ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

ANÁLISIS COMPARATIVO ENTRE VPN IPSEC Y DMVPN (DYNAMIC MULTIPOINT VIRTUAL PRIVATE NETWORK) PARA MEJORAR EL DESEMPEÑO DE REDES PRIVADAS SOBRE INTERNET

ALEX WLADIMIR JARAMILLO ZAMORA

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN INTERCONECTIVIDAD DE REDES

Riobamba - Ecuador

Noviembre 2018

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DEL TRABAJO DE TITULACIÓN CERTIFICA QUE:

El trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, titulado: "**ANÁLISIS COMPARATIVO ENTRE VPN IPSEC Y DMVPN (DYNAMIC MULTIPOINT VIRTUAL PRIVATE NETWORK) PARA MEJORAR EL DESEMPEÑO DE REDES PRIVADAS SOBRE INTERNET"**, de responsabilidad del señor Alex Wladimir Jaramillo Zamora, ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

Lic. Pepita Ivonne Alarcón Parra; M.Sc.
PRESIDENTE _____

Ing. Juan Manuel Lema Sevillano; M.Sc.
DIRECTOR DE TESIS _____

Ing. Ángel José Ordóñez Mendieta; M.Sc.
MIEMBRO DEL TRIBUNAL _____

Ing. Antonio Arquimides Ramírez Gonzalez; M.Sc.
MIEMBRO DEL TRIBUNAL _____

Riobamba, Octubre del 2018

DERECHOS INTELECTUALES

Yo, Alex Wladimir Jaramillo Zamora, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en este Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

_____

ALEX WLADIMIR JARAMILLO ZAMORA

No. Cédula 150063185-6

DECLARACIÓN DE AUTENTICIDAD

Yo, Alex Wladimir Jaramillo Zamora, declaro que el presente Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

Riobamba, octubre de 2018.

_____

ALEX WLADIMIR JARAMILLO ZAMORA

No. Cédula 150063185-6

DEDICATORIA

Dedico este trabajo de titulación a mi esposa, mi hijo e hija quienes son mi fuente de inspiración y fortaleza para buscar mi superación personal; a mi padre y madre por su apoyo incondicional; a mis hermanos y hermana por sus ánimos y aliento para cumplir mis metas.

Alex Wladimir Jaramillo Zamora.

AGRADECIMIENTO

Agradezco a mi tutor Ing. Juan Lema por ser un guía en este trabajo de titulación, quien de una manera acertada, coherente y profesional brindó sus conocimientos para concretar el desarrollo de la presente investigación.

A los miembros del tribunal que me brindaron su apoyo y consejos.

A todas aquellas personas que de alguna manera me brindaron su apoyo en el desarrollo del proyecto de titulación y poder culminarlo.

Alex Wladimir Jaramillo Zamora.

INDICE DE CONTENIDO

ÍNDICE DE ABREVIATURAS

VPN	RED PRIVADA VIRTUAL
DMVPN	VPN DINÁMICA MULTIPUNTO
NHRP	PROTOCOLO DE RESOLUCIÓN DEL SIGUIENTE SALTO
NBMA	RED DE ACCESO MÚLTIPLE DE NO DIFUSIÓN
RFC	REQUEST FOR COMMENTS
MGRE	MULTIPOINT GENERIC ROUTING ENCAPSULATION
IPSEC	SEGURIDAD DE PROTOCOLO EN INTERNET
AES	ADVANCED ENCRYPTION STANDARD
DES	DATA ENCRYPTION STANDARD
3DES	ALGORITMO DE CIFRADO DE DATOS TRIPLE
EIGRP	ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL
MD5	MESSAGE-DIGEST ALGORITHM 5
CISCO IOS	CISCO INTERNETWORK OPERATING SYSTEM
TCP	TRANSMISSION CONTROL PROTOCOL
UDP	USER DATAGRAM PROTOCOL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

RESUMEN

Se realizó el análisis comparativo entre Red privada virtual Protocolo de Internet Seguro (*VPN IPSEC)* y red privada virtual multipunto dinámica (*DMVPN)* para mejorar el desempeño de redes privadas sobre Internet. La solución tradicional de *VPN* se basa en *IPsec* punto a punto, la cual no permite una comunicación directa entre cada sitio y depende del estado de su concentrador para garantizar la comunicación. Se evaluó una nueva técnica que elimina las conexiones punto a punto y permita la convergencia de las aplicaciones, se analiza *DMVPN* como una solución que permitirá mejorar el desempeño de las *VPN* sobre Internet. Se implementó una red de un *HUB* y cuatro *SPOKE* para la transmisión y evaluación de paquetes de datos, voz y video. Analizados los resultados de las pruebas en ambos escenarios se obtiene que en la comunicación entre SPOKES predominó en arrojar resultados favorables con una mejora del 88,8% en el retardo, 64,1% en el jitter y 84,9% en la pérdida de paquetes. Aplicando la estadística inferencial se concluye que la técnica *DMVPN* arroja mejores valores en los indicadores de desempeño de la red que son retardo de paquetes, *jitter* y paquetes perdidos, de la misma manera muestra valores de dispersión más bajos. Como propuesta se desarrolló una guía de implementación de DMVPN incluyendo todas las consideraciones que se debe aplicar en la práctica producto de las pruebas realizadas.

Palabras Clave: TECNOLOGIA Y CIENCIAS DE LA INGENIERIA, TELECOMUNICACIONES, REDES DE COMUNICACIÓN, SEGURIDAD PROTOCOLO INTERNET (IPSEC), RED PRIVADA VIRTUAL MULTIPUNTO DINÁMICA (DMVPN), RED PRIVADA VIRTUAL (VPN), RETARDO DE PAQUETES, JITTER (VARIANZA DEL TIEMPO), INTERNET.

ABSTRACT

The comparative analysis between Virtual Private Network Internet Protocol Security (VPN IPSec) and Virtual Private Network Dynamic Multipoint (DMVPN) was made to improve the performance of private networks over the Internet. The traditional VPN solution is based on IPsec point to point, which does not allow direct communication between each site and depends on the status of its concentrator to ensure the communication. A new technique was evaluated; this eliminates point-to-point connections and enables the convergence of applications. DMVPN analyzed as a solution; that will improve the performance of VPNs over the Internet. A network of one HUB and four SPOKE was implemented for the transmission and evaluation of data, voice and video packages. Analyzed the results of the tests in both scenarios, it obtained that the communication between SPOKES predominated in throwing favorable results with an improvement of 88,8% in the delay, 64,1% in the jitter and 84,9% in the loss of packages. Applying the statistics inference concluded that the DMVPN technique yields better values in the performance indicators of the network that are packet delay, jitter, and lost packets, in the same way, it shows lower dispersion values. As a proposal, a DMVPN implementation guide was developed, including all the considerations that should be applied in the practice product of the tests performed.

Key Words: <TECHNOLOGY AND SCIENCE OF ENGINEERING>, <TELECOMMUNICATION>, <COMMUNICATION NETWORKS>, <INTERNET PROTOCOL SECURITY (IPsec)>, <VIRTUAL PRIVATE NETWORK DYNAMIC MULTIPOINT (DMVPN)>, <VIRTUAL PRIVATE NETWORK (VPN)>, <PACKETS DELAY>, <JITTER (TIME VARIANCE)>, <INTERNET>.

CAPÍTULO I

1. INTRODUCCIÓN

1.1. Situación problemática

Una Red Privada Virtual con sus siglas en inglés VPN (*Virtual Private Network*), es una "tecnología de red que permite una extensión segura de la Red de Área Local, LAN, sobre una red pública o no controlada como Internet" (González, 2014).

Las redes de comunicación están evolucionando para permitir establecer canales basados en software, facilitando su administración y permitiendo a las empresas intercambiar información y realizar transacciones seguras, no solamente entre sitios de su misma organización, sino también con otras empresas.

Al momento de establecer una VPN se debe considerar muchos aspectos, ya que existen diferentes protocolos y técnicas que permiten su implementación.

Las VPNs de capa 3 aplican como estándar una topología estrella del tipo "HUB and SPOKE", implementando túneles estáticos, generalmente GRE (*Generic Routing Encapsulation*) o IPsec (*Internet Protocol Security*). El "HUB o concentrador" se ubica en el centro de la red y los "SPOKES o clientes" lo rodearán. El tráfico que se genere entre los "SPOKES" debe ser desviado a través del "HUB" para que salga de un túnel e ingrese a otro. Al añadir un "spoke" a la red, se requiere realizar una configuración adicional en el equipo "HUB" y el tráfico que se genere entre los "SPOKES" debe ser desviado a través del "HUB" para que salga de un túnel e ingrese a otro.

Ésta forma de comunicación en ambientes pequeños puede ser una solución viable pero a gran escala se genera problemas de administración y afecta la transmisión de paquetes de servicios en tiempo real.

De lo antes expuesto surge la siguiente interrogante o cuestionamiento a resolver en el presente trabajo: ¿Existe una técnica que permita mejorar el desempeño en la transferencia de paquetes de vídeo, voz y datos en las Redes Privadas Virtuales sobre Internet?

Cisco ha considerado que la transmisión de información entre clientes va en aumento y la topología estrella de las técnicas comunes no lo consideran. En este sentido, Cisco ha desarrollado dos técnicas que permiten implementar conexiones multipunto a nivel de WAN, como son: GETVPN y DMVPN. GETVPN (*Group Encrypted Transport VPN*) fue desarrollado en 2015 como mejora a la seguridad que implementa IPsec; sin embargo, no utiliza túneles de extremo a extremo de un modo nativo y trabaja bien si se implementa sobre una red *full mesh*. GETVPN resulta ser más "escalable" que DMVPN, pero se limita a trabajar sólo en redes privadas como MPLS ya que para su funcionamiento requiere conservar la cabecera IP del paquete y al pasar por una infraestructura NAT, esto no es posible. El presente trabajo de tesis se enfoca en el mejoramiento del desempeño de VPNs sobre Internet, y por tal motivo, GETVPN no es una solución viable.

Por otra parte, DMVPN (*Dynamic Multipoint Virtual Private Network*) es una técnica que asocia túneles GRE, añadiendo seguridad con IPsec y proveyendo una resolución de direcciones mediante NHRP (*Next Hub Resolution Protocol*). La función principal de la técnica DMVPN es su habilidad de establecer dinámicamente túneles "*spoke and spoke*". A pesar de que esta técnica está disponible, es muy poco conocida en nuestro medio y carece de pruebas a detalle respecto al desempeño de servicios en tiempo real, cursando VPNs sobre Internet.

La empresa Cisco Systems especifica la condición "80-20", la cual indica que el 80% del tráfico debe ser entre el *Hub* y *Spoke*, mientras que el 20% debe ser entre *Spokes*. (Cisco Systems, Cisco Dynamic Multipoint VPN: Simple and Secure Branch-to-Branch Communications, 2015). Esta definición se convierte en un valor experimental, obtenido en determinados ambientes de prueba, pero no se sabe a ciencia cierta cuál será el desempeño del tráfico real en nuestro medio.

A nivel mundial existen estudios y consejos de implementación de DMVPN para corporaciones transnacionales. La mayor parte de estos estudios se encuentran en repositorios de Cisco. A nivel latinoamericano existe información en repositorios de universidades, sobre la aplicación de DMVPN para brindar redundancia a nivel de WAN, evaluando su característica de topología en malla y su nivel de convergencia. Por ejemplo, se tiene el trabajo de investigación de la Universidad de Porto de Brasil con el título "Estudio de la viabilidad de un servicio VPN basado en una arquitectura redundante" (Lima A. I., 2010), pero no evalúan su desempeño en la transferencia de servicios en tiempo real.

A nivel local se tiene una aplicación de DMVPN como herramienta para establecer redundancia y seguridad en la transferencia de datos. La fuente es una investigación como trabajo de titulación de maestría en la Pontifica Universidad Católica de Ecuador titulado: "Diseño de un sistema híbrido inalámbrico-fibra para transmisión de datos de medidores inteligentes de energía en redes smart grid". (Milton, 2016). Este trabajo de investigación evalúa el desempeño de la técnica DMVPN en la transferencia de datos, considerando los parámetros de latencia, jitter y pérdida de datos; sin embargo, no considera paquetes en tiempo real como vídeo y voz.

Por tal motivo, el presente trabajo se centra en la comparación de dos técnicas de VPN, VPN IPsec y DMVPN, para mejorar el desempeño de las redes privadas sobre Internet. Esto implica promover la transferencia privada y segura de servicios de voz, video y datos a través de los ISPs locales, lo cual es algo novedoso.

1.2. Formulación del problema

En base a la "Situación Problemática" expuesta en la sección anterior, realizamos la siguiente formulación del problema:

¿La aplicación de la técnica DMVPN permitirá mejorar el desempeño de las redes privadas sobre Internet?

1.3. Justificación de la investigación

El presente trabajo de investigación tiene como finalidad el estudio de la técnica DMVPN para determinar su desempeño en la provisión de servicios en tiempo real sobre una red pública, como es el Internet.

Los resultados permitirán analizar el rendimiento de una VPN aplicando la técnica DMVPN para brindar canales dinámicos de transmisión y ser considerada una alternativa técnica y económicamente viable en la implementación de enlaces seguros y estables para la compartición de información en tiempo real. El correcto aprovechamiento de esta tecnología, es una propuesta innovadora en nuestro país que requiere el desarrollo de pruebas, necesarias para su registro teórico y correcto funcionamiento.

El presente estudio permitirá evaluar el desempeño de la técnica DMVPN para el diseño de una red VPN segura, confiable y escalable, cuyo principal objetivo sería la provisión de servicios en tiempo real sobre Internet. La técnica DMVPN ofrece romper el esquema *Hub-Spoke* clásico de una topología estrella, estableciendo canales dinámicos *Spoke-Spoke* que permita el establecimiento de una red en malla.

La verificación y comprobación de esta técnica brindará datos teóricos y prácticos sobre el desempeño de DMVPN y permitirá a los administradores de redes obtener una solución probada para la transmisión de servicios en tiempo real con una disminución de costos de sus comunicaciones al no utilizar canales de datos dedicados como MPLS que no brinda seguridad.

1.4. Objetivos

1.4.1. Objetivo General

- Realizar el análisis comparativo entre VPN IPsec y DMVPN para mejorar el desempeño de las redes privadas sobre Internet.

1.4.2. Objetivos Específicos

- Analizar las características de VPN IPsec y DMVPN con el fin de identificar sus ventajas y desventajas; y así poder realizar la comparación de las mismas.
- Diseñar un escenario de pruebas para cursar tráfico de voz, datos y video, sobre VPN IPsec y DMVPN, y ambas sobre Internet. Esto permitirá llevar a la práctica la comparación teórica.
- Implementar el escenario de pruebas mediante el uso de equipamiento y configuraciones, necesarias para obtener mediciones que sustenten la comparación y que permitan identificar cómo mejorar las redes privadas virtuales sobre Internet.

- Evaluar los resultados de las pruebas con el fin de identificar las diferencias entre los dos modelos planteados. Del mismo modo, se va a determinar cuáles son los mejores parámetros de configuración de DMVPN y las condiciones requeridas, para así mejorar el desempeño de las redes privadas virtuales sobre Internet.

- Elaborar una guía de especificaciones técnicas para la correcta implementación de DMVPN sobre redes públicas.

1.5. Hipótesis

El presente trabajo plantea la siguiente hipótesis:

La aplicación de DMVPN mejora el desempeño de redes privadas virtuales sobre Internet, con respecto al uso de VPN IPsec.

De esta manera, se realizará el estudio de ambas técnicas y su implementación para poder obtener las conclusiones del caso.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Antecedentes del problema

La revisión de la literatura relacionada al tema planteado en el presente estudio, refleja los antecedentes detallados a continuación.

Uno de los primeros artículos revisados, corresponde a un *paper* investigativo del Departamento de Ciencia de la Computación de la *University for Business and Technology* con el título: "*Enterprise Integration, Networking and Virtual Communications*". Este *paper* realizado por Besnik Qehaja, Ardian Bajraliu, Ahmet Shabani y Edmond Hajrizi, analiza los componentes integrales que permiten la implementación de la tecnología DMVPN y plantea la siguiente conclusión:

> Las VPNs permiten a los usuarios o corporaciones conectarse a servidores remotos, sucursales o a otras empresas a través de una red pública, manteniendo al mismo tiempo el flujo de tráfico seguro. En todos estos casos, la conexión segura al usuario se ve como una comunicación de red privada. Hemos llegado a la conclusión de que muchas empresas no tienen determinación o conocimiento sobre cómo la seguridad representa el jugador clave y es el elemento entre el éxito o el fracaso de una organización. A través de este trabajo hemos tratado de aumentar la autoconciencia sobre las tecnologías VPN y proponer DMVPN como una solución, explicando en detalle todas las directivas que son parte de permitir la transmisión de información en el tiempo con un alto nivel de seguridad.
>
> (Besnik, Ardian, Ahmet, & Edmond, 2016)

De modo adicional, en el *paper* citado se miden algunos parámetros como: el tiempo de respuesta, porcentaje de pérdidas, errores, jitter, rendimiento del hardware (CPU y memoria) de acuerdo a los niveles de ancho de banda de la red. Estos parámetros les permitieron evaluar el desempeño

de una red híbrida de túneles dinámicos y estáticos. En la presente tesis, se propone la explotación de túneles dinámicos sobre Internet.

Por otra parte, en el repositorio de la Escuela Superior Politécnica del Ejército se encontró una tesis de Maestría en Redes de Información y Conectividad con el título: "Estudio comparativo entre IPsec y MPLS para redes privadas virtuales (VPN)" realizada por el señor Juan Carlos Brito Ayala en el año 2015. En esta tesis se evalúa los protocolos IPsec y MPLS por medio de la herramienta JPERF y Wireshark. De acuerdo a dicha evaluación realizada se concluye lo siguiente:

"Tanto para el sistema IPsec-Internet como para el sistema DMVPN-MPLS en la transmisión de un flujo simple, como con multiflujo TCP, los tiempos de transmisión se mantienen directamente proporcionales respecto al tamaño del MSS mayores a 1000 bytes y al BW hasta 20Mbps, donde los resultados son lineales" (Juan Carlos Brito Ayala, 2015). MSS se refiere al *Maximum Segment Size* y BW se refiere al ancho de banda de una determinada transmisión. Cuando se supera el valor de estos parámetros, "el sistema se vuelve inestable y degradado, no por temas inherentes al protocolo IPsec sino por *troughput* y procesamiento de los equipos CPEs" (Juan Carlos Brito Ayala, 2015). Así se puede concluir que la eficiencia de los sistemas IPsec-Internet y DMVPN-MPLS depende directamente de la capacidad de procesamiento de los CPEs. Este hecho demuestra una limitante común de ambos esquemas, pero no refleja las reales ventajas que DMVPN tiene sobre IPsec cuando el tráfico aumenta.

2.2. Bases teóricas

A nivel empresarial, ante la necesidad de obtener mayor seguridad y desempeño en el intercambio de información con la mejor calidad posible al transmitir paquetes de voz y video en tiempo real, se busca una tecnología que permita alcanzar este propósito, además de ser flexible, fácil de implementar y administrar.

Los túneles IPsec son ampliamente usados en conexiones empresariales que requieren seguridad y una solución de bajo costo. Su principal aplicación en Internet se ha limitado estrictamente a establecer una conexión punto a punto entre dos sitios remotos y que esto sirva como un enlace de respaldo ante una falla del canal principal WAN, que por lo general es MPLS. Esto funciona, pero se vuelve ineficaz si se rutea el tráfico de un *spoke* a otro, a través del *hub*. Aquí es donde DMVPN ofrece una solución.

DMVPN es el resultado de la aplicación de varias tecnologías como los túneles GRE multipunto y el protocolo NHRP *(Next Hop Resolution Procotol*), permitiendo el establecimiento de una arquitectura de malla dinámica. DMVPN elimina las complejas configuraciones de las conexiones punto a punto y reduce los cuellos de botella del tráfico generado hacia la comunicación con el *Hub*.

A continuación se presenta conceptos de VPN, VPN IPsec y DMVPN.

2.2.1. Concepto de Redes Privadas Virtuales

Como se mencionó en la sección 1.1: "Situación Problemática", una Red Privada Virtual con sus siglas en inglés VPN (*Virtual Private Network*), es una tecnología de red que permite una extensión segura de la Red de Area Local, LAN, sobre una red pública o no controlada como Internet (González, 2014).

Desde sus orígenes, las VPNs se implementaton en diferentes capas de red y fueron implementadas mediante diversos mecanismos y protocolos. En la Tabla 1, se muestra la clasificación de los diferentes tipos de VPNs, la capa del modelo OSI en que operan y su técnica de implementación.

Tabla 1-2: Tipos de VPNs, capas de funcionamiento e implementaciones

Tipo	Capa	Implementación
Frame Relay	2	DLCI
ATM	2	VC
Ethernet	2	VLAN / VPLS
GRE/L2TPv3	3	Tunel IP
IP	3	IPsec

IP	3	DMVPN

Fuente: (Kolon, 2006)
Realizado por: Alex Jaramillo

Frame Relay es una técnica de conmutación de circuitos y fue ampliamente usada para el establecimiento de canales dedicados entre clientes por medio de la creación de circuitos virtuales permanentes o conmutados. Ésta técnica trabaja en el ámbito WAN y corresponde a la capa 2 del modelo OSI, para lo cual requiere de equipos especiales para su funcionamiento. Brinda conexiones de alta velocidad para la transmisión de paquetes de datos y voz pero es ineficiente al tratar de transmitir paquetes en tiempo real, debido a que no garantiza la entrega de los datos; además, se suma la desventaja de que maneja tramas de longitud variable lo cual ocasiona una conmutación ineficiente.

Por otra parte, ATM es una técnica que usa el modo de transferencia asíncrono y al igual que *Frame Relay* trabaja en el ámbito WAN y la capa 2 del modelo OSI. ATM utiliza circuitos virtuales (*VC*) y celdas de tamaño fijo, permitiendo una reducción considerable del retardo y el manejo de prioridades. Las mayores desventajas de ATM, son el alto costo de implementación y alto costo de operación y mantenimiento, considerando los bajos anchos de banda transmitidos.

En el ámbito LAN, la separación e interconexión privada de redes dentro de las empresas es por medio de las VLANs o LAN Virtuales. Las VLANs corresponden al estándar IEEE 802.1q y utilizan "etiquetas" en la cabecera *Ethernet* para agrupar dispositivos en una conexión lógica y separada de otras VLANs. La solución WAN de este tipo de servicio se conoce como VPLS (*Virtual Private LAN Services*) y era ampliamente usada para brindar un canal en capa 2 a clientes matriz con sus sucursales. Esta agrupación o "dominio *bridge*" tiene lugar sobre redes IP/MPLS. Una desventaja que se apreciaba fue la no aplicación de QoS en los canales interurbanos y adicionalmente era necesario establecer acuerdos de ocupación de rangos de VLAN para que no sean duplicados con otros clientes del proveedor del servicio.

En la actualidad las VPNs de capa 3 son las más populares entre los clientes que no están dispuestos a manejar los esquemas de enrutamiento y desean servicios de valor agregado. Por ejemplo, L2TP (*Layer 2 Tunneling Protocol*) es una variación de un protocolo de encapsulamiento IP y crea túneles encapsulando tramas en paquetes UDP, los cuales a su vez se encapsulan en IP. IPsec puede ser utilizado para proteger la información en el túnel. Posteriormente surge la demanda de proveer mejor escalabilidad y la necesidad de implementar VPNs multipunto, como DMVPN.

Las siguientes secciones se enfocan en el análisis de las VPNs de capa 3 y posteriormente se estudiará a profundidad DMVPN que es el tema principal de esta tesis.

2.2.2. Utilización de las VPNs a nivel empresarial

Las tecnologías de redes privadas virtuales conectan a las empresas en cualquier parte, permiten la transmisión de información corporativa y datos más allá de los firewalls de la empresa, y proporcionan una conexión segura y fiable en una red privada a través de la infraestructura de la red pública.

Con el uso de una conexión VPN, las empresas pueden garantizar la privacidad de la información transmitida. Las empresas también pueden incrementar su productividad y eficiencia proporcionando un intercambio de información seguro y veloz, estableciendo comunicación remota segura con la oficina.

Se predice que las Redes Privadas Virtuales (*VPN*) serán una tecnología de red dominante durante el siglo XXI, abriendo numerosas posibilidades, como en su mayoría describe Pérez (2001):

- Redes extranet altamente escalables.
- Redes para el comercio electrónico.
- Redes para proveedores de aplicaciones y servicios.

Conforme las VPNs se convierten en una tecnología global, proporcionan soluciones flexibles para varios tipos de usuarios:

- Servicios VPN compartidos para usos individuales.
- Servicios VPN dedicados para pequeñas y medianas empresas.
- Servidores VPN “in situ” para grandes corporaciones.

De este modo, los proveedores de servicios de Internet están proporcionando nuevas soluciones a las demandas de hoy en día; por ejemplo, la necesidad de reducir costos del pago del servicio de transmisión de datos, conservando las características de seguridad y desempeño.

2.2.3. Seguridad en las VPNs

Las VPNs procuran mantener la conexión y los datos seguros. Debido a que los datos viajan sobre una red pública, la confidencialidad de los datos se logra encriptándolos para que solamente el equipo destinatario pueda descifrarlo. La encriptación se puede lograr con varias técnicas o métodos, como: IPsec, PPTP (*Point to Point Tunneling Protocol*) y L2TP/IPsec.

2.2.3.1. VPN IPsec

IPsec (*Internet Protocol Security Protocol*) proporciona confidencialidad, integridad y un mecanismo de autenticación a la conexión. IPsec tiene dos modos de encriptación: modo túnel y modo transporte. El modo túnel encripta el encabezado y datos del paquete, mientras que el modo transporte sólo encripta los datos. IPsec será analizado con mayor detalle en la sección 2.2.6.3.2 "IPsec".

2.2.3.2. Ventajas y desventajas de las VPN IPsec

VPN IPsec presenta las ventajas y desventajas descritas a continuación.

Ventajas:

- ✓ Es basada en estándares del IETF, lo que la vuelve un estándar global.
- ✓ Proporciona un nivel de seguridad común y homogénea para todas las aplicaciones.
- ✓ Es independiente de la tecnología física empleada.
- ✓ Se integra en IPv4 y se incluye por defecto en IPv6.
- ✓ Es compatible con las tecnologías de transmisión de datos.
- ✓ Es flexible y escalable hasta cierto nivel.
- ✓ Posibilita nuevas aplicaciones como el acceso seguro y transparente de un nodo IP remoto.

- ✓ Proporciona una infraestructura segura para realizar transacciones usando cualquier aplicación.
- ✓ Permite construir una red corporativa segura sobre redes públicas, eliminando la gestión y el coste de líneas dedicadas.
- ✓ Ofrece al usuario el mismo nivel de confidencialidad de que dispone una red local de su empresa.
- ✓ IPsec es transparente para los usuarios y aplicaciones.

Desventajas:

- ✓ IPsec no es seguro si el sistema no lo es: los gateways de seguridad deben estar en perfectas condiciones para poder confiar en el buen funcionamiento de IPsec.
- ✓ IPsec no provee seguridad de usuario a usuario: IPsec no provee la misma clase de seguridad que otros sistemas de niveles superiores.
- ✓ IPsec autentica máquinas, no usuarios: el concepto de identificación y contraseña de usuarios no es entendido por IPsec. Si lo que se necesita es limitar el acceso a recursos dependiendo del usuario que quiere ingresar, entonces habrá que utilizar otros mecanismos de autenticación en combinación con IPsec.
- ✓ IPsec no evita los ataques DoS (*Denial of Service*): estos ataques se basan en sobrecargar la máquina atacada de tal modo de que sus usuarios no puedan utilizar los servicios que dicha máquina les provee.

2.2.4. Arquitectura de las VPN

Existen básicamente dos tipos de arquitectura para una VPN, como es el caso de las VPNs IPsec: de acceso remoto y de punto a punto. Estos tipos de arquitectura se describen a continuación.

2.2.4.1. VPNs de acceso remoto

Las VPNs de acceso remoto ahorran costos a las empresas ya que los usuarios sólo necesitan establecer una conexión de Internet con un ISP. Una vez que se ha establecido la conexión, el usuario puede acceder a los recursos de la intranet privada de la empresa.

Las VPNs de acceso remoto admiten las necesidades de los empleados a distancia, los usuarios móviles y del tráfico de extranet de cliente a empresa, dado que le permiten acceder a los recursos de la empresa siempre que lo requieran.

Una VPN de acceso remoto se crea cuando la información de VPN no se configura de forma estática, pero permite el intercambio dinámico de información y permite habilitarla o deshabilitarla. Esto hace que el *host* o dispositivo logre comunicarse con la red de la empresa a través de la VPN. Cómo se puede apreciar en la Figura 1, el *host* previamente tiene instalado un Cliente VPN; de este modo, el usuario será capaz de conectarse a la red corporativa, sin importar donde se encuentre. Cuando el *host* intenta enviar cualquier tipo de tráfico, el software Cliente VPN encapsula y cifra dicho tráfico. Después los datos cifrados se envían por Internet al Server VPN en el perímetro de la red de destino. Al recibirlos, el Server VPN se comporta como lo hace para las VPN de punto a punto, que veremos a continuación.

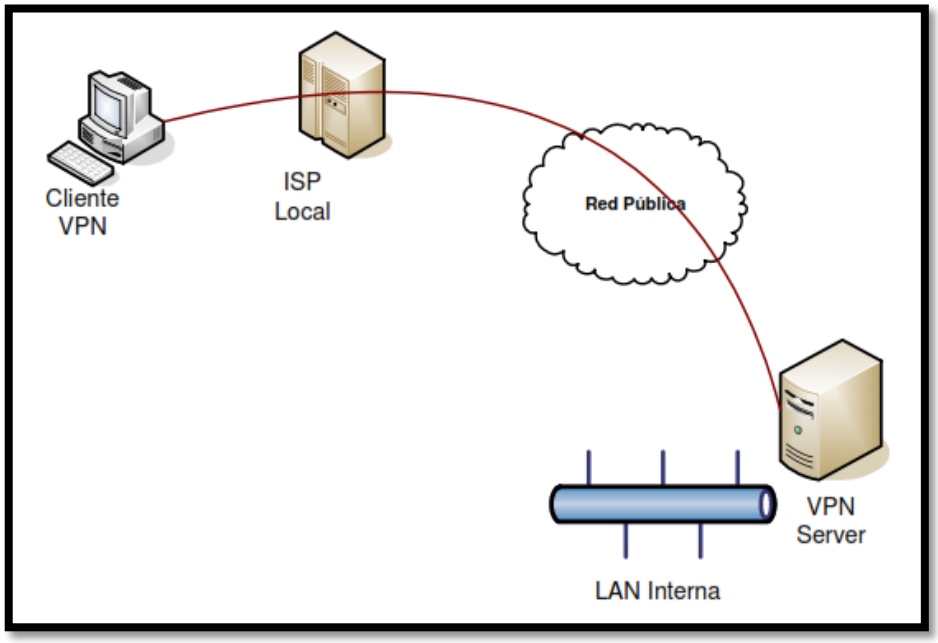

Figura 1-2: Funcionamiento VPN acceso remoto

Fuente: (Trujillo, 2006)

2.2.4.2. VPNs de punto a punto

Las VPNs de punto a punto son utilizadas para conectar sitios geográficamente separados. Los costos de la comunicación también se reducen porque el cliente sólo paga el acceso a Internet; sin

embargo, el mecanismo de conexión es diferente a las VPNs de acceso remoto. Una VPN de punto a punto se crea cuando los dispositivos en ambos lados de la conexión VPN conocen la configuración de VPN con anticipación. La VPN permanece estática y los *hosts* internos no saben que existe una VPN.

Como se muestra en la Figura 2, los *hosts* terminales envían y reciben tráfico TCP/IP de modo normal a través de un "gateway VPN". El gateway VPN es el responsable de encapsular y cifrar el tráfico saliente para todo el tráfico de un sitio en particular. Después, el gateway VPN envía el tráfico por un túnel VPN a través de Internet a un gateway VPN llamado *peer* en el sitio de destino. Al recibir el tráfico, el gateway VPN *peer* elimina los encabezados, descifra el contenido y transmite el paquete hacia el *host* de destino dentro de su red privada.

Las VPN de sitio a sitio conectan redes enteras entre sí. De esta forma se pueden crear redes WAN utilizando una VPN. Una Empresa puede hacer que sus redes se conecten utilizando un ISP local y establezcan una conexión de sitio a sitio a través de Internet.

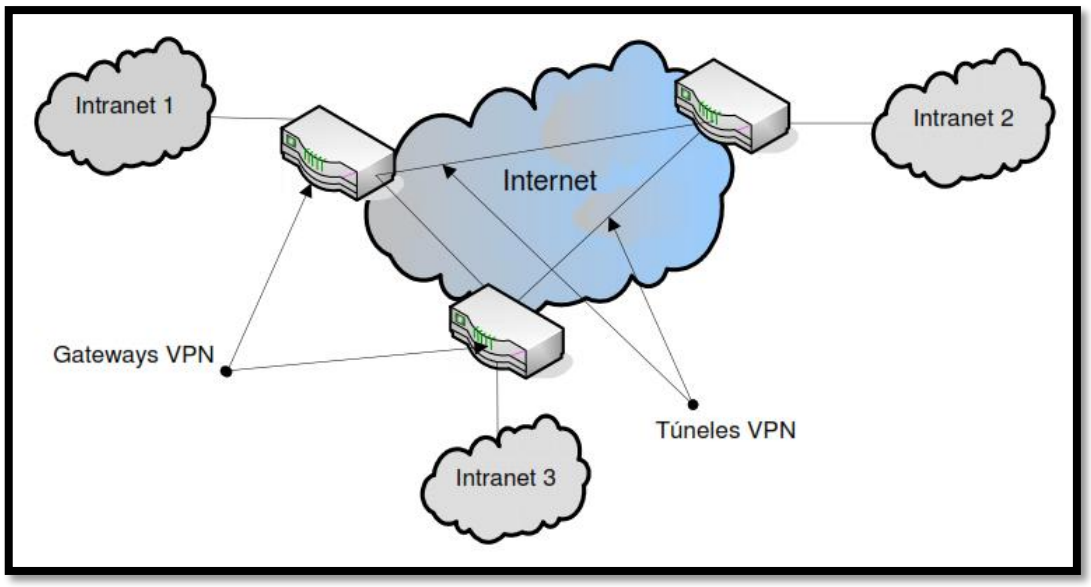

Figura 2-2: Funcionamiento de VPN punto a punto
Fuente: (Trujillo, 2006)

Considerando los problemas comerciales que resuelven, las VPNs punto a punto se subdividen en VPN intranet y VPN extranet.

