no incurrir en cargos de larga distancia por minuto[2].

Tanto el tráfico de voz como de video necesitan ser priorizados en una red. La latencia que puede existir entre los puntos finales al trasmitir voz tiene que ser inferior a 150 ms, mientras que el tráfico de video es más tolerante a la latencia. Aun cuando la latencia resulta ser molesta no imposibilita la comunicación. Si la pérdida de paquetes, la fluctuación o la latencia son demasiado altas, se va a reducir drásticamente la efectividad[2].

1.4.1.3.4 Bring your own device (BYOD)

Desde el 2010 los trabajadores de las empresas comenzaron a utilizar sus computadoras personales, teléfonos inteligentes y tablets para realizar su trabajo. Empresas permitieron esto ya que mediante estudios lograron anticipar un aumento en la productividad y un ahorro de costos[2].

Debido a que los dispositivos que los trabajadores llevan no pueden ser administrados de forma centralizada, las empresas tienen que tomar medidas para que su propiedad intelectual no se vea comprometida. Si una red está diseñada correctamente los dispositivos BYOD van a estar separados de los dispositivos que son administrados por la empresa[2].

Al momento que sea necesario actualizar las aplicaciones o el sistema operativo en los dispositivos se va a consumir ancho de banda que es utilizado por las aplicaciones relacionadas con la empresa. La mayoría de los trabajadores conectan sus dispositivos a la red de la empresa únicamente para evitar las tarifas de uso de datos que están asociados con sus proveedores de servicios inalámbricos[2].

1.4.1.3.5 Acceso a Internet para invitados

Existen dos razones por las cuales las empresas ofrecen redes de invitados, la conveniencia y la seguridad[2].

- **Conveniencia:** Por lo general las empresas proporcionan a socios y visitantes acceso a internet para su comodidad. Esta conectividad permite tener acceso a la red de la empresa ya sea para usar correo electrónico, acceso a las VPN para el uso de archivos[2].
- **Seguridad:** Se tiene que separar los recursos corporativos seguros de los dispositivos que no son administrados[2].

2 CISCO INTELLIGENT WAN (iWAN)

Una parte muy importante que existe en las comunicaciones entre oficinas remotas y clientes son las redes WAN, es más ahora se puede decir que la supervivencia de las empresas va a depender de la disponibilidad y el rendimiento de la red. La única forma que existía para poder lograr una conectividad confiable y tener un rendimiento predecible es que se aproveche la WAN privada usando MPLS o bien un servicio de línea alquilada. Lamentablemente el alto costo de estas tecnologías hace que no sean rentables para que una organización las utilice, peor aún con el aumento en la exigencia de ancho de banda para la conectividad de sitios remotos[3]. La mayoría de administradores de red no descartarían la oportunidad de reducir el costo de operación de una red de área amplia mientras se mantenga o mejore el rendimiento. Estas capacidades existen en forma de WAN inteligente [7].

Antes que la empresa CISCO proponga la tecnología Cisco Intelligent WAN (iWAN), las empresas utilizaban la optimización de la WAN, que son soluciones en las cuales permiten administrar y acelerar el flujo de datos a los administradores, a través de una red de área amplia; para lograr lo antes mencionado se utilizan técnicas como la compresión de datos, almacenamiento en caché y tunelización de red privada virtual (VPN). Estas técnicas permiten priorizar el tráfico y garantizar una cantidad de ancho de banda para aplicaciones que transporten tráfico crítico[7].

La tecnología Cisco Intelligent WAN (iWAN) va más allá que la optimización de la WAN, ofrece a los administradores muchas más formas de maximizar el rendimiento de las redes de área amplia[7]. Permite a las empresas utilizar alternativas de transporte WAN con un

menor costo, sin que la confiabilidad, la seguridad o el rendimiento se vean afectados, para así poder ofrecer un mayor ancho de banda. En Cisco Intelligent WAN (iWAN) el tráfico es enrutado dinámicamente y esto dependerá del acuerdo de nivel de servicio (SLA). iWAN ayuda a que las empresas puedan ahorrar, estos ahorros permiten pagar las actualizaciones de la infraestructura además que también recursos son liberados para que la empresa pueda innovar[1].

2.1 CASOS DE USO EMPRESARIAL PARA iWAN

Las empresas necesitan que la WAN proporcione suficiente rendimiento y confiabilidad para que los usuarios de sitio remoto puedan realizar su trabajo de forma efectiva y así ser un apoyo para el negocio. El diseño de la WAN debe brindar una experiencia común de acceso a los recursos, sin que la ubicación en la que se encuentren los trabajadores tenga gran importancia [1].

2.1.1 COMUNICACIONES WAN SEGURAS DE SITIO A SITIO[1]

Ayuda a las empresas a conectar sitios remotos a través de redes IP privadas (MPLS) y públicas (Internet) de manera eficiente y segura.

Algunas de las siguientes capacidades de red son:

- Comunicaciones seguras y cifradas para hasta 2000 ubicaciones mediante el uso de una configuración de superposición de túnel Ipsec de VPN multipunto dinámico (DMVPN)
- Una solución de alojamiento múltiple que puede tener dos o más opciones de conectividad para el uso eficiente de todo el ancho de banda WAN, utilizando enrutadores simples o duales en ubicaciones remotas.
- QoS para tráfico WAN como voz, video, aplicaciones de datos críticos, aplicaciones de datos masivos y tráfico de administración.

2.1.2 ESCALA Y ALTA DISPONIBILIDAD [1]

Ayuda a las organizaciones a escalar sus implementaciones de iWAN más allá de un enrutador de borde de hub único por DMVPN.

Algunas de las siguientes capacidades de red son:

- Escalabilidad horizontal a través de múltiples enrutadores de borde en un solo DMVPN para utilizar toda la capacidad WAN.

- Si falla el canal actual se va a buscar un canal alternativo en la misma red.
- Controlador maestro concentrador redundante mediante Anycast IP

2.1.3 MÚLTIPLES TRANSPORTES WAN [1]

Ayuda a las organizaciones a escalar sus implementaciones de iWAN más allá de un solo par de transportes WAN en un punto de presencia (POP).

Algunas capacidades son:

- Hasta nueve transportes WAN en cada punto de presencia (POP) con uno designado como ruta de último recurso
- Convergencia entre transportes WAN cuando todos los canales de un transporte determinado fallan o alcanzan sus límites de ancho de banda máximo
- Hasta tres transportes WAN en un sitio remoto de un solo enrutador.
- Hasta cinco transportes WAN en un sitio remoto de doble enrutador.

2.1.4 MÚLTIPLES INSTANCIAS DE ENRUTAMIENTO Y REENVÍO VIRTUAL[1]

Ayuda a las empresas a segmentar su tráfico a través de su WAN utilizando múltiples instancias de enrutamiento y reenvío virtual (VRF) en la superposición de sus transportes WAN.

Algunas capacidades son:

- Aislamiento de tráfico de un extremo a otro
- Hasta veinte VRF en un sitio de tránsito
- Hasta siete VRF en un sitio remoto

2.2 MODELOS DE IMPLEMENTACIÓN DE CISCO iWAN

La tecnología Cisco Intelligent WAN (iWAN) posee algunos modelos mediante los cuales puede ser implementada esta tecnología, pero existen tres principales como podemos observar en la figura 2.1 [2].

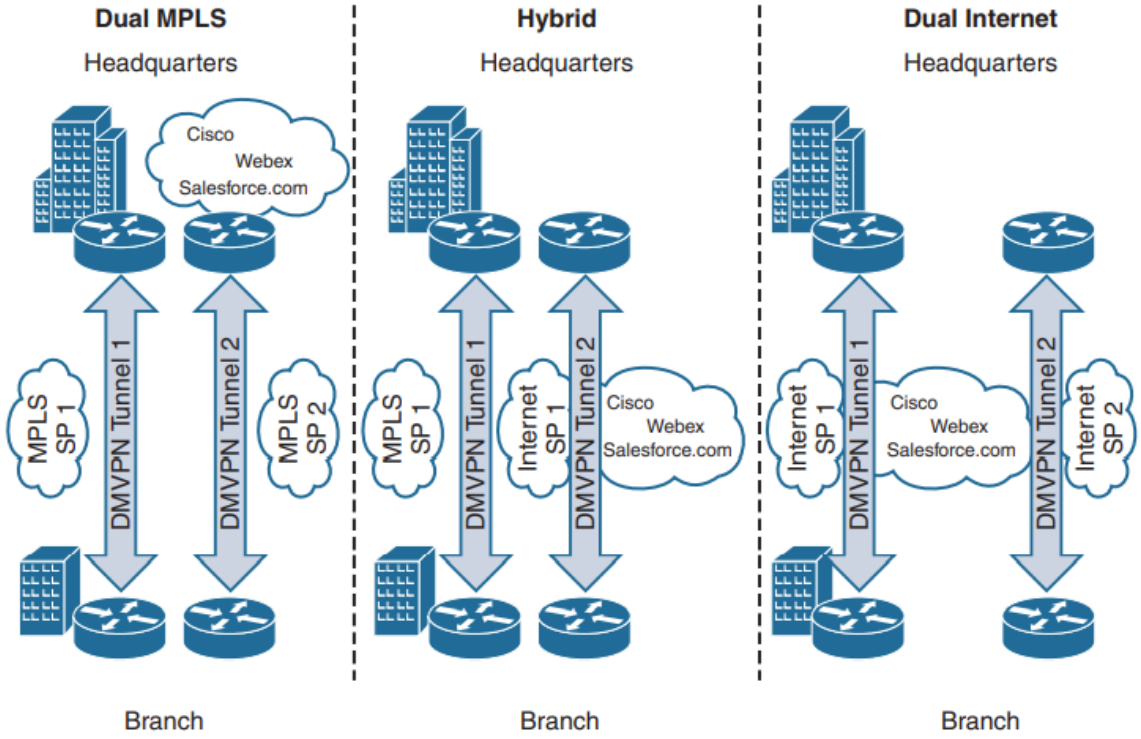


Figura 2.1 Modelos de diseño de Cisco iWAN[8]

Cada uno de estos modelos tiene la capacidad de escalar hasta 2000 sitios remotos, ya que la arquitectura iWAN no limita el diseño de la WAN. Un ejemplo es que se puede utilizar dos SP diferentes los cuales pueden ofrecer transporte VPN MPLS y un tercer SP que puede proporcionar conectividad a internet. Cada uno de los transportes van a usar DMVPN que ayudará a mantener el enrutamiento y a que la topología sea consistente[2].

2.2.1 iWAN HIBRIDO

Este modelo usa MPLS con Internet como transportes WAN, este es el diseño que se implementa más comúnmente. Este diseño permite que el tráfico crítico sea transportado utilizando MPLS mientras que el tráfico que no es crítico utiliza internet para su transporte. Esto ayuda a que se obtenga un mejor rendimiento sin la necesidad de aumentar el ancho de banda, de igual forma, se van a reducir los costos al momento en que sea utilizado el ancho de banda de internet, ya que este tiene un menor precio[1].

Características:

- Utiliza al menos un portador MPLS
- Utiliza al menos un operador de Internet

- Utiliza front – door virtual routing and forwarding (FVRF) tanto en MPLS como en Internet, con enrutamiento estático predeterminado en FVRF.
- Puede escalar a 2000 sitios remotos.

En la figura 2.2 podemos observar el modelo de diseño híbrido de iWAN.