- Las VPNs intranet se utilizan para una comunicación interna de una empresa, donde se enlazan la oficina matriz con las sucursales, realizando una conexión VPN punto a punto fija y enrutando las redes internas de las oficinas.

- Las VPNs extranet, se utilizan para conectar clientes, proveedores o socios con la red privada de la empresa. Las amenazas en la seguridad de la red extranet son mayores que la red de intranet.

2.2.5. Topología en las VPNs

La topología en las VPNs se decide en función de los problemas que va a resolver. Una misma topología puede ofrecer distintas soluciones en diferentes compañías u organizaciones.

En una VPN podemos encontrar las siguientes topologías:

Para las VPN de sitio a sitio:

- Topología radial.
- Topología de malla completa o parcial.
- Topología híbrida.

Para las VPN de acceso remoto:

- Topología de acceso remoto.

A continuación se describen detalles de las topologías antes mencionadas.

Topología radial

La topología radial es la más común en las VPN de punto a punto. Las sucursales remotas se conectan a un punto central, intercambiando información entre ellas y siempre pasando a través del punto central. La técnica más común que implementa ésta topología es con IPsec.

Topología en malla

Las organizaciones o empresas que no poseen una estructura jerárquica compleja implementan la topología en malla. En este caso, las sucursales realizan el intercambio de datos entre ellas de manera directa. Las conexión podrían ser utilizando una topología de malla completa o parcial; todo depende en gran mayoría si las sucursales intercambian información de manera constante entre ellas. La técnica que aplica este tipo de topología es la DMVPN.

Topología híbrida

Éste tipo de topología resulta de la combinación de la topología radial con la topología de malla parcial. Son a menudo implementadas por las empresas multinacionales, que implementan una topología radial para la conexión de sus sedes en cada país y aplican la topología de malla parcial para su red principal internacional.

Topología de acceso remoto

La topología de acceso remoto consiste en establecer una comunicación punto a punto entre un usuario remoto y el servidor VPN utilizando protocolos de tunelización de capa 3, comúnmente sobre IP.

2.2.6. DMVPN

DMVPN son las siglas de *Dynamic Multipoint VPN* o Red Privada Virtual Multipunto Dinámica. DMVPN es una tecnología que engloba varios protocolos para permitir el establecimiento de túneles privados de manera dinámica sobre redes IP públicas o privadas. Estos túneles son más flexibles que las VPN tradicionales punto a punto o de topología "*Hub and Spoke*".

Mediante una topología tradicional o genérica "*Hub and Spoke*" se implementa túneles estáticos (usando típicamente GRE o IPsec) entre un router "*hub*" ubicado en el centro y sus "*Spokes*" o clientes, los cuales generalmente conectan oficinas o sucursales a la sede central. Cuando se tiene una topología mallada completa o parcial, donde existe un gran número de sitios remotos, la administración de las listas de acceso y túneles punto a punto se vuelve compleja. Además del problema de escalabilidad, se genera una sobrecarga al CPU y memoria del equipo central o "*hub*" incluyendo una posible saturación del ancho de banda asignado a la conexión del "*hub"*.

Ante los problemas mencionados de VPN usando la topología "*Hub and Spoke*" con un número significativo de comunicaciones "*Spoke to Spoke*", DMVPN surge como una interesante alternativa para dinamizar la creación de túneles en topologías en malla.

2.2.6.1. Características de DMVPN

De acuerdo a la documentación emitida por Cisco, DMVPN presenta las siguientes características:

Tabla 2-2: Características de DMVPN

Característica	**Descripción**
Enrutamiento dinámico a través de VPN	• Soporta protocolos de enrutamiento dinámico como: EIGRP, OSPF y BGP.
Reduce la configuración de la cabecera	• DMVPN elimina la necesidad de configurar los mapas criptográficos vinculados a la interfaz física, simplificando drásticamente el número de líneas de configuración requerida para una implementación VPN. • Simplifica la configuración de la división de túnel. Centraliza los cambios de configuración en el concentrador de modo que sea ese el que controle el comportamiento de la división del túnel.
Túneles sitio a sitio dinámicos	• Los túneles directos entre sedes eliminan la necesidad de que el tráfico generado entre ellos atraviese por el concentrador. • Reduce la latencia para el despliegue de voz sobre IP y mejora el rendimiento efectivo del router principal. • Los túneles son creados dinámicamente cuando se requiere y se eliminan cuando se cierra la conexión, permitiendo que el sistema escale de mejor manera.
Direccionamiento dinámico para los routers de las sedes remotas	• Los equipos de las sedes remotas pueden usar direcciones IP dinámicas, lo cual es un requisito frecuente para las conexiones a Internet por cable y ADSL.
Network Address Translation (NAT)	• DMVPN soporta routers de las sedes remotas con NAT o detrás de dispositivos con NAT dinámicos, habilitando mejor seguridad para las subredes de las sucursales.
Soporta IP multicast	• DMVPN soporta tráfico IP multicast (entre la sede matriz y la sucursal); el IPsec nativo soporta solamente IP Unicast. Esto proporciona una distribución eficiente y escalable del tráfico punto-multipunto y multipunto-multipunto.
Soporta QoS	• Permite la asignación de tráfico en las interfaces del *Hub* por *Spoke* o por grupos de *Spokes*. • Permte configurar políticas de QoS en conexiones *Hub to Spoke* y *Spoke to Spoke*.

	• Permte configurar políticas de QoS dinámico en el que las plantillas de QoS se unen automáticamente a los túneles que vayan surgiendo.
Alta disponibilidad	• Permite el enrutamiento basado en conmutación por error. • Enlaces WAN *dual* y redundancia HUB proporcionan una mayor disponibilidad. DMVPN soporta diseños de doble HUB, donde cada *Spoke* disponga de dos concentradores, proporcionando *failover* rápido.
Escalabilidad	• DMVPN escala a miles de *Spokes* que utilizan el equilibrio de carga del servidor (SLB). El cifrado se puede integrar en el dispositivo del SLB o distribuido a los routers VPN cabecera reservados. • El rendimiento se puede escalar progresivamente añadiendo HUBs.
Soporta el Protocolo Múltiple de Intercambio de Etiquetas (MPLS)	• Redes MPLS pueden ser encriptadas sobre túneles DMVPN.

Fuente: (Cisco Systems, Cisco Dynamic Multipoint VPN: Simple and Secure Branch-to-Branch Communications, 2015)

Realizado por: Alex Jaramillo

Por lo indicado anteriormente se puede concluir que DMVPN es muy flexible, dinámico y seguro, y que puede adaptarse a diversos tipos de implementaciones. DMVPN también permite controlar el tráfico y seleccionar el trayecto usando el protocolo dinámico de ruteo.

2.2.6.2. Topologías de diseño

De acuerdo a la información tomada de Cisco, la tecnología DMVPN se implementa por fases en dos esquemas o topologías: *Hub-and-Spoke* y *Spoke-to-Spoke*. Estas topologías se describen en la Figura 3 y son explicadas a continuación.

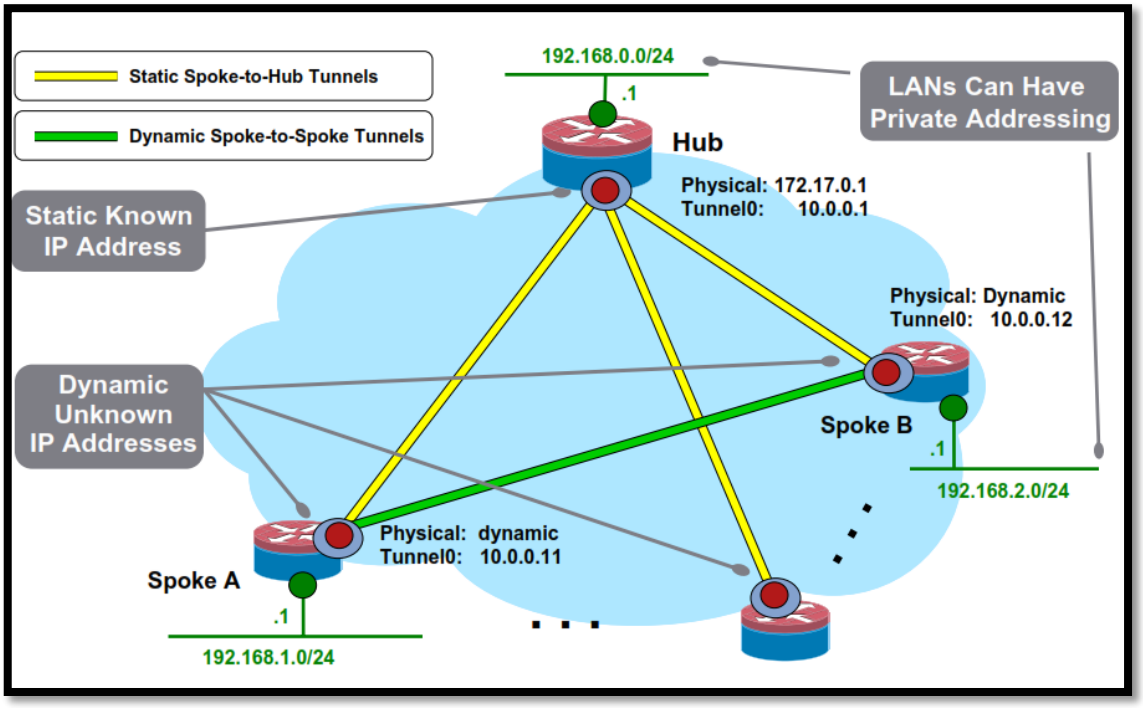

Figura 3-2: Topologías DMVPN

Fuente: (Cisco Systems, Cisco IOS DMVPN: Overview, 2008)

- Topología Hub-Spoke

DMVPN en su inicio establece túneles permanentes IPsec entre el *hub* y sus *spokes*. No se configuran túneles IPsec entre *spokes.* A continuación, cada *spoke* se registra como "cliente" del servidor de NHRP (*Next Hop Resolution Protocol*) que se implementa en el *hub*.

- Topología Spoke- Spoke

Cuando un *spoke* necesita enviar un paquete a una subred de destino privada, sobre otro *spoke*, éste solicita al servidor de NHRP la dirección externa o pública de dicho *spoke* de destino. Una vez que el *spoke* de origen ha aprendido la ubicación real de su "par", éste puede iniciar un túnel IPsec dinámico al *spoke* de destino. Entonces, el túnel *spoke – spoke* es creado sobre la interface GRE (*Generic Routing Encapsulation*) multipunto, la cual permite encapsular el protocolo de enrutamiento utilizado. De este modo, todos los enlaces *spoke – spoke* se establecen bajo demanda en cualquier instante en que exista tráfico entre los mismos. Por lo tanto, los paquetes pueden saltarse o evitar pasar por el *hub* y usar el túnel entre *spokes*.

2.2.6.3. Arquitectura de DMVPN

Como se vio en el apartado anterior, DMVPN es la combinación de las siguientes técnicas y protocolos:

- *mGRE* (*Multipoint Generic Routing Encapsulation*).
- NHRP (*Next Hop Resolution Protocol*).
- Protocolos de enrutamiento dinámico: EIGRP, RIP, OSPF, BGP.
- Encriptación dinámica IPsec.
- CEF (*Cisco Express Forwarding*).

Las principales características de GRE, IPsec y NHRP se explican a continuación.

- **GRE**

GRE (*Generic Routing Encapsulation*) es un protocolo de *tunneling* desarrollado por Cisco que puede encapsular una amplia variedad de tipos de paquete y protocolos dentro de túneles IP. GRE está definido en la RFC 1701 y en la RFC 1702.

Como se puede apreciar en la Figura 4, GRE encapsula paquetes IP y los transporta a través de túneles VPN. IPsec, que es un mecanismo estándar para proporcionar seguridad en redes IP, no puede cifrar paquetes de multidifusión. Sin embargo, estos paquetes se pueden encapsular dentro de un túnel GRE y luego enrutar a través de una conexión VPN, de modo que los paquetes encapsulados estén protegidos por el túnel IPsec.

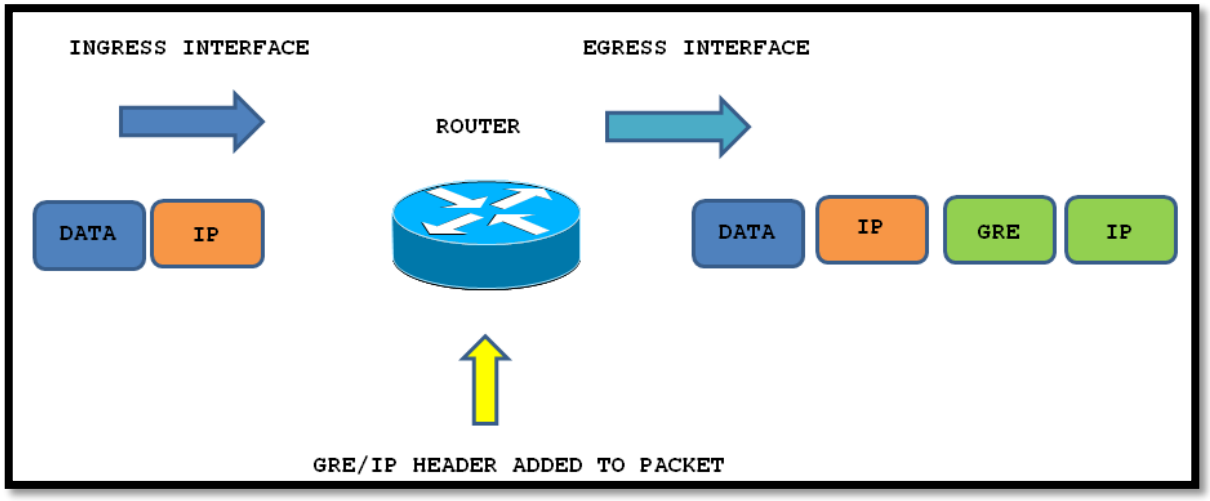

Figura 4-2: Flujo GRE

Fuente: (Rodriguez, 2013)

Características de GRE

Las características de GRE son las siguientes:

- GRE se define como un estándar IETF (RFC 1701 y 1702).
- En el encabezado IP externo, en el campo de protocolo se utiliza el número 47 para indicar que lo que sigue es un encabezado GRE.
- La encapsulación de GRE utiliza un campo de "tipo de protocolo" en el encabezado para admitir la encapsulación de cualquier protocolo de capa 3 del modelo OSI. Los tipos de protocolo se definen en RFC 1700 como "EtherTypes".
- GRE no incluye ningún mecanismo sólido de seguridad para proteger su contenido.
- El encabezado GRE, junto con el encabezado de tunneling IP añade por lo menos 24 bytes a la cabecera de los paquetes que se envían por el túnel.
- GRE permite emplear protocolos de enrutamiento especializados que obtengan el camino óptimo entre los extremos de la comunicación.

Cabecera GRE

El protocolo de encapsulado GRE está descrito en la RFC1701 y el caso de IP sobre IP con GRE está en la RFC1702.

El protocolo GRE añade un mínimo de 24 bytes a la cabecera de los paquetes que pasan por el túnel.

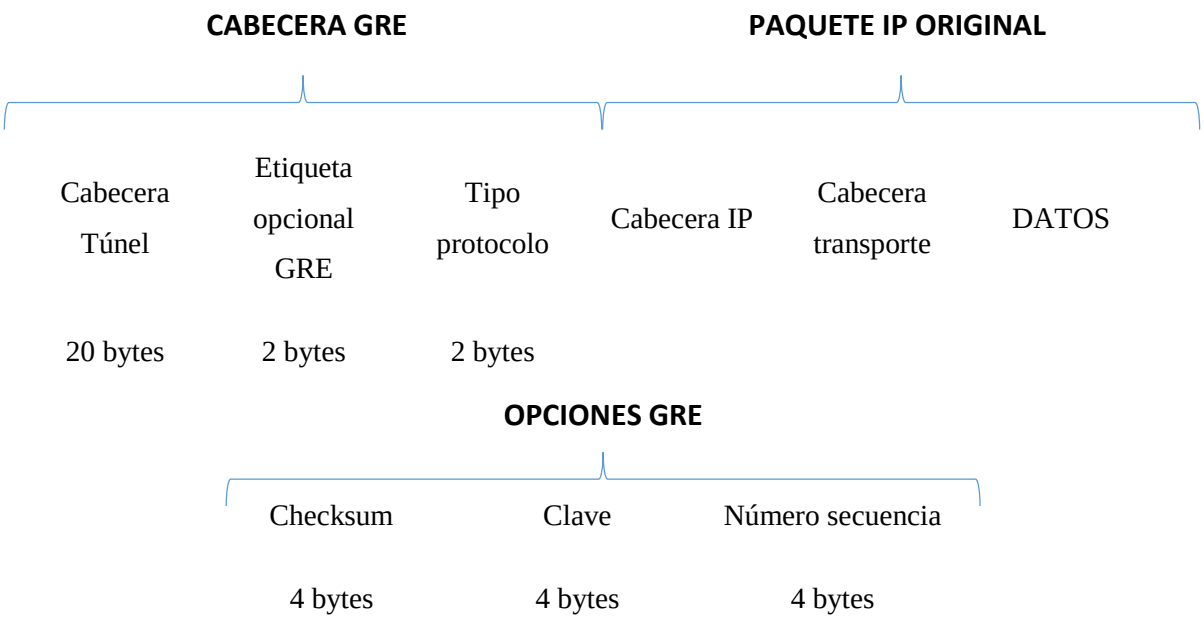

Figura 5-2: Trama GRE

Fuente: (Alejandro, 2017)

Como se muestra en la Figura 5, de los 24 bytes nuevos, 20 bytes se ocupan para la nueva cabecera IP especificando la dirección origen y destino.

De los 4 bytes restantes, los dos primeros se usan para parámetros opcionales. Los dos últimos bytes indican el tipo de protocolo que está transportando el túnel. En la Figura 6 se describe los campos de estos 4 bytes de la cabecera GRE a nivel de bits.

Bits 0-4					**5-7**	**8-12**	**13-15**	**16-31**
C	**R**	**K**	**S**	**S**	**Recur**	**Flags**	**Version**	**Tipo protocolo**
Checksum (opcional)								**Offset (opcional)**
Key (opcional)								
Sequence number (opcional)								
Routing (opcional)								

Figura 6-2: Cabecera GRE

Fuente: (Wikipedia, Wikipedia, 2014)

A continuación se detalla el significado de los parámetros indicados en la Figura 6-2:

- ***C*** (bit 0), representa la opción *Checksum Present*. Si está en 1 quiere decir que se activa el campo opcional Checksum de la cabecera GRE y también debe agregarse el campo offset. Normalmente no es necesario puesto los protocolo de capas superiores ya realizan el checksum para detectar paquetes corruptos.
- ***R*** (bit 1), representa la opción Routing. Por lo general ya no es usado, pero si se ubica en 1 deberá ser acompañado por los campos Checksum y Offset.
- ***K*** (bit 2), representa la opción Key. Si está en 1 añade el campo de seguridad y proporciona un sistema básico de seguridad comprobando que cada extremo del túnel tiene la misma clave.
- ***S*** (bit 3), representa la opción Sequence number. Si se ubica en 1 quiere decir que el campo opcional del número de secuencia está presente.
- ***s*** (bit 4), representa el campo Strict Source Route. Recomiendan ponerlo a 1 sólo si toda la información de enrutamiento está formada por rutas estrictas.
- ***Recur*** (bits 5-7), representa el campo de Control de Recursión. Contiene un entero positivo de 3 bits que indica el número de encapsulaciones adicionales que están permitidas. Siempre posee el valor 0.
- ***Flags*** (bits 8-12), es un campo reservado y se recomienda permanecerlo en 0.
- ***Ver*** (bits 13-15), representa al número de versión de GRE. El valor 0 representa a GRE y 1 a PPTP.
- ***Protocol type*** (bits 16-31), representa el campo de protocolo. Permite identificar qué tipo de paquete está atravesando el túnel, siendo 0x0800 el usado para IP.
- ***Checksum*** (2 bytes), representa el campo opcional de la cabecera GRE. Contiene el Checksum IP de la cabecera GRE y paquete interno.
- ***Offset*** (2 bytes), representa el campo opcional de GRE e indica el desplazamiento en octetos desde el inicio del campo routing hasta la primera ruta que debe ser examinada.
- ***Key*** (4 bytes), representa un campo opcional de GRE. Contiene un número insertado por la parte encapsuladora del túnel que puede utilizarse en destino para propósitos de comprobación del remitente correcto
- ***Sequence number*** (4 bytes), representa el campo opcional de GRE del número de secuencia. Corresponde al número usado por el receptor para asegurar el correcto orden de llegada de los paquetes.
- ***Routing*** (variable), representa un campo opcional que contiene una lista de rutas.

El tamaño máximo de toda la cabecera GRE sería de 36 bytes si se añaden los 12 bytes correspondientes a los parámetros opcionales que este protocolo posee.

Configuración de GRE

La configuración de GRE necesita crear una interfaz lógica mediante el *Tunnel Interface* en los routers extremos del túnel. Después de esto se configura en cada interfaz lógica las direcciones IPs de WAN de dichos routers como *source* y *destination*. Por último, se debe agregar un direccionamiento privado de cualquier máscara y asignarla a la interfaz lógica.

A continuación la Figura 7 y la Tabla 3 muestran un ejemplo de configuración de GRE:

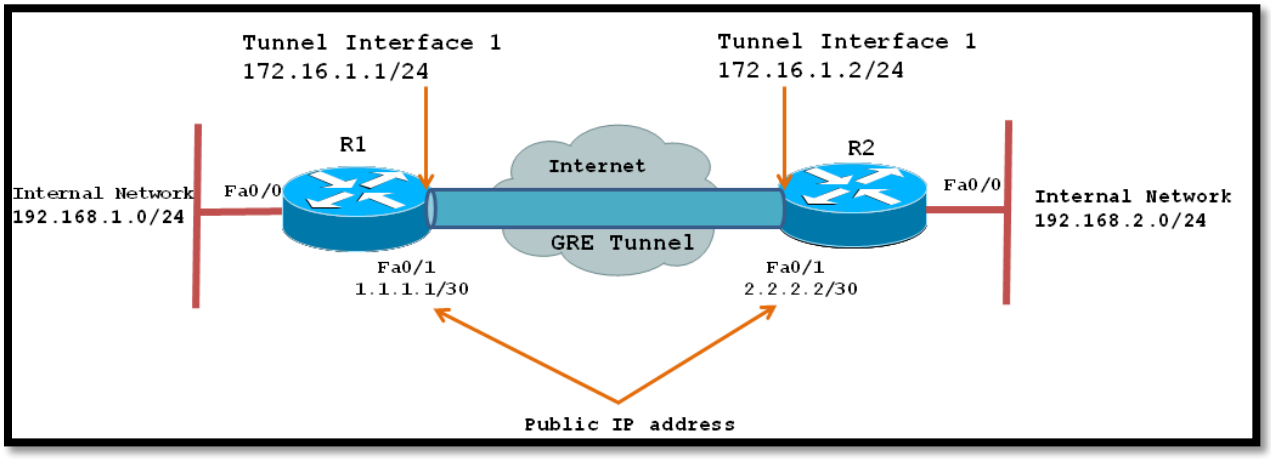

Figura 7-2: Configuración de GRE

Fuente: (Rodriguez, 2013)

Tabla 3-2: Ejemplo de configuración de GRE

R1	R2
R1(config)# interface Tunnel1	R2(config)# interface Tunnel1
R1(config-if)# ip address 172.16.1.1 255.255.255.0	R2(config-if)# ip address 172.16.1.2 255.255.255.0
R1(config-if)# ip mtu 1400	R2(config-if)# ip mtu 1400
R1(config-if)# ip tcp adjust-mss 1360	R2(config-if)# ip tcp adjust-mss 1360
R1(config-if)# tunnel source 1.1.1.1	R2(config-if)# tunnel source 2.2.2.2
R1(config-if)# tunnel destination 2.2.2.2	R2(config-if)# tunnel destination 1.1.1.1

Fuente: (Rodriguez, 2013)

- **IPsec**

IPsec son las siglas de *IP Security*. IPsec es un conjunto de estándares del IETF que proporciona servicios de seguridad a la capa IP y a todos los protocolos de capas superiores basados en IP. IPsec se desarrolla en base a la necesidad creciente de garantizar un nivel de seguridad al protocolo IP. La arquitectura IPsec se describe en el RFC2401.

IPsec combina tecnologías de clave pública (RSA), algoritmos de cifrado (DES, 3DES, IDEA, AES, CAMELLIA, BLOWFISH), algoritmos de hash (MD5, SHA-1, SHA-256, SHA-512) y certificados digitales X509v3, para proporcionar confidencialidad, integridad y autenticidad respectivamente. (González, 2014)

Se distinguen los siguientes componentes que conforman IPsec, los cuales se describen a detalle más adelante:

- **Protocolos de seguridad:** el *IP Authentication Header* (AH) y el *IP Encapsulating Security Payload* (ESP); ambos proveen mecanismos de seguridad para proteger el tráfico IP.
- **Protocolo de gestión de claves**, denominado *Internet Key Exchange* (IKE) que permite a dos puntos negociar las claves y todos los demás parámetros para establecer una conexión por AH o ESP.

Características de IPsec

A continuación se detallan algunas características de IPsec.

1. Permite implementar una red corporativa segura sobre redes públicas, eliminando la gestión y el coste de canales dedicados de datos.
2. Proporciona una comunicación segura sobre la que se pueda realizar transacciones usando cualquier aplicación.
3. Ofrece el mismo nivel de confidencialidad que una red local.
4. Proporciona confidencialidad, integridad y autenticidad de los datagramas IP para la transmisión segura de datos sensibles de una organización.

Cabecera IPsec

La cabecera IPsec se compone de acuerdo a los protocolos AH o ESP que se aplique y a su modo de funcionamiento. De acuerdo a su funcionamiento la cabecera IPsec lo conformaría todo el paquete IP o solamente la información de capas superiores.

Protocolo de cabecera de autenticación – AH

AH es el protocolo que se ocupa de garantizar la integridad y autenticación de los datagramas IP. Esto se logra insertando una cabecera de autenticación denominada AH entre la cabecera IP (IPv4 o IPv6) y los datos transportados (por ejemplo: TCP, UDP o ICMP), como se puede apreciar en la Figura 8.

IANA (*Internet Assigned Numbers Authority*) le ha asignado a AH, el número decimal 51; esto quiere decir, que el campo "protocolo" de la cabecera IP contiene el valor 51, en lugar los valores 6 que representa a TCP o 17 a UDP.

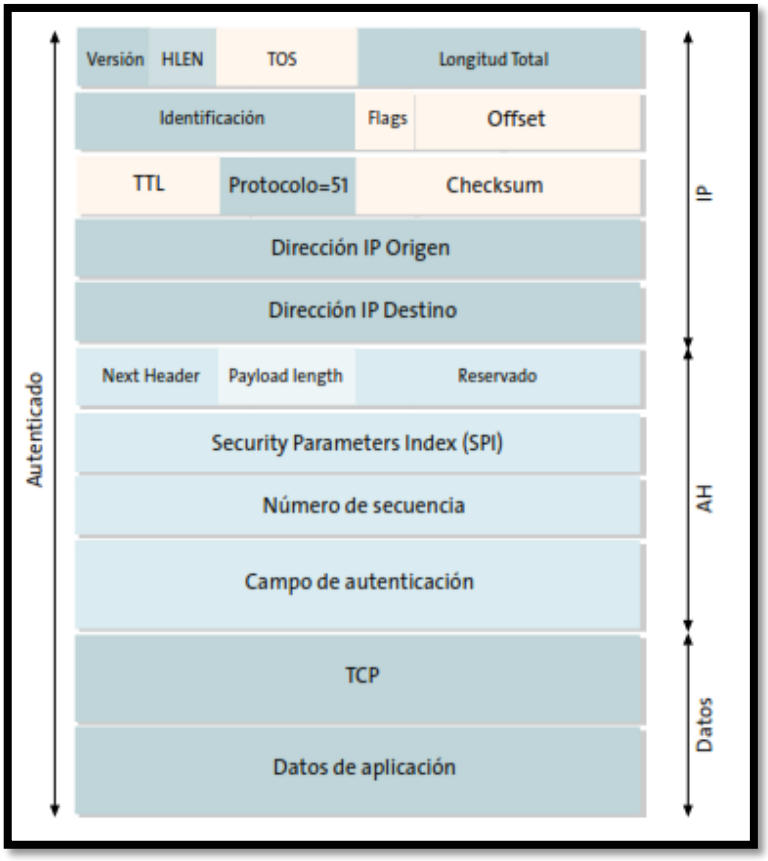

Figura 8-2: Estructura del datagrama AH

Fuente: (Pérez, 2001)

AH garantiza la integridad mediante el uso de un *message digest* o compendio del mensaje generado por un algoritmo como HMAC-MD5 o HMAC-SHA. Si los datos originales son alterados, entonces el *message digest* cambia y el cliente es alertado. La autenticación del origen de los datos se ejecuta mediante el uso de una "clave secreta" compartida que sirve para crear el *message digest*. AH por ende autentica las cabeceras de IP y sus cargas, a excepción de los campos variables del encabezado que cambian durante el tránsito como: ToS, flags, offset, checksum y TTL.

Protocolo de Carga de Seguridad Encapsulada – ESP

El protocolo ESP proporciona confidencialidad al paquete transmitido a través de IPsec. Para hacer este trabajo, define el cifrado y la forma en que se ubicarán los datos en un nuevo datagrama IP. El protocolo ESP también proporciona integridad y autenticación usando mecanismos

similares a AH; la diferencia básica radica en que AH no realiza ningún cifrado de la información. No obstante, la estructura de ESP es más compleja que AH, debido a que aporta más funciones. Los paquetes pueden transmitirse vía TCP, UDP o un datagrama IP completo. En la Figura 9 se puede apreciar la estructura de ESP.

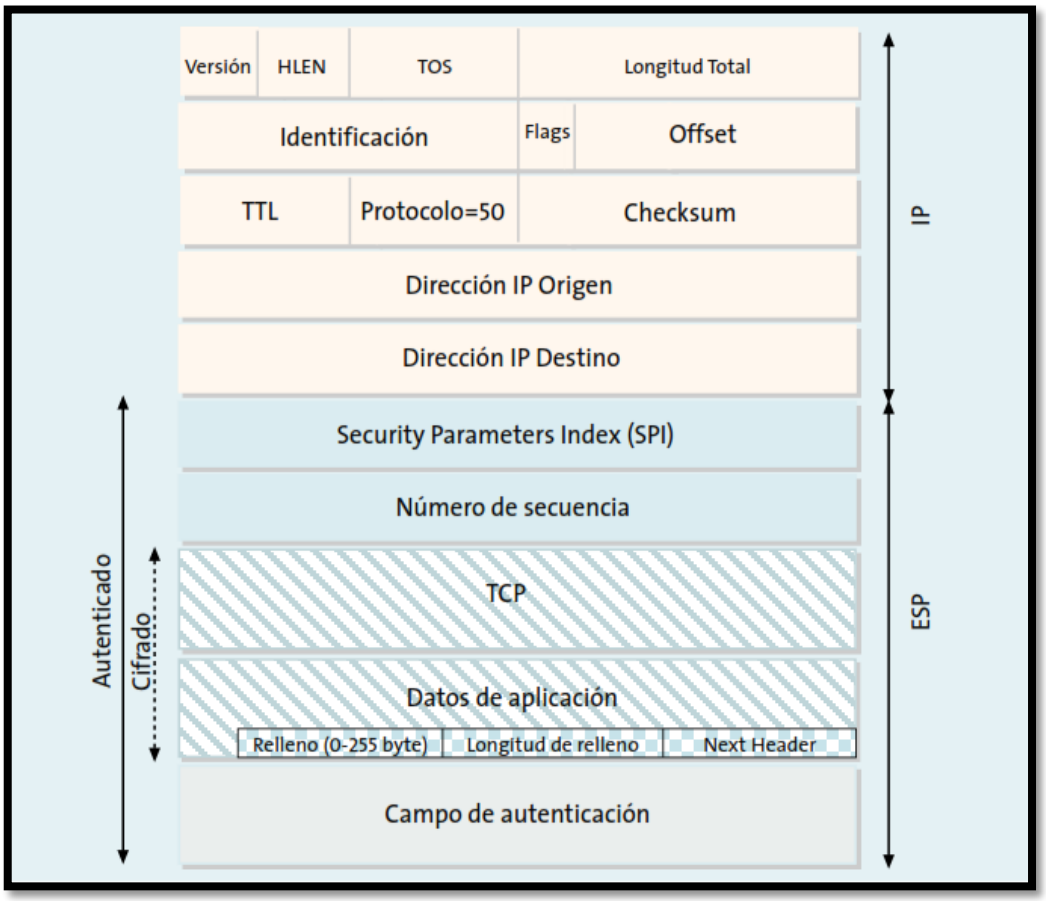

Figura 9-2: Estructura del datagrama ESP

Fuente: (Pérez, 2001)

La cabecera ESP está conformada por un campo de 32 bits que especifica el "Índice de Parámetros de Seguridad" (SPI), que es donde se indica el *Security Association* (*SA*) a emplear para para desencapsular el ESP. Una asociación de seguridad es una conexión unidireccional que ofrece servicios de seguridad al tráfico transportado por éste. El siguiente campo de 32 bits indica el "Número de Secuencia", empleado para protegerse de ataques del tipo DoS (*Denial of Service*). Los siguientes campos corresponden al proceso de cifrado, iniciando con un campo denominado TCP que corresponde al contenido o carga útil que no precisamente puede ser TCP, pero al viajar cifrado no importa qué tipo de contenido es; el tamaño que representa es de 32 bits y cuya función es asegurar que dos cargas idénticas generen dos cargas cifradas diferentes.

ESP usa algoritmos de cifrado en bloque, de tal forma que la longitud de los datos a cifrar debe ser del mismo tamaño o múltiplo del bloque; en la mayoría de los casos son de 8 o 16 bytes de tamaño. Si el tamaño de la carga no es un múltiplo se aplica el campo de relleno, dónde se añade caracteres al campo de datos para ocultar su longitud real. Luego se incluye el campo "Next Header" de 2 bytes que indica el tipo de la siguiente cabecera. Como último campo se tiene el de "Autenticación", donde se añaden 96 bits de HMAC (*Hash Message Authentication Code*) para asegurar la integridad del paquete. En este proceso de cálculo sólo se incluye la carga del paquete, no la cabecera IP.

Protocolo de gestión de claves Internet Key Exchange – IKE

La distribución de claves de forma segura es un requisito esencial para el funcionamiento de ESP y AH. Así mismo es importante que el emisor y el receptor estén de acuerdo en el algoritmo de cifrado y el resto de parámetros comunes a aplicar. Por tal motivo se debe utilizar un gestor de claves que se encargue en negociar y controlar estos parámetros; este gestor es denominado IKE.

IKE es un protocolo que permite establecer una "Asociación de Seguridad" (SA) en el protocolo IPsec. Tanto AH como ESP, hacen uso de asociaciones de seguridad y una función importante de IKE es el establecimiento y mantenimiento de las asociaciones de seguridad. En una asociación de seguridad se definen las direcciones IP origen y destino de la comunicación. En una sola SA se puede proteger un sentido del tráfico; sin embargo, para proteger ambos sentidos, IPsec necesita de dos SA unidireccionales.

IKE es un protocolo híbrido que es resultado de la integración de dos protocolos, ISAKMP y Oakley. ISAKMP define la sintaxis de los mensajes que se utiliza en IKE, mientras que Oakley especifica la lógica de cómo realizar el intercambio de una clave de forma segura entre dos partes que no se conocen previamente.

Modos de funcionamiento de IPsec

IPsec permite su aplicación en dos modos de funcionamiento: el modo transporte y modo túnel.

Modo Transporte.

En el modo transporte, la información transportada dentro del datagrama AH o ESP corresponde a los datos de la capa de transporte; por ejemplo, los datos de TCP o UDP. La cabecera IPsec se inserta después de la cabecera IP y antes de los datos de protocolos de capas superiores. El modo transporte asegura la comunicación extremo a extremo, requiriendo que ambos extremos manejen el protocolo IPsec.

Modo Túnel.

En el modo túnel, la información del datagrama AH o ESP es un datagrama IP completo, incluido la cabecera IP original; de esta forma se añade una nueva cabecera IP que se utilizará para encaminar el paquete a través de la red. La cabecera IPsec aparece después de la cabecera IP externa y antes de la interna.

El modo túnel se puede aplicar de varias formas. La forma que se empleará para la presente investigación es la que permite establecer redes privadas virtuales a través de redes públicas, permitiendo usar ESP o AH como método de autenticación.

En la Figura 10 se muestran los dos modos de funcionamiento de IPsec.

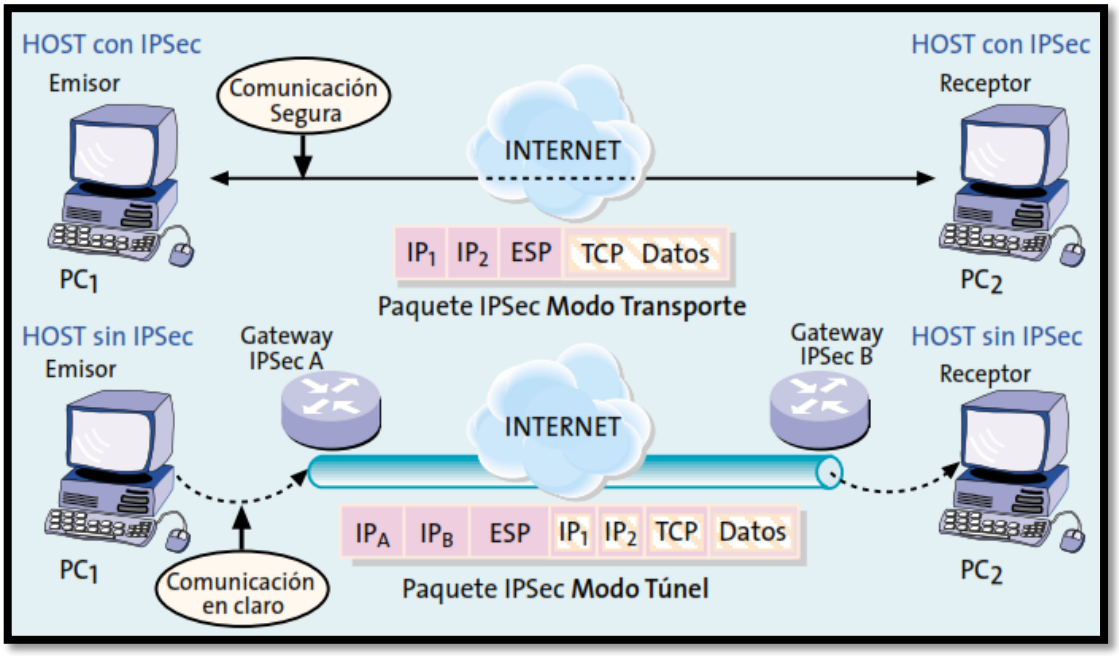

Figura 10-2: Modos de funcionamiento IPsec

Fuente: (González, 2014)

En la parte superior de la Figura 10 se visualiza la comunicación del paquete IPsec en modo transporte, donde la información que se protege es únicamente el protocolo de transporte TCP o UDP y los datos. Por otra parte en la parte inferior se observa, la comunicación del paquete IPsec en modo túnel, donde se realiza por medio de dos Gateway IPsec que por lo general son routers de frontera de las dos redes privadas que intercambiarán información. Los Gateway establecen el túnel IPsec protegiendo las cabeceras IP, protocolos de transporte y datos, permitiendo a los host una comunicación transparente y segura.

Configuración de IPsec

Para configurar correctamente el protocolo IPsec en equipos Cisco, se requiere el establecimiento de dos túneles, los cuales se crean en dos fases. La primera fase llamada IKE *(Internet Key*

Exchange), se ocupa de crear un túnel entre ambos sitios para que se comuniquen entre ellos y puedan intercambiar información de control; por lo tanto, se debe crear una política con ISAKMP (*Internet Security Association and Key Management Protocol*) para compartir y negociar las siguientes variables:

- Método de autenticación.
- Algoritmo de cifrado.
- Algoritmo *Hash*.
- Grupo *Diffie-Hellman*.
- *Lifetime* o tiempo de vida del túnel.

Sí y sólo sí se establecen con éxito la comunicación de ambos routers, se avanza a la segunda fase.

La segunda fase llamada "IPsec" es la encargada de establecer el túnel por donde se transmitirá la información de una manera cifrada. En esta fase es donde se establecen los parámetros de la clave compartida, las listas de acceso para las redes que se comunicarán LAN a LAN y los parámetros de cifrado.

De acuerdo a esta información, a continuación se describen los pasos a seguir en la configuración de cada fase.

Fase 1.

1. En modo de configuración de terminal, se crea la política `crypto isakmp` con cualquier número como identificador.
   ```
   #crypto isakmp policy 10
   ```
2. Se establece el método de autenticación.
   ```
   #authentication pre-share
   ```
3. Se escoge el algoritmo de cifrado; debido a que el objetivo del presente trabajo es evaluar el rendimiento de IPsec y DMVPN escogeremos un algoritmo que brinde la seguridad necesaria sin afectar el rendimiento del procesador y RAM del Router.
   ```
   #encryption 3des
   ```
4. Se selecciona el algoritmo *hash*; en este caso es "md5".
   ```
   #hash md5
   ```
5. El grupo 2 *Diffie-Hellman* permite el intercambio de claves en tramas de 1024 bit, una longitud soportada por la mayoría de routers.
   ```
   #group 2
   ```

Fase 2.

1. Se configura el "IPsec t*ransform*"
   `#crypto ip sec transform-set ESP-AES-SHA` (es el nombre de cifrado que se le da) `esp-aes esp-sha-hmac`
2. Se define la contraseña compartida a utilizar entre ambos routers.
   `#crypto isakmp key cisco address` (IP del equipo remoto)
3. Se configura la lista de acceso, ACL, para el permiso de transferencia a ciertas subredes.
   `#ip access-list extended 100`
   `#permit` (RED LAN) `wilcard` (RED LAN REMOTA) `wilcard`
4. Se configura el "*crypto map*".
   `#crypto map VPN 10 ipsec-isakmp`
   `#set peer` (IP WAN REMOTO)
   `#set transform-set ESP-AES-SHA` (nombre del cifrado)
   `#match address 100` (número o nombre de ACL)
5. Se habilita y aplica el "*crypto map*" en la interfaz WAN
   `#crypto isakmp enable`
   `#interface fastethernet 1` (WAN)
   `#crypto map VPN`

Los mismos pasos se debe replicar en el Router de llegada.

- NHRP

Next Hop Resolution Protocol (NHRP) o Protocolo de Resolución del Siguiente Salto se encuentra definido en la RFC2332. NHRP facilita el establecimiento del túnel dinámico al proveer una resolución de direcciones de túnel a interfaz física. El protocolo además permite la simplificación de la configuración de los equipos; por ejemplo, en DMVPN los equipos que funcionan como *hubs* no necesitan tener configurada la dirección de ninguno de los *spokes* y por lo tanto las direcciones de los *spokes* pueden ser asignados dinámicamente. Unicamente en los *spokes* es necesario configurar la dirección de uno o todos los *hubs* de la red.

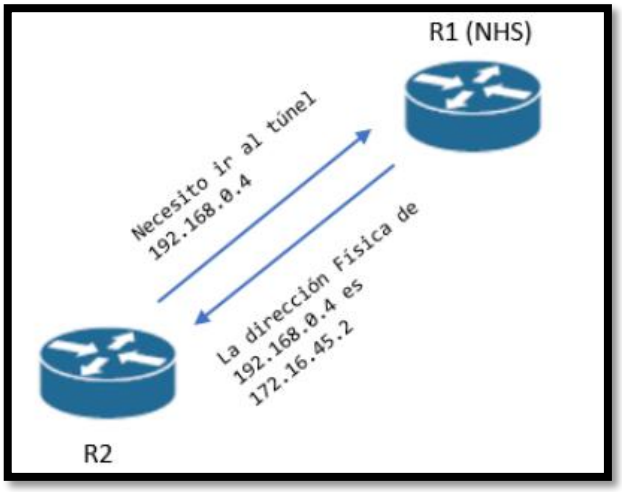

Figura 11-2: Funcionamiento NHRP

Fuente: http://3.bp.blogspot.com/-xbHrPiFvK44/Vi7tE7fxLmI/AAAAAAAAAg8/k8yOmG1WeQg/s400/NHRP.png

Cada *spoke* de la red debe registrarse en el *hub* que tenga configurado, estableciendo un túnel permanente entre ambos. Como se observa en la Figura 11, el router R1 o *hub* tiene registradas las rutas de cada *spoke.* Cuando el router R2, que es uno de los *spokes*, intenta comunicarse con otro *spoke*, el router R1 le informa de las rutas aprendidas enviando la dirección física del destino. De esta manera, cuando el *spoke* necesite comunicarse con otro *spoke* pueda realizarlo sin problemas y de manera directa, como si se tratara de una red mallada.

Características de NHRP

El protocolo NHRP posee varias características que lo vuelven viable para el establecimiento túneles dinámicos.

NHRP es un protocolo similar a un protocolo de resolución de direcciones (ARP) que mapea dinámicamente una red de acceso múltiple sin difusión (NBMA). Con NHRP, los sistemas conectados a una red NBMA pueden aprender dinámicamente la dirección NBMA (física) de los otros sistemas que forman parte de esa red, permitiendo que estos sistemas se comuniquen directamente.

NHRP es un protocolo de cliente y servidor donde el concentrador es el *Next Hop Server* (NHS) y los clientes son los *Next Hop Clients* (NHC). El *hub* mantiene una base de datos NHRP de las direcciones de interfaz pública de cada *spoke*. Cada *spoke* registra su dirección real cuando arranca y consulta la base de datos NHRP para obtener direcciones reales de los *spoke* de destino para construir túneles directos.

Cuando NHRP se combina con IPsec, la red NBMA es básicamente una colección de enlaces de túnel lógico punto a punto a través de una red IP física.

NHRP permite dos funciones para ayudar a respaldar estas redes NBMA:

1. **Registro de NHRP**. NHRP permite que los *Next Hop Clients* (NHC) se registren dinámicamente con los *Next Hop Servers* (NHS). Esta función de registro permite que los NHC se unan a la red NBMA sin cambios de configuración en los NHS; especialmente en casos donde el NHC tiene una dirección IP física dinámica o está detrás de un enrutador de traducción de direcciones de red (NAT) que cambia dinámicamente la dirección IP física.

2. **Resolución NHRP.** Con NHRP, los sistemas conectados a una red NBMA aprenden dinámicamente la dirección NBMA de los otros sistemas que forman parte de esa red, permitiendo que estos sistemas se comuniquen directamente sin requerir que el tráfico use un salto intermedio. Esta función alivia la carga en el salto intermedio (NHS) y puede aumentar el ancho de banda total de la red NBMA para que sea mayor que el ancho de banda del enrutador del concentrador.

En el protocolo NHRP existen siete tipos de paquetes que viajan entre los NHC y los NHS (Lima L. , Implementación de una red privada virtual dinámica DMVPN con protocolos IPsec, MGRE y NHRP, 2017), los cuales se detallan a continuación:

1. ***Registration Request:*** petición de registro de un NHC ante un NHS.
2. ***Registration Reply:*** respuesta del NHS al pedido de registro del NHC.
3. ***Resolution Request:*** petición de resolución de una dirección del siguiente salto enviada por el NHC al NHS.
4. ***Resolution Reply***: respuesta del NHS al NHC con la dirección solicitada.
5. ***Purge Request*:** petición de borrado de una entrada de caché enviada por el NHS a un NHC cuando deja de ser válida.
6. ***Purge Reply*:** respuesta del NHC al NHS a una petición de borrado.
7. ***Error indicator***: paquete de error que indica un problema en algún paquete recibido en el equipo que generó el paquete de error.

CAPITULO III

3. METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Tipos y diseño de la investigación

3.1.1. Tipo de la investigación

La presente investigación se clasifica como “aplicada” y “descriptiva”.

- **Aplicada**: debido a que se basa en conocimientos o descubrimientos existentes, como lo es la técnica DMVPN, y ya que es derivada de investigaciones y desarrollos previos.
- **Descriptiva**: ya que describirá e interpretará las variables y resultados obtenidos para realizar la comparación de tecnologías (IPsec y DMVPN) en busca de la optimización del desempeño de VPNs sobre Internet.

3.1.2. Diseño de la investigación

El presente trabajo de investigación se considera como “cuasi-experimental”.

Cuasi-Experimental porque la investigación va más allá de la descripción de conceptos, ya que propone comparar la técnica DMVPN con VPN IPsec para optimizar el rendimiento de las redes privadas virtuales con el desarrollo de escenarios prácticos donde se medirá el efecto de las variables independientes sobre la variable dependiente.

3.2. Métodos de la investigación

En la presente investigación se utilizaron los siguientes métodos:

- **Método científico:** mismo que servirá para recolectar la información obtenida de los escenarios de pruebas a ser implementado, ya que las ideas, conceptos, y teorías expuestas en este anteproyecto de tesis son verificables como válidos.

- **Método hipotético-deductivo:** debido que al estudiar de manera general la técnica DMVPN y compararla a IPsec, se crea la hipótesis de que con una adecuada configuración se puede mejorar el rendimiento de las VPNs; así se deducirá los parámetros que ayuden a comprobar dicha hipótesis y se los comparará con la experiencia obtenida en la práctica.

3.3. Enfoque de la investigación

El presente trabajo investigativo toma un enfoque "cuantitativo". Éste enfoque utiliza la efectividad como el criterio para juzgar el valor de la investigación y son las circunstancias de los experimentos las que determinan el grado en que se utilizan las aproximaciones cuantitativas. Debido a que los datos son producto de mediciones, se representan mediante números y se van analizar a través de métodos estadísticos (Hernández, Fernández, & Baptista, 2010).

3.4. Alcance de la investigación

El presente estudio tiene un alcance de investigación "correlacional" y "explicativo". El primer alcance es debido a que se realizará la comparación de dos esquemas, los cuales bajo un mismo *set* de *hardware* y configuraciones (variables independientes), arrojarán resultados distintos de desempeño (variables dependientes). El segundo alcance es debido a que se tratará de explicar las condiciones y parámetros en los cuales se puede mejorar en el desempeño de las VPNs

implementadas mediante la técnica DMVPN en lugar de IPsec y en redes públicas basadas en Internet.

3.5. Población de estudio

La población de estudio en la presente investigación la conforman la "cantidad de pruebas" o "experimentos" a realizarse; las cuales serán 208 en total. Los experimentos se separan en 104 basados en túneles *IPsec* y otros 104 basados en *DMVPN*. De las 104 pruebas de cada escenario se realizarán 26 pruebas por cada túnel formado, es decir 26 pruebas del túnel *spoke*1 a *hub*, *spoke*1 a *spoke*2, *spoke*1 a *spoke*3, *spoke*1 a *spoke*4.

3.6. Unidad de análisis

Los objetos de estudio o unidad de análisis de la presente investigación corresponden a cada uno de los "escenarios de prueba" que serán implementados. Cada "escenario de prueba" consiste en la implementación de laboratorios en diferentes localidades y la transmisión de archivos de datos, audio y video entre los sitios que simulan sucursales y el sitio que simula la matriz. Los detalles de las implementaciones de los "escenarios de prueba" serán cubiertos en el Capítulo III. Como se mencionó antes, se utilizarán dos esquemas: el primer esquema implementado mediante túneles *IPsec* y el segundo esquema implementado mediante *DMVPN*.

3.7. Selección de la muestra

En la presente investigación, se toma una muestra de tamaño definido a partir de toda la población de cada túnel establecido por cada escenario.

3.8. Tamaño de la muestra

Se aplica la siguiente fórmula para determinar el tamaño de la muestra:

$$n = \frac{N \cdot Z^2 \cdot p \cdot (1-p)}{(N-1) \cdot e^2 + Z^2 \cdot p \cdot (1-p)}$$

Fórmula 1-3: Fórmula para calcular el tamaño de la muestra.

Fuente: (Feedback Networks, 2013)

Dónde:

n = número de pruebas que debemos seleccionar aleatoriamente.

Población de estudio: ***N***=26

Error máximo aceptable: ***e***=5% = 0,05

Nivel de confianza: ***Z***=95% = 1,96

Porcentaje estimado de la muestra: ***p***=50% = 0,5

$$n = \frac{26 \cdot 1{,}96^2 \cdot 0{,}5 \cdot (1-0{,}5)}{(26-1) \cdot 0{,}05^2 + 1{,}96^2 \cdot 0{,}5 \cdot (1-0{,}5)}$$

$$n = \frac{26 \cdot 3{,}8416 \cdot 0{,}5 \cdot 0{,}5}{25 \cdot 0{,}0025 + 3{,}8416 \cdot 0{,}5 \cdot 0{,}5}$$

$$n = \frac{24{,}9704}{0{,}0625 + 0{,}9604}$$

$$n = 24{,}41$$

Obtenemos que ***n*** = 24.

El resultado indica que se debe obtener 24 muestras al azar de las 26 realizadas por cada túnel para determinar el desempeño de la VPN. Debido que el número de muestras no se aleja en gran medida al de la población, se toma como muestra la misma población, es decir serán analizadas

las 26 pruebas obtenidas por cada túnel del esquema IPsec y 26 pruebas de cada túnel del esquema DMVPN para realizar la comparación entre estos esquemas.

3.9. Identificación de variables

En base a la hipótesis de investigación planteada en el presente trabajo, la misma que indica lo siguiente: *La aplicación de DMVPN mejora el desempeño de redes privadas virtuales sobre Internet, con respecto al uso de VPN IPsec*, se determinan las siguientes variables:

- Variables independientes
    - Escenario con IPsec
    - Escenario con DMVPN
- Variables dependientes
    - Retardo
    - Jitter
    - Paquetes perdidos

3.10. Técnicas de recolección de datos primarios y secundarios

Las técnicas de recolección de datos, que son utilizadas en la presente investigación son:

- *Realización de Pruebas:* la implementación y configuración de equipos tales como routers, switches, CPEs; así como la disposición de los servidores para transacción de información, arrojarán los parámetros de desempeño requeridos en esta investigación.
- *Uso de Instrumentos:* mediante el uso de instrumentos en *hardware* y *software* (detallados en la siguiente sección) se puede realizar las mediciones del rendimiento de IPsec y DMVPN en los escenarios de prueba correspondientes.
- *Observación:* permite leer y registrar los datos obtenidos de las pruebas. Los datos que serán registrados son: la latencia, jitter y pérdida de datos.
- *Análisis:* permite tomar en cuenta únicamente los datos que tengan lógica y que estén dentro del rango esperado.

Los datos primarios se obtienen directamente como resultado de los experimentos realizados en esta tesis, mientras que los datos secundarios se obtendrán de experimentos realizados por otros investigadores y servirán únicamente como referencia.

3.11. Instrumentos de recolección de datos primarios y secundarios

- Ficha de Observación: Se elabora una ficha por cada día de pruebas conteniendo la hora, indicadores, valoración y observación.
- *Hardware*: Laptops, Routers Cisco 1800, Cables Ethernet UTP cat. 6 longitud 3 pies.
- *Software*: Wireshark, Windows 7, D-ITG, STG, Microsoft Excel.

3.12. Instrumentos para procesar los datos recopilados

Los instrumentos para procesar los datos son los siguientes:

- *Software SIAE*: es un programa estadístico que permite la validación de hipótesis por medio del análisis de una o dos variables.
- Hojas de cálculo *Excel*: permitirá un análisis primario de los datos, creación de tablas y gráficas.

3.13. Escenarios de prueba

Con el objeto de poder realizar las mediciones de desempeño, se considera cumplir algunos requerimientos comunes para los escenarios IPsec y DMVPN, mismos que se detallan en las siguientes secciones.

Se diseña e implementa una red privada virtual formada por un *hub* ubicado en un sitio que simula la oficina matriz y cuatro *spokes* ubicados en diferentes localidades, que serían sus sucursales. Como se observa en la Figura 1-3 los sitios están geográficamente separados y tienen acceso a Internet. Se tiene la necesidad de intercambiar tráfico de datos, vídeo y telefonía de una manera

segura a través de la red pública. De modo específico, se consideran los siguientes escenarios de pruebas:

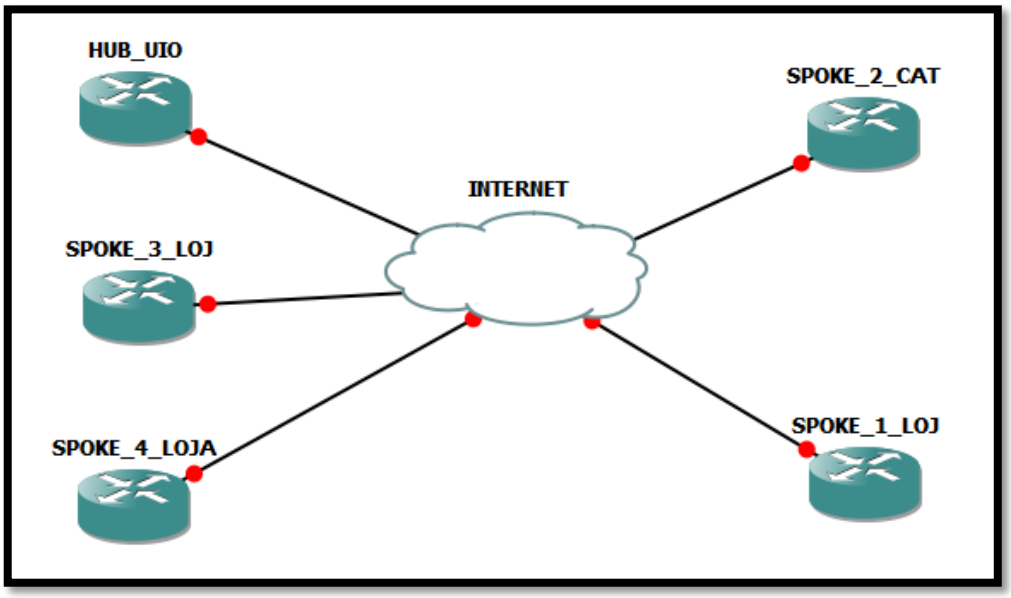

Figura 12-3: Esquema de interconexión

Realizado por: Alex Jaramillo

En el primer escenario se establece la implementación de la VPN con IPsec de manera estática, lo cual corresponde a canales de conexión punto a punto del tipo estrella.

En el segundo escenario se establece la implementación de la VPN aplicando la técnica DMVPN, lo cual corresponde a canales de conexión dinámicos del tipo malla.

La evaluación y comparación de ambos escenarios se realiza bajo las mismas condiciones de implementación; es decir: tecnología de última milla (fibra óptica), número de dispositivos de ruteo y servidores en cada sucursal y matriz, carga para transferencia de archivos de datos, audio y video, y parámetros comunes de configuración.

Se mide los valores de: latencia, pérdida de datos y *jitter*. Todo esto en base a las técnicas de recolección de datos e instrumentos de medición y procesamiento de datos antes indicados.

Las localidades del *hub* y *spokes*; así como el proveedor de la conexión a Internet y sus detalles se indican en la Tabla 4-3.

Tabla 4-3: Proveedor y velocidad de los sitios a interconectar

FUNCIÓN	CIUDAD	DIRECCION	VELOCIDAD

HUB	QUITO	Calle S12A #Oe5-106. Santa Anita 2	2 Mbps
SPOKE_1	LOJA	Av. Emiliano Ortega y Juan de Salinas	2 Mbps
SPOKE_2	CATAMAYO	Olmedo entre 24 de mayo y Av. Catamayo	2 Mbps
SPOKE_3	LOJA	Crisantemos y Anturios	2 Mbps
SPOKE_4	LOJA	18 de Noviembre entre Celica y Gonzanamá	2 Mbps

Realizado por: Alex Jaramillo

3.13.1. Requerimientos en hardware y software

Para el desarrollo del proyecto se debe considerar las características técnicas en hardware y software que soporten la aplicación de las configuraciones para los escenarios IPsec y DMVPN, así como para la implementación de los instrumentos de medición.

3.13.1.1. Instrumentos en hardware

Se realiza un análisis comparativo de los modelos de Router Cisco que soportan la configuración de IPsec y DMVPN, además se verifica la versión recomendada de IOS para nuestra implementación.

Tabla 5-3: Modelo de plataforma hardware que soporta IPsec y DMVPN

PLATFORM	VPN ACCELERATION MODULE
Cisco 870, 880, 890, 812, 819 Series Integrated Services Routers	Onboard encryption
Cisco 1801, 1802, 1803, 1811, 1812, 1841, 2800, 3825, and 3845 Integrated Services Routers	Onboard encryption

Cisco 1841 Integrated Services Routers	Advanced Integration Module (AIM)-VPN/SSL-1
Cisco 2800 Series Integrated Services Routers	AIM-VPN/SSL-2
Cisco 3825 Integrated Services Routers	AIM-VPN/SSL-3
Cisco 3845 Integrated Services Routers	AIM-VPN/SSL-3
Cisco 1900, 2900, and 3900 Next Generation Integrated Services Routers	Onboard encryption
Cisco 7200 Series Routers	VPN Acceleration Module 2+ (VAM2+)
Cisco 7200VXR Routers with Network Processing Engine NPE-G2	VPN Services Adapter (VSA)
Cisco 7301 Routers	VAM2+
Cisco 7600 Series Routers (Supports DMVPN phase 1 & 2 only)	IPsec VPN Shared Port Adapter (SPA)
Cisco Catalyst 6500 Series Switches (Supports DMVPN phase 1 & 2 only)	IPsec VPN SPA
Cisco ASR 1000 Series Routers	Onboard encryption
Cisco ISR 4000 Series Routers	Onboard encryption

Fuente: (Cisco, 2017)

Realizado por: Alex Jaramillo

Tabla 6-3: Requisitos en versión de IOS

HARDWARE	**Cisco 870, 1800, 1900, 2800, 2900, 3800, 3900, 7200 Series and Cisco 7301 routers**
Cisco IOS Software Release	● Cisco IOS Software Release 12.3(2)T or later recommended for Cisco 870, 1800, 2800, 3800, and 7200 Series Routers and Cisco 7301 Routers ● Cisco IOS Software Release 15.0 or later recommended for Cisco 1900, 2900 and 3900 Series Routers ● Cisco IOS Software Release 12.2(18)SXE2 or later for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers ● Cisco IOS XE Release 2.0.0 or later for Cisco ASR 1000 Series Routers ● Cisco IOS XE release – 3.16.5S or later for Cisco ISR 4000 series routers
Cisco IOS Software Feature Set	● Advanced Security or higher ● Cisco ASR 1000 Series Routers also require VPN license

	• Cisco ISR 4000 series routers need SECK9 license or higher

Fuente: (Cisco, 2017)

Realizado por: Alex Jaramillo

De acuerdo a las recomendaciones de Cisco expuestas en las tablas anteriores, para nuestros escenarios se emplea el router Cisco 1841 con versión de IOS 12.4 para el *Hub* y *Spoke*.

Se considera un computador en cada sitio para la instalación del software de simulación y medición de indicadores, que posee las siguientes características.

Tabla 7-3: Características de equipo informático

Parámetros	Emisor	Receptor
Microprocesador	Intel Core i5	Intel Celeron 1.5 GHz
Memoria RAM	8 GB	4 GB
Sistema operativo	Windows 7 x64 bits	Windows 7 x32 bits
Tarjeta de red	Ethernet 1 Gb	Ethernet 100 Mb

Realizado por: Alex Jaramillo

3.13.2. Diseño de los escenarios

Para poder establecer una conexión VPN sobre Internet entre todos los sitios antes descritos, es necesario cumplir con los siguientes requisitos:

- Poseer una dirección pública en cada sitio.
- Los routers deben ser marca Cisco y poseer el mismo modelo *firmware* y *hardware*.
- Distinto direccionamiento LAN en cada sitio.

Esto se aplica a los dos escenarios: IPsec y DMVPN.

El protocolo de internet escogido para el direccionamiento LAN y WAN es la versión 4 debido a que la versión 6 aún no es adoptado de manera oficial por nuestros proveedores de internet. El direccionamiento que se aplica en cada sitio se describe en la Tabla 8-3 y Tabla 9-3 correspondientemente.

Tabla 8-3: Direccionamiento LAN en cada sitio

FUNCIÓN	CIUDAD	DIRECCIONAMIENTO LAN	VELOCIDAD
HUB	QUITO	192.168.60.254/24	2 Mbps
SPOKE_1	LOJA	192.168.70.254/24	2 Mbps
SPOKE_2	CATAMAYO	192.168.80.254/24	2 Mbps
SPOKE_3	LOJA	192.168.90.254/24	2 Mbps
SPOKE_4	LOJA	192.168.100.254/24	2 Mbps

Realizado por: Alex Jaramillo.

Tabla 9-3: Direccionamiento WAN de los sitios remotos

FUNCIÓN	CIUDAD	IP PÚBLICA
HUB	QUITO	200.105.228.6
SPOKE_1	LOJA	190.57.168.37
SPOKE_2	CATAMAYO	201.182.151.5
SPOKE_3	LOJA	190.12.61.137
SPOKE_4	LOJA	190.57.168.203

Realizado por: Alex Jaramillo.

Al implementar nuevas tecnologías las cabeceras de los paquetes cambian, es por eso que debemos manipular el MTU (*Maximum Transmission Unit*). El MTU es un término de redes de comunicaciones que establece el tamaño máximo en *bytes* que puede enviarse usando un protocolo de comunicaciones. El MTU que se considera en la práctica para los equipos de redes es de 1500 bytes.

Otro parámetro que debemos considerar es el MSS (*Maximum Segment Size*) que es el tamaño más grande de datos que un dispositivo puede manejar en una única pieza, sin fragmentar. Cuando se usa el protocolo TCP para establecer la comunicación, su cabecera tiene una longitud variable de al menos 20 bytes, al igual que la cabecera IP. El MSS se puede obtener de la diferencia entre el MTU menos las cabeceras IP y TCP.

El MTU estándar definido en IEEE 802.3 (Ethernet) es de 1500 bytes y en circunstancias normales el MSS será de 1460 (si consideramos la cabecera IP y TCP de 20 bytes cada uno).

En el presente proyecto, es necesario recalcular el MTU y MSS debido a las cabeceras adicionales que se insertan al configurar una VPN; es así que para el escenario con IPsec el valor del MTU se obtiene aplicando la siguiente fórmula:

$$MTU_{IPsec} = MTU_{eth} - CabeceraIPnueva - CabecerasIPsec$$

Fórmula 2-3: Fórmula para obtener el valor de MTU para el escenario IPsec.
Fuente: (Brito, 2015).

El MTU Ethernet es igual a 1500 bytes, la cabecera IP nueva es de 20 bytes y la cabecera IPsec, considerando el tipo de cifrado "esp-3des esp-sha-md5" para ambos escenarios según (Cisco Systems, Cisco VPN services port adapter configuration guide, 2013), es de 58 bytes como máximo. Entonces,

$$MTU_{IPsec} = 1500bytes - 20bytes - 58bytes$$

$$MTU_{IPsec} = 1422bytes$$

El MSS para TCP se calcula con la fórmula 3.

$$MSS_{IPsec} = MTU_{IPsec} - CabeceraIP - CabeceraTCP$$

Fórmula 3-3: Fórmula para calcular el valor de MSS en el escenario de IPsec.
Fuente: (Brito, 2015)

Obteniendo,

$$MSS_{IPsec} = 1422bytes - 20bytes - 20bytes$$

$$MSS_{IPsec} = 1382bytes$$

Por otra parte, para el escenario con DMVPN se debe adicionar el tamaño de la cabecera GRE que es de 24 bytes y al establecer el modo IPsec como transporte se disminuye 20 bytes de su cabecera, lo que tendremos una cabecera de 38 bytes; por lo tanto el cálculo sería:

$$MTU_{DMVPN} = MTU_{eth} - CabecerasIPsec - CabeceraGRE$$

$$MTU_{DMVPN} = 1500bytes - 38bytes - 24bytes$$

$$MTU_{DMVPN} = 1438 \approx 1430bytes$$

El MSS se calcula con la misma fórmula usada en el escenario IPsec.

$$MSS_{DMVPN} = MTU_{DMVPN} - CabeceraIP - CabeceraTCP$$

$$MSS_{DMVPN} = 1438bytes - 20bytes - 20bytes$$

$$MSS_{DMVPN} = 1398bytes \approx 1390bytes$$

3.13.3. Implementación de escenarios.

Los escenarios de pruebas IPSec y DMVPN comparten los siguientes parámetros de configuración con el fin de no favorecer a uno u otro en el resultado de las pruebas.