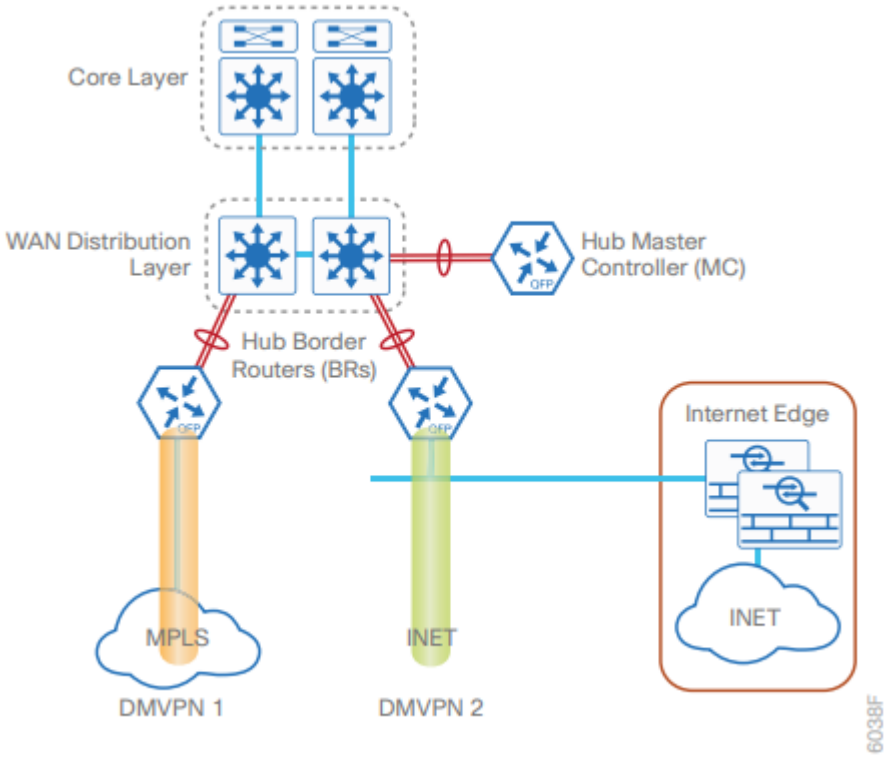


Figura 2.2 Modelo de diseño híbrido iWAN[1]

2.2.2 INTERNET DUAL iWAN

Este diseño tiene un costo recurrente menor, ya que al usar internet no existen garantías de ancho de banda la empresa tiene que proporcionar el SLA. En este modelo se tiene que determinar la ruta por donde se va a transportar el tráfico crítico, por lo general esta ruta va a ser escogida dependiendo el proveedor que tenga más ancho de banda; aunque también se puede ser elegido dependiendo de las resoluciones de emparejamiento más favorables o a su bien en la que se tenga conexiones directas en la mayoría de sus sitios remotos [1].

Características:

- Utiliza al menos dos operadores de internet

- Utiliza FVRF en ambos enlaces de internet, con enrutamiento predeterminado estático dentro de FVRF
- Puede escalar a 2000 sitios remotos

En la figura 2.3 podemos observar el modelo de diseño de Internet dual iWAN.

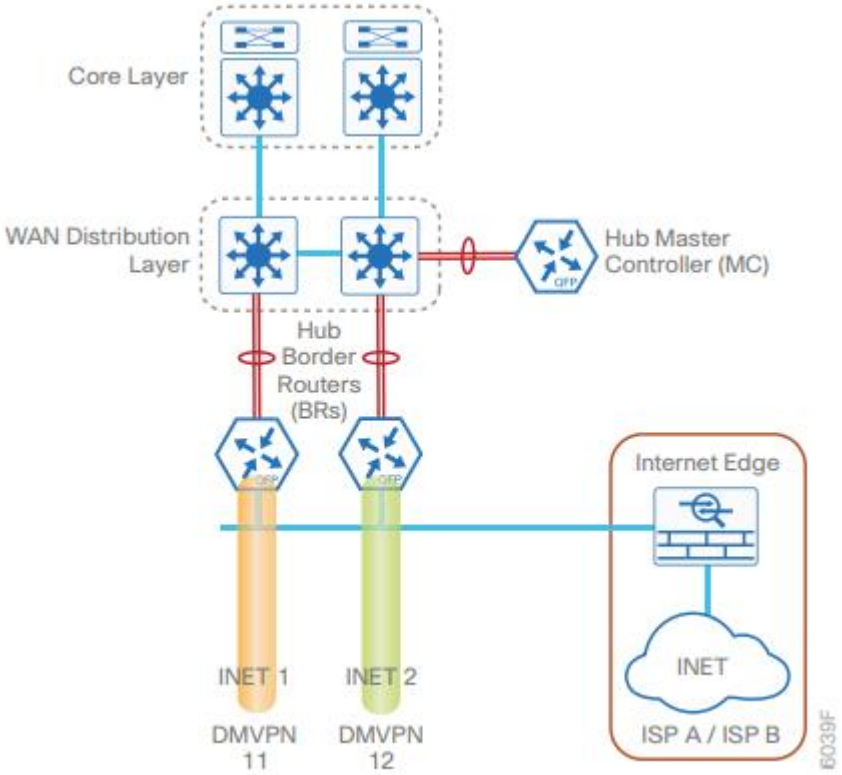


Figura 2.3. Modelo de diseño de Internet dual iWAN[1]

2.2.3 MPLS DUAL

En este diseño se tienen dos transportes VPN MPLS los cuales pueden ser proporcionados cada uno por distintos SP, en el caso de que los dos proveedores de servicio utilicen el mismo tipo de VPN MPLS va a ser posible utilizar el mismo protocolo de enrutamiento[2].

2.3 COMPONENTES iWAN

2.3.1 INDEPENDENCIA DE TRANSPORTE

La principal idea detrás de este componente que es la independencia de transporte es que cuando sea posible y apropiado el tráfico puede y tiene que ser trasladado a enlaces de Internet menos costosos, sin que se vea comprometida la seguridad, confiabilidad o

desempeño. La independencia de transporte tiene la capacidad de ofrecer a los administradores de la red la opción de distribuir el tráfico de las diferentes sucursales a través de múltiples opciones de transporte tales como son MPLS, redes WAN móviles e Internet, mientras se mantiene un dominio de enrutamiento. Los sellos distintivos de este componente incluyen la flexibilidad del proveedor, el diseño modular y escalable [7].

La independencia de transporte se fundamenta en tecnologías que incluyen la Dynamic Multipoint Virtual Private Network (DMVPN) y la seguridad del protocolo de Internet (IPSec). DMVPN es una solución de software que ofrece cisco la cual utiliza una arquitectura centralizada que ayuda a que se facilite la implementación con las comunidades de usuarios, esta tecnología ayuda a que las sucursales puedan comunicarse directamente mediante la WAN pública o Internet siempre y cuando se utilicen aplicaciones como Voice over IP, sin que sea necesario utilizar una VPN permanente entre los sitios. El uso de la tecnología de cifrado IPSec brinda un alto nivel de autenticación y seguridad gracias al uso de cifrado[7].

Cisco iWAN VPN multipunto dinámico (DMVPN) logra proporcionar independencia de transporte mediante enrutamiento superpuesto. El enrutamiento superpuesto simplifica el plano de control para cualquier transporte WAN, lo que permite a las organizaciones implementar un diseño de enrutamiento consistente en cualquier transporte y facilita un mejor control del tráfico y distribución de carga, y admite protocolos de enrutamiento, eliminando cualquier barrera para equal cost multipatbing (ECMP). El enrutamiento superpuesto tiene la capacidad de brindar independencia de transporte para que un cliente tenga la capacidad de poder seleccionar la tecnología WAN que más se ajuste a sus necesidades tales como: VPN MPLS, Internet directo, metro ethernet, high speed radios. La independencia de transporte facilita la combinación de opciones de transporte o el cambio de proveedor de servicio para cumplir con los requisitos comerciales.

Un ejemplo puede ser cuando una nueva sucursal necesita conectividad de red. La instalación de un circuito físico puede llegar a tardar entre seis a doce semanas, si el pedido no se lo realiza lo suficientemente pronto o se encuentran complicaciones, la conectividad WAN para la sucursal se retrasa. La independencia de transporte de Cisco iWAN permite el uso temporal de un módem celular hasta que se realice la instalación del circuito físico sin requerir cambios en la configuración del protocolo de enrutamiento del enrutador, porque DMVPN reside en la parte superior del transporte celular. El cambio de transporte no afecta el diseño de enrutamiento superpuesto. [2]

2.3.1.1 BENEFICIOS DE LA INDEPENDENCIA DE TRANSPORTE

Cada uno de los transportes pueden usar el protocolo de enrutamiento que más se adapte a sus necesidades. Se tiene que tener en cuenta que algunos medios de transporte no van a estar siempre disponibles o a su bien no son rentables en todos los lugares. [2]

El personal que este encargado de la arquitectura de red tiene que planificar los circuitos de respaldo ya sea que estén activos únicamente cuando falla el circuito principal, o a su bien circuitos dobles que puedan ser usados al mismo tiempo. También hay que decidir el número de enrutadores que van a ser ubicados en cada sitio, o si un enrutador está dedicado a cada circuito o si deben conectarse al mismo enrutador.[2]

Al usar un solo enrutador con un solo transporte este va a proporcionar un 99,9% de disponibilidad, lo que significa que puede tener entre cuatro y nueve horas de tiempo de inactividad al año. Si se usa un solo enrutador, pero ahora con dos transportes va a proporcionar un 99,995% de disponibilidad, lo que corresponde a 26 minutos de tiempo de inactividad al año. Si se tienen dos enrutadores y cada uno con su propio transporte se va a obtener un 99,999% de disponibilidad lo que corresponde a cinco minutos de tiempo de inactividad al año.[2]

DMVPN utiliza enrutamiento superpuesto de malla completa para poder proporcionar independencia de transporte. Esta tecnología ayuda a que las organizaciones puedan utilizar numerosos transportes WAN, puesto que el tipo de transporte está asociado con la red subyacente y es irrelevante para la red superpuesta. La red superpuesta es coherente y normalizada con el túnel DMVPN. [2]

La independencia de transporte proporciona lo siguiente:

- **Dominio de enrutamiento único:** Los protocolos de enrutamiento son encargados de elegir la mejor ruta en función del costo asignado estáticamente. Ya que DMVPN presenta una topología plana, proporciona una topología consistente que permite el equilibrio de carga del protocolo de enrutamiento Multipath de igual coste (Equal cost multi-path, ECMP) en los túneles DMVPN. [2]
- **Solución de problemas coherente:** Este proceso puede ser utilizado para solucionar problemas de conectividad para el túnel DMVPN y también para la red subyacente. A pesar de que el transporte subyacente cambia, estas se basan en la conectividad IP básica entre los puntos finales del túnel.[2]

- **Topología consistente:** Existe una topología y una metodología coherentes para implementar otros servicios, como el enrutamiento de rendimiento.[2]

En la figura 2.4 R1 y R2 utilizan un túnel DMVPN para cada ruta diferente. Es posible usar el mismo protocolo de enrutamiento en cada una de las rutas mientras se mantenga una topología consistente. También es posible realizar un cambio en las rutas de WAN sin que se afecte el diseño general de la WAN. [2]