Estos parámetros son:

- Método de cifrado en IPsec y DMVPN, esp-3des.
- Método de autenticación en IPsec y DMVPN, esp-sha-md5.
- Tipo de NAT, extended.
- MTU y MSS.
- Grupo *Diffie-Hellman*.

3.13.3.1. Implementación y desarrollo del escenario IPsec

En la Figura 13-3 se muestra el diagrama de red con el direccionamiento IP. A modo de ejemplo, se muestran los pasos para configurar una VPN mediante IPsec entre el router *hub* y el router *spoke* número 1. La configuración completa se incluye en el Anexo A "Show run de los equipos hub y spoke en el escenario IPsec".

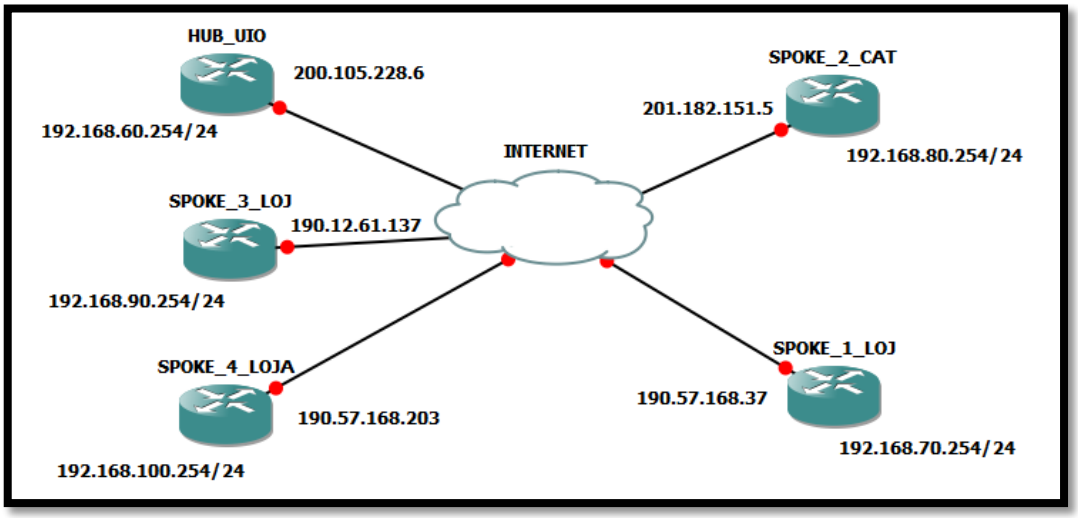

Figura 13-3: Esquema de conexión "Hub and spoke" con direccionamiento WAN y LAN

Fuente: Alex Jaramillo

Para el desarrollo de las pruebas en el escenario IPsec se debe considerar el diseño e implementación de la topología de red en sus dos ambientes, WAN y LAN, de la conexión en cada sitio.

3.13.3.1.1. Implementación de la red WAN del escenario IPsec

En la sección 3.12.212 "Diseño de los escenarios", se muestra el direccionamiento WAN que se aplicará en cada sitio, a continuación se observa dicha tabla.

Tabla 10-3: Direccionamiento WAN

FUNCIÓN	CIUDAD	IP PÚBLICA
HUB	QUITO	200.105.228.6
SPOKE_1	LOJA	190.57.168.37
SPOKE_2	CATAMAYO	201.182.151.5
SPOKE_3	LOJA	190.12.61.137
SPOKE_4	LOJA	190.57.168.203

Realizado por: Alex Jaramillo.

Se inicia la configuración de los equipos *Router* de acuerdo a los pasos que se presentan a continuación. A modo de ejemplo se ejecutará y se capturará la configuración del *Router HUB.*

Paso 1. Comprobar conectividad.

Se configura la dirección pública en la interfaz WAN con la puerta de enlace por defecto entregada por el Proveedor de Internet.

```
interface FastEthernet0
 description WAN
 ip address 200.105.228.6 255.255.255.252
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 crypto map VPN
```

Figura 14-3: Configuración de interfaz WAN

Realizado por: Alex Jaramillo

```
ip route 0.0.0.0 0.0.0.0 200.105.228.5
```

Figura 15-3: Ruta por defecto

Realizado por: Alex Jaramillo

```
HUB_UIO#ping 190.57.168.37

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.57.168.37, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/12 ms
HUB_UIO#
```

Figura 16-3: Ping a la ip pública del spoke_1_LOJ

Realizado por: Alex Jaramillo

Paso 2. Realizar el "NAT"

Se configura el NAT del tipo extendido con sobrecarga.

```
ip nat inside source list NAT interface FastEthernet0 overload
!
ip access-list extended NAT
 deny   ip 192.168.60.0 0.0.0.255 192.168.70.0 0.0.0.255
 deny   ip 192.168.60.0 0.0.0.255 192.168.80.0 0.0.0.255
 deny   ip 192.168.60.0 0.0.0.255 192.168.90.0 0.0.0.255
 deny   ip 192.168.60.0 0.0.0.255 192.168.100.0 0.0.0.255
 permit ip 192.168.60.0 0.0.0.255 any
```

Figura 17-3: Configuración del NAT con lista extendida

Realizado por: Alex Jaramillo

Se puede observar que se deniega el acceso a través del NAT a todo tráfico que se realiza hacia las redes LAN de los *spoke*, esto es para que dicho tráfico pase siempre por el túnel IPsec.

Paso 3. Configurar política "ISAKMP" para establecer el "IKE".

Se configura los parámetros necesarios para establecer la política ISAKMP del intercambio de claves hacia cada *spoke*.

```
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 6 Tesis2018 address 190.57.168.37
crypto isakmp key 6 Tesis2018 address 190.12.61.137
crypto isakmp key 6 Tesis2018 address 201.182.151.5
crypto isakmp key 6 Tesis2018 address 190.57.168.203
!
```

Figura 18-3: Configuración del "ISAKMP"

Realizado por: Alex Jaramillo

Paso 4. Definir el "transform-set" de IPsec.

Se establece el método de autenticación, cifrado y modo de encapsulación.

```
!
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
!
```

Figura 19-3: Configuración del "transform-set"

Realizado por: Alex Jaramillo

Paso 5. Crear la lista de acceso y "crypto map" para IPsec.

Se establece la comunicación con su par para el inicio del intercambio de tráfico, siempre y cuando el intercambio de claves sea exitoso.

```
!
crypto map VPN 1 ipsec-isakmp
 set peer 190.57.168.37
 set transform-set ESP-3DES-MD5
 match address 101
crypto map VPN 2 ipsec-isakmp
 set peer 201.182.151.5
 set transform-set ESP-3DES-MD5
 match address 102
crypto map VPN 3 ipsec-isakmp
 set peer 190.12.61.137
 set transform-set ESP-3DES-MD5
 match address 103
crypto map VPN 4 ipsec-isakmp
 set peer 190.57.168.203
 set transform-set ESP-3DES-MD5
 match address 104
!
```

Figura 20-3: Configuración del "crypto map"

Realizado por: Alex Jaramillo

Se configura la lista de acceso sobre las redes que se encaminarán sobre el túnel y serán cifradas.

```
!
access-list 101 permit ip 192.168.60.0 0.0.0.255 192.168.70.0 0.0.0.255
access-list 101 permit ip 192.168.80.0 0.0.0.255 192.168.70.0 0.0.0.255
access-list 101 permit ip 192.168.90.0 0.0.0.255 192.168.70.0 0.0.0.255
access-list 101 permit ip 192.168.100.0 0.0.0.255 192.168.70.0 0.0.0.255
access-list 102 permit ip 192.168.60.0 0.0.0.255 192.168.80.0 0.0.0.255
access-list 102 permit ip 192.168.100.0 0.0.0.255 192.168.80.0 0.0.0.255
access-list 102 permit ip 192.168.90.0 0.0.0.255 192.168.80.0 0.0.0.255
access-list 102 permit ip 192.168.70.0 0.0.0.255 192.168.80.0 0.0.0.255
access-list 103 permit ip 192.168.60.0 0.0.0.255 192.168.90.0 0.0.0.255
access-list 103 permit ip 192.168.80.0 0.0.0.255 192.168.90.0 0.0.0.255
access-list 103 permit ip 192.168.70.0 0.0.0.255 192.168.90.0 0.0.0.255
access-list 103 permit ip 192.168.100.0 0.0.0.255 192.168.90.0 0.0.0.255
access-list 104 permit ip 192.168.60.0 0.0.0.255 192.168.100.0 0.0.0.255
access-list 104 permit ip 192.168.80.0 0.0.0.255 192.168.100.0 0.0.0.255
access-list 104 permit ip 192.168.70.0 0.0.0.255 192.168.100.0 0.0.0.255
access-list 104 permit ip 192.168.90.0 0.0.0.255 192.168.100.0 0.0.0.255
```

Figura 21-3: Configuración de las listas de acceso

Realizado por: Alex Jaramillo

Paso 6. Aplicar el crypto map a la interfaz de salida del Router, el MTU y MSS a la interfaz LAN.

Se configura el "crypto map" en la interfaz WAN del Router.

```
!
interface FastEthernet0
 description WAN
 ip address 200.105.228.6 255.255.255.252
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 crypto map VPN
!
```

Figura 22-3: Aplicación del crypto map en la interfaz WAN

Realizado por: Alex Jaramillo

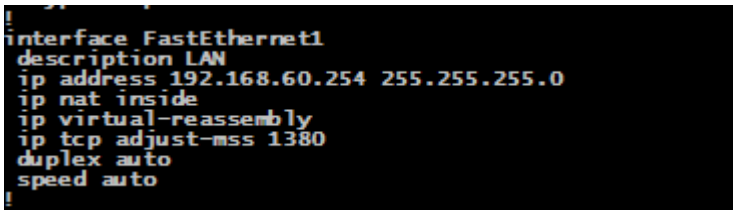

Figura 23-3: Aplicación del MSS en la interfaz LAN

Realizado por: Alex Jaramillo

- **Implementación de la red LAN del escenario IPsec**

Se debe considerar que cada red LAN de los sitios involucrados debe ser distinta para su correcto enrutamiento. Por lo tanto se debe planificar correctamente la segmentación previendo una futura ampliación de sitios o sucursales en un ambiente real.

Para nuestro proyecto se realiza una segmentación de la red privada 192.168.0.0 con máscara 255.255.255.0.

A continuación se muestra la Tabla 11-3 conteniendo el direccionamiento privado a considerarse en cada sitio.

Tabla 11-3: Direccionamiento LAN privado

FUNCIÓN	CIUDAD	DIRECCIONAMIENTO LAN
HUB	QUITO	192.168.60.254/24
SPOKE_1	LOJA	192.168.70.254/24
SPOKE_2	CATAMAYO	192.168.80.254/24
SPOKE_3	LOJA	192.168.90.254/24
SPOKE_4	LOJA	192.168.100.254/24

Realizado por: Alex Jaramillo.

Por cuestión del desarrollo de las pruebas se conecta en cada sitio sólo un computador y se ejecuta el software D-ITG como servidor en el *SPOKE_1* y cliente en los demás *SPOKE* y *HUB*, para la simulación del tipo de tráfico y medición de indicadores.

A continuación se muestra la Tabla 12-3 con el direccionamiento de los equipos de pruebas instalados en cada sitio.

Tabla 12-3: Direccionamiento interno de cada servidor

FUNCIÓN	DIRECCIONAMIENTO SERVIDOR
HUB	192.168.60.4/24

SPOKE_1	192.168.70.200/24
SPOKE_2	192.168.80.2/24
SPOKE_3	192.168.90.200/24
SPOKE_4	192.168.100.2/24

Realizado por: Alex Jaramillo.

3.13.3.2. Implementación y desarrollo del escenario DMVPN

Para la implementación del escenario DMVPN, se debe considerar un nuevo direccionamiento para los túneles *GRE* de cada sitio y los pasos de configuración que se presentan más adelante. A modo de ejemplo, se muestran los comandos para implementar DMVPN entre el router *hub* y el router *spoke* número 1. La configuración completa se incluye en el Anexo B "Show run de los equipos en el escenario DMVPN".

En la Figura 24-3 se muestra el diagrama de red incluyendo el nuevo direccionamiento para GRE, mismo que se halla tabulado en la Tabla 13-3.

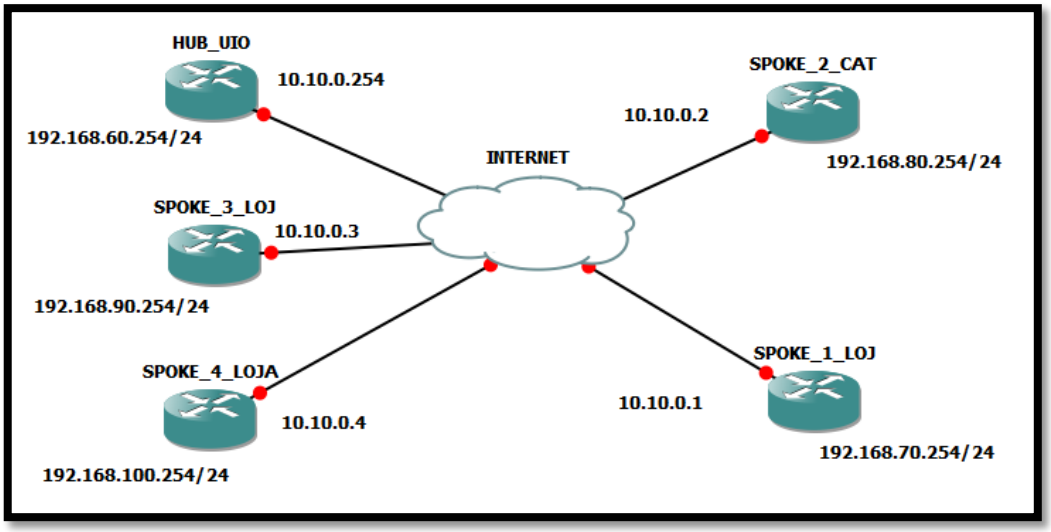

Figura 24-3: Esquema de direccionamiento WAN para las interfaces GRE

Realizado por: Alex Jaramillo

Se considera el mismo direccionamiento WAN y LAN descrito en el escenario IPsec con la diferencia que en este escenario se añade un direccionamiento para la configuración de los túneles GRE.

- **Implementación de la red WAN del escenario DMVPN**

A modo de ejemplo se ejecutará y se capturará la configuración del *Router HUB*.

Paso 1. Comprobar conectividad.

Se configura la dirección pública en la interfaz WAN con la puerta de enlace por defecto entregada por el Proveedor de Internet.

```
!
interface FastEthernet0
 description WAN
 ip address 200.105.228.6 255.255.255.252
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
```

Figura 25-3: Configuración de interfaz WAN

Realizado por: Alex Jaramillo

```
ip route 0.0.0.0 0.0.0.0 200.105.228.5
!
```

Figura 26-3: Ruta por defecto

Realizado por: Alex Jaramillo

```
HUB_UIO#ping 190.57.168.37

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.57.168.37, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/12 ms
HUB_UIO#
```

Figura 27-3: Ping a la ip pública del spoke_1_LOJ

Realizado por: Alex Jaramillo

Paso 2. Realizar el "NAT"

Se configura el NAT del tipo extendido con sobrecarga.

```
ip nat inside source list NAT interface FastEthernet0 overloa
!
ip access-list extended NAT
 deny   ip 192.168.60.0 0.0.0.255 192.168.70.0 0.0.0.255
 deny   ip 192.168.60.0 0.0.0.255 192.168.80.0 0.0.0.255
 deny   ip 192.168.60.0 0.0.0.255 192.168.90.0 0.0.0.255
 deny   ip 192.168.60.0 0.0.0.255 192.168.100.0 0.0.0.255
 permit ip 192.168.60.0 0.0.0.255 any
!
```

Figura 28-3: Configuración del NAT con lista extendida

Realizado por: Alex Jaramillo

Se puede observar que se deniega el acceso a través del NAT a todo tráfico que se realiza hacia las redes LAN de los *spoke*, esto es para que dicho tráfico pase siempre por el túnel IPsec.

Paso 3. Configurar política "ISAKMP" para establecer el "IKE".

Se configura los parámetros necesarios para establecer la política ISAKMP del intercambio de claves hacia los *spoke*.

```
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 6 Tesis2018 address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
 mode transport
!
```

Figura 29-3: Configuración del "ISAKMP"

Realizado por: Alex Jaramillo

Paso 4. Definir el "transform-set" de IPsec.

Se establece el método de autenticación, cifrado y modo de encapsulación.

```
!
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
 mode transport
!
```

Figura 30-3: Configuración del "transform-set"

Realizado por: Alex Jaramillo

Paso 5. Crear el perfil ipsec para el intercambio de claves.

Se establece la comunicación con su par para el inicio del intercambio de tráfico, siempre y cuando el intercambio de claves sea exitoso.

```
!
crypto ipsec profile DMVPN_profile
 set transform-set ESP-3DES-MD5
!
```

Figura 31-3: Configuración del "crypto map"

Realizado por: Alex Jaramillo

Paso 6. Crear la interfaz tunnel GRE con el direccionamiento de la tabla 10-3, aplicando el MTU y MSS.

Tabla 13-3: Direccionamiento interno de cada servidor

FUNCIÓN	DIRECCIONAMIENTO TUNEL GRE
HUB	10.10.0.254/24
SPOKE_1	10.10.0.1/24
SPOKE_2	10.10.0.2/24
SPOKE_3	10.10.0.3/24
SPOKE_4	10.10.0.4/24

Fuente: Alex Jaramillo.

```
!
interface Tunnel0
 ip address 10.10.0.254 255.255.255.0
 no ip redirects
 ip mtu 1430
 no ip next-hop-self eigrp 100
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp redirect
 ip tcp adjust-mss 1390
 no ip split-horizon eigrp 100
 tunnel source 200.105.228.6
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN_profile
!
```

Figura 32-3: Configuración del túnel GRE

Realizado por: Alex Jaramillo

Paso 7. Configurar el enrutamiento dinámico con el protocolo EIGRP.

```
!
router eigrp 100
 network 10.10.0.254 0.0.0.0
 network 192.168.60.0
 auto-summary
!
```

Figura 33-3: Configuración del protocolo eigrp con identidad 100

Realizado por: Alex Jaramillo

- **Implementación de la red LAN del escenario DMVPN**

La red LAN se considera el mismo aplicado en el escenario IPsec apartado 3.12.3.1.2. "*Implementación de la red LAN del escenario IPsec".* Referirse a esa sección para mayores detalles.

3.13.4. Obtención de indicadores de evaluación

Para proceder con la obtención de los valores de las métricas de desempeño, primero se configura el D-ITG en el SPOKE_1 como emisor. Se debe considerar que el canal máximo establecido para este proyecto es de 2 Mbps en cada sitio, por este motivo para el caso de las pruebas con tráfico de datos se ha determinado emplear los parámetros que se muestran en la Tabla 14-3. El tiempo establecido para las pruebas es de 180 segundos considerando que es un valor medio de transferencia de paquetes, conversación telefónica y reproducción de vídeo.

Tabla 14-3: Valores de los parámetros para tráfico de datos

PARÁMETROS	VALORES
Métrica	One-Way-Delay
Duración (s)	180
Inicio del retardo (s)	0
Protocolo	UDP
Tasa de transmisión (Kbps)	1656
Tasa de paquetes (pkt/s)	150
Tamaño del paquetes (Bytes)	1380
Host destino	IP receptor

Realizado por: Alex Jaramillo.

En el caso de la inyección de tráfico de voz se establece los valores indicados en la Tabla 15-3.

Tabla 15-3: Valores de los parámetros para tráfico de voz

PARÁMETROS	VALORES
Métrica	One-Way-Delay
Duración (s)	180
Inicio del retardo (s)	0
Protocolo	UDP
Codec	G.729 – 2 samples/pkt
cRTP	Habilitado
Tasa de transmisión (Kbps)	20
Tasa de paquetes (pkt/s)	50
Tamaño del paquetes (Bytes)	50
Host destino	IP receptor

Realizado por: Alex Jaramillo.

Para el caso del tráfico de vídeo se establece los siguientes valores, considerando que la fuente de paquetes de vídeo es externo no es necesario generar paquetes para saturar el canal si no solamente para la obtención de los indicadores.

Tabla 16-3: Valores de los parámetros para tráfico de vídeo

PARÁMETROS	VALORES
Métrica	One-Way-Delay
Duración (s)	180
Inicio del retardo (s)	0
Protocolo	UDP
Tasa de transmisión (Kbps)	62,4
Tasa de paquetes (pkt/s)	100
Tamaño del paquetes (Bytes)	50
Host destino	IP receptor

Realizado por: Alex Jaramillo.

Los parámetros que deben definirse en el lado del receptor se muestran en la Tabla 17-3 y se ubican en la pestaña *settings* del ITGGUI.

Tabla 17-3: Parámetros en equipo receptor

PARÁMETRO	TIPO
Registro del emisor	*None*
Registro del receptor	*None*
Receptor local	*None*

Realizado por: Alex Jaramillo.

CAPITULO IV

4. RESULTADOS Y DISCUSIÓN

4.1. Análisis de resultados por cada indicador

Para evaluar el desempeño de los **servicios de datos, voz y video** en Internet se eligió medir los siguientes **indicadores o variables**:

- El retardo de los paquetes.
- El *jitter* de los paquetes.
- Número de Paquetes perdidos.

Estos indicadores corresponden a las variables dependientes que adquieren un valor determinado, en respuesta al funcionamiento de los **escenarios, IPsec y DMVPN**. Para estos escenarios se estableció condiciones iguales, en términos de ancho de banda asignado a los enlaces, el uso del mismo *hardware* y *software*, misma herramienta de simulación, mismo tipo de paquetes de los servicios, etc.

Para el análisis y comparación de los indicadores se ha considerado, por cuestiones de síntesis en el presente trabajo, utilizar los valores obtenidos en las mediciones de los **túneles establecidos entre el *SPOKE_1* al *HUB*** y del ***SPOKE_1* al *SPOKE_4.*** El resto de canales de comunicación, en espaciadas y repetidas pruebas, brindaron resultados similares y en ese sentido fueron muy útiles para corroborar que los datos obtenidos sean fidedignos y no parte de alguna casualidad. En el Anexo C "Resultado de las mediciones de los indicadores" se encuentran detallados los valores obtenidos del resto de canales, en ambos escenarios de prueba.

Como se indicó en la sección 3.8 "Tamaño de la muestra", el número de valores a tomar en cuenta en cada escenario, por cada túnel, por cada servicio y por cada variable, para el análisis y comparación, es 26.

4.1.1. Mediciones respecto al Retardo de los paquetes

Como se dijo antes, se toma 26 muestras de cada variable dependiente en su contexto de servicio, túnel y escenario. La presente sección se enfoca en el estudio de la variable "retardo". De este grupo de muestras se obtiene la media y la desviación estándar para realizar el análisis y comparación estadísticos.

A. Túnel SPOKE_1 a HUB

Los valores promedio de la variable "retardo" para los servicios de datos, voz y video, en la comunicación entre SPOKE_1 y HUB se muestran en la Tabla 18-4 y servirán para establecer si existe o no una diferencia significativa entre cada técnica aplicada (IPsec y DMVPN).

Tabla 18-4: Valores de la media y desviación estándar del retardo en los servicios cursados entre SPOKE_1 y HUB de cada escenario.

	PROMEDIO (ms)		**DESVIACIÓN ESTÁNDAR (ms)**	
	IPsec	**DMVPN**	**IPsec**	**DMVPN**
Datos	14,4345	13,8362	4,8955	2,5764
Voz	11,0896	11,0295	1,5438	0,1929
Video	24,6411	24,1784	7,1405	3,6058

Realizado por: Alex Jaramillo.

Cómo se puede observar en la Figura 34-4, DMVPN tiene valores menores de retardo de los paquetes en los tres servicios, respecto a IPsec; sin embargo, no se demuestra una diferencia amplia en estos promedios.

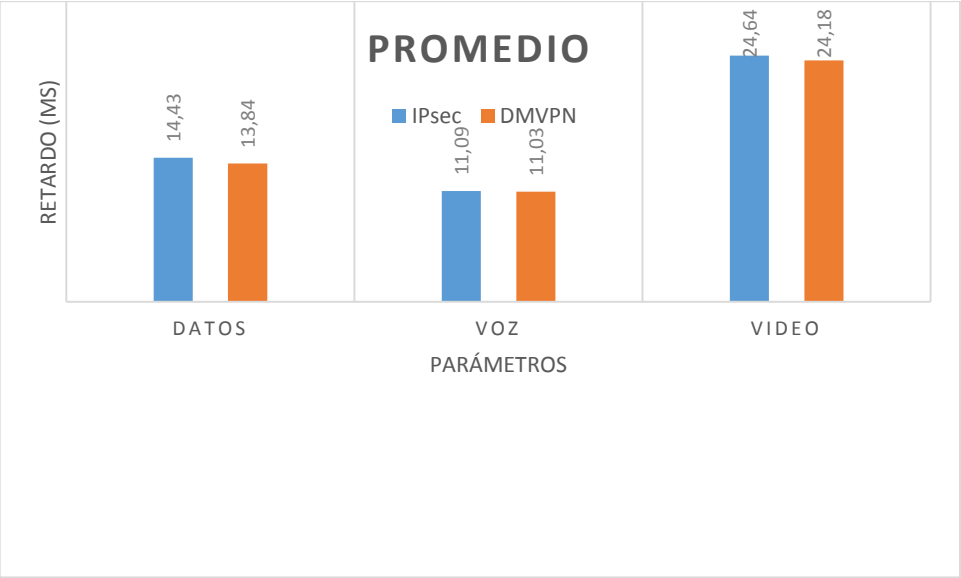

Gráfico 1-4: Promedio del retardo de los servicios de datos, voz y video entre SPOKE_1 y HUB de cada escenario.

Realizado por: Alex Jaramillo.

Por otra parte, en la Tabla 18-4 se puede observar que los valores de desviación estándar sí muestran una diferencia visible entre IPsec y DMVPN, denotando una mayor estabilidad en los resultados de las pruebas realizadas en DMVPN (menores desviaciones).

De esta manera, se estableció la hipótesis alternativa (H1) y la hipótesis nula (H0) para los tipos de paquetes de datos, voz y video con el objetivo de comprobar si existe una diferencia estadísticamente significativa sobre este indicador.

Hipótesis aplicadas para cada tipo de servicio: Datos, Voz y Video:

- **H1: Existe** una diferencia significativa entre la media del retardo en la transferencia de paquetes en el escenario IPsec y la media del retardo en el escenario DMVPN.
- **H0: No existe** una diferencia significativa entre la media del retardo en la transferencia de paquetes en el escenario IPsec y la media del retardo en el escenario DMVPN.

En el análisis de las hipótesis se utilizó el software SIAE para demostrar si existe una diferencia estadísticamente significativa entre las técnicas IPsec y DMVPN, utilizando los datos de la Tabla 18-4 y empleando el método estadístico "*T-student*" con un nivel de significancia del 5%.

1. **Datos**

Como se puede observar en la Figura 35-4, se acepta la hipótesis nula porque el valor T=0,54 resultó dentro de la región de aceptación de esta hipótesis. En otras palabras, **No existe** una

diferencia significativa entre la media del retardo en la transferencia de paquetes de Datos en el escenario IPsec y la media del retardo en el escenario DMVPN; medido en el túnel *SPOKE_1 y HUB.*

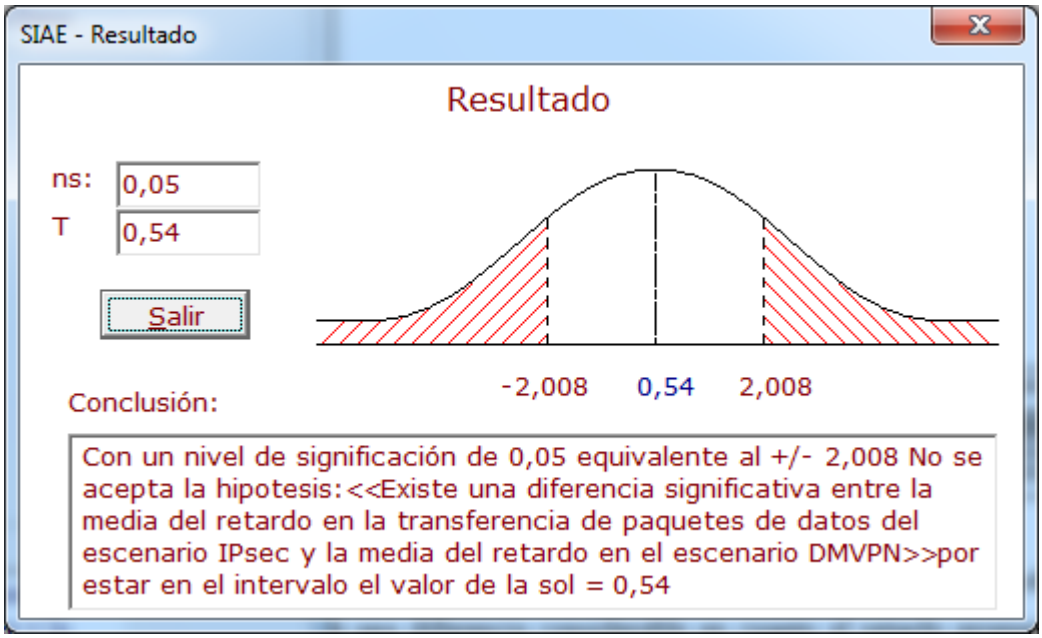

Figura 34-4: Resultado del análisis estadístico del retardo en la transferencia de datos entre SPOKE_1 y HUB de cada escenario.

Realizado por: Alex Jaramillo

2. Voz

Como se puede observar en la Figura 36-4, se acepta la hipótesis nula porque el valor T=0,193 resultó dentro de la región de aceptación de esta hipótesis. En otras palabras, **No existe** una diferencia significativa entre la media del retardo en la transferencia de paquetes de Voz en el escenario IPsec y la media del retardo en el escenario DMVPN; medido en el túnel *SPOKE_1 y HUB.*

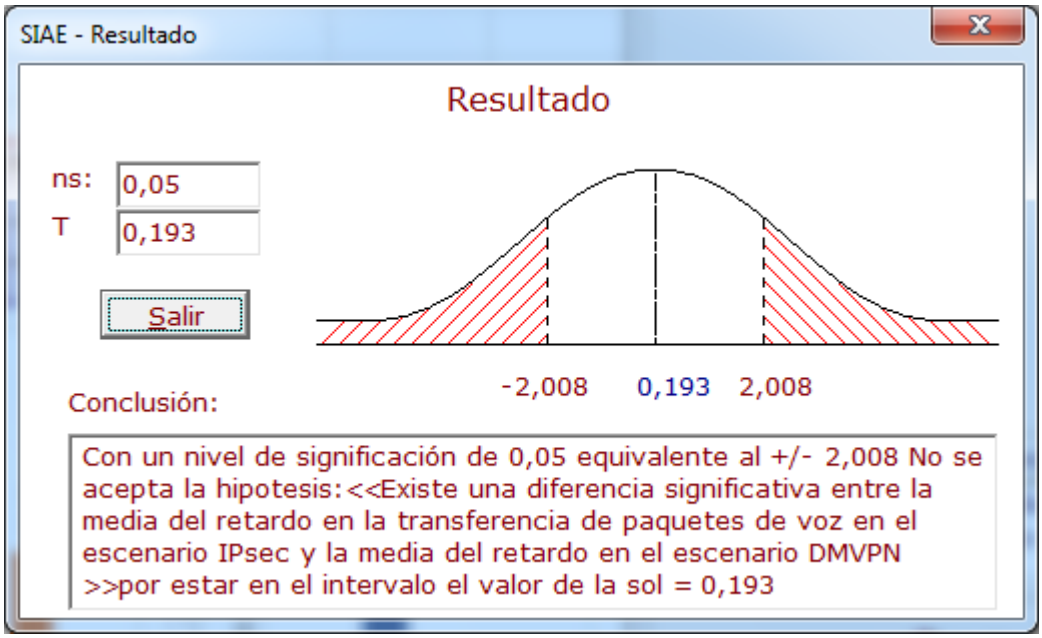

Figura 35-4: Resultado del análisis estadístico del retardo en la transferencia de voz entre SPOKE_1 y HUB de cada escenario.

Realizado por: Alex Jaramillo

3. Vídeo

Como se puede observar en la Figura 37-4, se acepta la hipótesis nula porque el valor T=0,288 resultó dentro de la región de aceptación de esta hipótesis. En otras palabras, **No existe** una diferencia significativa entre la media del retardo en la transferencia de paquetes de Video en el escenario IPsec y la media del retardo en el escenario DMVPN; medido en el túnel *SPOKE_1 y HUB.*

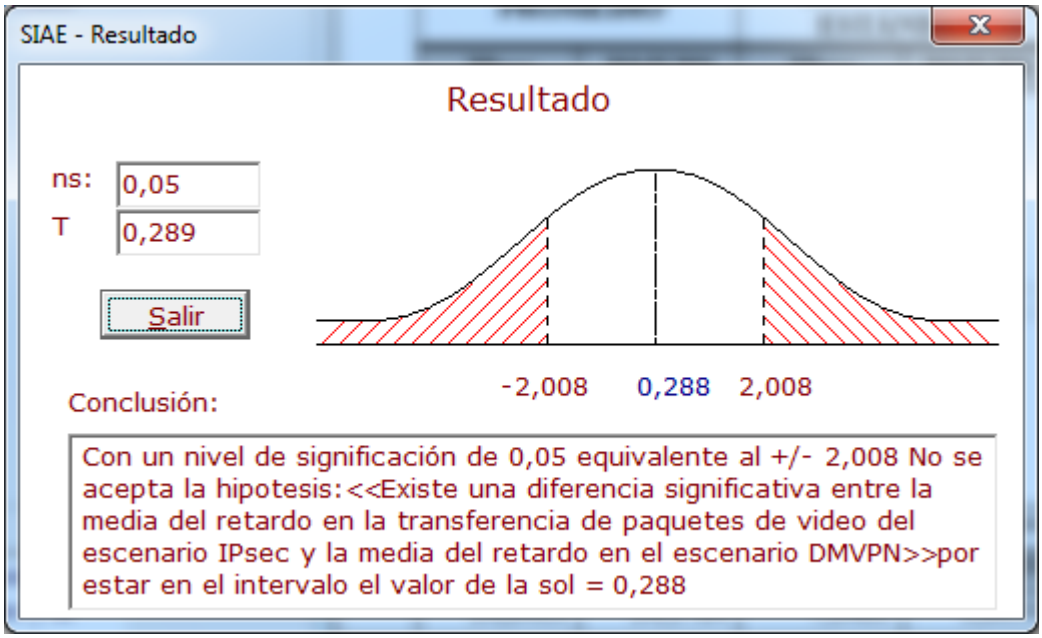

Figura 36-4: Resultados del análisis estadístico del retardo en la transmisión de paquetes de vídeo entre SPOKE_1 y HUB de cada escenario.

Realizado por: Alex Jaramillo

B. Túnel SPOKE_1 a SPOKE_4

En la Tabla 19-4 se muestra el valor promedio y desviación estándar de las muestras de la medición del retardo de los paquetes para el túnel SPOKE_1 a SPOKE_4, en los escenarios de IPsec y DMVPN.

Tabla 19-4: Valores promedio y desviación estándar del retardo en los servicios cursados entre SPOKE_1 y SPOKE_4 de cada escenario.

	PROMEDIO (ms)		**DESVIACIÓN ESTÁNDAR (ms)**	
	IPsec	**DMVPN**	**IPsec**	**DMVPN**
Datos	45,9318	4,0192	11,1489	1,9463
Voz	24,9439	2,0397	4,0347	0,1310
Video	31,4134	5,2362	4,5462	3,3386

Realizado por: Alex Jaramillo.

En la Figura 38-4 se aprecia de manera gráfica los valores promedio del retardo obtenido por cada servicio transmitido en el túnel SPOKE_1 a SPOKE_4, en los escenarios de IPsec y DMVPN.

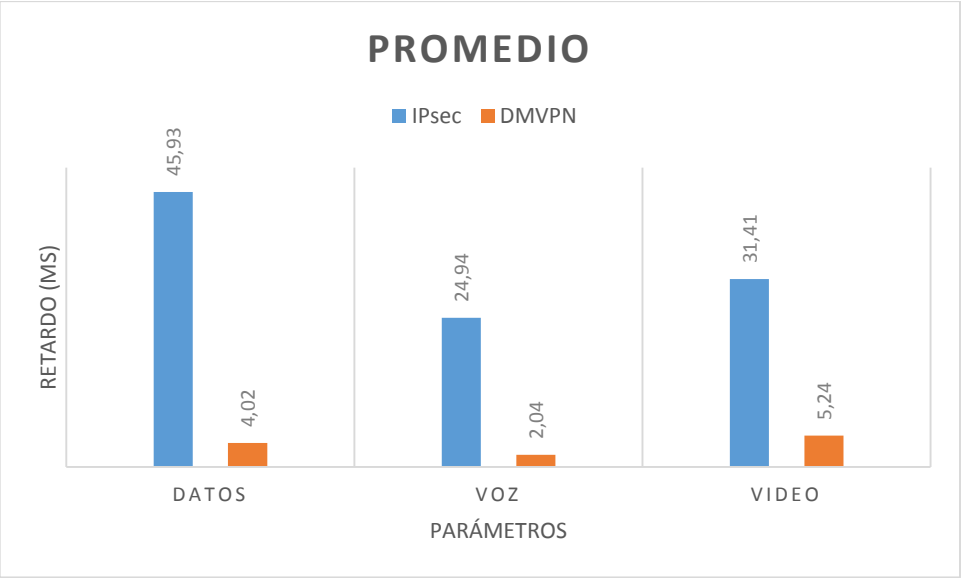

Gráfico 2-4: Valores promedio del retardo en IPsec y DMVPN de los servicios de datos, voz y video en el túnel SPOKE_1 a SPOKE_4

Realizado por: Alex Jaramillo.

Como se puede observar en la Figura 38-4, existe una diferencia notable en los valores obtenidos en los escenarios IPsec y DMVPN. Aquí resulta más evidente que la aplicación de la técnica DMVPN reduce el retardo en la transmisión de datos, voz y video. Como lo indica la teoría, al establecerse con DMVPN el túnel de manera directa, sin necesidad de atravesar por el HUB se reduce el retardo.

Se estableció la hipótesis alternativa (H1) y nula (H0) para los tipos de paquetes de datos, voz y video con el objetivo de comprobar si existe una diferencia estadísticamente significativa sobre este indicador.

Hipótesis aplicadas para cada tipo de servicio: Datos, Voz y Video:

- **H1: Existe** una diferencia significativa entre la media del retardo en la transferencia de paquetes del escenario IPsec y la media del retardo en el escenario DMVPN.
- **H0: No existe** una diferencia significativa entre la media del retardo en la transferencia de paquetes del escenario IPsec y la media del retardo en el escenario DMVPN.

En el análisis de las hipótesis se utilizó el software SIAE para demostrar si existe una diferencia significativa, utilizando los datos de la Tabla 19-4 y empleando el método estadístico "*T-student*" con un nivel de significancia del 5%.

1. **Datos**

Como se puede observar en la Figura 39-4, el valor T=18,515 está en la región crítica o de rechazo de la hipótesis nula (H0) para paquetes de datos. En otras palabras, **Existe** una diferencia significativa entre la media del retardo en la transferencia de paquetes de Datos en el escenario IPsec y la media del retardo en el escenario DMVPN; medido en el túnel *SPOKE_1 y SPOKE_4.*

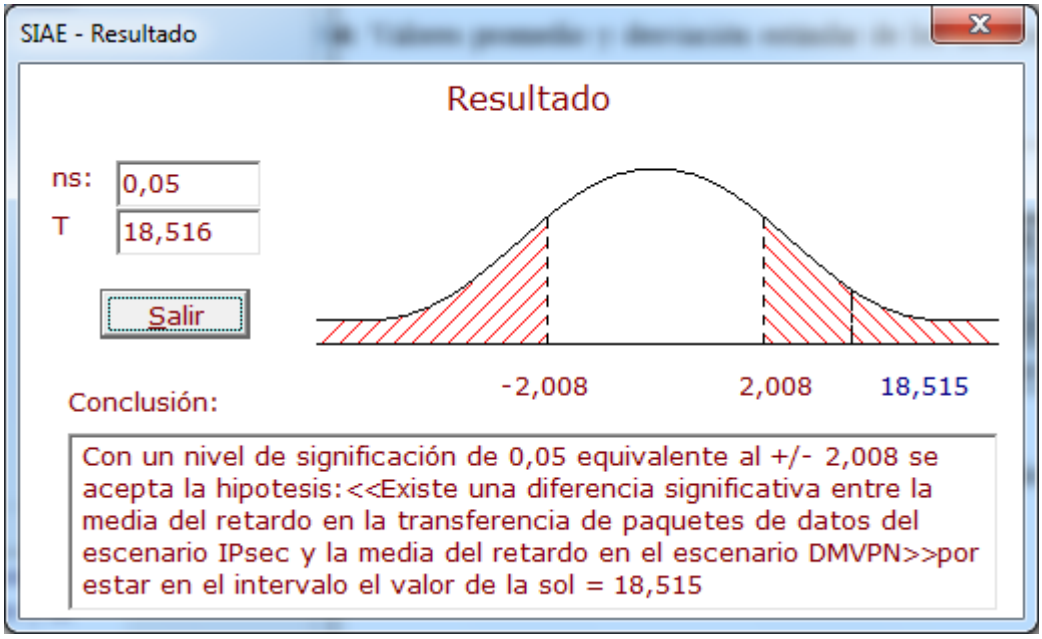

Figura 37-4: Resultado del análisis estadístico del retardo en la transferencia de datos SPOKE_1 a SPOKE_4, en los escenarios de IPsec y DMVPN.

Realizado por: Alex Jaramillo

2. Voz

Como se puede observar en la Figura 40-4, el valor T=28,368 está en la región crítica o de rechazo de la hipótesis nula (H0) para paquetes de voz. En otras palabras, **Existe** una diferencia significativa entre la media del retardo en la transferencia de paquetes de voz en el escenario IPsec y la media del retardo en el escenario DMVPN; medido en el túnel *SPOKE_1 y SPOKE_4.*

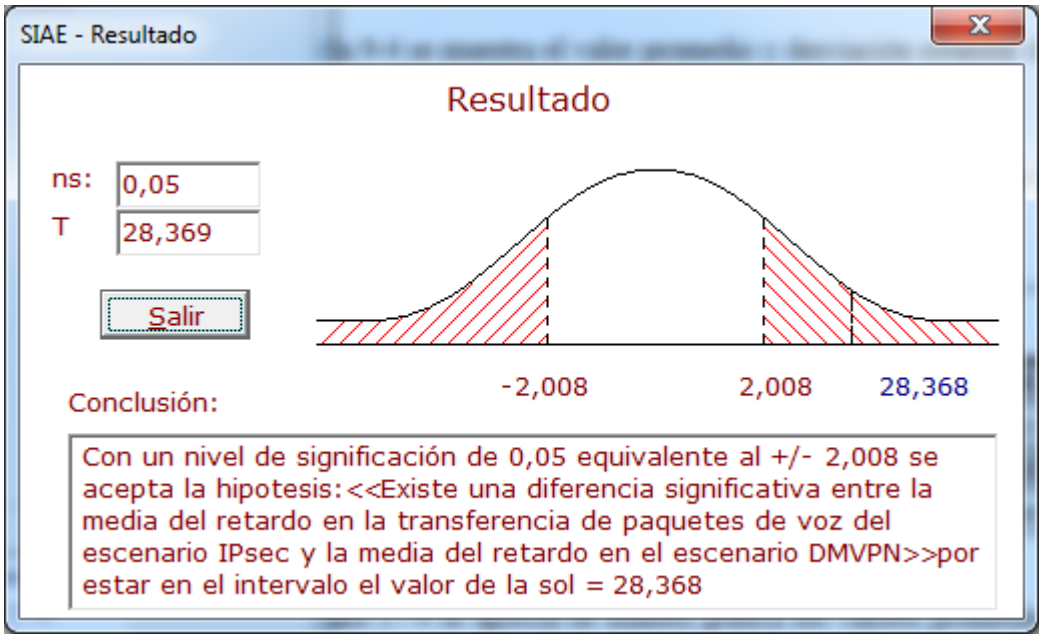

Figura 38-4: Resultado del análisis estadístico del retardo en la transferencia de voz en SPOKE_1 a SPOKE_4, en los escenarios de IPsec y DMVPN.

Realizado por: Alex Jaramillo

3. Vídeo

Como se puede observar en la Figura 41-4, el valor T=23,204 está en la región crítica o de rechazo de la hipótesis nula (H0) para paquetes de video. En otras palabras, **Existe** una diferencia significativa entre la media del retardo en la transferencia de paquetes de Video en el escenario IPsec y la media del retardo en el escenario DMVPN; medido en el túnel *SPOKE_1 y SPOKE_4.*

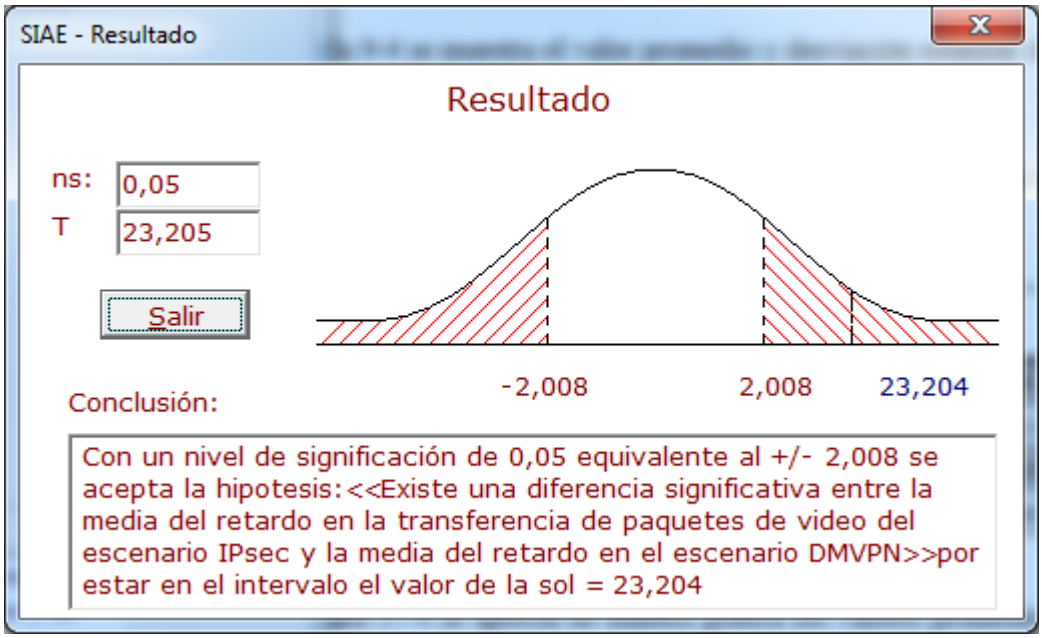

Figura 39-4: Resultados del análisis estadístico del retardo en la transmisión de paquetes de vídeo SPOKE_1 a SPOKE_4, en los escenarios de IPsec y DMVPN.

Realizado por: Alex Jaramillo

4.1.2. Mediciones respecto al Jitter de los paquetes

De la misma forma que en el retardo, en esta sección se evalúa los resultados obtenidos de las mediciones del *jitter*, en los servicios de datos, voz y video, transmitidos sobre los túneles SPOKE_1 a HUB y de SPOKE_1 a SPOKE_4; en los escenarios de IPsec y DMVPN.

A. Túnel SPOKE_1 a HUB

Los resultados de las mediciones realizadas en este túnel se analizan por medio del promedio y desviación estándar y se muestran en la Tabla 20-4.

Tabla 20-4: Valores promedio y desviación estándar del *jitter* de los servicios cursados entre SPOKE_1 y HUB de cada escenario.

	PROMEDIO (ms)		**DESVIACIÓN ESTÁNDAR (ms)**	
	IPsec	**DMVPN**	**IPsec**	**DMVPN**
Datos	0,9085	0,8560	0,1989	0,1541
Voz	0,6568	0,6326	0,1126	0,0532
Video	3,5274	3,5014	0,5674	0,4512

Realizado por: Alex Jaramillo.

Cómo se puede observar los valores de promedio y desviación estándar obtenidos para cada servicio transmitido en el escenario IPsec y DMVPN, tienen una diferencia pequeña a favor de DMVPN.

En la Figura 42-4 se puede apreciar de manera gráfica los resultados del promedio del *jitter* en los escenarios IPsec y DMVPN para los servicios de datos, voz y video.

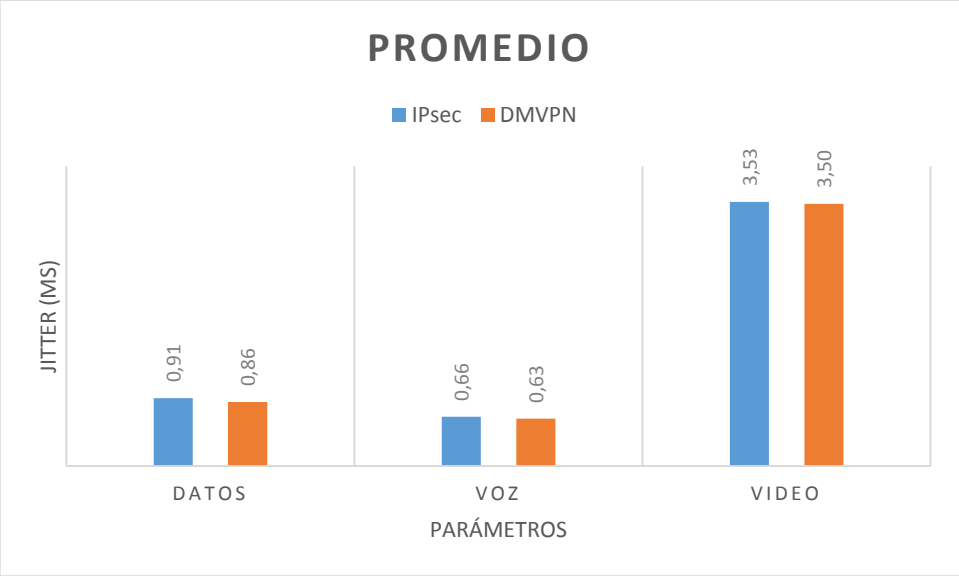

Gráfico 3-4: Promedio del *jitter* en IPsec y DMVPN de los servicios de datos, voz y video sobre el túnel SPOKE_1 y HUB

Realizado por: Alex Jaramillo.

Del mismo modo, se estableció la hipótesis alternativa (H1) y nula (H0) para los tipos de paquetes de datos, voz y video con el objetivo de comprobar por medio del método estadístico "T-student" si existe una diferencia significativa sobre este indicador.

Hipótesis aplicadas para cada tipo de servicio: Datos, Voz y Video:

- **H1: Existe** una diferencia significativa entre la media del *jitter* en la transferencia de paquetes del escenario IPsec y la media del *jitter* en el escenario DMVPN.
- **H0: No existe** una diferencia significativa entre la media del *jitter* en la transferencia de paquetes del escenario IPsec y la media del *jitter* en el escenario DMVPN.

En el análisis de las hipótesis se utilizó el software SIAE para demostrar si existe una diferencia significativa, utilizando los datos de la Tabla 20-4 y empleando el método estadístico "*T-student*" con un nivel de significancia del 5%.

1. **Datos**

Como se puede observar en la Figura 43-4, se acepta la hipótesis nula porque el valor T=1,042 resultó dentro de la región de aceptación de esta hipótesis. En otras palabras, **No existe** una diferencia significativa entre la media del *jitter* en la transferencia de paquetes de Datos en el escenario IPsec y la media del *jitter* en el escenario DMVPN; medido en el túnel *SPOKE_1 y HUB.*

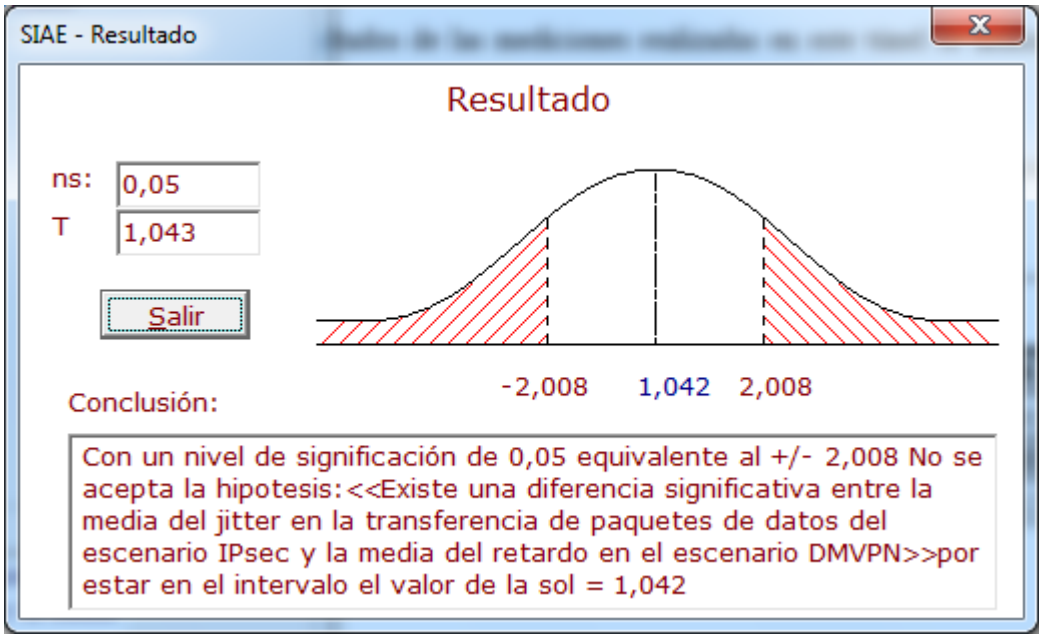

Figura 40-4: Resultado del análisis estadístico del *jitter* en la transferencia de datos en IPsec y DMVPN para el túnel SPOKE_1 y HUB.

Realizado por: Alex Jaramillo.

2. **Voz**

Como se puede observar en la Figura 44-4, se acepta la hipótesis nula porque el valor T=2,007 resultó dentro de la región de aceptación de esta hipótesis. En otras palabras, **No existe** una diferencia significativa entre la media del *jitter* en la transferencia de paquetes de Voz en el escenario IPsec y la media del *jitter* en el escenario DMVPN; medido en el túnel *SPOKE_1 y HUB.*

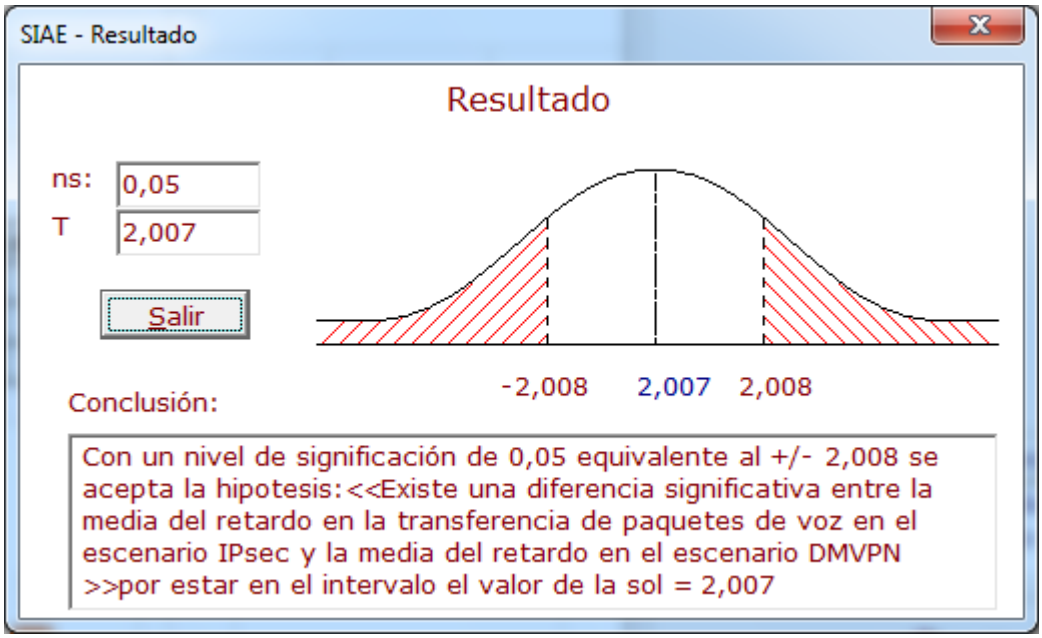

Figura 41-4: Resultados del análisis estadístico del *jitter* en la transferencia de paquetes de voz entre IPsec y DMVPN para el túnel SPOKE_1 y HUB.

Realizado por: Alex Jaramillo.

3. Vídeo

Como se puede observar en la Figura 45-4, se acepta la hipótesis nula porque el valor T=0,179 resultó dentro de la región de aceptación de esta hipótesis. En otras palabras, **No existe** una diferencia significativa entre la media del *jitter* en la transferencia de paquetes de Video en el escenario IPsec y la media del *jitter* en el escenario DMVPN; medido en el túnel *SPOKE_1 y HUB.*

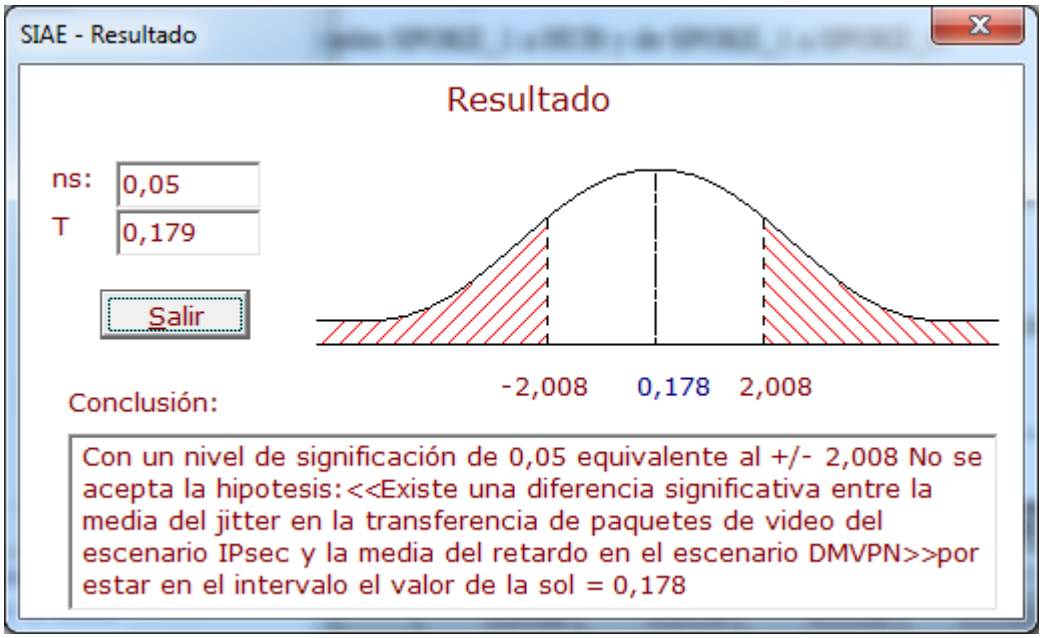

Figura 42-4: Resultados del análisis estadístico del *jitter* en la transferencia de paquetes de vídeo entre IPsec y DMVPN para el túnel SPOKE_1 y HUB.

Realizado por: Alex Jaramillo

B. Túnel SPOKE_1 a SPOKE_4

En la Tabla 21-4 se muestra el valor promedio y desviación estándar de las muestras de *jitter* obtenidas en los escenarios de IPsec y DMVPN, para los servicios de datos, voz y video sobre el túnel SPOKE_1 a SPOKE_4.

Tabla 21-4: Valores promedio y desviación estándar del *jitter* de los servicios cursados entre SPOKE_1 y SPOKE_4 de cada escenario.

	PROMEDIO (ms)		**DESVIACIÓN ESTÁNDAR (ms)**	
	IPsec	**DMVPN**	**IPsec**	**DMVPN**
Datos	3,1138	0,6914	4,5427	0,3365
Voz	1,0990	0,2685	0,1144	0,0406
Video	1,8822	1,1486	0,3452	0,4279

Realizado por: Alex Jaramillo.

Cómo se puede observar los valores de promedio y desviación estándar obtenidos para cada servicio transmitido en el escenario IPsec y DMVPN, se evidencia una diferencia grande en el promedio a favor de DMVPN, en la desviación estándar resulta una diferencia significativa en los servicios de datos y voz a favor de DMVPN pero para el vídeo se tiene una desviación favorable para IPsec que podría deberse a problemas intrínsecos del software usado para la transferencia de vídeo ya que en cuanto a valores se demuestra una mejora para DMVPN.

En la Figura 46-4 se aprecia de manera gráfica los valores promedio del *jitter* obtenido por cada servicio transmitido en el túnel.

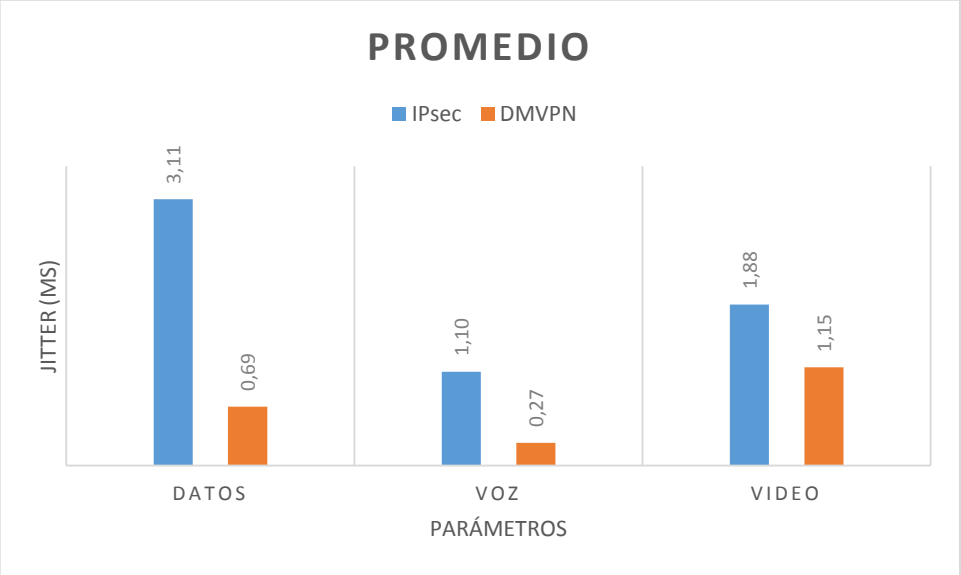

Gráfico 4-4: Valores promedio del *jitter* en IPsec y DMVPN de los servicios de datos, voz y video entre SPOKE_1 y SPOKE_4.

Realizado por: Alex Jaramillo.

Se estableció la hipótesis alternativa (H1) y nula (H0) para los tipos de paquetes de datos, voz y video con el objetivo de comprobar por medio del método estadístico "*T-student*" si existe una diferencia significativa sobre este indicador.

Hipótesis aplicadas para cada tipo de servicio: Datos, Voz y Video:

- **H1: Existe** una diferencia significativa entre la media del *jitter* en la transferencia de paquetes del escenario IPsec y la media del *jitter* en el escenario DMVPN.
- **H0: No existe** una diferencia significativa entre la media del *jitter* en la transferencia de paquetes del escenario IPsec y la media del *jitter* en el escenario DMVPN.

Para el análisis de las hipótesis se utilizó el software SPSS y demostrar si existe una diferencia significativa, utilizando los datos de la Tabla 21-4 y empleando el método estadístico "*T-student*" con un nivel de significancia del 5%.

1. **Datos**

Como se puede observar en la Figura 47-4, el valor T=2,657 está en la región crítica o de rechazo de la hipótesis nula (H0) para paquetes de datos. En otras palabras, **Existe** una diferencia

significativa entre la media del retardo en la transferencia de paquetes de datos en el escenario IPsec y la media del retardo en el escenario DMVPN; medido en el túnel *SPOKE_1 y SPOKE_4.*

.

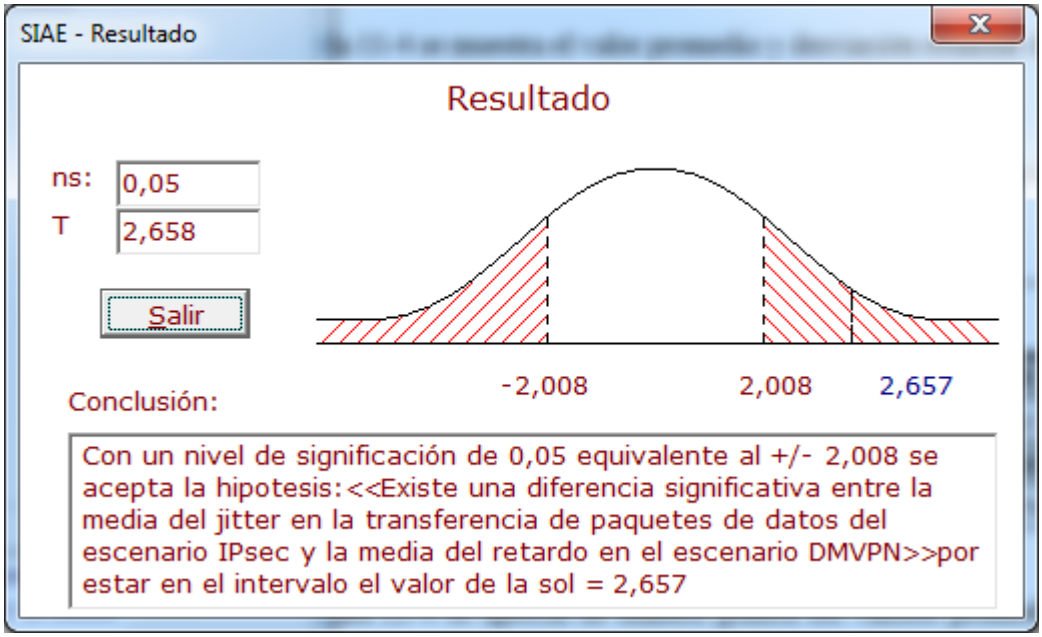

Figura 43-4: Resultado del análisis estadístico del *jitter* en la transferencia de datos en IPsec y DMVPN

Realizado por: Alex Jaramillo.