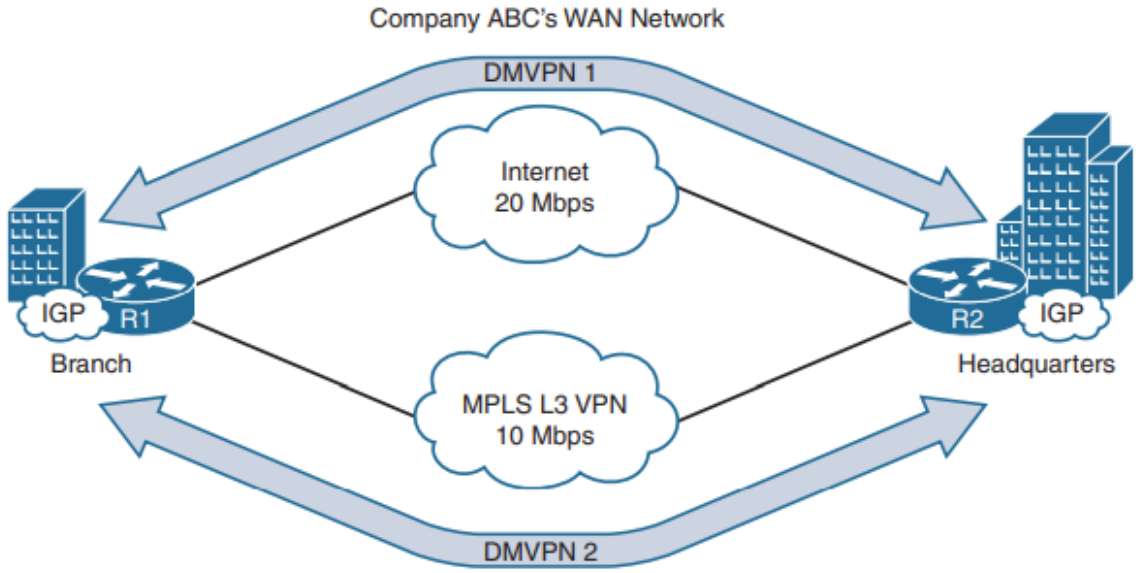


Figura 2.4. Simplificación con Independencia de Transporte. [2]

Un ejemplo de uso para la independencia de transporte es el caso en el que una empresa tenga que implementar una nueva sucursal. Para poder instalar nuevos circuitos un proveedor de servicio puede tardar entre 60 a 90 días. Pero una empresa puede realizar la implementación de un enrutador usando un plan de datos móviles y posteriormente cambiarlo al circuito solicitado realizando cambios mínimos en la configuración. El modelo de soporte operativo va a ser el mismo sin importar la ruta WAN que sea utilizada.[2]

2.3.2 CONTROL DE RUTA INTELIGENTE

Los enrutadores son los encargados de enviar los paquetes dependiendo de la dirección de destino, el cálculo de la ruta va a depender de que protocolo de enrutamiento sea utilizado. Estos protocolos no son capaces de tomar en cuenta la pérdida de paquetes, el retraso o la utilización del enlace mientras se está calculando la ruta; esto puede provocar que se use de una manera incorrecta la ruta para una determinada aplicación. [2]

Este componente es considerado como el central de iWAN ya que este posee una herramienta poderosa como es el Performance Routing (PfR). Esta herramienta es capaz

de proporcionar un control de ruta inteligente en función de la aplicación. Dependiendo del tipo de tráfico esta herramienta va a ser la encargada de supervisar el rendimiento de la aplicación, además tiene la capacidad de elegir la mejor ruta para reenviar los paquetes de dicha aplicación. Si llega a suceder que la ruta se vuelva inaceptable, PfR es capaz de modificar la ruta para dicha aplicación hasta que la ruta original se encuentre nuevamente dentro de las especificaciones de la aplicación. Es decir, PfR se asegura que la ruta por la cual se esté transmitiendo la información cumpla con los requisitos establecidos para esa aplicación.[7]

PfR ha tenido algunas mejoras para que pueda ser apto para el control de ruta inteligente de Cisco, se ha integrado con DMVPN para poder convertirse en un componente vital de la arquitectura iWAN. Proporciona una supervisión de aplicaciones mejorada, una convergencia más rápida y una configuración centralizada simple. [2]

Para poder obtener una red de alta disponibilidad es necesario realizar algunos cambios, uno de ellos es la eliminación de los puntos únicos de falla (SPoF). El segundo circuito a más de brindar redundancia, es capaz de proporcionar ancho de banda adicional gracias a la independencia de transporte y PfR. Esto ayuda a que los gastos operativos de la WAN puedan reducirse sin importar el modelo de implementación de iWAN. [2]

En la figura 2.5 se puede observar un ejemplo de topología, la cual proporciona conectividad de R1 a R5 a través de dos rutas diferentes. Tanto R1 como R5 han logrado identificar el túnel DMVPN 100 como la mejor ruta gracias al protocolo de enrutamiento utilizado, por lo que continúan enviando información VoIP hasta la capacidad límite de ese túnel. Como R1 también usa ese túnel para enviar archivos, la cantidad total de tráfico de red excede la capacidad de ancho de banda del túnel 100. Gracias a las políticas de QoS se puede garantizar que el tráfico de VoIP no se vea afectado, mientras que el tráfico de archivos si sea afectado. El túnel DMVPN 200 podría usarse para poder transferir el tráfico afectado, es decir transferir archivos con control de ruta inteligente. PfR logra que ambos túneles DMVPN sean utilizados sin que los paquetes sean descartados. [2]

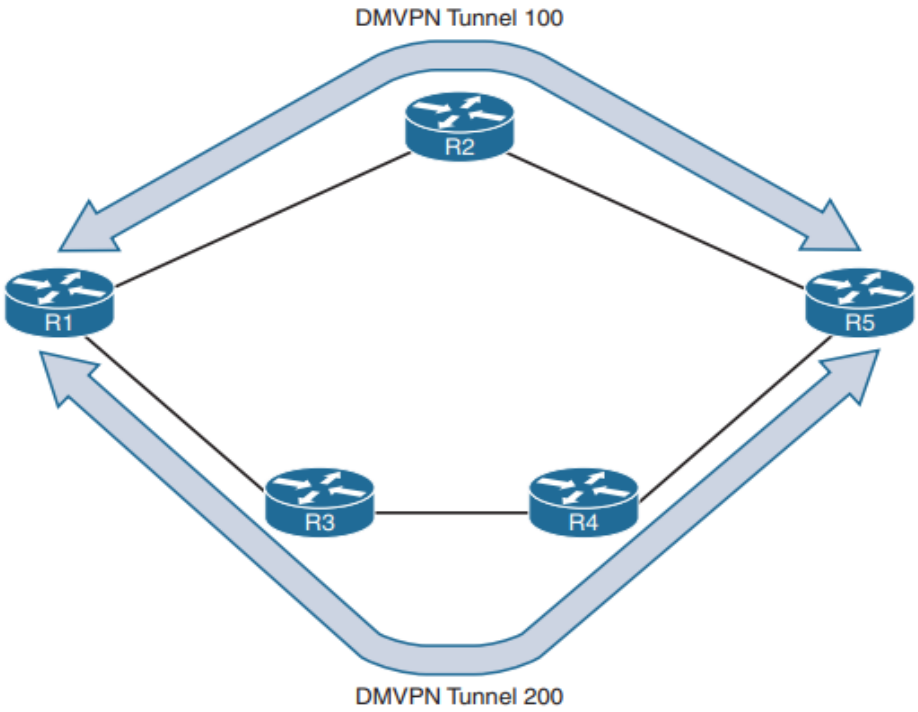


Figura 2.5. Optimización con control de ruta inteligente.[2]

Los protocolos de enrutamiento clásicos o el control de ruta con enrutamiento basado en políticas (PBR) no son capaces de detectar problemas de rendimiento por lo que retroceden el tráfico afectado a una ruta alternativa. El control de ruta inteligente es capaz de resolver este problema ya que monitorea el rendimiento real de la aplicación en la ruta que están atravesando para así poderla dirigir por la ruta adecuada. [2]

Al momento en que la ruta actual sufra de una degradación de rendimiento, el control de ruta inteligente de Cisco va a ser el encargado de mover los flujos afectados tomando en cuenta las políticas que fueron definidas por el usuario. [2]

En la figura 2.6 podemos observar otro ejemplo en el cual R31 envía tráfico a R11, al momento que la ruta que utiliza MPLS empieza a experimentar problemas de rendimiento, únicamente el tráfico afectado va a ser enviado por la otra ruta que es la de Internet. Por ejemplo, los flujos de aplicaciones comerciales o de voz van a ser reenviados por la ruta secundaria, mientras que el tráfico de mejor esfuerzo va a permanecer en la ruta MPLS. [2]

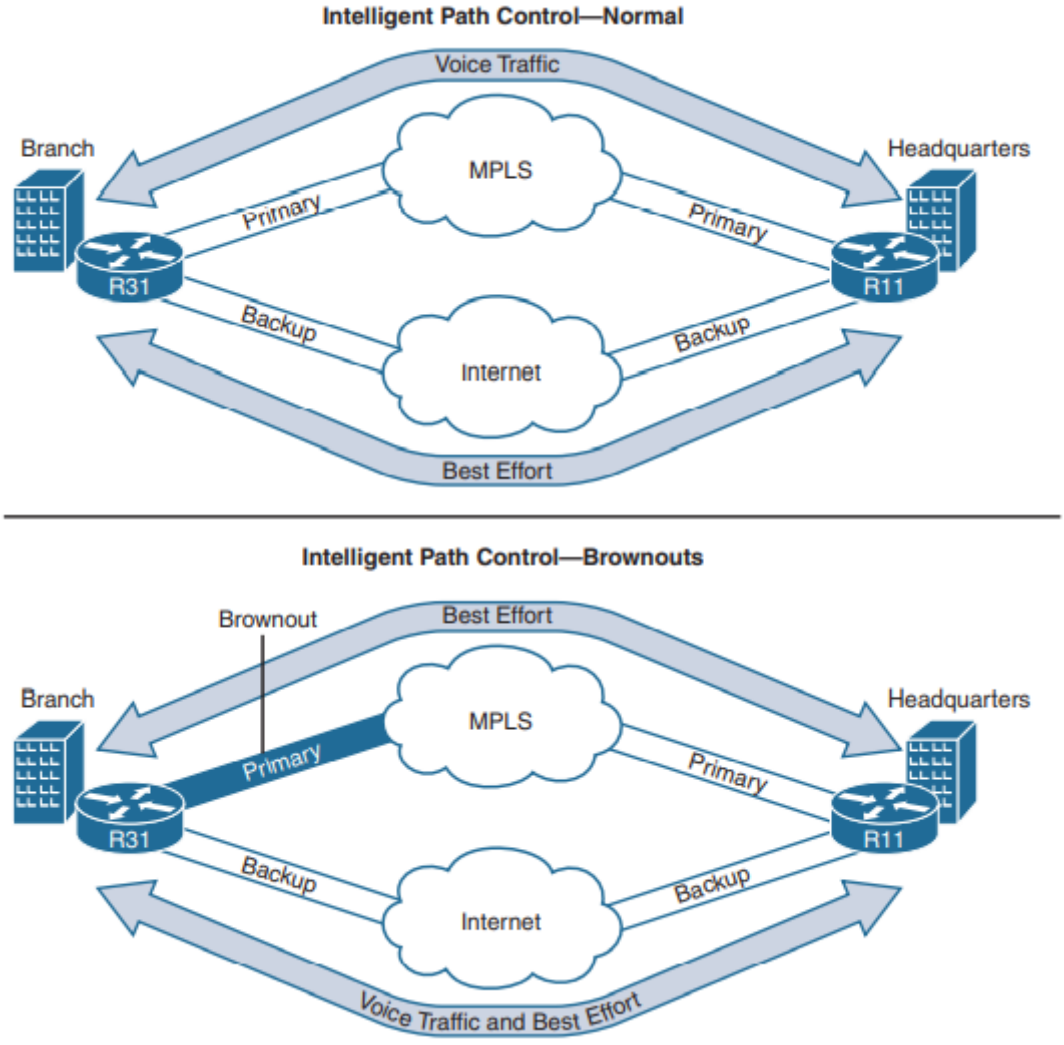


Figura 2.6. Flujo de tráfico a través de múltiples enlaces con Cisco Intelligent Path Control[2]