2. **Voz**

Como se puede observar en la Figura 48-4, el valor T=34,207 está en la región crítica o de rechazo de la hipótesis nula (H0) para paquetes de voz. En otras palabras, **Existe** una diferencia significativa entre la media del retardo en la transferencia de paquetes de voz en el escenario IPsec y la media del retardo en el escenario DMVPN; medido en el túnel *SPOKE_1 y SPOKE_4.*

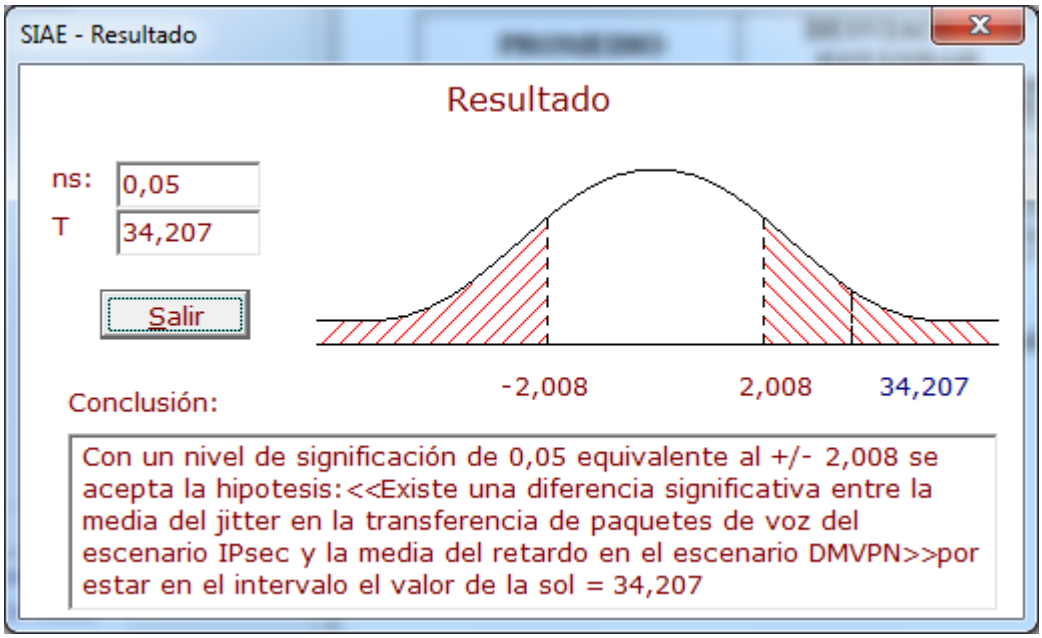

Figura 44-4: Resultado del análisis estadístico del *jitter* en la transferencia de voz en IPsec y DMVPN

Realizado por: Alex Jaramillo.

3. Vídeo

Como se puede observar en la Figura 49-4, el valor T=6,671 está en la región crítica o de rechazo de la hipótesis nula (H0) para paquetes de video. En otras palabras, **Existe** una diferencia significativa entre la media del retardo en la transferencia de paquetes de video en el escenario IPsec y la media del retardo en el escenario DMVPN; medido en el túnel *SPOKE_1 y SPOKE_4.*

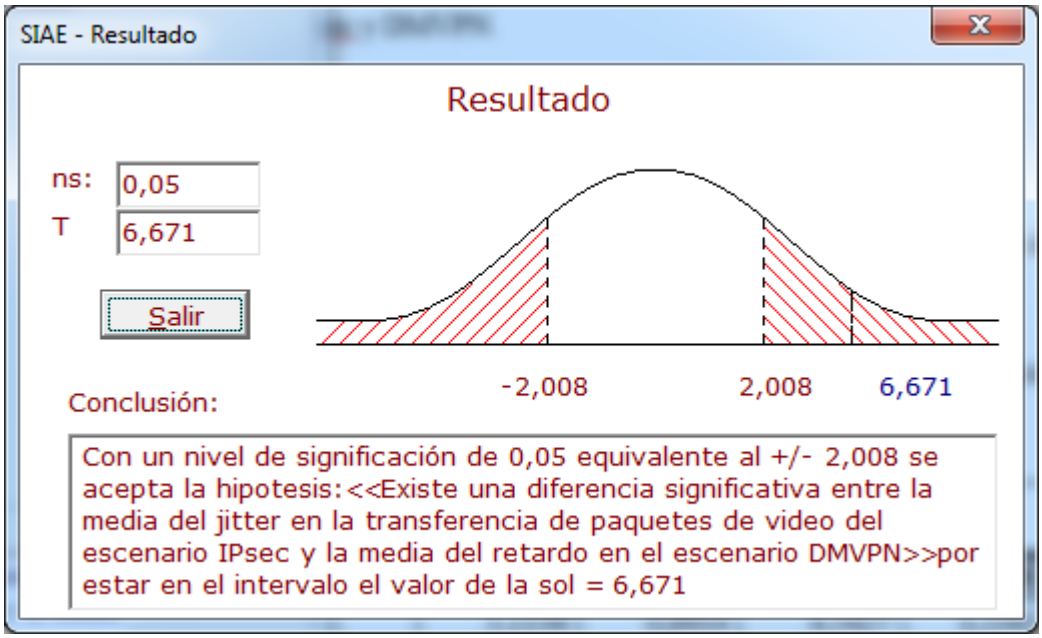

Figura 45-4: Resultado del análisis estadístico del *jitter* en la transferencia de vídeo en IPsec y DMVPN

Realizado por: Alex Jaramillo.

4.1.3. Mediciones respecto a la Pérdida de paquetes

La evaluación de este indicador se realizará de la misma manera que en los anteriores indicadores; es decir se evaluará los resultados de las mediciones obtenidas para las pérdidas de paquetes de los túneles SPOKE_1 a HUB y de SPOKE_1 a SPOKE_4; en los escenarios de IPsec y DMVPN.

A. Túnel SPOKE_1 a HUB

Los resultados de las mediciones realizadas en este túnel se analizan obteniendo el valor promedio y desviación estándar de las muestras y el resultado se detalla en la Tabla 22-4.

Tabla 22-4: Resultado de los valores promedio y desviación estándar de la pérdida de paquetes en los servicios cursados entre SPOKE_1 y HUB de cada escenario

	PROMEDIO (%)		DESVIACIÓN ESTÁNDAR (%)	
	IPsec	**DMVPN**	**IPsec**	**DMVPN**
Datos	0,1315	0,1058	0,3514	0,3334
Voz	0,0496	0,0019	0,1522	0,0039
Video	10,3804	8,3258	1,2366	1,7829

Realizado por: Alex Jaramillo.

Cómo se puede observar los valores promedio y desviaciones estándar obtenidas para cada servicio transmitido en el escenario IPsec y DMVPN no exponen una diferencia considerable pero sí se aprecia una mejora en los valores del escenario DMVPN, salvo la excepción del valor de desviación estándar del video donde los paquetes aparecen más dispersos. Al analizar el comportamiento de cada muestra, se evidencia que en el escenario DMVPN por ocasiones los valores de pérdidas disminuyen y en otras alcanzan los valores de IPsec, por este motivo que se obtienen valores bastante dispersos.

En la Figura 50-4 se puede apreciar de manera gráfica los resultados del promedio de la pérdida de paquetes de los escenarios IPsec y DMVPN para los servicios de datos, voz y video.

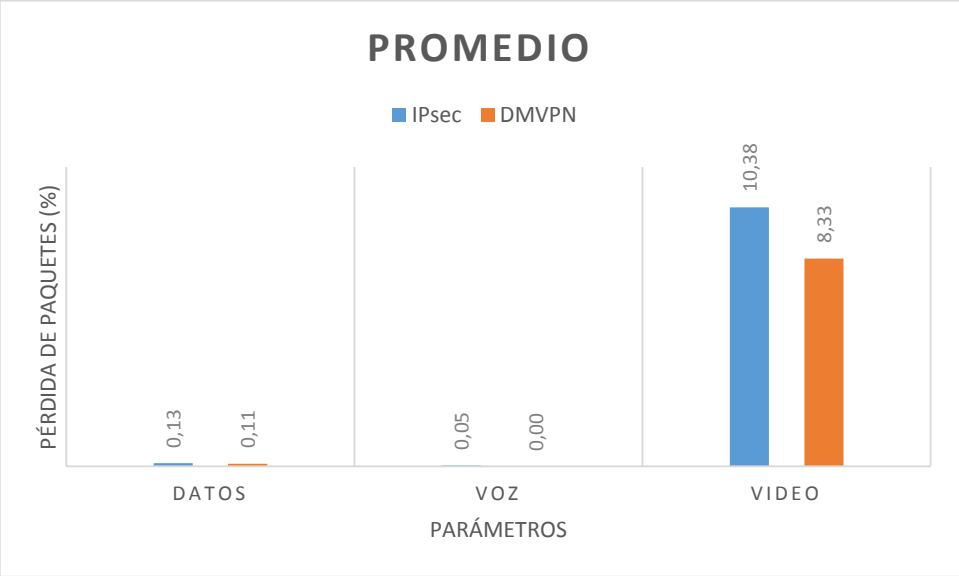

Gráfico 5-4: Promedio del porcentaje de paquetes perdidos en IPsec y DMVPN de los servicios de datos, voz y video sobre el túnel SPOKE_1 y HUB

Realizado por: Alex Jaramillo.

Se estableció la hipótesis alternativa (H1) y nula (H0) para los tipos de paquetes de datos, voz y video con el objetivo de comprobar por medio del método estadístico *T-student* si existe una diferencia significativa sobre este indicador.

Hipótesis aplicadas para cada tipo de servicio: Datos, Voz y Video:

- **H1: Existe** una diferencia significativa entre la media del porcentaje de paquetes perdidos en la transferencia de paquetes del escenario IPsec y la media del porcentaje de paquetes perdidos en el escenario DMVPN.

- **H0: No existe** una diferencia significativa entre la media del porcentaje de paquetes perdidos en la transferencia de paquetes del escenario IPsec y la media del porcentaje de paquetes perdidos en el escenario DMVPN.

En el análisis de las hipótesis se utilizó el software SIAE para demostrar si existe una diferencia significativa, utilizando los datos de la Tabla 22-4 y empleando el método estadístico "*T-student*" con un nivel de significancia del 5%.

1. **Datos**

Como se puede observar en la Figura 51-4, se acepta la hipótesis nula porque el valor T=0,265 resultó dentro de la región de aceptación de esta hipótesis. En otras palabras, **No existe** una diferencia significativa entre la media del porcentaje de paquetes perdidos en la transferencia de paquetes de Datos en el escenario IPsec y la media del porcentaje de paquetes perdidos en el escenario DMVPN; medido en el túnel *SPOKE_1 y HUB.*

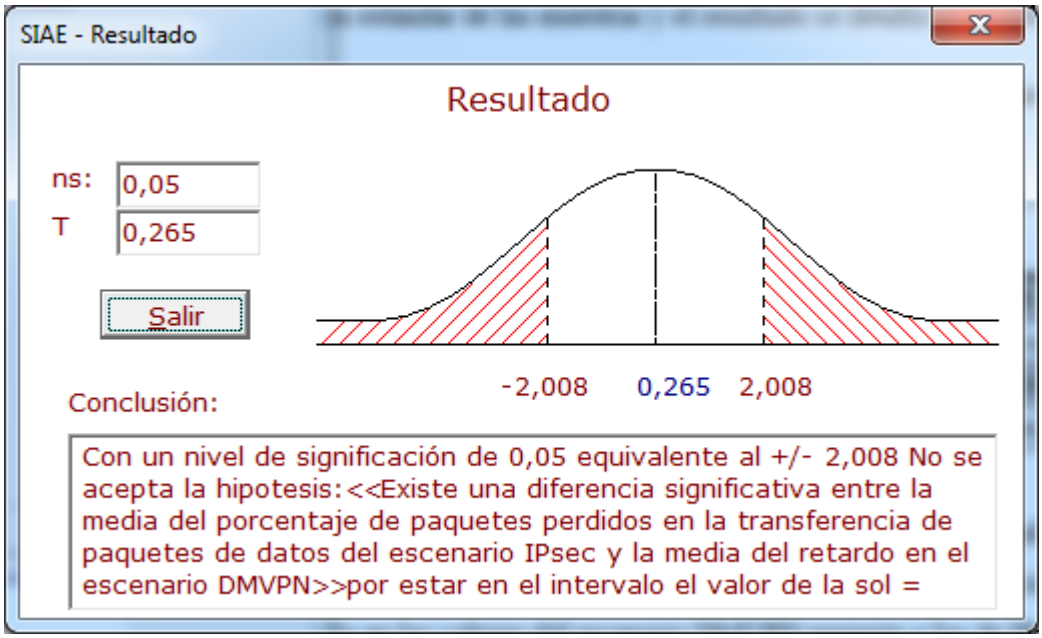

Figura 46-4: Resultado del análisis estadístico de los paquetes perdidos durante la transferencia de datos en IPsec y DMVPN para el túnel SPOKE_1 y HUB.

Realizado por: Alex Jaramillo.

2. **Voz**

Como se puede observar en la Figura 52-4, se acepta la hipótesis nula porque el valor T=1,566 resultó dentro de la región de aceptación de esta hipótesis. En otras palabras, **No existe** una diferencia significativa entre la media del porcentaje de paquetes perdidos en la transferencia de paquetes de voz en el escenario IPsec y la media del porcentaje de paquetes perdidos en el escenario DMVPN; medido en el túnel *SPOKE_1 y HUB.*

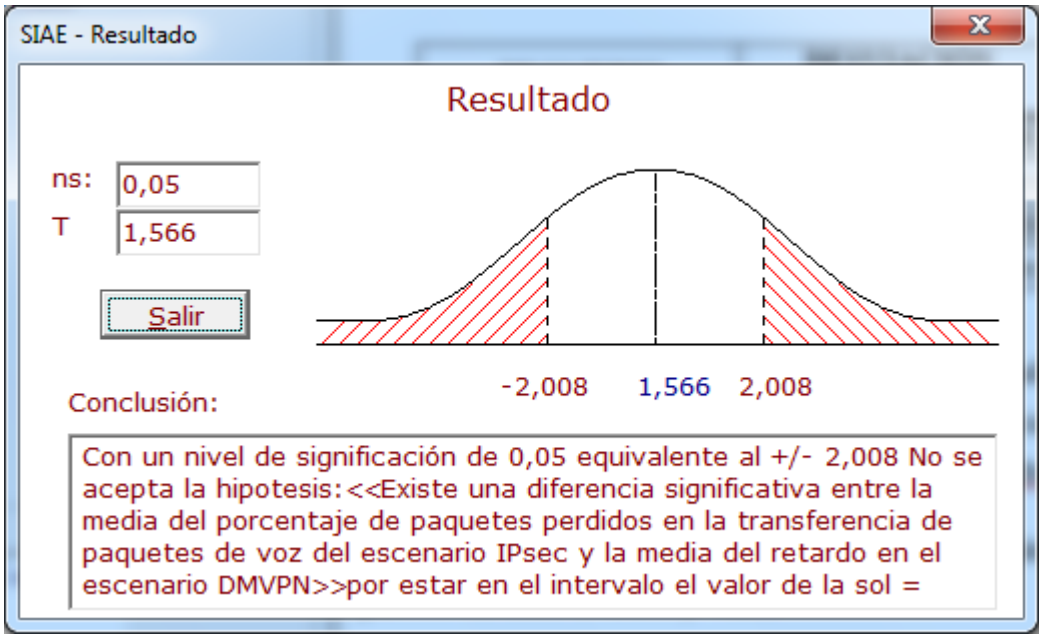

Figura 47-4: Resultados del análisis estadístico de los paquetes perdidos durante la transferencia de paquetes de voz en IPsec y DMVPN para el túnel SPOKE_1 y HUB.

Realizado por: Alex Jaramillo.

3. Vídeo

Como se puede observar en la Figura 53-4, el valor T=4,722 está en la región crítica o de rechazo de la hipótesis nula (H0) para paquetes de video. En otras palabras, **Existe** una diferencia significativa entre la media del porcentaje de paquetes perdidos en la transferencia de paquetes del escenario IPsec y la media del porcentaje de paquetes perdidos en el escenario DMVPN.; medido en el túnel *SPOKE_1 y HUB.*

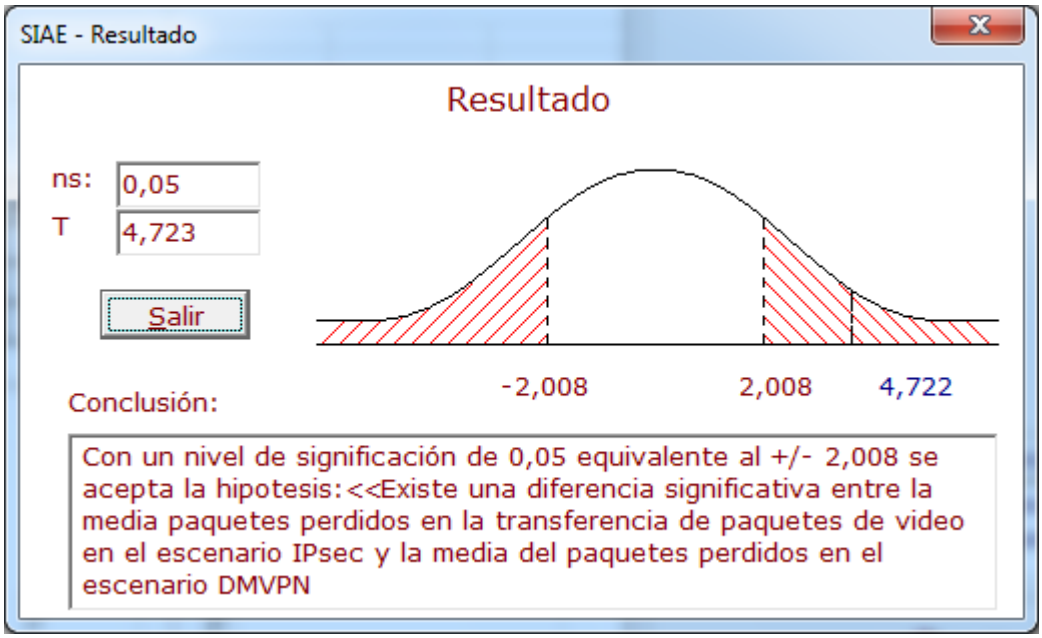

Figura 48-4: Resultados del análisis estadístico de los paquetes perdidos durante la transferencia de paquetes de vídeo en IPsec y DMVPN para el túnel SPOKE_1 y HUB.

Realizado por: Alex Jaramillo.

B. Túnel SPOKE_1 a SPOKE_4

En la Tabla 23-4 se muestra el valor promedio y desviación estándar de las muestras obtenidas de porcentaje de pérdida de paquetes en los escenarios de IPsec y DMVPN, para los servicios de datos, voz y video sobre el túnel SPOKE_1 a SPOKE_4.

Tabla 23-4: Valores promedio y desviación estándar de los servicios cursados entre SPOKE_1 y SPOKE_4 de cada escenario

	PROMEDIO (%)		**DESVIACIÓN ESTÁNDAR (%)**	
	IPsec	**DMVPN**	**IPsec**	**DMVPN**
Datos	8,8277	0,0473	17,5506	0,1587
Voz	0,0219	0,0004	0,1076	0,0019
Video	1,3048	0,5584	1,3675	0,4451

Realizado por: Alex Jaramillo.

Cómo se puede observar los valores promedio y desviaciones estándar obtenidas para cada servicio transmitido en el escenario IPsec y DMVPN no exponen una diferencia considerable pero sí se aprecia una mejora en los valores del escenario DMVPN, excepto el valor de desviación estándar del video donde los paquetes aparecen más dispersos. Como en el túnel *hub* a *spoke* 1, se valida que los valores se presentan más dispersos debido que en algunas pruebas se obtienen valores cercanos a cero y en otros llegan alcanzara los valores máximos obtenidos en IPsec.

En la Figura 54-4 se aprecia de manera gráfica los valores promedio del porcentaje de paquetes perdidos obtenido por cada servicio transmitido en el túnel.

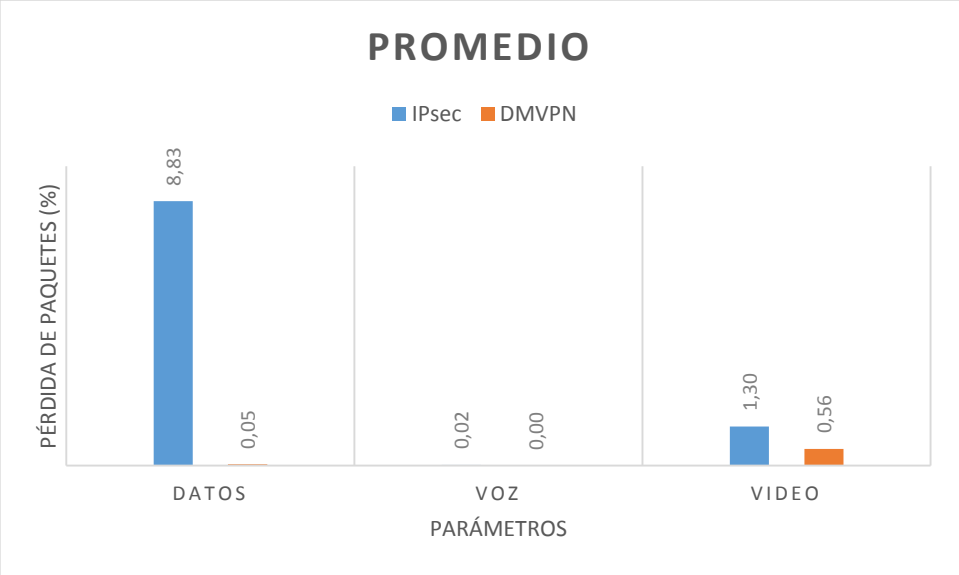

Gráfico 6-4: Valores promedio de paquetes perdidos en IPsec y DMVPN de los servicios de datos, voz y video.

Realizado por: Alex Jaramillo.

Se estableció la hipótesis alternativa (H1) y nula (H0) para los tipos de paquetes de datos, voz y video con el objetivo de comprobar por medio del método estadístico *T-student* si existe una diferencia significativa sobre este indicador.

Hipótesis aplicadas para cada tipo de servicio: Datos, Voz y Video:

- **H1: Existe** una diferencia significativa entre la media del porcentaje de paquetes perdidos en la transferencia de paquetes del escenario IPsec y la media del porcentaje de paquetes perdidos en el escenario DMVPN.
- **H0: No existe** una diferencia significativa entre la media del porcentaje de paquetes perdidos en la transferencia de paquetes del escenario IPsec y la media del porcentaje de paquetes perdidos en el escenario DMVPN.

En el análisis de las hipótesis se utilizó el software SIAE para demostrar si existe una diferencia significativa, utilizando los datos de la Tabla 23-4 y empleando el método estadístico "*T-student*" con un nivel de significancia del 5%.

1. **Datos**

Como se puede observar en la Figura 55-4, el valor T=2,501 está en la región crítica o de rechazo de la hipótesis nula (H0) para paquetes de datos. En otras palabras, **Existe** una diferencia significativa entre la media del porcentaje de paquetes perdidos en la transferencia de paquetes de datos del escenario IPsec y la media del porcentaje de paquetes perdidos en el escenario DMVPN; medido en el túnel *SPOKE_1 y SPOKE_4.*

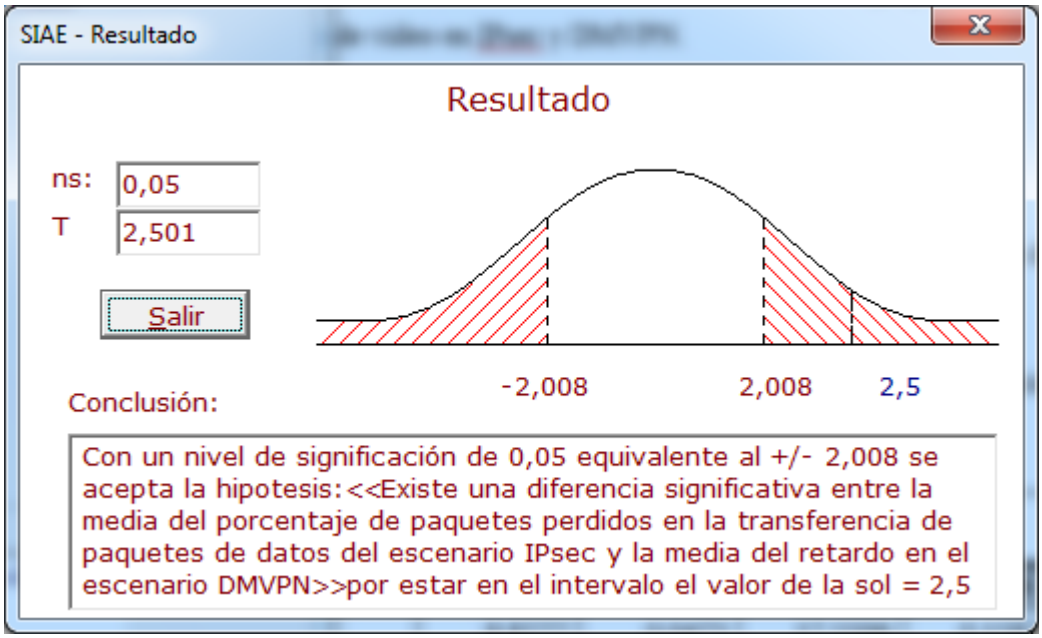

Figura 49-4: Resultado del análisis estadístico de los paquetes perdidos durante la transferencia de datos en IPsec y DMVPN sobre el túnel SPOKE_1 a SPOKE_4.

Realizado por: Alex Jaramillo.

2. **Voz**

Como se puede observar en la Figura 56-4, se acepta la hipótesis nula porque el valor T=0,997 resultó dentro de la región de aceptación de esta hipótesis. En otras palabras, **No existe** una diferencia significativa entre la media del porcentaje de paquetes perdidos en la transferencia de paquetes de voz del escenario IPsec y la media del porcentaje de paquetes perdidos en el escenario DMVPN; medido en el túnel *SPOKE_1 y SPOKE_4.*

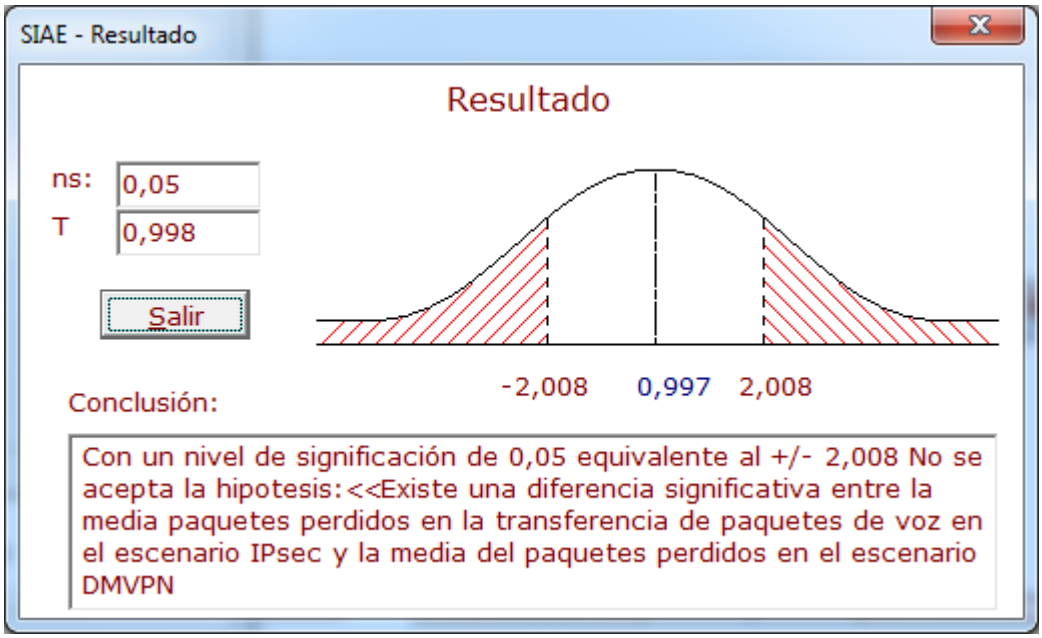

Figura 50-4: Resultados del análisis estadístico de los paquetes perdidos durante la transferencia de paquetes de voz en IPsec y DMVPN sobre el túnel SPOKE_1 a SPOKE_4.

Realizado por: Alex Jaramillo.

3. Vídeo

Como se puede observar en la Figura 57-4, se acepta la hipótesis alternativa porque el valor T=2,572 resultó fuera de la región de aceptación de la hipótesis nula. En otras palabras, **existe** una diferencia significativa entre la media del porcentaje de paquetes perdidos en la transferencia de paquetes de video del escenario IPsec y la media del porcentaje de paquetes perdidos en el escenario DMVPN; medido en el túnel *SPOKE_1 y SPOKE_4.*

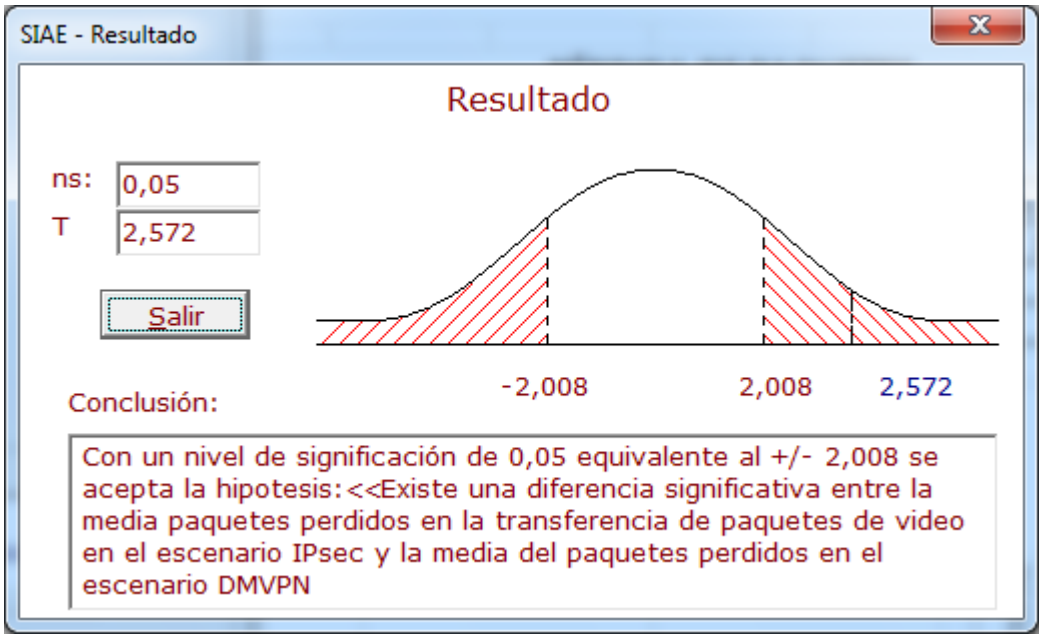

Figura 51-4: Resultados del análisis estadístico de los paquetes perdidos durante la transferencia de paquetes de vídeo en IPsec y DMVPN sobre el túnel SPOKE_1 a SPOKE_4.

Realizado por: Alex Jaramillo.

4.2. Discusión de resultados

En esta sección se procede a analizar y evaluar los resultados para determinar cuál de las dos técnicas, DMVPN o IPsec, obtuvo el "mejor valor" en cada indicador y si estadísticamente existe una diferencia significativa entre los indicadores de ambas técnicas. Como "mejor valor" se entiende: un menor valor de retardo, menor valor de *jitter* y menor porcentaje de paquetes perdidos; ya que esto significa una mejora en el desempeño de la transmisión de servicios como los datos, voz y video sobre una red como Internet.

A continuación se muestra el resumen y síntesis finales de todos los resultados obtenidos al medir los indicadores o variables: retardo, *jitter* y paquetes perdidos; esto con respecto a paquetes de los servicios de datos, voz y video. Cabe recordar que los mencionados paquetes fueron transmitidos

sobre los dos tipos de túnel: HUB – SPOKE y SPOKE - SPOKE y todo esto se evaluó globalmente en los dos escenarios: DMVPN y IPsec.

En la Tabla 24-4 se detallan los indicadores para el servicio de datos y se ha inscrito en cada celda cuál de las dos técnicas tiene el "mejor valor". De modo adicional, se ha pintado de "color verde" los casos donde existe una diferencia significativa entre los valores de DMVPN y IPsec. De esta manera se observa que la técnica DMVPN tiene los "mejores valores" en todos los campos y que especialmente en el canal SPOKE_1 a SPOKE_4 obtuvo una diferencia significativa frente a IPsec. Por lo tanto se concluye que para el tráfico de datos la técnica DMVPN permite un mejor desempeño y este se hace más significativo cuando existe comunicación entre "*spokes*" ya que no hay necesidad de cursar tráfico por el *hub*.

Tabla 24-4: Mejor valor y diferencia significativa de cada indicador para el caso de datos

MEJOR VALOR Y DIFERENCIA SIGNIFICATIVA	DATOS		
	RETARDO	**JITTER**	**PÉRDIDA DE PAQUETES**
SPOKE_1 A HUB	DMVPN	DMVPN	DMVPN
SPOKE_1 A SPOKE_4	DMVPN	DMVPN	DMVPN

Realizado por: Alex Jaramillo.

Del mismo modo, en la Tabla 25-4 se observa que para el tráfico de voz la técnica DMVPN brinda un mejor rendimiento en todos los indicadores. De modo adicional, los indicadores retardo y *jitter* de DMVPN obtuvieron una diferencia significativa frente a IPsec el canal SPOKE_1 a SPOKE_4. En el indicador del porcentaje de paquetes perdidos no existe una diferencia significativa entre IPsec y DMVPN para los túneles analizados puesto que los valores son cercanos a cero y no existe mucho margen de análisis. Por lo antes expuesto se concluye que para el tráfico de voz la técnica DMVPN permite un mejor desempeño.

Tabla 25-4: Mejor valor y diferencia significativa de cada indicador para el caso de voz

MEJOR VALOR Y DIFERENCIA SIGNIFICATIVA	VOZ		
	RETARDO	**JITTER**	**PÉRDIDA DE PAQUETES**
SPOKE_1 A HUB	DMVPN	DMVPN	DMVPN
SPOKE_1 A SPOKE_4	DMVPN	DMVPN	DMVPN

Realizado por: Alex Jaramillo.

Por último, en la Tabla 26-4 se observa que la técnica DMVPN brinda los mejores valores en todos los campos de las pruebas de tráfico de video, resaltando una diferencia significativa en el canal SPOKE_1 a SPOKE_4 sobre el retardo, *jitter* y paquetes perdidos, mientras que en el canal

SPOKE_1 a HUB se obtiene solamente una diferencia significativa en el porcentaje de paquetes perdidos. Por lo tanto se concluye que para el tráfico de video la técnica DMVPN permite un mejor desempeño.

Tabla 26-4: Mejor valor y diferencia significativa de cada indicador para el caso de video

MEJOR VALOR Y DIFERENCIA SIGNIFICATIVA	VIDEO		
	RETARDO	**JITTER**	**PÉRDIDA DE PAQUETES**
SPOKE_1 A HUB	DMVPN	DMVPN	DMVPN
SPOKE_1 A SPOKE_4	DMVPN	DMVPN	DMVPN

Realizado por: Alex Jaramillo.