2.3.3 OPTIMIZACION DE APLICACIONES

La mayoría de usuarios creen que en una WAN la capacidad de respuestas de las aplicaciones está directamente relacionado únicamente con el ancho de banda que se encuentra disponible en el enlace de red. Esta es una idea incorrecta ya que la capacidad de respuesta de la aplicación está directamente asociada con las siguientes variables: ancho de banda, latencia de la ruta, congestión y comportamiento de la aplicación. [2]

La mayoría de aplicaciones han sido diseñadas para entornos LAN los cuales proporcionan enlaces de alta velocidad que no poseen congestión. Estas aplicaciones no toman en cuentan las características de la red, es decir, dependen de protocolos subyacentes como TCP para que puedan comunicarse entre computadoras. Algunas aplicaciones transmiten

paquetes de ida y vuelta, lo que hace necesario que se realice un reconocimiento en cada dirección.[2]

Existen dos tecnologías que proporcionan una solución completa para lograr superar las variables que puedan llegar a afectar el rendimiento de las aplicaciones en un circuito WAN, son Cisco Wide Area Application Service (WAAS) y Akamai Connect. [2]

Cisco WAAS agrega la eliminación de la redundancia da datos (DRE), esta tecnología ayuda a identificar los patrones de datos en el tráfico de la red para poder reducirlos a medida que los paquetes van atravesando la red. Cisco WAAS va a ser el encargado de examinar los paquetes, buscar patrones en incrementos de 256 bytes, 1 KB, 4KB y 16 KB, y crear una firma para cada uno de esos patrones. Si se envía un patrón por segunda vez, el primer dispositivo WAAS va a reemplazar los datos con una firma. La firma va a ser enviada a través del enlace WAN y el segundo dispositivo WAAS va a ser el encargado de reemplazar la firma con los datos. Este proceso va a lograr que se reduzca el tamaño del paquete drásticamente mientras que va cruzando por la WAN, manteniendo la carga útil original entre los dispositivos de comunicación. [2]

Tanto Cisco WAAS como Akamai Connect proporcionan un método para almacenar objetos localmente en caché. Al almacenar el contenido repetido localmente en caché se va a poder reducir la latencia en aplicaciones de conversación. [2]

2.3.4 CONEXIÓN SEGURA

Como ya sabemos el objetivo principal de los enrutadores es reenviar los paquetes a un destino. Además, los enrutadores corporativos que poseen acceso directo a Internet tienen que estar correctamente configurados para protegerlos de personas externas malintencionadas, de esta manera los usuarios pueden acceder a Internet mientras que los dispositivos externos solo pueden acceder a recursos corporativos apropiados. Algunos componentes de conectividad segura de iWAN. [2]

Cortafuegos basado en zonas

Para poder filtrar el tráfico de red en un enrutador se utiliza las listas de control de acceso (ACL). Va a controlar el acceso dependiendo del protocolo, los puertos utilizados, la dirección IP de origen y la dirección IP de destino. Al no tener estado los paquetes no son inspeccionados para poder detectar si los piratas informáticos están usando un puerto que han encontrado abierto.[2]

Los firewalls con estado pueden examinar desde la cuarta hasta la séptima capa de un paquete de red y así poder verificar el estado de la transmisión. También puede detectar

si un puerto está superpuesto y así poder realizar una denegación de servicio distribuida (DDoS), es decir, mitigar intrusiones. [2]

Cisco posee un firewall con estado que ya viene integrado en los enrutadores el cual reduce la necesidad de un segundo dispositivo de seguridad, este es el Firewall basado en zonas (ZBFW). Como Cisco ZBFW utiliza una configuración basada en zonas, las interfaces del enrutador son asignadas a zonas de seguridad específicas y posteriormente el tráfico entre zonas va a ser aceptado o denegado dependiendo de la política de seguridad. Este modelo proporciona flexibilidad y supera la carga administrativa de los enrutadores con múltiples interfaces en la misma zona de seguridad.[2]

Seguridad web en la nube

Para la mayoría de las empresas es muy importante garantizar una política de seguridad coherente para el acceso distribuido a Internet para así evitar problemas para la red. Para evitar inconvenientes se implementan un dispositivo de seguridad de contenido en cada ubicación, lo que va a generar un costo adicional de hardware y va a aumentar la administración de los dispositivos de seguridad.[2]

Los enrutadores Cisco iWAN al conectarse a Cisco Cloud Web Security (CWS) logran utilizar el acceso distribuido a Internet al mismo tiempo que proporcionan una política de seguridad coherente y administrada de forma centralizada. Cisco CWS proporciona seguridad contra amenazas y malware sin la necesidad de comprar y administrar un dispositivo de seguridad dedicado para cada sucursal.[2]

Es decir, todo tráfico HTTP o HTTPS que va a salir a través de la WAN se va a redirigir hacia algún centro de datos globales de CWS el que esté más cerca. Ahí se va a verificar la política de acceso dependiendo del usuario, la ubicación o el dispositivo que está realizando esa solicitud para así poder verificar el acceso adecuado a Internet. Todo el tráfico va a ser analizado en búsqueda de posibles amenazas a la seguridad.[2]

3 DYNAMIC MULTIPOINT VIRTUAL PRIVATE NETWORK (DMVPN)

Dynamic Multipoint (DMVPN) es una solución de la empresa Cisco que es capaz de proporcionar una arquitectura VPN que sea escalable. Es una red segura capaz de intercambiar datos entre enrutadores sin que el tráfico tenga pasar a través del servidor o enrutador de la red privada virtual (VPN) de una organización ubicada en su sede. DMVPN

ayuda a las organizaciones a obtener una red VPN con múltiples sitios, sin que se tenga que configurar dispositivos de forma estática. [9][10][2]

Cisco DMVPN es usado para combinar sucursales empresariales, teletrabajadores y conectividad de extranet. DMVPN crea una topología VPN en malla, en esta malla el enrutador de cada sitio remoto va a poder conectarse al dispositivo hub VPN de la empresa para así poder tener acceso a los recursos necesarios. Cada sitio remoto va a tener la capacidad de conectarse directamente con los demás sitios remotos sin que su ubicación tenga importancia y sin tener que pasar por el hub. [9][10][2]

Los administradores de red pueden obtener los siguientes beneficios al momento de usar DMVPN: [9][10][2]

- **Aprovisionamiento sin contacto:** Los hubs DMVPN no requieren de una configuración adicional al momento que se añaden spokes adicionales.
- **Despliegue escalable:** La red va a poder ser escalable ya que esta no se encuentra condicionada por el dispositivo (lógico, físico o virtual).
- **Túneles Spoke and Spoke:** DMVPN es capaz de brindar conectividad de malla completa únicamente configurando el túnel inicial del spoke al hub. Los túneles dinámicos de spoke a spoke solo van a ser creados cuando sea necesario y al momento que no sean necesarios se los van a derribar. Un spoke va a poder reenviar información únicamente con los spokes que se está comunicando.
- **Topologías de red flexibles:** Para evitar congestión o un punto único de falla, el plano de control DMVPN se puede utilizar en un modelo resistente y altamente distribuido que va a permitir que se obtenga una escala masiva.
- **Soporte multiprotocolo:** DMVPN admite MPLS, IPv4 e IPv6 como protocolos de red de superposición o transporte.
- **Soporte de multidifusión:** DMVPN soporta que el tráfico de multidifusión fluya a través de las interfaces del túnel.
- **Conectividad adaptable:** Los enrutadores DMVPN logran establecer conectividad detrás de Network Address Translation (NAT). Los enrutadores radiales son capaces de utilizar las direcciones IP dinámicas, también pueden utilizar Dynamic Host Configuration Protocol (DHCP).

- **Bloques de construcción estandarizados:** DMVPN utiliza tecnologías estandarizadas por la industria para construir una red superpuesta tales como NHRP, GRE e IPsec. Esto ayuda a que se minimice la curva de aprendizaje y facilite la resolución de problemas.

3.1 CÓMO FUNCIONA UN DMVPN

Gracias a DMVPN vamos a poder comunicar las sucursales utilizando los mismos recursos ya sea a través de una WAN pública o una conexión a Internet. DMVPN es ejecutado en enrutadores VPN y hubs de firewall. En cada sitio remoto se va a tener un enrutador que va a estar configurado para que se pueda conectar al hub VPN de la sede de la empresa. [9][10][2]

Al momento en que dos spokes desean intercambiar datos, por ejemplo, para realizar una llamada de voz sobre IP un spoke se va a comunicar con el hub para así poder obtener la información necesaria sobre el segundo spoke y va a crear un túnel VPN IPsec dinámico entre ellos. Los spokes no van a utilizar una conexión VPN permanente; por lo que se comunicaban a través de un modelo hub and spoke centralizado en el cual se puede aplicar protección VPN y controles de acceso granulares según sea necesario. [9][10][2]

DMVPN es capaz de admitir el cifrado a través de IPsec. Todas estas características hacen a DMVPN una topología popular para poder conectar sucursales a través de Internet. [9][10][2]

3.2 ARQUITECTURA

Al momento de realizar implementaciones de VPN de sitio a sitio ya sea de mediana o gran escala se necesita de soportes para los servicios de red IP avanzados tales como: [10]

- IP Multicast: es utilizado para que las comunicaciones sean mas eficientes y escalables ya sea de uno a muchos por ejemplo la transmisión por Internet o de muchos a muchos por ejemplo las conferencias, y generalmente es necesario para aplicaciones de voz, video y algunas aplicaciones de datos. [10]
- Protocolos de enrutamiento dinámico: son requeridos en todas las implementaciones, excepto en las más pequeñas, o en los diseños en los cuales el enrutamiento estático no es óptimo o manejable. [10]

- QoS: es obligatorio para que el rendimiento pueda ser garantizado y que las aplicaciones de datos, voz y video puedan tener una mayor calidad en tiempo real. [10]

Tradicionalmente, admitir estos servicios requería tunelizar IPsec dentro de protocolos como Generic Route Encapsulation (GRE), que introdujo una red superpuesta, lo que dificultaba la configuración y administración, y limitaba la escalabilidad de la solución. De hecho, IPsec tradicional solo es compatible con IP Unicast, lo que hace que sea ineficiente implementar aplicaciones que involucran comunicaciones de uno a muchos y de muchos a muchos. [10]

En la figura 3.1 podemos observar la arquitectura DMVPN. [9][10][2]

Figura 3.1. Arquitectura Cisco DMVPN. [10]

3.3 COMPONENTES

DMVPN consta de cuatro componentes principales, como podemos observar en la figura 3.2.

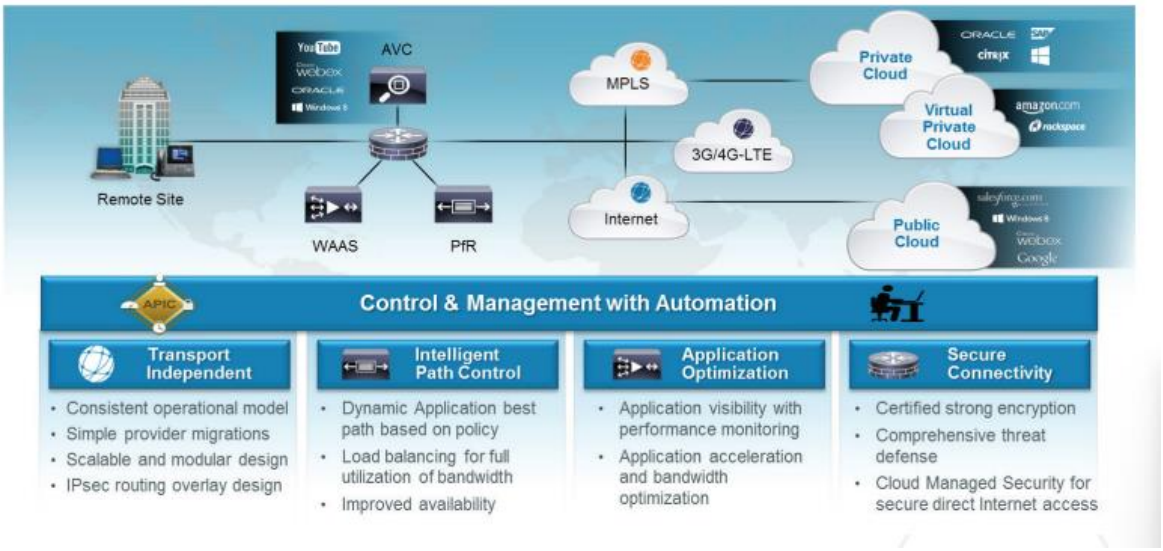


Figura 3.2. Componente de Cisco iWAN

3.3.1 INTERFACES DE TÚNEL GRE MULTIPUNTO

Para una red empresarial en la cual las sucursales necesitan conectarse entre sí, las conexiones a Internet con múltiples interfaces de túnel GRE pueden complicarse y ser difíciles de escalar. DMVPN Y GRE multipunto (mGRE) permiten que se puedan agregar múltiples destinos con solo una interfaz de túnel en cada enrutador. [9][10][2]

Al momento de encapsular y reenviar los paquetes a través de una red basada en IP, el túnel GRE tiene la posibilidad de proporcionar conectividad a una gran cantidad de protocolos de capa de red. Anteriormente los túneles GRE eran utilizados para suministrar un mecanismo de transporte para protocolos heredados no enrutables tales como IPX, Systems Network Architecture (SNA) o DECnet. Una solución instantánea para los malos diseños de enrutamiento o a su bien son utilizados como un método para que el tráfico pase a través de un ACL o firewall, son los túneles GRE. Para que puedan ser eliminados la mayoría de los problemas de soporte que se encuentran asociados con otras tecnologías VPN, DMVPN es capaz de admitir protocolos de enrutamiento dinámico y de utilizar la encapsulación GRE multipunto (mGRE). Los túneles GRE están clasificados como red superpuesta ya que están construidos sobre una red de transporte existente y es conocida como red subyacente. [9][10][2]

Al momento en el que el paquete vaya a ser encapsulado en el enrutador se va a agregar información de encabezado adicional para así poder ser enviado a través del túnel GRE. Esta nueva información que es parte del encabezado posee la dirección IP del extremo remoto como destino. Los nuevos encabezados IP van a permitir enrutar el paquete entre los dos extremos del túnel sin que sea necesario realizar una inspección de la carga útil

del paquete. El momento en el que el paquete llegue al punto final remoto o también llamado destino los encabezados GRE van a ser eliminados y el paquete original va a ser reenviado fuera del enrutador remoto. [9][10][2]

No obstante, si dos enrutadores de sucursales tienen la necesidad de tunelizar el tráfico, es posible que mGRE y GRE no sepan que direcciones IP tengan que usar. Para poder solucionar este problema se utiliza Next Hop Resolution Protocol (NHRP). [9][10][2]

3.3.2 NEXT HOP RESOLUTION PROTOCOL (NHRP)

El protocolo de resolución de próximo salto (NHRP) está definido en RFC 2332 como un método que proporciona la resolución de direcciones para hosts o redes para el acceso múltiple sin difusión (NBMA) tales como Frame Relay y ATM. NHRP es capaz de proporcionar un método para que los dispositivos puedan aprender el protocolo y la red NBMA, lo que les va a permitir comunicarse directamente entre sí. [9][10][2]

NHRP es un protocolo cliente – servidor el cual admite que los dispositivos puedan ser registrados a través de redes dispares o conectadas directamente. Los servidores de siguiente salto (NHS) son los encargados de registrar las direcciones o redes, mantener un repositorio NHRP y responder a cualquier inquietud recibida por parte de los clientes del siguiente salto (NHC). Tanto el NHC y el NHS son de naturaleza transaccional. [9][10][2]

DMVPN utiliza túneles GRE multipunto, el cual necesita de un método de mapeo de direcciones de túnel IP a la dirección IP de transporte (subyacente). NHRP logra proporcionar la tecnología necesaria para mapear esas direcciones IP. Los spokes de DMVPN (NHC) son configurados de forma estática con la dirección IP de los hubs (NHS) para que su túnel pueda ser registrado y la dirección IP de NBMS con los hubs (NHS). Al momento en que se tenga que establecer un túnel spoke to spoke, los mensajes NHRP van a brindar la información que sea necesaria para que los spokes se puedan ubicar entre sí y así poder construir un túnel DMVPN de spoke to spoke. Estos mensajes NHRP también van a permitir que un spoke pueda localizar una red remota. Cisco ha sido el encargado de ir agregando más tipos de mensajes NHRP adicionales a los que ya han sido definidos en RFC2332 para así sean proporcionadas algunas mejoras en DMVPN. [9][10][2]

Todos los paquetes NHRP tienen que incorporar el tipo de mensaje NHRP, dirección del protocolo de origen y el de destino, también la dirección NBMA de origen. La dirección NBMA se refiere a la red de transporte y la dirección del protocolo se refiere a la dirección IP asignada a la red superpuesta, es decir, a la dirección IP del túnel o una dirección de red o host). Los tipos de mensajes NHRP se indican en la tabla 3.1.

Tabla 3.1. Tipos de mensajes NHRP.[2]

Tipo de mansaje	Descripción
Registro	Estos mensajes son enviados por el NHC (spokes de DMVPN) hacia los NHS (hubs de DMVPN). Este registro permite a los hubs conocer la información NBMA del spoke. El NHC también tiene que especificar la cantidad de tiempo que el HNS tiene que mantener ese registro conjuntamente con los otros atributos.
Resolución	En NHRP los mensajes encargados de localizar y proporcionar la información que se necesita para la resolución de dirección del enrutador de salida hacia el destino, son los mensajes de resolución. Se va a enviar una solicitud de resolución durante la consulta real, y esta va a proporcionar una respuesta en la cual se va a obtener la dirección IP NBMA del spoke remoto y la dirección IP del túnel.
Redirigir	Estos mensajes de redireccionamiento son un componente esencial de DMVPN, los cuales permiten que un enrutador intermedio realice una notificación al encapsulador diciendo que se puede llegar a una red específica mediante una ruta más óptima (túnel spoke to spoke). Para que las solicitudes de rendimiento puedan ser suprimidas al transcurrir un período de tiempo específico, el encapsulador tiene que ser capaz de enviar un mensaje de supresión de rendimiento. Este proceso se lo realiza si una ruta más óptima no es factible o la política no lo permite.
Purga	Estos mensajes son enviados para eliminar una entrada NHRP la cual esta almacenada en caché. Los mensajes de purga van a notificar a los enrutadores si una ruta que ha sido utilizada por NHRP ha sido perdida. Usualmente, un NHS va a enviar un mensaje de tipo purga a los NHC para indicar que una dirección que ya había respondido ya no se encuentra válida, un ejemplo puede ser cuando la red no se encuentra disponible desde la estación original o cuando esta se ha cambiado de posición. Estos mensajes de purga van a tomar la ruta más rápida, es decir, el túnel de spoke a spoke únicamente si es posible. Si no está establecido un túnel de spoke a spoke, estos mensajes van a ser reenviados a través del hub.
Error	Estos mensajes de error son utilizados para enviar notificaciones al emisor de un paquete NHRP y así avisar que un error se ha producido.

Los tipos de mensajes antes mencionados son capaces de contener información adicional la cual va a ser incluida en la parte de extensión de un mensaje. En la tabla 3.2 se puede observar las extensiones de mensajes NHRP más comunes. [9][10][2]

Tabla 3.2. Extensiones de mensajes NHRP.[2]

Extensión NHRP	Descripción
Dirección de respuesta	Se utiliza para determinar la dirección del nodo que responde a los mensajes de respuesta
Registro del NHS de tránsito directo	Contiene una lista de NHS que el paquete de solicitud NHRP puedo haber atravesado.
Registro de NHS de tránsito inverso	Contiene una lista de NHS que el paquete de respuesta NHRP puedo haber atravesado.
Autenticación	Esto transmite información de autenticación entro los que se encuentran activos de NHRP. La autenticación se va a realizar por pares, salto por salto. Este campo es transmitido en texto plano.
Proveedor privado	Esta extensión va a transmitir información privada sobre el proveedor entre los que se encuentran activos de NHRP.
NAT	DMVPN va a funcionar cuando un hub o spoke reside detrás de un dispositivo el cual realice NAT y cuando el túnel esté encapsulado en IPsec. Esta extensión NHRP es capaz de detectar la dirección NBMA (dentro de la dirección local) utilizando la dirección de protocolo de origen del paquete NHRP y la dirección IP global interna de los encabezados IP del paquete NHRP en sí.

3.3.3 IPsec TUNNEL ENDPOINT DISCOVERY

Los túneles DMVPN no se encuentran cifrados de forma predeterminada por lo que se utiliza IPsec para poder cifrarlos. IPsec es capaz de proporcionar cifrado a través de seguridad basado en criptografía y fue diseñado tomando en cuenta la interoperabilidad. Al momento en que IPsec se integra con los túneles DMVPN, los túneles DMVPN cifrados van a proporcionar una red superpuesta segura sobre cualquier transporte la cual posee las siguientes funciones: [9][10][2]

- **Autenticación de origen:** La autenticación de origen se puede lograr mediante una clave pre-compartida o mediante autenticación basada en certificaciones.