4.3. Comprobación de la hipótesis

Aplicando la estadística inferencial a los valores de la muestra, se concluye que la técnica DMVPN en términos generales, mejora el desempeño de redes privadas sobre internet, por lo cual se acepta la hipótesis que "La aplicación de DMVPN mejora el desempeño de redes privadas virtuales sobre Internet, con respecto al uso de VPN IPsec".

CAPITULO V

5. PROPUESTA

Como propuesta del presente trabajo de investigación se realiza una guía de implementación con especificaciones técnicas de hardware, software y recomendaciones en las configuraciones de los equipos, misma que se puede seguir para implementar una red DMVPN considerablemente estable y escalable.

5.1. Especificaciones de hardware

En nuestro estudio, DMVPN hace uso de la red pública o Internet para establecer las conexiones entre los distintos puntos. Por este motivo, los dispositivos principales de red que se necesita, son los enrutadores o *Routers* –los cuales deben soportar DMVPN. En la Tabla 5-3 del capítulo III se encuentra detallado los modelos de *Router* que soportan DMVPN.

Cada modelo de *Router* presentado en la mencionada tabla tiene capacidades diferentes, por lo que se sugiere utilizar el *Router* Cisco de la serie 870 para los *spoke* y de la serie 1800 para los *hub*. La elección del modelo dependerá de la cantidad de tráfico que se cursará por cada equipo y la cantidad de interfaces que necesitemos para nuestra red LAN.

5.2. Especificaciones de software

Aquí se establece la versión mínima del sistema operativo que deberá poseer el Router. En la Tabla 6-3 del capítulo III se indica que, por recomendación de Cisco, la versión mínima que deben poseer los *routers* es la versión 12.3 del IOS. Se debe considerar, como recomendación, mantener actualizados los equipos a la versión más reciente que lo soporten y todos los equipos que conforman la red deben tener la misma versión.

5.3. Especificaciones de recursos lógicos

Se debe considerar las siguientes especificaciones a nivel lógico para calificar a nuestro proveedor de última milla y servicio de Internet:

1. Todos los canales de Internet deben permitir la administración de la dirección IP pública.
2. La IP pública asignada para el HUB debe ser de manera estática; es decir no debe cambiar ante un reinicio del equipo.
3. Todos los puntos deben contar con canales de conexión a Internet.
4. No debe existir ningún bloqueo de puertos o de protocolos, por lo que se aconseja contratar canales corporativos de Internet.

Las especificaciones antes mencionadas corresponden a nivel WAN.

A nivel LAN es necesario que las redes de los *spoke* y *hub* se encuentren segmentadas para evitar duplicación de IPs y que esto afecte a la propagación de las redes durante la ejecución del protocolo de enrutamiento dinámico que se aplique.

5.4. Guía de implementación de DMVPN

Una vez definidas las especificaciones a considerarse para una correcta implementación, como lo son el modelo de *Router* Cisco, versión de *firmware*, y el direccionamiento *WAN* y *LAN*, se deberá completar la Tabla 27-5 para llevar un orden en el desarrollo del diseño y configuración.

Tabla 27-5: Modelo de tabla para registro de información

SITIO	FUNCIÓN	WAN	LAN	TUNEL
Ciudad_matriz	*HUB*			
Ciudad_sucursal_1	SPOKE			
Ciudad_sucursal_2	SPOKE			
Ciudad_sucursal_3	SPOKE			
Ciudad_sucursal_4	SPOKE			

Realizado por: Alex Jaramillo

WAN: Direccionamiento público otorgado por el proveedor de Internet.

LAN: Direccionamiento privado interno de cada sitio remoto o sucursal.

TUNEL: Direccionamiento privado diferente al LAN para lograr conectividad entre los túneles *GRE*.

El sitio que se elija como HUB por su importancia y cantidad de tráfico, debe cumplir las siguientes consideraciones:

- El sitio que posea la mejor tecnología de UM.
- El sitio que posea por lo menos el 50% de la capacidad de ancho de banda de la sumatoria de todos los sitios remotos.
- El sitio que posea una conexión de backup que brinde redundancia.
- El sitio que posea el servidor que realice más transacciones de datos, voz o vídeo para evitar el congestionamiento.

Seguido se brinda unas pautas que deben ser consideradas para una correcta implementación:

1. Cada *spoke* debe tener un túnel IPsec permanente hacia el *hub*; no hacia otro *spoke*.
2. Los *spokes* necesitan enviar un paquete a un destino de subred o a otro *spoke*.
3. Luego que el *spoke* inicia el envío, aprende la dirección del PEER; el objetivo es iniciar el túnel IPsec.
4. La comunicación *spoke-spoke* se construye sobre el túnel mGRE.
5. Los canales *spoke-spoke* son construidos por demanda cuando se necesite cursar tráfico entre los *spokes*.

5.4.1. Configuración lógica

En esta sección se presenta un modelo de 4 puntos para la configuración, los cuales deben ser considerados de manera secuencial y en orden.

1. Configurar el HUB de la red DMVPN.
2. Configurar los SPOKE,
3. Configurar IPsec,
4. Configurar el enrutamiento dinámico con EIGRP.

1. Configurar el HUB del DMVPN

Paso 1. Configurar la interfaz WAN y LAN, realizar el *NAT* para la salida a Internet desde la red LAN.

HUB#configure terminal

HUB(config)#interface fastethernet 0

HUB(config-if)#ip address ***IP_PUBLICA_WAN MASCARA***

HUB(config-if)#no shutdown

HUB(config-if)#exit

HUB(config)#interface fastethernet 1

HUB(config-if)#ip address ***IP_PRIVADA_LAN MASCARA***

HUB(config-if)#no shutdown

HUB(config-if)#exit

HUB(config)#ip access-list extended NAT

HUB(config-ext-nacl)#deny ip ***SUBRED_LAN WILCARD SUBRED_SPOKE_1 WILCARD***

HUB(config-ext-nacl)#deny ip ***SUBRED_LAN WILCARD SUBRED_SPOKE_2 WILCARD***

HUB(config-ext-nacl)#deny ip ***SUBRED_LAN WILCARD SUBRED_SPOKE_3 WILCARD***

HUB(config-ext-nacl)#deny ip ***SUBRED_LAN WILCARD SUBRED_SPOKE_4 WILCARD***

HUB(config-ext-nacl)#permit ip ***SUBRED_LAN WILCARD*** any

HUB(config)#int f0

HUB(config-if)#ip nat outside

HUB(config)#int f1

HUB(config-if)#ip nat inside

HUB(config)#ip nat inside source list NAT interface f0 overload

Paso 2. Crear la interfaz túnel *GRE*.

Se debe tener en cuenta que cada interfaz debe funcionar en modo multipunto y el direccionamiento debe permanecer a una misma subred.

HUB(config)#interface Tunnel0

HUB(config-if)#ip address ***IP_TUNEL MASCARA***

HUB(config-if)#tunnel source ***IP_PUBLICA_WAN***

HUB(config-if)#tunnel mode gre multipoint

HUB(config-if)#ip mtu 1430

HUB(config-if)# ip tcp adjust-mss 1390

Paso 3. Configuración de *NHRP*.

Los comandos deben ser incluidos en la interfaz GRE.

HUB(config-if)#ip nhrp map multicast dynamic

HUB(config-if)#ip nhrp network-id 1

HUB(config-if)#ip nhrp redirect

2. Configurar los *SPOKE*

Paso 1. Configurar la interfaz WAN y LAN, realizar el *NAT* para la salida a Internet desde la red LAN.

SPOKE1#configure terminal

SPOKE1(config)#interface fastethernet 0

SPOKE1(config-if)#ip address ***IP_PUBLICA_WAN MASCARA***

SPOKE1(config-if)#no shutdown

SPOKE1(config-if)#exit

SPOKE1(config)#interface fastethernet 1

SPOKE1(config-if)#ip address ***IP_PRIVADA_LAN MASCARA***

SPOKE1(config-if)#no shutdown

SPOKE1(config-if)#exit

SPOKE1(config)#ip access-list extended NAT

SPOKE1(config-ext-nacl)#deny ip ***SUBRED_LAN WILCARD SUBRED_HUB WILCARD***

SPOKE1(config-ext-nacl)#deny ip ***SUBRED_LAN WILCARD SUBRED_SPOKE_2 WILCARD***

SPOKE1(config-ext-nacl)#deny ip ***SUBRED_LAN WILCARD SUBRED_SPOKE_3 WILCARD***

SPOKE1(config-ext-nacl)#deny ip ***SUBRED_LAN WILCARD SUBRED_SPOKE_4 WILCARD***

SPOKE1(config-ext-nacl)#permit ip ***SUBRED_LAN WILCARD*** any

SPOKE1(config)#int f0

SPOKE1(config-if)#ip nat outside

SPOKE1(config)#int f1

SPOKE1(config-if)#ip nat inside

SPOKE1(config)#ip nat inside source list NAT interface f0 overload

Paso 2. Crear la interfaz túnel *GRE*.

Se debe tener en cuenta que cada interfaz debe funcionar en modo multipunto y el direccionamiento debe permanecer a una misma subred.

SPOKE1(config)#interface Tunnel0

SPOKE1(config-if)#ip address ***IP_TUNEL MASCARA***

SPOKE1(config-if)#tunnel source ***IP_PUBLICA_WAN***

SPOKE1(config-if)#tunnel mode gre multipoint

SPOKE1(config-if)#ip mtu 1430

SPOKE1(config-if)# ip tcp adjust-mss 1390

Paso 3. Configuración de *NHRP*.

Los comandos deben ser incluidos en la interfaz GRE.

SPOKE_1(config-if)#ip nhrp map 10.10.0.1 1.1.1.2

SPOKE_1(config-if)#ip nhrp map multicast 1.1.1.2

SPOKE_1(config-if)#ip nhrp network-id 1

SPOKE_1(config-if)#ip nhrp nhs 10.10.0.1

SPOKE_1(config-if)#ip nhrp shortcut

Los mismos comandos se deben replicar para los demás *SPOKE*.

Con el comando "show dmvpn" podemos revisar las entradas del *hub* y *spoke*. En el caso del *hub* visualizaremos entradas dinámicas, mientras que en los *spokes* se visualizan solamente entradas estáticas; es decir, se levantarán entradas dinámicas, solo cuando sea necesario establecer una conexión directa hacia otro *spoke*.

3. Configurar IPsec

La configuración de IPsec es la misma en *HUB* y *SPOKES*.

HUB(config)#crypto isakmp enable

HUB(config)#crypto isakmp policy 10

HUB(config-isakmp)#authentication pre-share

HUB(config-isakmp)#encryption 3des

HUB(config-isakmp)#hash md5

HUB(config-isakmp)#group 2

HUB(config-isakmp)#lifetime 86400

HUB(config-isakmp)#exit

HUB(config)#crypto isakmp key tesis2018 address 0.0.0.0 0.0.0.0

HUB(config)#crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac

HUB(cfg-crypto-trans)#mode transport

HUB(config)#crypto ipsec profile DMVPN_profile

HUB(ipsec-profile)#set transform-set ESP-3DES-MD5

El siguiente comando permite encriptar el tunel GRE utilizando el perfil IPsec creado.

HUB(config)#interface tunnel 0

HUB(config-if)#tunnel protection ipsec profile DMVPN_profile

4. Configurar el enrutamiento dinámico con EIGRP

El protocolo escogido es *EIGRP* por tratarse de un protocolo propietario de Cisco y por ser del tipo vector distancia avanzado, que ofrece lo mejor de los protocolos vector distancia y estado de enlace.

Se activa el proceso *EIGRP* 100 y se añade las redes que participarán en el intercambio de rutas.

A continuación se muestra el ejemplo para un spoke.

SPOKE1(config)#router eigrp 100

SPOKE1(config-router)#network ***SUBRED_LAN WILCARD***

SPOKE1(config-router)#network ***IP_TUNEL WILCARD***

SPOKE1(config)#interface tunnel 0

SPOKE1(config-if)#no ip split-horizon eigrp 100

SPOKE1(config-if)#no ip next-hop-self eigrp 100

CONCLUSIONES

El desarrollo del presente análisis comparativo entre las técnicas IPsec y DMVPN sobre redes públicas, devolvió las siguientes conclusiones:

- En base al análisis teórico y de otros trabajos relacionados al uso de ambas técnicas, se establece de modo general que DMVPN ofrece mejor desempeño para el intercambio de todo tipo de tráfico con la formación de los canales dinámicos; por otra parte, DMVPN ofrece una reducción de comandos para su configuración y operación.

- En el diseño de la red se consideró el uso correcto de los valores de MTU y MSS, por tal motivo se realiza el cálculo para obtener el valor correcto que permita evitar la fragmentación de los paquetes y altere nuestros resultados.

- Durante la fase de implementación, IPsec resultó en un inicio más simple de configurar; sin embargo, a la medida que se incrementaron los *spokes*, la administración y control se volvió un tema complejo, sobre todo en el *hub*, debido que para cada spoke adicional se debe configurar los parámetros del peer para establecer la conexión y así sucesivamente por cada *spoke* que se añada. DMVPN por su lado brindó una escalabilidad rápida sin necesidad de configurar ninguna configuración adicional en el *hub* para añadir más *spoke*.

- En la evaluación de las pruebas de la técnica DMVPN frente a IPsec se evidenció que DMVPN, en los túneles – *HUB* a *SPOKE* siempre tuvo "los mejores valores", denotados como menores valores de *jitter*, menor retardo y menor porcentaje de paquetes perdidos. Esto sucedió para el tráfico de Datos, Voz y Video. En este caso la diferencia entre los valores de DMVPN y los valores de IPsec no fue estadísticamente significativa.

- Para el caso de los túneles SPOKE a SPOKE, el desempeño de DMVPN fue mucho más destacado, al presentar valores muy inferiores en cuanto a retardo, *jitter* y porcentaje de paquetes perdidos en el intercambio de tráfico de Datos, Voz y Vídeo. En este caso la diferencia fue estadísticamente significativa y esta se acentuó más inclusive, cuando se evaluó los canales formados con un mismo proveedor de Internet.

- De las dos conclusiones anteriores se puede colegir que DMVPN en comparación a IPsec, siempre mejora el desempeño de las redes privadas sobre Internet en cuanto a la transmisión de paquetes de Datos, Voz y Vídeo y que el mayor potencial de DMVPN se da lugar cuando se establecen canales de tráfico entre SPOKEs.

- La guía de especificaciones presentada, para la implementación de DMVPN, brinda de una manera sencilla y concreta los aspectos más relevantes de esta técnica e indica lo que fue desarrollado en la práctica.

RECOMENDACIONES

Producto del presente trabajo se obtienen las siguientes recomendaciones:

- Considerar la aplicación de DMVPN con el protocolo IPv6 y evaluar su desempeño, conociendo que se evitará el retardo generado por la traducción de direccionamiento privado a público que se produce en IPv4.

- Para el diseño se recomienda dimensionar correctamente el direccionamiento, ancho de banda a considerarse para seleccionar el equipo Router a utilizar y evitar retardos que pudieran producirse con equipos que no soporten dicha capacidad.

- En el desarrollo de la implementación se debe procurar mantener el uso de los mismos equipos en cada sitio, tanto a nivel de hardware y firmware, así como los mismos protocolos propietarios de enrutamiento dinámico. El fin es no suscitar puntos de falla o dudas en el proceso de implementación.

- Para obtener los valores del indicador retardo de manera confiable es necesario ocupar la métrica *round trip time* (RTT); de esta manera se recibe un valor de retardo sin errores. DITG permite el uso de este tipo de métrica y de una sola vía. Para el caso de una sola vía es necesario que el emisor y receptor se encuentren sincronizados, caso contrario presentará errores o incluso valores negativos.

- Se debe implementar la red con direccionamiento público estático para disminuir el procesamiento del equipo y reducir los tiempos en el establecimiento de las rutas; de modo adicional, esto permitirá al administrador de la red mayor control ante una urgencia o pruebas que realice.

BIBLIOGRAFÍA

Alejandro, A. (2017). *Diseño de redes privadas virtuales con routers cisco.* Valencia: Universidad Politécnica de Valencia.

Besnik, Q., Ardian, B., Ahmet, S., & Edmond, H. (2016). Enterprise Integration, Networking and Virtual Communications. *ScienceDirect*, 3.

Brito, J. (September de 2015). Estudio comparativo entre IPsec y MPLS para redes privadas virtuales. *Universidad de las Fuerzas Armadas, 17*(3), 90-124. Obtenido de http://dl.acm.org/citation.cfm?id=132276

Cisco Systems, I. (2008). *Cisco IOS DMVPN: Overview.* Obtenido de http://www.cisco.com/c/dam/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/DMVPN_Overview.pdf

Cisco Systems, I. (2013). Cisco VPN services port adapter configuration guide. En I. Cisco Systems. San José.

Cisco Systems, I. (13 de Marzo de 2015). *Cisco Dynamic Multipoint VPN: Simple and Secure Branch-to-Branch Communications.* Obtenido de http://www.cisco.com/c/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/data_sheet_c78-468520.html

Cisco, S. (25 de Julio de 2017). *Cisco Dynamic Multipoint VPN: Simple and Secure Branch-to-Branch Communications Data Sheet.* Obtenido de https://www.cisco.com/c/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/data_sheet_c78-468520.html

Feedback Networks. (2013). Obtenido de https://www.feedbacknetworks.com/cas/experiencia/sol-preguntar-calcular.html

González, A. (28 de Julio de 2014). *Redes Privadas Virtuales (VPN).* Obtenido de https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=20&cad=rja&uact=8&ved=0ahUKEwjclY6ntOXZAhXS6lMKHdQ2AsQ4ChAWCGMwCQ&url=http%3A%2F%2Fprofesores.elo.utfsm.cl%2F~agv%2Felo322%2F1s14%2Fprojects%2Freports%2FG20%2FRedes%2520Privadas%2520Virtuales%2

Hernández, R., Fernández, C., & Baptista, P. (2010). *Metodología de la investigación.* México D.F.: Mc Graw Hill.

Juan Carlos Brito Ayala. (September de 2015). Estudio comparativo entre IPsec y MPLS para redes privadas virtuales. *Universidad de las Fuerzas Armadas, 17*(3), 97-124. Obtenido de http://dl.acm.org/citation.cfm?id=132276

Kolon, M. (2006). *MFA Forum.* Obtenido de http://www.webtorials.com/main/MPLScon2006/Kolon.pdf

Lima, A. I. (2010). *Estudio de la viabilidad de un servicio VPN basado en una arquitectura redundante.* Porto: Universidad de Porto.

Lima, L. (2017). Implementación de una red privada virtual dinámica DMVPN con protocolos IPsec, MGRE y NHRP. La Paz, Bolivia.

Lima, L. (2017). *Implementación de una red privada virtual dinámica multipunto DMVPN con protocolos IPsec, MGRE y NHRP.* La Paz: Universidad Mayor de San Andrés.

Milton, R. (2016). *Diseño de un sistema híbrido inalámbrico-fibra para transmisión de datos de medidores inteligentes de energía en redes smart grid.* Quito: Pontificia Universidad Católica de Ecuador.

Pérez, S. (2001). Análisis del protocolo IPSec: el estándar de seguridad en IP. En *Comunicaciones de Telefónica Investigación y Desarrollo* (págs. 51-64). Obtenido de http://www.frlp.utn.edu.ar/materias/internetworking/apuntes/IPSec/IPSec.pdf

Rodriguez, E. (02 de 11 de 2013). *Comunidad de soporte de Cisco*. Obtenido de https://supportforums.cisco.com/t5/routing-y-switching-documentos/como-configurar-un-tunel-gre/ta-p/3150385

Soriano, M. (s.f.). *Seguridad en redes y seguridad en la información.* Obtenido de http://improvet.cvut.cz/project/download/C2ES/Seguridad_de_Red_e_Informacion.pdf

Spichiger, J. (25 de Diciembre de 2016). *Blog de Netlearning Academy*. Obtenido de https://www.netlearning.cl/blog/356250/dmvpn-parte-2

Trujillo, E. (2006). *Diseño e Implementación de una VPN en una empresa comercializadora utilizando IPsec.* Quito: Escuela Politécnica Nacional.

Wikipedia. (01 de 03 de 2014). *Wikipedia.* Obtenido de https://es.wikipedia.org/wiki/GRE

Wikipedia. (2 de Mayo de 2018). *Wikipedia: La enciclopedia libre*. Obtenido de https://es.wikipedia.org/wiki/Microsoft_Excel

ANEXO A:

SHOW RUN DE LOS EQUIPOS *HUB* Y *SPOKE* EN EL ESCENARIO *IPSEC*

HUB

```
hostname HUB_UIO
enable password 7 000100160B5803
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 6 Tesis2018 address 190.57.168.37
crypto isakmp key 6 Tesis2018 address 190.12.61.137
crypto isakmp key 6 Tesis2018 address 201.182.151.5
crypto isakmp key 6 Tesis2018 address 190.57.168.203
!
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
!
crypto map VPN 1 ipsec-isakmp
 set peer 190.57.168.37
 set transform-set ESP-3DES-MD5
 match address 101
crypto map VPN 2 ipsec-isakmp
 set peer 201.182.151.5
 set transform-set ESP-3DES-MD5
 match address 102
crypto map VPN 3 ipsec-isakmp
 set peer 190.12.61.137
```

```
 set transform-set ESP-3DES-MD5
 match address 103
crypto map VPN 4 ipsec-isakmp
 set peer 190.57.168.203
 set transform-set ESP-3DES-MD5
 match address 104
!
archive
 log config
  hidekeys
!
interface FastEthernet0
 description WAN
 ip address 200.105.228.6 255.255.255.252
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 crypto map VPN
!
interface FastEthernet1
 description LAN
 ip address 192.168.60.254 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 ip tcp adjust-mss 1380
 duplex auto
 speed auto
```

```
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 200.105.228.5
!
no ip http server
no ip http secure-server
ip nat inside source list NAT interface FastEthernet0 overload
!
ip access-list extended NAT
 deny   ip 192.168.60.0 0.0.0.255 192.168.70.0 0.0.0.255
 deny   ip 192.168.60.0 0.0.0.255 192.168.80.0 0.0.0.255
 deny   ip 192.168.60.0 0.0.0.255 192.168.90.0 0.0.0.255
 deny   ip 192.168.60.0 0.0.0.255 192.168.100.0 0.0.0.255
 permit ip 192.168.60.0 0.0.0.255 any
!
access-list 101 permit ip 192.168.60.0 0.0.0.255 192.168.70.0 0.0.0.255
access-list 101 permit ip 192.168.80.0 0.0.0.255 192.168.70.0 0.0.0.255
access-list 101 permit ip 192.168.90.0 0.0.0.255 192.168.70.0 0.0.0.255
access-list 101 permit ip 192.168.100.0 0.0.0.255 192.168.70.0 0.0.0.255
access-list 102 permit ip 192.168.60.0 0.0.0.255 192.168.80.0 0.0.0.255
access-list 102 permit ip 192.168.100.0 0.0.0.255 192.168.80.0 0.0.0.255
access-list 102 permit ip 192.168.90.0 0.0.0.255 192.168.80.0 0.0.0.255
access-list 102 permit ip 192.168.70.0 0.0.0.255 192.168.80.0 0.0.0.255
access-list 103 permit ip 192.168.60.0 0.0.0.255 192.168.90.0 0.0.0.255
access-list 103 permit ip 192.168.80.0 0.0.0.255 192.168.90.0 0.0.0.255
```

```
access-list 103 permit ip 192.168.70.0 0.0.0.255 192.168.90.0 0.0.0.255
access-list 103 permit ip 192.168.100.0 0.0.0.255 192.168.90.0 0.0.0.255
access-list 104 permit ip 192.168.60.0 0.0.0.255 192.168.100.0 0.0.0.255
access-list 104 permit ip 192.168.80.0 0.0.0.255 192.168.100.0 0.0.0.255
access-list 104 permit ip 192.168.70.0 0.0.0.255 192.168.100.0 0.0.0.255
access-list 104 permit ip 192.168.90.0 0.0.0.255 192.168.100.0 0.0.0.255
snmp-server community tesis RO
!
line con 0
line aux 0
line vty 0 4
 password 7 001016150D4859565E79
 login
!
end
```

SPOKE 1

```
hostname SPOKE_1_LOJ
enable password 7 06031C31434D01
!
no ip domain lookup
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 6 Tesis2018 address 200.105.228.6
```

```
!
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
!
crypto map VPN 1 ipsec-isakmp
 set peer 200.105.228.6
 set transform-set ESP-3DES-MD5
 match address 101
!
interface FastEthernet0
 description WAN
 ip address 190.57.168.37 255.255.255.240
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 crypto map VPN
!
interface FastEthernet1
 description LAN
 ip address 192.168.70.254 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 ip tcp adjust-mss 1380
 duplex auto
 speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 190.57.168.33
```

```
!
no ip http server
no ip http secure-server
ip nat inside source list NAT interface FastEthernet0 overload
!
ip access-list extended NAT
 deny   ip 192.168.70.0 0.0.0.255 192.168.60.0 0.0.0.255
 deny   ip 192.168.70.0 0.0.0.255 192.168.80.0 0.0.0.255
 deny   ip 192.168.70.0 0.0.0.255 192.168.90.0 0.0.0.255
 deny   ip 192.168.70.0 0.0.0.255 192.168.100.0 0.0.0.255
 permit ip 192.168.70.0 0.0.0.255 any
!
access-list 101 permit ip 192.168.70.0 0.0.0.255 192.168.60.0
0.0.0.255
access-list 101 permit ip 192.168.70.0 0.0.0.255 192.168.80.0
0.0.0.255
access-list 101 permit ip 192.168.70.0 0.0.0.255 192.168.90.0
0.0.0.255
access-list 101 permit ip 192.168.70.0 0.0.0.255 192.168.100.0
0.0.0.255
snmp-server community tesis RO
!
line con 0
line aux 0
line vty 0 4
 password 7 001016150D4859565E79
 login
!
end
```

SPOKE 2

```
hostname SPOKE_2_CAT
!
enable password 7 0116151454080E
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 6 Tesis2018 address 200.105.228.6
!
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
!
crypto map VPN 2 ipsec-isakmp
 set peer 200.105.228.6
 set transform-set ESP-3DES-MD5
 match address 102
!
interface FastEthernet0
 description WAN
 ip address 201.182.151.5 255.255.255.248
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 crypto map VPN
```

```
!
interface FastEthernet1
 description LAN
 ip address 192.168.80.254 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 ip tcp adjust-mss 1380
 duplex auto
 speed auto
!
ip route 0.0.0.0 0.0.0.0 201.182.151.1
!
no ip http server
no ip http secure-server
ip nat inside source list NAT interface FastEthernet0 overload
!
ip access-list extended NAT
 deny   ip 192.168.80.0 0.0.0.255 192.168.60.0 0.0.0.255
 deny   ip 192.168.80.0 0.0.0.255 192.168.70.0 0.0.0.255
 deny   ip 192.168.80.0 0.0.0.255 192.168.90.0 0.0.0.255
 deny   ip 192.168.80.0 0.0.0.255 192.168.100.0 0.0.0.255
 permit ip 192.168.80.0 0.0.0.255 any
!
access-list 102 permit ip 192.168.80.0 0.0.0.255 192.168.60.0
0.0.0.255
access-list 102 permit ip 192.168.80.0 0.0.0.255 192.168.100.0
0.0.0.255
access-list 102 permit ip 192.168.80.0 0.0.0.255 192.168.70.0
0.0.0.255
```

```
access-list 102 permit ip 192.168.80.0 0.0.0.255 192.168.90.0
0.0.0.255
snmp-server community tesis RO
!
line con 0
line 1
 modem InOut
 stopbits 1
 speed 115200
 flowcontrol hardware
line aux 0
line vty 0 4
 password 7 105A0C0A0C04405B5D5C
 login
!
end
```

SPOKE 3

```
hostname SPOKE_3_LOJ
!
enable password 7 121C16071D0804
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 6 Tesis2018 address 190.57.168.37
```

```
!
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
!
crypto map VPN 1 ipsec-isakmp
 set peer 190.57.168.37
 set transform-set ESP-3DES-MD5
 match address 103
!
interface FastEthernet0
 description WAN
 ip address 190.12.61.137 255.255.255.240
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 crypto map VPN
!
interface FastEthernet1
 description LAN
 ip address 192.168.90.254 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 ip tcp adjust-mss 1380
 duplex auto
 speed auto
!
ip route 0.0.0.0 0.0.0.0 190.12.61.129
!
```

```
no ip http server
no ip http secure-server
ip nat inside source list NAT interface FastEthernet0 overload
!
ip access-list extended NAT
 deny   ip 192.168.90.0 0.0.0.255 192.168.60.0 0.0.0.255
 deny   ip 192.168.90.0 0.0.0.255 192.168.70.0 0.0.0.255
 deny   ip 192.168.90.0 0.0.0.255 192.168.80.0 0.0.0.255
 deny   ip 192.168.90.0 0.0.0.255 192.168.100.0 0.0.0.255
 permit ip 192.168.90.0 0.0.0.255 any
!
access-list 103 permit ip 192.168.90.0 0.0.0.255 192.168.60.0
0.0.0.255
access-list 103 permit ip 192.168.90.0 0.0.0.255 192.168.70.0
0.0.0.255
access-list 103 permit ip 192.168.90.0 0.0.0.255 192.168.80.0
0.0.0.255
access-list 103 permit ip 192.168.90.0 0.0.0.255 192.168.100.0
0.0.0.255
snmp-server community tesis RO
!
line con 0
line 1
 modem InOut
 stopbits 1
 speed 115200
 flowcontrol hardware
line aux 0
line vty 0 4
```

```
 password 7 044F0E1506321E1E5841
 login
!
end
```

SPOKE 4

```
hostname SPOKE_4_LOJ
!
enable password 7 1517181C0B2923
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 6 Tesis2018 address 200.105.228.6
!
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
!
crypto map VPN 1 ipsec-isakmp
 set peer 200.105.228.6
 set transform-set ESP-3DES-MD5
 match address 104
!
interface FastEthernet0
 description WAN
 ip address 190.57.168.203 255.255.255.224
 ip nat outside
```

```
 ip virtual-reassembly
 duplex auto
 speed auto
 crypto map VPN
!
interface FastEthernet1
 description LAN
 ip address 192.168.100.254 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 ip tcp adjust-mss 1380
 duplex auto
 speed auto
!
ip route 0.0.0.0 0.0.0.0 190.57.168.193
!
no ip http server
no ip http secure-server
ip nat inside source list NAT interface FastEthernet0 overload
!
ip access-list extended NAT
 deny   ip 192.168.100.0 0.0.0.255 192.168.60.0 0.0.0.255
 deny   ip 192.168.100.0 0.0.0.255 192.168.70.0 0.0.0.255
 deny   ip 192.168.100.0 0.0.0.255 192.168.80.0 0.0.0.255
 deny   ip 192.168.100.0 0.0.0.255 192.168.90.0 0.0.0.255
 permit ip 192.168.100.0 0.0.0.255 any
!
```

```
access-list 104 permit ip 192.168.100.0 0.0.0.255 192.168.60.0
0.0.0.255

access-list 104 permit ip 192.168.100.0 0.0.0.255 192.168.70.0
0.0.0.255

access-list 104 permit ip 192.168.100.0 0.0.0.255 192.168.80.0
0.0.0.255

access-list 104 permit ip 192.168.100.0 0.0.0.255 192.168.90.0
0.0.0.255

snmp-server community tesis RO

!

line con 0

line aux 0

line vty 0 4

 password 7 0835495D000A57474353

 login

!

end
```

ANEXO B:

SHOW RUN DE LOS EQUIPOS *HUB* Y *SPOKE* EN EL ESCENARIO *DMVPN*

HUB

```
hostname HUB_UIO
enable password 7 000100160B5803
!
no ip domain lookup
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 6 Tesis2018 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
 mode transport
!
crypto ipsec profile DMVPN_profile
 set transform-set ESP-3DES-MD5
!
interface Tunnel0
 ip address 10.10.0.254 255.255.255.0
 no ip redirects
 ip mtu 1430
 no ip next-hop-self eigrp 100
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
```

```
 ip nhrp redirect
 ip tcp adjust-mss 1390
 no ip split-horizon eigrp 100
 tunnel source 200.105.228.6
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN_profile
!
interface FastEthernet0
 description WAN
 ip address 200.105.228.6 255.255.255.252
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet1
 description LAN
 ip address 192.168.60.254 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
router eigrp 100
 network 10.10.0.254 0.0.0.0
 network 192.168.60.0
 auto-summary
!
```

```
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 200.105.228.5
!
no ip http server
no ip http secure-server
ip nat inside source list NAT interface FastEthernet0 overload
!
ip access-list extended NAT
 deny   ip 192.168.60.0 0.0.0.255 192.168.70.0 0.0.0.255
 deny   ip 192.168.60.0 0.0.0.255 192.168.80.0 0.0.0.255
 deny   ip 192.168.60.0 0.0.0.255 192.168.90.0 0.0.0.255
 deny   ip 192.168.60.0 0.0.0.255 192.168.100.0 0.0.0.255
 permit ip 192.168.60.0 0.0.0.255 any
!
snmp-server community tesis RO
!
line con 0
line aux 0
line vty 0 4
 password 7 001016150D4859565E79
 login
!
end
```

SPOKE 1

```
hostname SPOKE_1_LOJ
enable password 7 06031C31434D01
!
```

```
no ip domain lookup
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 6 Tesis2018 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
 mode transport
!
crypto ipsec profile DMVPN_profile
 set transform-set ESP-3DES-MD5
!
interface Tunnel0
 ip address 10.10.0.1 255.255.255.0
 no ip redirects
 ip mtu 1430
 ip nhrp map 10.10.0.254 200.105.228.6
 ip nhrp map multicast 200.105.228.6
 ip nhrp network-id 1
 ip nhrp nhs 10.10.0.254
 ip tcp adjust-mss 1390
 tunnel source 190.57.168.37
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN_profile
!
```

```
interface BRI0
 no ip address
 encapsulation hdlc
 shutdown
!
interface FastEthernet0
 description WAN
 ip address 190.57.168.37 255.255.255.240
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 traffic-shape rate 2048000 51200 51200 1000
!
interface FastEthernet1
 description LAN
 ip address 192.168.70.254 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
 traffic-shape rate 2048000 51200 51200 1000
!
router eigrp 100
 network 10.10.0.1 0.0.0.0
 network 192.168.70.0
 auto-summary
!
```

```
ip forward-protocol nd

no ip http server

no ip http secure-server

ip nat inside source list NAT interface FastEthernet0 overload

!

ip access-list extended NAT

 deny   ip 192.168.70.0 0.0.0.255 192.168.60.0 0.0.0.255

 deny   ip 192.168.70.0 0.0.0.255 192.168.80.0 0.0.0.255

 deny   ip 192.168.70.0 0.0.0.255 192.168.90.0 0.0.0.255

 deny   ip 192.168.70.0 0.0.0.255 192.168.100.0 0.0.0.255

 permit ip 192.168.70.0 0.0.0.255 any

!

snmp-server community tesis RO

!

line con 0

line aux 0

line vty 0 4

 password 7 001016150D4859565E79

 login

!

end
```