- **Confidencialidad de los datos:** Se utiliza una variedad de algoritmos de encriptación para preservar la confidencialidad.
- **Integridad de los datos:** Los algoritmos hash aseguran que los paquetes no sean modificados mientras están en tránsito.
- **Detección de repetición:** Esto ayuda a protegernos contra piratas informáticos los cuales intentan capturar e insertar tráfico de red.
- **Cambio de clave periódico:** Se crean nuevas claves de seguridad entre puntos finales cada intervalo de tiempo especificado o dentro de un volumen específico de tráfico.
- **Secreto directo perfecto:** Cada clave de sesión se va a derivar independientemente de la clave anterior. El compromiso de una clave no va a comprometer las claves futuras.

La arquitectura de seguridad IPsec está compuesta de los siguientes componentes independientes:

- Protocolos de seguridad
- Asociaciones de seguridad
- Gestión de claves

3.3.3.1 PROTOCOLOS DE SEGURIDAD

IPsec utiliza dos protocolos los cuales ayudan a proporcionar integridad y confidencialidad de los datos. Estos protocolos pueden ser aplicados individualmente o a su vez combinarse dependiendo de las necesidades. [2]

3.3.3.1.1 Encabezado de autenticación

El encabezado de autenticación de IP es el encargado de proporcionar integridad de datos, autenticación y protección contra piratas informáticos que van a reproducir paquetes. El protocolo de encabezado de autenticación va a garantizar que el paquete de datos original no haya sufrido modificaciones durante el transporte en la red pública. Se va a crear una firma digital similar a una suma de verificación la cual va a garantizar que el paquete no haya sufrido modificaciones, se va a utilizar el número de protocolo 51 que va a estar ubicado en el encabezado IP. [2]

3.3.3.1.2 Carga útil de seguridad encapsulada (ESP) Encapsulating Security Payload

La carga útil de seguridad encapsulada ESP va a proporcionar confidencialidad de datos, autenticación y protección contra piratas informáticos que reproducen paquetes. Por lo general, carga útil se refiere a los datos reales sin los encabezados, pero al hablar de ESP, la carga útil va a ser la parte del paquete original que va a ser encapsulado dentro de los encabezados de IPsec. El protocolo ESP va a garantizar que la carga útil original es decir la que se encuentra antes de que se realice la encapsulación mantenga la confidencialidad de los datos cifrando la carga útil y agregando un nuevo conjunto de encabezados durante el transporte a través de una red pública. ESP utiliza el protocolo 50 que se encuentra ubicado en el encabezado de IP. [2]

3.3.3.2 GESTIÓN DE CLAVES

Un componente crítico al momento de realizar el cifrado seguro es la comunicación de las claves utilizadas para cifrar y descifrar el tráfico que se va a transportar a través de la red insegura. El proceso de generar, distribuir y almacenar estas claves lleva el nombre de gestión de claves. IPsec utiliza el intercambio de claves de internet (IKE) como protocolo por defecto.[2]

RFC 4306 definió la segunda iteración de IKE que fue llamada IKEv2, el cual proporciona autenticación mutua de cada parte. IKEv2 introdujo el soporte de autenticación extensible (EAP) esta autenticación está basada en certificador, también existe una reducción del consumo de ancho de banda y la capacidad de detectar si un túnel aún está activo.[2]

3.3.3.3 ASOCIACIONES DE SEGURIDAD

Un componente vital de la arquitectura IPsec son las asociaciones de seguridad (SA) y contienen los parámetros de seguridad que se han acordado entre los dos dispositivos de punto final. Existen dos tipos de SA:[2]

- **IPsec SA:** Utilizado para proteger los datos transmitidos entre dos sitios diferentes.[2]
- **IKE SA:** Es utilizada para funciones del plano de control como la gestión de claves IPsec y la gestión de IPsec SA.[2]

Las SA de IPsec son unidireccionales y requieren al menos dos SA de IPsec, es decir, una para la entrada y otra para la salida para así poder intercambiar tráfico de red entre dos sitios. [2]

3.3.3.4 MODOS ESP

IPsec tradicional proporciona dos modos ESP de protección de paquetes: túnel y transporte.[2]

- En el modo túnel todo el paquete original va a ser encriptado y también se va a agregar un nuevo conjunto de encabezados IPsec. Estos nuevos encabezados van a ser utilizados para enrutar el paquete y para proporcionar funciones superpuestas.[2]
- En el modo de transporte se va a encriptar y autenticar únicamente la carga útil del paquete. En este modo no se va a proporcionar funciones superpuestas ni rutas basadas en los encabezados IP originales.[2]

En la figura 3.3 se puede observar un paquete original, un paquete IPSec en modo de transporte y un paquete IPSec en modo de túnel.[2]

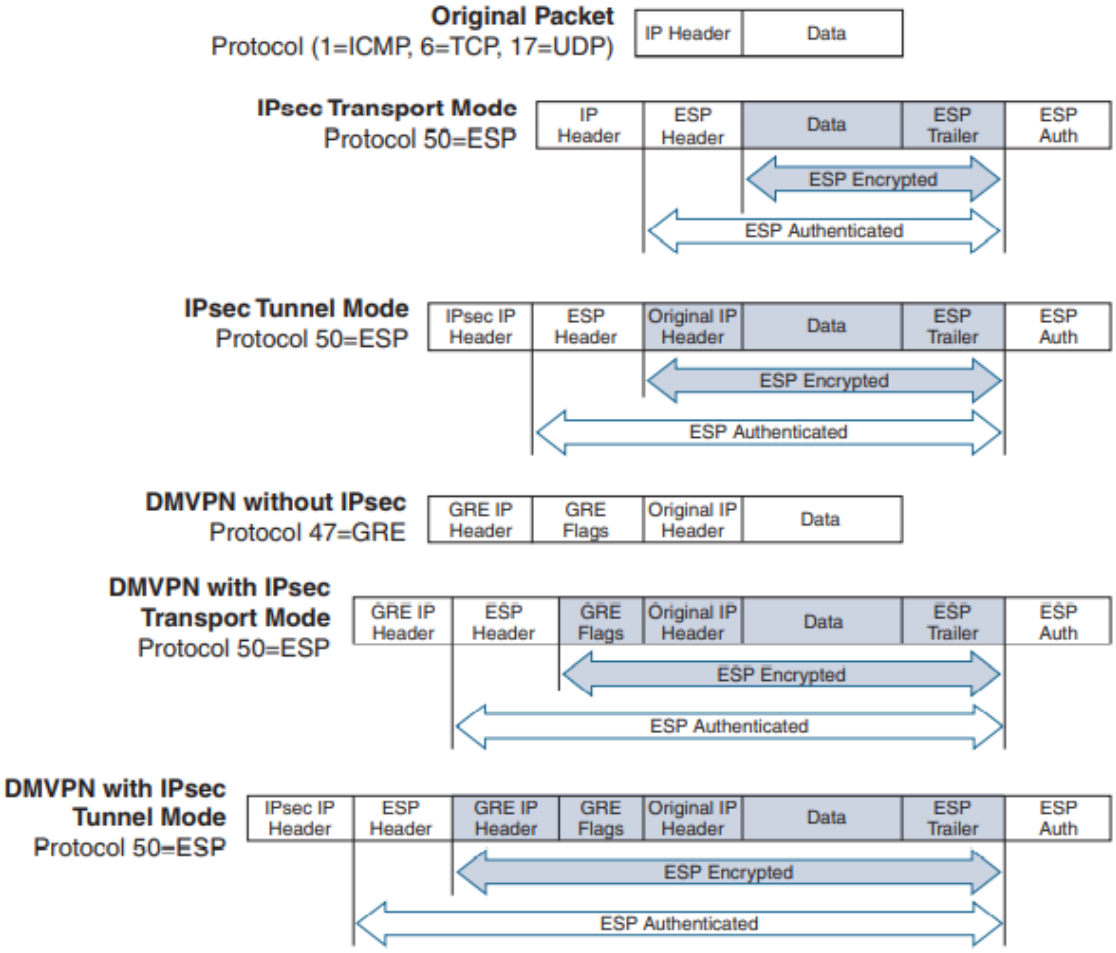


Figura 3.3. Encabezados de paquetes DMVPN.[2]

3.3.3.4.1 DMVPN sin IPSec

En los paquetes DMVPN que no están cifrados, los paquetes originales poseen banderas GRE agregadas y posteriormente se va a agregar el nuevo encabezado IP GRE para que así los paquetes puedan ser enrutados por la red de transporte, es decir la red subyacente. El encabezado IP GRE agrega 20 bytes adicionales de sobrecarga, mientras que las banderas GRE agregan 4 bytes adicionales de sobrecarga. [2]

3.3.3.4.2 DMVPN con IPSec en modo de transporte

Para los paquetes DMVPN que, si están encriptados y que usan el modo de transporte ESP, los paquetes originales tienen los indicadores GRE agregados y posteriormente esa parte va a ser encriptada. Se va a agregar una firma para la carga útil que ya se encuentra cifrada y después el encabezado IP GRE el cual va ayudar para enrutar los paquetes en la red de transporte (subyacente).[2]

El encabezado IP GRE agrega 20 bytes adicionales de sobrecarga, las banderas GRE agregan 4 bytes adicionales de sobrecarga y, dependiendo del mecanismo de cifrado la cantidad de bytes que van a ser agregados para la firma cifrada van a ser variables.[2]

3.3.3.4.3 DMVPN con IPSec en modo túnel

Para los paquetes DMVPN encriptados y que usan el modo de túnel ESP, los paquetes originales poseen los indicadores GRE agregados y posteriormente el encabezado IP GRE va a ser agregado para que los paquetes puedan ser enrutados en la red de transporte (subyacente). Esta parte de los paquetes se va a cifrar, se agrega una firma para la carga útil cifrada y luego se va a agregar un encabezado IP de IPSec para que los paquetes sean enrutados en la red de transporte (subyacente).[2]

El encabezado IP GRE agrega 20 bytes adicionales de sobrecarga, las banderas GRE agregan 4 bytes adicionales de sobrecarga, el encabezado IPSec IP agrega 20 bytes adicionales de sobrecarga, y dependiendo del mecanismo de cifrado que se utilice se va a agregar una cantidad variable de bytes para la firma cifrada.[2]

3.3.4 PROTOCOLOS DE ENRUTAMIENTO

Un protocolo de enrutamiento se puede clasificar como un protocolo de puerta de enlace interior (IGP) o un protocolo de puerta de enlace exterior (EGP). Los IGP son diseñados y optimizados para que sean enrutados dentro de un solo dominio administrativo de control, el cual en redes es denominado como sistema autónomo (AS). Por otro lado, un EGP es usado típicamente para intercambiar rutas entre diferentes AS. Cada uno de los protocolos

de enrutamiento utiliza una lógica diferente para anunciar, calcular la mejor ruta y almacenar las rutas entre enrutadores. Los tres tipos más comunes son:[2]

- **Vector distancia:** Los protocolos de vector distancia no tienen un mapa de toda la red. Su base de datos va a reflejar que un enrutador vecino sabe cómo llegar a la red de destino y que tan distante está el enrutador vecino de la red de destino. Esta distancia generalmente se mide por el conteo de saltos.[2]

- **Estado de enlace:** Los protocolos de enrutamiento de estado de enlace anuncian el estado del enlace y la métrica del enlace para cada uno de sus enlaces conectador y enrutadores conectados directamente a cada enrutador de red. Todos los enrutadores mantienen una copia idéntica de los estados de enlace para que todos los enrutadores de la red tengan un mapa sincronizado idéntico de la red.[2]

  Cada enrutador de la red va a realizar el mismo cálculo de la mejor ruta en comparación con este mapa para obtener la mejor y más corta ruta sin bucles a todos los destinos.[2]

- **Vector ruta:** Un protocolo de vector de ruta es similar a un protocolo de vector distancia. La principal diferencia es que en lugar de observar el número de saltos para poder determinar la mejor ruta sin bucles analiza varios atributos de ruta para identificar la mejor ruta.[2]

3.4 MODELOS DE IMPLEMENTACIÓN

Cisco DMVPN puede ser implementado de dos maneras:[10]

3.4.1 MODELO DE IMPLEMENTACIÓN HUB AND SPOKE

Esta es una topología tradicional en el cual los sitios remotos, es decir, los spokes van a ser agregados a un dispositivo VPN de cabecera en la sede corporativa, es decir, los hub. El tráfico que va a ser enviado desde cualquier sitio remoto o spoke hacia otro sitio remoto siempre va a tener que atravesar por el dispositivo de cabecera o hub. Cisco DMVPN admite enrutamiento dinámico, QoS y multidifusión IP al mismo tiempo que reduce de gran manera el esfuerzo de configuración. En la figura 3.4 podemos observar el modelo hub and spoke. [10]

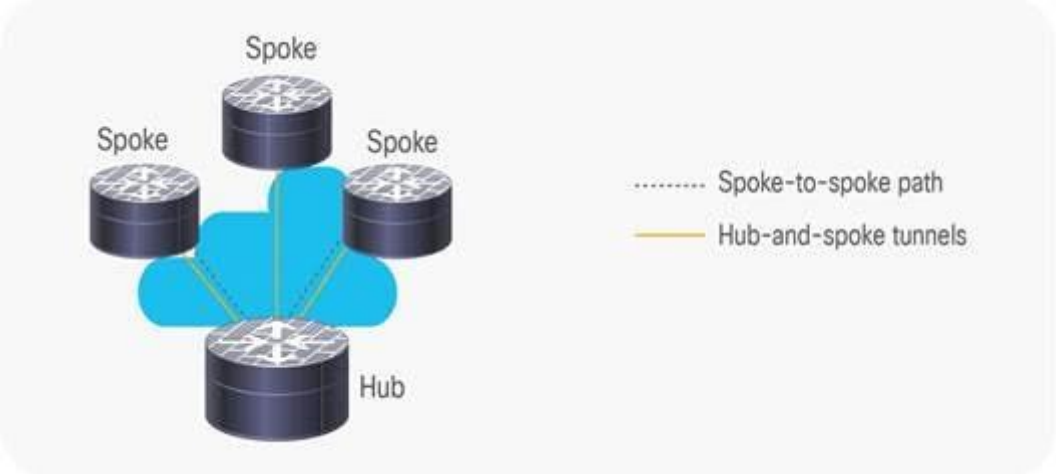


Figura 3.4. Modelo de implementación hub and spoke de Cisco DMVPN.[10]

3.4.2 MODELO DE IMPLEMENTACIÓN DE SPOKE TO SPOKE

Cisco DMVPN es capaz de crear la creación de una VPN de malla completa, en la cual tradicionalmente la conectividad se la realiza desde el hub to spoke se va a complementar con túneles IPSec que van a ser creados dinámicamente directamente entre los spokes. Gracias a los túneles directos entre spoke and spoke, el tráfico no va a tener la necesidad de atravesar con el hub; esto va a eliminar los retrasos adicionales y también va a conservar el ancho de banda de la WAN. En la figura 3.5 podemos observar el modelo spoke to spoke.[10]

Figura 3.5. Modelo de implementación de spoke to spoke de Cisco DMVPN.[10]

Para poder saber cuál es el método que deseamos utilizar podemos utilizar la regla de tráfico 80:20. [10]

- Para que el modelo de hub to spoke sea implementado, el 80% o más del tráfico de los spokes va a estar dirigido a la propia red del hub. [10]

- Para que el modelo de spoke to spoke pueda ser implementado, el 20% o más parte del tráfico tiene que estar destinado a otros spokes. [10]

Cuando las redes poseen un mayor volumen de tráfico multidifusión IP, por lo general es preferible que el modelo que se va a utilizar sea el hub and spoke. [10]

3.5 FASES DMVPN

DMVPN fue lanzado en tres fases, y cada una de las fases se basó en la anterior solo que con funciones adicionales. Las tres fases de DMVPN solo tienen la necesidad de una interfaz de túnel en un enrutador. Los spokes DMVPN pueden utilizar direccionamiento estático o DHCP para las redes de transporte y superposición. [9][10][2]

3.5.1 FASE 1: SPOKE TO HUB

En la fase 1, los spokes de DMVPN van a ser registrados en el hub. En esta fase temprana, no existe comunicación directa entre los spokes, por lo que todo el tráfico tiene que pasar por el hub. Cada spoke utiliza interfaces de túnel GRE punto a punto regulares y solo requiere una ruta resumida o predeterminada al hub para así poder llegar a otros spokes. Por lo que esta configuración de enrutamiento en esta fase es simple. [9][10][2]

3.5.2 FASE 2: SPOKE TO SPOKE

La fase 2 de DMVPN proporciona capacidad adicional que la fase 1, esta fase permite la comunicación spoke to spoke con los enrutadores que utilizan túneles GRE multipunto. Estos túneles spoke to spoke van a estar bajo demanda, es decir, se van a activar en función del tráfico de spoke. Esto significa que los datos no van a tener la necesidad de viajar hacia el hub central. Si el bien hub se usa para el plano de control, pero no necesariamente en el plano de datos. Este hecho hace la diferencia entre la fase 2 y la fase 1. La fase 2 de DMVPN no permite la preservación del siguiente salgo, por lo que, tampoco se admite la comunicación de spoke to spoke entre diferentes redes DMVPN. [9][10][2]

3.5.3 FASE 3: HIERARCHICAL TREE SPOKE TO SPOKE

La fase 3 de DMVPN pule la conectividad de spoke to spoke perfeccionando la mensajería NHRP e interactuando con la tabla de enrutamiento. En la fase 3 de DMVPN, el hub tiene que enviar un mensaje de redireccionamiento NHRP al spoke que originó el flujo de paquetes. El mensaje de redireccionamiento de NHRP va a proporcionar la información necesaria para que el spoke que inicio la transmisión de datos pueda iniciar una resolución de host / red de destino. Cisco PfRv3 también agrega compatibilidad con API para DMVPN fase 3. [9][10][2]

En la fase 3, NHRP va a instalar las rutas en la tabla de enrutamiento para los accesos directos que crea. Estos accesos directos de NHRP van a modificar la entrada del siguiente salto para las rutas existentes o agregan una entrada de ruta más explícita a la tabla de enrutamiento. Gracias a que los accesos directos de NHRP instalan rutas más explícitas en la tabla de enrutamiento, la fase 3 pude admitir el resumen de redes en el hub al mismo tiempo que proporciona un enrutamiento óptimo entre los enrutadores spoke. Los accesos directos de NHRP permite tener una topología de árbol jerárquica para que un hub regional sea el responsable de administrar el tráfico y las subredes de NHRP dentro de esa región, pero los túneles de spoke to spoke se pueden establecer fuera de esa región. [9][10][2]

En la figura 3.6 se puede observar las diferencias entre los patrones de tráfico para las tres fases antes mencionadas. Como podemos ver los tres modelos aprueban la comunicación directa de spoke to hub. El flujo de paquetes de spoke to spoke en DMVPN fase 1 es diferente del flujo de paquetes en la fase 2 y 3, es decir que en la fase 1 el tráfico debe atravesar el hub mientras que para la fase 2 y 3 un túnel dinámico de spoke to spoke se crea para poder tener una comunicación directa.[2]

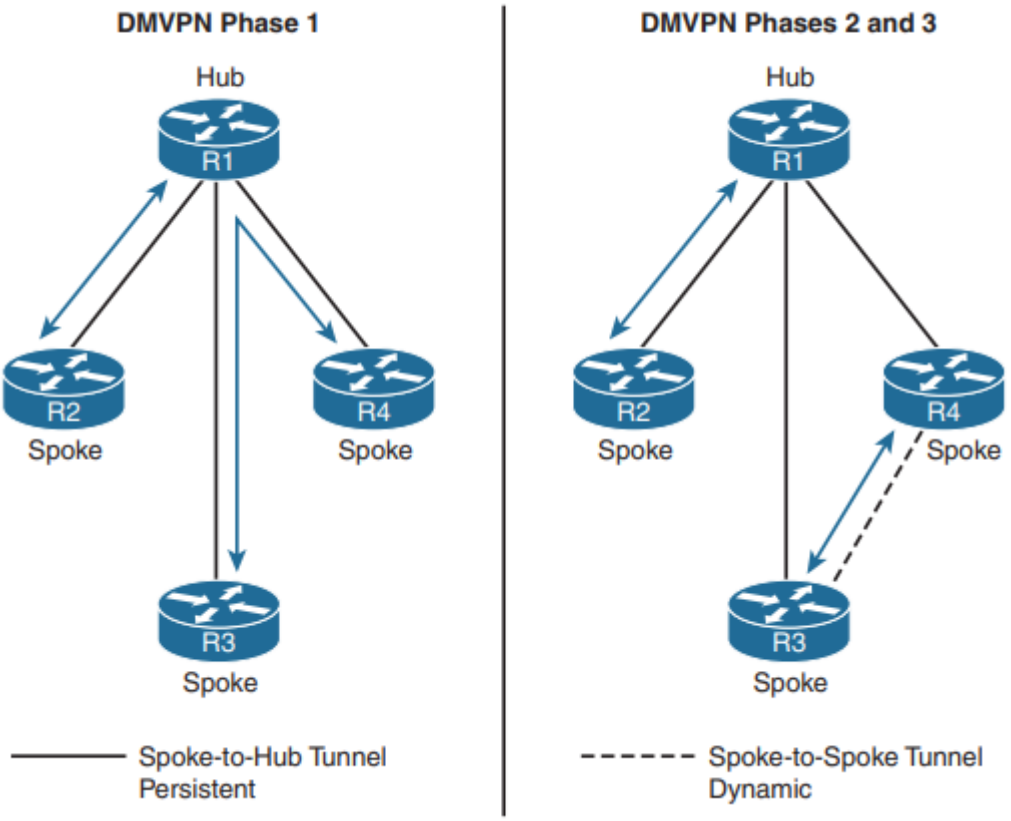


Figura 3.6. Patrones de tráfico DMVPN en las diferentes fases de DMVPN.[2]

Se tiene que tener en cuenta que cada una de las fases DMVPN tiene su propia configuración específica. Lo que no se recomienda es mezclar fases DMVPN en la misma red de túneles. [2]

3.6 CARACTERÍSTICAS Y BENEFICIOS DE CISCO DMVPN

La tabla 3.3 enumera las características y beneficios de Cisco DMVPN. [10]

Tabla 3.3. Características y beneficios de Cisco DMVPN

Característica	Descripción y Beneficio
Enrutamiento dinámico sobre VPN	• Posibilita a que las tablas de enrutamiento IP sean distribuidas de forma segura entre el spoke y el hub a través de túneles encriptados. Permite mejorar la accesibilidad sin que sea necesario que las rutas permitidas sean definidas de forma manual. • Existen algunos protocolos que son admitidos tales como: Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF) y Border Gateway Protocol (BGP).
Sobrecarga de configuración reducida.	• Las líneas de configuración que son requeridas para una implementación de VPN pueden ser simplificadas gracias a que DMVPN tiene la capacidad de eliminar la configuración de mapas criptográficos vinculados a la interfaz física (por ejemplo, para una implementación de 1000 sitios, DMVPN reduce el esfuerzo de configuración en el hub de 3900 líneas a 13 líneas). • Agregar nuevos spokes a la VPN no va a requerir realizar cambios en el hub. • La configuración de los túneles divididos es simplificada. El cambio de configuración centralizado en el hub controla el comportamiento de tunelización dividida. En IPSec tradicional, todos los spokes tienen que ser modificarse.
Implementación sin contacto	• Para poder brindar aprovisionamiento seguro a los dispositivos basados en PKI, Cisco DMVPN puede ser ejecutado mediante modelos de implementación sin

	intervención gracias a Easy Secure Device Deployment. Los dispositivos pueden ser arrancados de forma remota, lo que evita la necesidad de operaciones de preparación extensas.
Túneles dinámicos de spoke to spoke	• Los túneles directos de spoke to spoke eliminan la necesidad de que el tráfico de spoke to spoke atraviese por el hub. • Reduce la latencia para implementaciones de voz sobre IP (VoIP) sobre DMVPN, además mejora el rendimiento efectivo del enrutador ubicado en el hub. • Los túneles son creados dinámicamente cuando es necesario y van a ser derribados después de su uso, lo que permite que el sistema sea escalable.
Direccionamiento dinámico para enrutadores radiales	• Los enrutadores que se encuentran en los spokes pueden usar direcciones IP dinámicas, el cual es un requisito frecuente al momento de realizar conexiones a Internet por cable y DSL.
Traducción transversal de direcciones de red (NAT)	• DMVPN admite que los enrutadores que se encuentran en los spokes ejecuten NAT o detrás de dispositivos NAT dinámicos, lo que permite obtener una seguridad mejorada para las subredes que se encuentran en las sucursales.
Compatibilidad con multidifusión IP	• DMVPN puede admitir tráfico de multidifusión IP entre hubs y spokes; IPSec únicamente admite IP unicast. Gracias a esto se puede proporcionar una distribución más eficiente y escalable del tráfico de muchos a muchos y de uno a muchos.
Soporte QoS	• Política de QoS de hub to spoke y de spoke to spoke • Políticas dinámicas de QoS en las que las plantillas de QoS van a ser adjuntadas automáticamente a los túneles mientras van surgiendo. • Vigilancia de QoS por spoke, lo que ayuda a diferenciar los spokes y así poder proteger la red para que no sea invadida por otros spokes que tengan la necesidad de ancho de banda.

Alta disponibilidad	• Gracias a los enlaces WAN duales y a la redundancia del hub se puede brindar una mayor disponibilidad.
Escalabilidad	• DMVPN tiene la posibilidad de escalar a miles de spokes gracias al equilibrio de carga del servidor (SLB). • El rendimiento puede ir aumentando gradualmente al momento en que se incremente hubs.

3.7 APLICACIONES

Cisco DMVPN es la solución que las organizaciones prefieren al momento que desean tener una conectividad WAN cifrada entre sitios remotos. [10]

- **Empresas medianas y grandes:** ya sea en sectores como el financiero, el de seguros o el de comercio minorista, es decir, que numerosos sitios van a estar conectados a la sede corporativa. Algunas de las aplicaciones críticas pueden ser las que utilizan los cajeros automáticos de los bancos o las máquinas de puntos de venta, estas aplicaciones van a ser implementadas a través de estas conexiones. Cisco DMVPN permite que todos estos sitios se puedan conectar a través de internet, lo que proporciona privacidad e integridad de datos al mismo tiempo que es capaz de cumplir con los requisitos de rendimiento de las aplicaciones críticas para el negocio. [10]
- **Pequeña oficina empresarial / oficina doméstica (SOHO):** Cisco DMVPN proporciona una integración mejorada con QoS que puede ser usado para que tanto voz como datos sean admitidos para que los empleados puedan acceder a la red desde un entorno SOHO.[10]
- **Extranet empresarial:** por lo general las grandes empresas necesitan tener conectividad con una gran cantidad se socios comerciales. Cisco DMVPN puede ser utilizado para proteger el tráfico entre la empresa y los lugares en los que se encuentren los socios, va a proporcionar segregación de red al ayudar a garantizar que no se permita el tráfico de spoke to spoke, incluso a través del hub. [10]
- **Respaldo de conectividad de WAN empresarial:** Cisco DMVPN puede ser usado como una solución de respaldo para las WAN privadas, esto permite que los sitios remotos puedan conectarse de forma segura a la oficina central de la empresa a través de enlaces de internet. [10]

- **Servicios VPN de proveedores de servicios:** Cisco DMVPN admite que los proveedores de servicio ofrezcan servicios VPN administrados. El tráfico de varios clientes puede ser agregado en un solo enrutador de borde de proveedor y este puede mantenerse aislado mediante funciones como el enrutamiento y reenvío virtual (VRF).[10]

4 CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- Gracias al estudio realizado se puede concluir que Cisco iWAN ofrece una solución en la cual se es factible el reemplazo de los servicios de Internet rentables por servicios WAN de alta gama y con una gran calidad, sin que se tenga que poner en riesgo la calidad, la disponibilidad o la seguridad de la red; y así se pueda ofrecer un mayor ancho de banda.

- La tecnología Cisco iWAN permite que las organizaciones puedan escalar de forma horizontal, sin importar el modelo que se escoja para su diseño.

- Mediante los estudios realizados se ha logrado demostrar que existe un ahorro en el costo del servicio de transporte entre en 34 y 81%.

- Uno de los componentes que posee la tecnología Cisco iWAN es la independencia de transporte la cual permite que el tráfico sea trasladado a enlaces menos costosos, además que los administradores de la red pueden escoger entre diferentes opciones de transporte según las necesidades, esto se logra ya que se utiliza el enrutamiento superpuesto.

- El control de ruta inteligente se considera como uno de los componentes más importantes de la tecnología Cisco iWAN ya que se usa una herramienta muy importante que es el Performance Routing (PfR). Esta herramienta es la encargada de elegir el mejor camino para que se reenvíen los paquetes además tiene que supervisar el rendimiento de dicha aplicación.

- Al integrarse PfR con DMVPN se convierten en un componente que es vital para la arquitectura de la tecnología de Cisco iWAN, lo cual permite proporcionar a las aplicaciones una supervisión mejorada, una configuración centralizada simple y una convergencia más rápida.

- Cisco WAAS ayuda a que la redundancia de datos sea eliminada, es decir, va a identificar los patrones de datos en el tráfico de la red para que puedan ser reducidos, estos patrones van a ser reemplazados con una firma; logrando que el paquete se reduzca de tamaño mientras va cruzando por la red WAN y así exista optimización de las aplicaciones.

- Cuando Cisco iWAN se conecta con Cisco Cloud Web Security (CWS) se puede lograr proporcionar seguridad contra amenazas y malware sin que sea necesario la compra o la administración de dispositivos de seguridad dedicados para cada una de las sucursales.

- Al realizar un estudio sobre DMVPN pudimos concluir que esta tecnología es capaz de ofrecer un mayor desempeño al momento en el que se tenga que intercambiar cualquier tipo de tráfico gracias a que se tienen que construir canales dinámicos, también una gran ventaja es que existe una reducción de los comandos que son necesarios para su configuración y operación.

- La arquitectura Cisco iWAN en compañía con las funciones de seguridad e IPSec VPN, es capaz de proporcionar el mismo nivel de seguridad, integridad y privacidad de datos de igual forma que las WAN privadas, es capaz de brindar confianza a las organizaciones gubernamentales y empresariales para que puedan usar internet público como un medio de transporte WAN que va a ser altamente seguro para poder establecer comunicación de la sucursal.

- Los túneles GRE al agregar información adicional en forma de encabezado permiten que el paquete sea enrutado sin que se necesite realizar un control exhaustivo de la carga útil del paquete.

- El instante en el cual IPSec se integra con los túneles DMVPN, los túneles cuando ya se encuentren cifrados van a proporcionar una red superpuesta que va a ser segura.

- Existen varios protocolos de seguridad que la tecnología Cisco iWAN utiliza, uno de ellos es el encabezado de autenticación el cual se va a encargar de la integridad de los datos, autenticación y la protección contra los piratas informáticos, este protocolo va a garantizar que el paquete original no haya sido modificado durante su transporte.

- La gestión de claves cumple un papel muy importante en la tecnología Cisco iWAN ya que este es el encargado de la comunicación de las claves que fueron utilizadas para cifrar los paquetes que van a ser transmitidos a través de la red.
- Cisco DMVPN fue lanzado en tres fases, pero al momento que se realice la implementación de esta tecnología se tiene que tener en cuenta que no es recomendable mezclas dichas fases DMVPN si se está trabajando en una misma red de túneles.

4.2 RECOMENDACIONES

- Se recomienda que antes de hacer algún cambio en la red de alguna empresa siempre se realice un estudio para que se tenga en cuenta la inversión que se tenga que hacer si fuera necesario y en cuanto tiempo se empezarían a obtener ganancias después de que ya se haya implementado la nueva tecnología.
- Se recomienda tener en cuenta las necesidades de la empresa al momento de realizar el diseño para que se pueda escoger de manera adecuada la tecnología WAN que más se ajuste a las necesidades de la misma.
- Se recomienda siempre estar atentos de cualquier tipo de actualización que la empresa Cisco realice para que la red de la organización en la cual esta implementada esta tecnología no se vea afectada.
- Se recomienda que se tomen muy en cuenta las recomendaciones que realiza la empresa Cisco al momento de la implementación de la nueva tecnología para que así pueda ser aprovechada al máximo todos los aplicativos que se ofrecen.

5 BIBLIOGRAFÍA

[1] "Cisco Validated Design."

[2] B. Edgeworth, *Cisco Intelligent WAN (IWAN)*.

[3] C. V. Design, "REFERENCE NETWORK ARCHITECTURE CISCO VALIDATED DESIGN REFERENCE NETWORK ARCHITECTURE Intelligent WAN Technology Design Guide," 2016.

[4] "Evolución de las Redes WAN | Centro de Educación Virtual." https://puceapex.puce.edu.ec/web/cev/evolucion-de-las-redes-wan/ (accessed Nov. 17, 2021).

[5] "Arpanet - Glosario | MDN." https://developer.mozilla.org/es/docs/Glossary/Arpanet (accessed Dec. 06, 2021).

[6] “Qué es... MPLS (MultiProtocol Label Switching).” https://www.ramonmillan.com/tutoriales/mpls.php (accessed Dec. 12, 2021).

[7] “INTELLIGENT-WAN-Network-optimization-getting-started-with-intelligent-WAN-MKT14F012”.

[8] “Fundamentos-de-CiscoiWAN”.

[9] “What is dynamic multipoint VPN and how does it work?” https://www.techtarget.com/searchnetworking/definition/dynamic-multipoint-VPN-DMVPN?utm_source=CAM (accessed Feb. 02, 2022).

[10] “Cisco Dynamic Multipoint VPN: Simple and Secure Branch-to-Branch Communications Data Sheet - Cisco.” https://www.cisco.com/c/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/data_sheet_c78-468520.html?dtid=osscdc000283 (accessed Feb. 02, 2022).