SPOKE 2

```
hostname SPOKE_2_CAT

enable password 7 0116151454080E

!

crypto isakmp policy 10

 encr 3des
```

```
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 6 Tesis2018 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
 mode transport
!
crypto ipsec profile DMVPN_profile
 set transform-set ESP-3DES-MD5
!
interface Tunnel0
 ip address 10.10.0.2 255.255.255.0
 no ip redirects
 ip mtu 1430
 ip nhrp map 10.10.0.254 200.105.228.6
 ip nhrp map multicast 200.105.228.6
 ip nhrp network-id 1
 ip nhrp nhs 10.10.0.254
 ip tcp adjust-mss 1390
 tunnel source 201.182.151.5
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN_profile
!
interface FastEthernet0
 description WAN
 ip address 201.182.151.5 255.255.255.248
 ip nat outside
```

```
 ip virtual-reassembly
 duplex auto
 speed auto
 traffic-shape rate 2048000 51200 51200 1000
!
interface FastEthernet1
 description LAN
 ip address 192.168.80.254 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
 traffic-shape rate 2048000 51200 51200 1000
!
router eigrp 100
 network 10.10.0.2 0.0.0.0
 network 192.168.80.0
 auto-summary
!
no ip http server
no ip http secure-server
ip nat inside source list NAT interface FastEthernet0 overload
!
ip access-list extended NAT
 deny   ip 192.168.80.0 0.0.0.255 192.168.60.0 0.0.0.255
 deny   ip 192.168.80.0 0.0.0.255 192.168.70.0 0.0.0.255
 deny   ip 192.168.80.0 0.0.0.255 192.168.90.0 0.0.0.255
 deny   ip 192.168.80.0 0.0.0.255 192.168.100.0 0.0.0.255
```

```
 permit ip 192.168.80.0 0.0.0.255 any
!
snmp-server community tesis RO
!
line con 0
line 1
 modem InOut
 stopbits 1
 speed 115200
 flowcontrol hardware
line aux 0
line vty 0 4
 password 7 105A0C0A0C04405B5D5C
 login
!
end
```

SPOKE 3

```
hostname SPOKE_3_LOJ
enable password 7 0116151454080E
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 6 Tesis2018 address 0.0.0.0 0.0.0.0
!
```

```
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
 mode transport
!
crypto ipsec profile DMVPN_profile
 set transform-set ESP-3DES-MD5
!
interface Tunnel0
 ip address 10.10.0.3 255.255.255.0
 no ip redirects
 ip mtu 1430
 ip nhrp map 10.10.0.254 200.105.228.6
 ip nhrp map multicast 200.105.228.6
 ip nhrp network-id 1
 ip nhrp nhs 10.10.0.254
 ip tcp adjust-mss 1390
 tunnel source 190.12.61.137
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN_profile
!
interface FastEthernet0
 description WAN
 ip address 190.12.61.137 255.255.255.240
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 traffic-shape rate 2048000 51200 51200 1000
!
```

```
interface FastEthernet1
 description LAN
 ip address 192.168.90.254 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
 traffic-shape rate 2048000 51200 51200 1000
!
router eigrp 100
 network 10.10.0.3 0.0.0.0
 network 192.168.90.0
 auto-summary
!
no ip http server
no ip http secure-server
ip nat inside source list NAT interface FastEthernet0 overload
!
ip access-list extended NAT
 deny   ip 192.168.90.0 0.0.0.255 192.168.60.0 0.0.0.255
 deny   ip 192.168.90.0 0.0.0.255 192.168.70.0 0.0.0.255
 deny   ip 192.168.90.0 0.0.0.255 192.168.80.0 0.0.0.255
 deny   ip 192.168.90.0 0.0.0.255 192.168.100.0 0.0.0.255
 permit ip 192.168.90.0 0.0.0.255 any
!
access-list 103 permit ip 192.168.90.0 0.0.0.255 192.168.60.0 0.0.0.255
access-list 103 permit ip 192.168.90.0 0.0.0.255 192.168.70.0 0.0.0.255
access-list 103 permit ip 192.168.90.0 0.0.0.255 192.168.80.0 0.0.0.255
```

```
access-list 103 permit ip 192.168.90.0 0.0.0.255 192.168.100.0 0.0.0.255
snmp-server community tesis RO
!
line con 0
line 1
 modem InOut
 stopbits 1
 speed 115200
 flowcontrol hardware
line aux 0
line vty 0 4
 password 7 044F0E1506321E1E5841
 login
!
end
```

SPOKE 4

```
hostname SPOKE_4_LOJ
enable password 7 1517181C0B2923
!
no ip domain lookup
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 6 Tesis2018 address 0.0.0.0 0.0.0.0
```

```
!
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
 mode transport
!
crypto ipsec profile DMVPN_profile
 set transform-set ESP-3DES-MD5
!
interface Tunnel0
 ip address 10.10.0.4 255.255.255.0
 no ip redirects
 ip mtu 1430
 ip nhrp map 10.10.0.254 200.105.228.6
 ip nhrp map multicast 200.105.228.6
 ip nhrp network-id 1
 ip nhrp nhs 10.10.0.254
 ip tcp adjust-mss 1390
 tunnel source 190.57.168.203
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN_profile
!
interface FastEthernet0
 description WAN
 ip address 190.57.168.203 255.255.255.224
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 traffic-shape rate 2048000 51200 51200 1000
```

```
!
interface FastEthernet1
 description LAN
 ip address 192.168.100.254 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
 traffic-shape rate 2048000 51200 51200 1000
!
router eigrp 100
 network 10.10.0.4 0.0.0.0
 network 192.168.100.0
 auto-summary
!
no ip http server
no ip http secure-server
ip nat inside source list NAT interface FastEthernet0 overload
!
ip access-list extended NAT
 deny   ip 192.168.100.0 0.0.0.255 192.168.60.0 0.0.0.255
 deny   ip 192.168.100.0 0.0.0.255 192.168.70.0 0.0.0.255
 deny   ip 192.168.100.0 0.0.0.255 192.168.80.0 0.0.0.255
 deny   ip 192.168.100.0 0.0.0.255 192.168.90.0 0.0.0.255
 permit ip 192.168.100.0 0.0.0.255 any
!
snmp-server community tesis RO
!
```

```
line con 0

line aux 0

line vty 0 4

 password 7 0835495D000A57474353

 login

!

end
```

ANEXO C:

RESULTADO DE LAS MEDICIONES DE LOS INDICADORES

Se presenta la media y desviación estándar de los indicadores retardo, *jitter* y paquetes perdidos de todos los escenarios con IPsec y DMVPN.

1. RETARDO

A. TUNEL HUB A SPOKE 1

Tabla 28-C: Promedio del retardo para los indicadores de datos, voz y vídeo para los escenarios IPsec y DMVPN

PROMEDIO	IPsec	DMVPN
Datos	14,43	13,84
Voz	11,09	11,03
Video	24,64	24,18

Realizado por: Alex Jaramillo

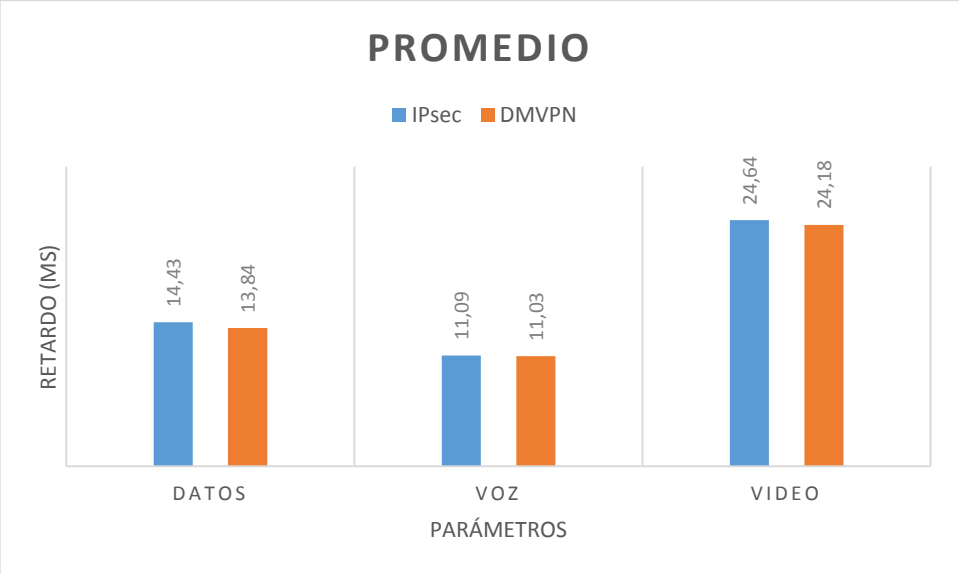

Figura 52-C: Promedio del retardo para los indicadores de datos, voz y vídeo para los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

Tabla 29-C: Desviación estándar del retardo para datos, voz y video de los escenarios IPsec y DMVPN

DESVIACIÓN ESTANDAR	IPsec	DMVPN

Datos	4,90	2,58
Voz	1,54	0,19
Video	7,14	3,61

Realizado por: Alex Jaramillo

Figura 53-C: Desviación estándar del retardo para datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

B. TUNEL SPOKE 1 A SPOKE 2

Tabla 30-C: Promedio del retardo para datos, voz y video de los escenarios IPsec y DMVPN

PROMEDIO	IPsec	DMVPN
Datos	106,24	83,46
Voz	88,34	80,22
Video	110,58	92,32

Realizado por: Alex Jaramillo

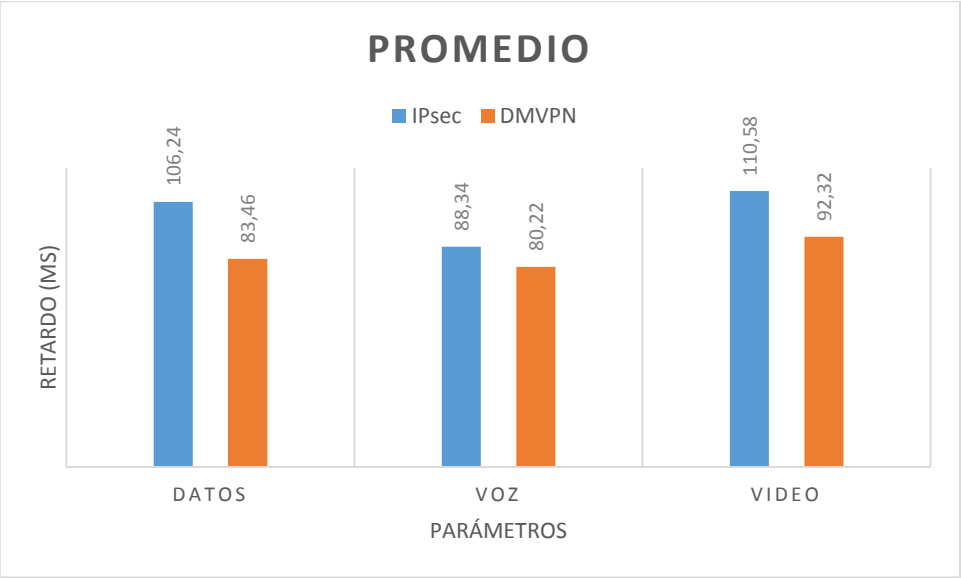

Figura 54-C: Promedio del retardo para datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

Tabla 31-C: Desviación estándar del retardo para datos, voz y video de los escenarios IPsec y DMVPN

DESVIACIÓN ESTANDAR	IPsec	DMVPN
Datos	16,07	0,84
Voz	0,63	0,55
Video	49,24	4,78

Realizado por: Alex Jaramillo

Figura 55-C: Desviación estándar del retardo para datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

C. TUNEL SPOKE 1 A SPOKE 3

Tabla 32-C: Promedio del retardo para datos, voz y video de los escenarios IPsec y DMVPN

PROMEDIO	IPsec	DMVPN
Datos	43,01	3,30
Voz	18,18	2,04
Video	15,06	4,46

Realizado por: Alex Jaramillo

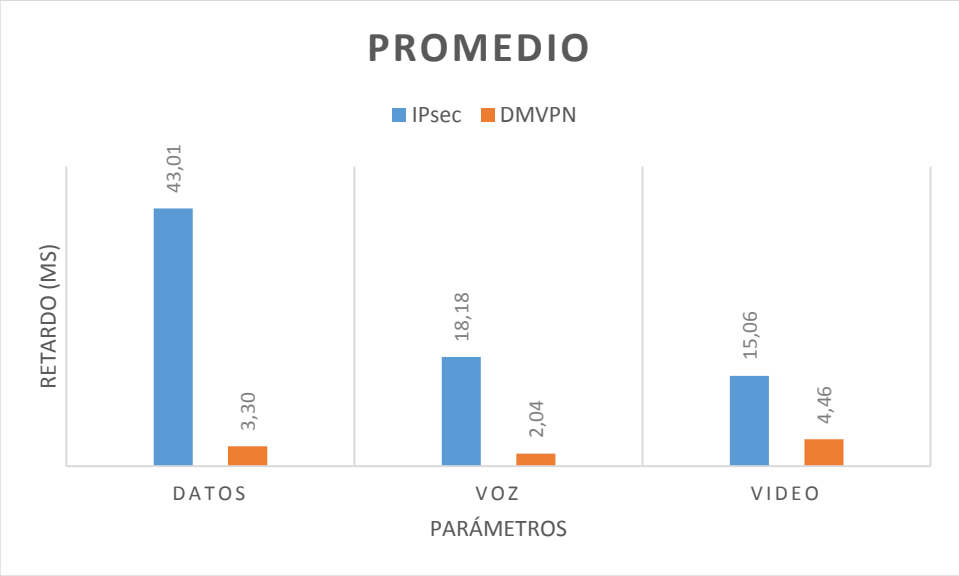

Figura 56-C: Promedio del retardo para datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

Tabla 33-C: Desviación estándar del retardo para datos, voz y video de los escenarios IPsec y DMVPN

DESVIACIÓN ESTANDAR	IPsec	DMVPN
Datos	7,36	1,10
Voz	23,38	0,10
Video	0,35	2,52

Realizado por: Alex Jaramillo

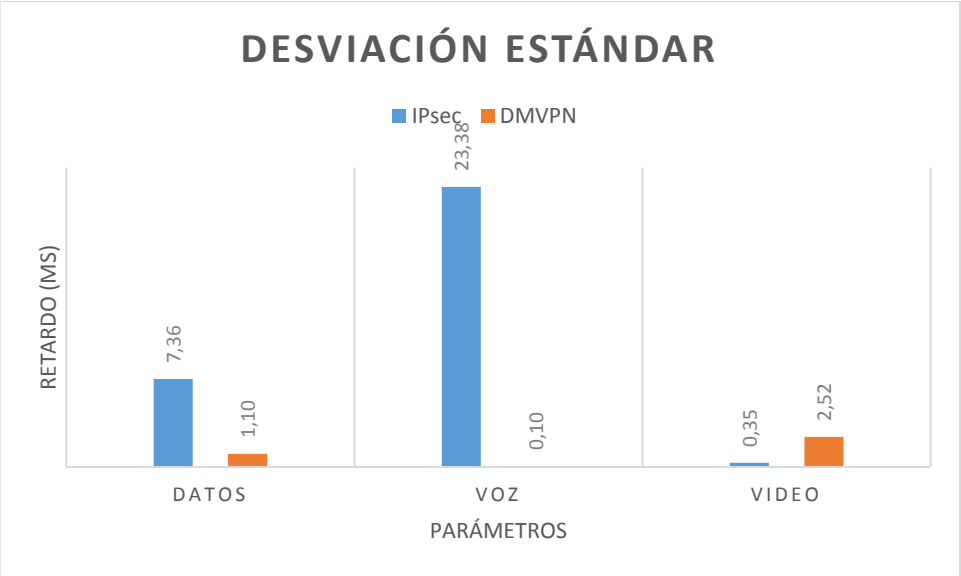

Figura 57-C: Desviación estándar del retardo para datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

D. TUNEL SPOKE 1 A SPOKE 4

Tabla 34-C: Promedio en ms del retardo para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

PROMEDIO	IPsec	DMVPN
Datos	45,93	4,02
Voz	24,94	2,04
Video	31,41	5,24

Realizado por: Alex Jaramillo

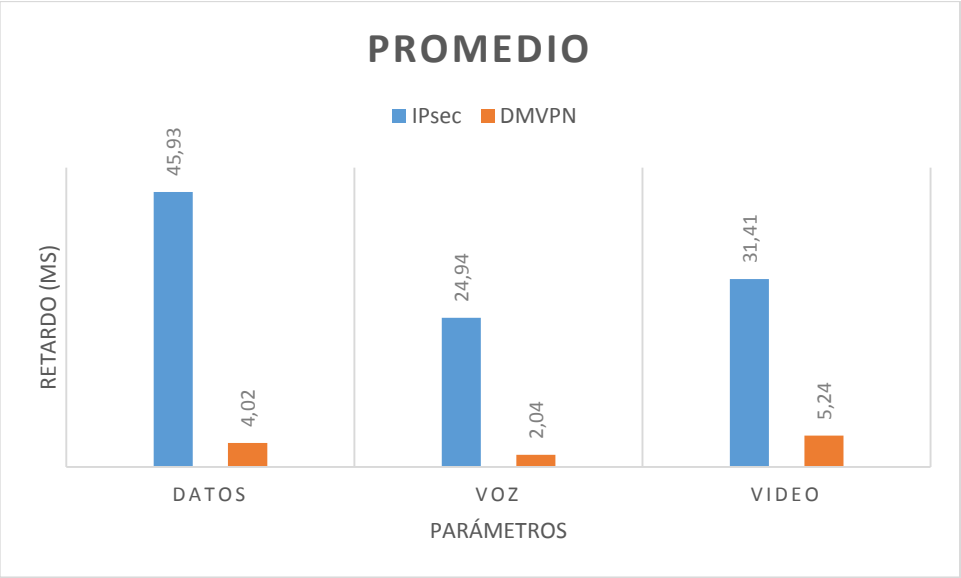

Figura 58-C: Promedio en ms del retardo para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

Tabla 35-C: Desviación estándar en ms del retardo para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

DESVIACIÓN ESTANDAR	IPsec	DMVPN
Datos	11,15	1,95
Voz	4,03	0,13
Video	4,55	3,34

Realizado por: Alex Jaramillo

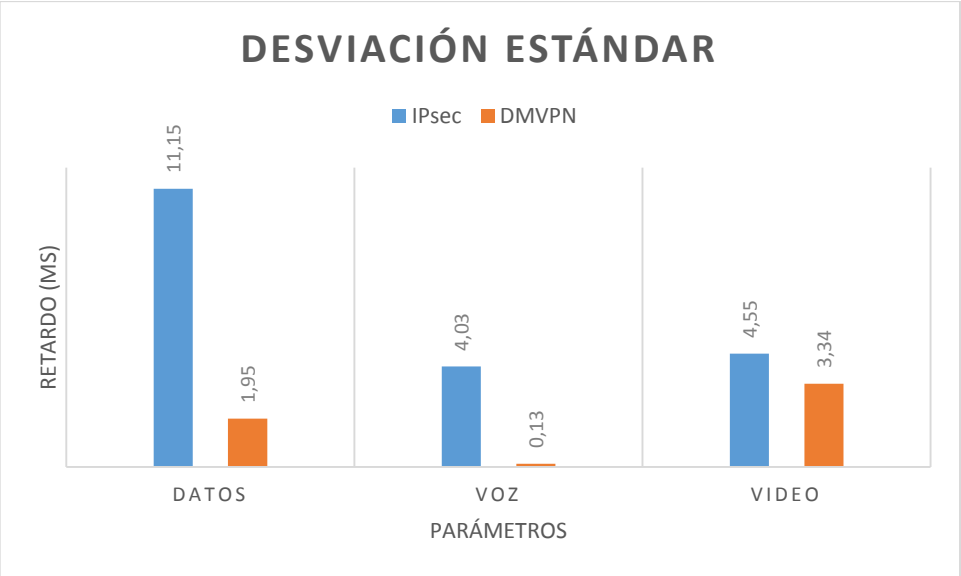

Figura 59-C: Desviación estándar en ms del retardo para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

2. JITTER

A. TUNEL HUB A SPOKE 1

Tabla 36-C: Promedio en ms del jitter para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

PROMEDIO	IPsec	DMVPN
Datos	0,91	0,86
Voz	0,66	0,63
Video	3,53	3,50

Realizado por: Alex Jaramillo

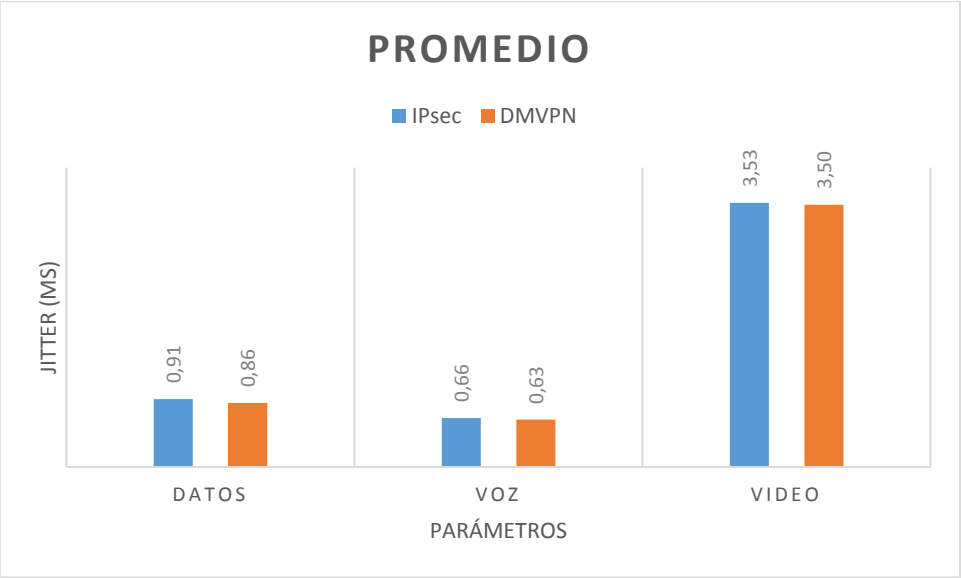

Figura 60-C: Promedio en ms del jitter para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

Tabla 37-C: Desviación estándar en ms del jitter para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

DESVIACIÓN ESTANDAR	IPsec	DMVPN
Datos	0,20	0,15
Voz	0,11	0,12
Video	0,57	0,45

Realizado por: Alex Jaramillo

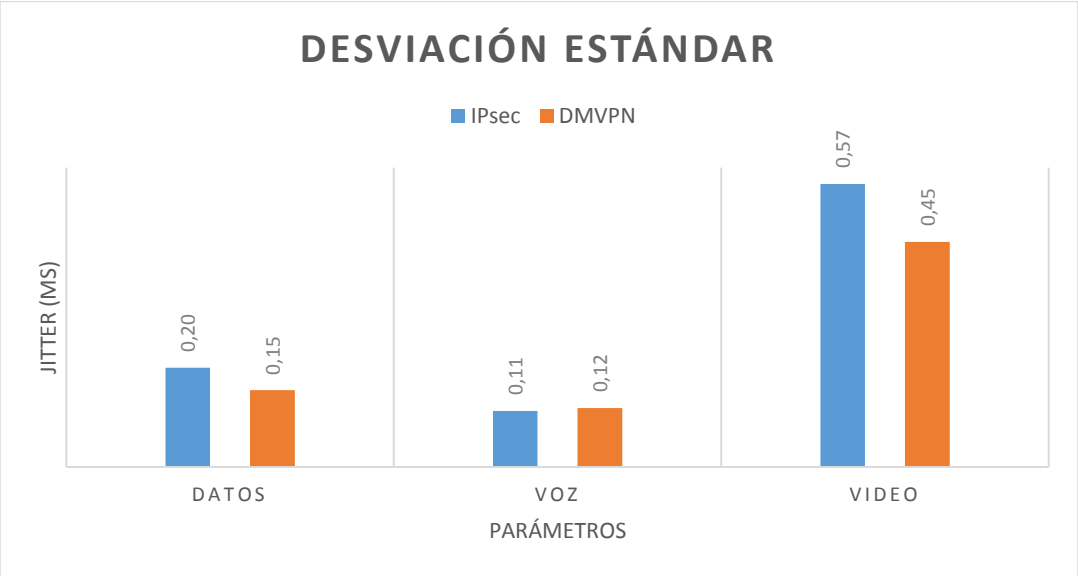

Figura 61-C: Desviación estándar en ms del jitter para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

B. TUNEL SPOKE 1 A SPOKE 2

Tabla 38-C: Promedio en ms del jitter para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

PROMEDIO	IPsec	DMVPN
Datos	1,02	0,59
Voz	1,02	0,65
Video	2,70	2,33

Realizado por: Alex Jaramillo

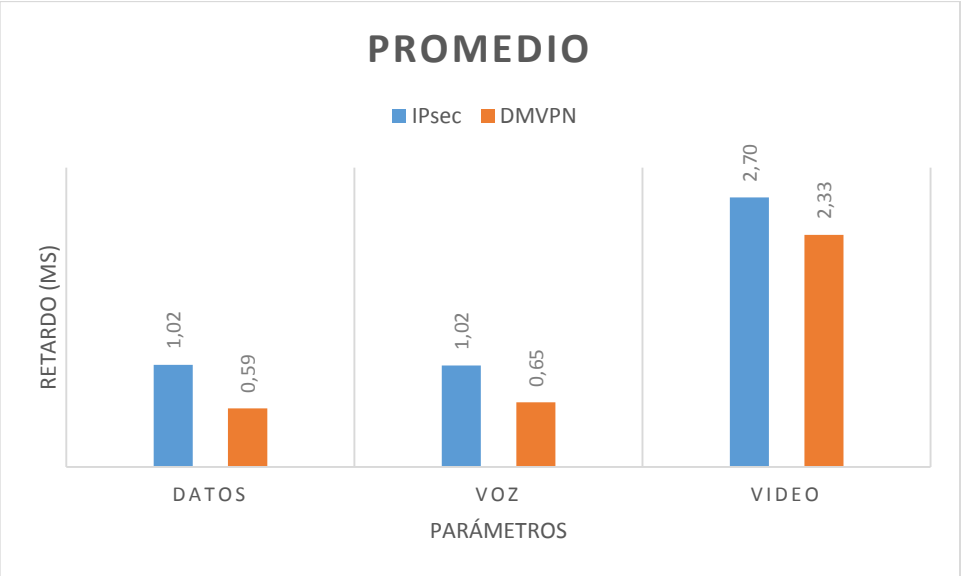

Figura 62-C: Promedio en ms del jitter para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

Tabla 39-C: Desviación estándar en ms del jitter para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

DESVIACIÓN ESTANDAR	IPsec	DMVPN
Datos	0,06	0,06
Voz	0,12	0,07
Video	1,52	0,61

Realizado por: Alex Jaramillo

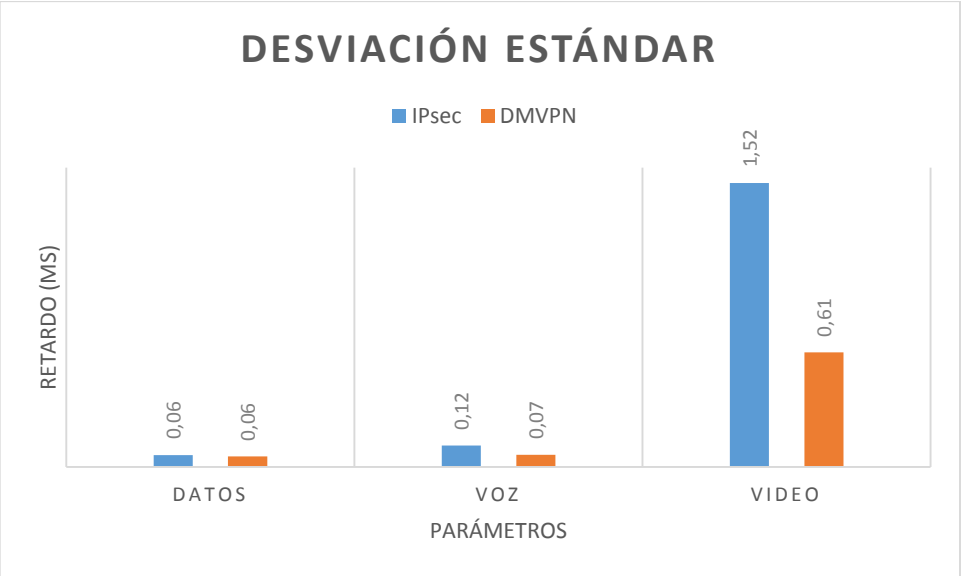

Figura 63-C: Desviación estándar en ms del jitter para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

C. TUNEL SPOKE 1 A SPOKE 3

Tabla 40-C: Promedio en ms del jitter para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

PROMEDIO	IPsec	DMVPN
Datos	2,98	0,62
Voz	1,10	0,27
Video	7,34	1,20

Realizado por: Alex Jaramillo

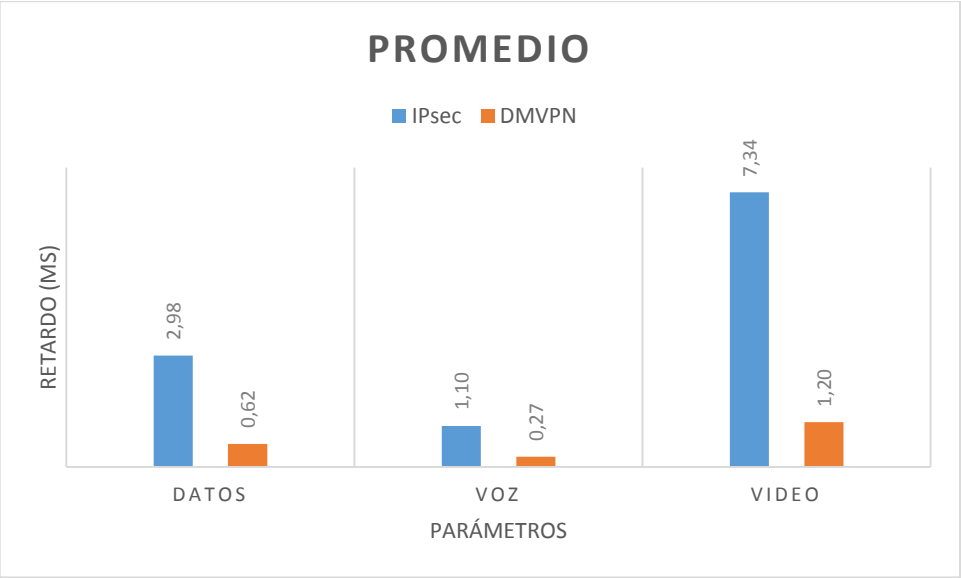

Figura 64-C: Promedio en ms del jitter para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

Tabla 41-C: Desviación estándar en ms del jitter para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

DESVIACIÓN ESTANDAR	IPsec	DMVPN
Datos	4,14	0,42
Voz	0,25	0,03
Video	0,30	0,39

Realizado por: Alex Jaramillo

Figura 65-C: Desviación estándar en ms del jitter para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

D. TUNEL SPOKE 1 A SPOKE 4

Tabla 42-C: Promedio en ms del jitter para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

PROMEDIO	IPsec	DMVPN
Datos	3,11	0,69
Voz	1,10	0,27
Video	1,88	1,15

Realizado por: Alex Jaramillo

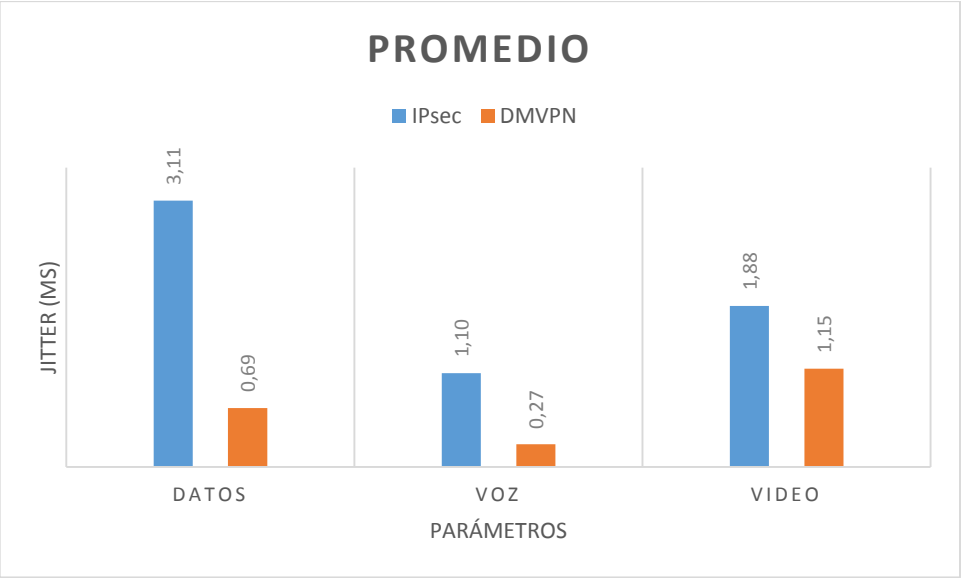

Figura 66-C: Promedio en ms del jitter para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

Tabla 43-C: Desviación estándar en ms del jitter para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

DESVIACIÓN ESTANDAR	IPsec	DMVPN
Datos	4,54	0,34
Voz	0,11	0,04
Video	0,35	0,43

Realizado por: Alex Jaramillo

Figura 67-C: Desviación estándar en ms del jitter para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

3. PAQUETES PERDIDOS

A. TUNEL HUB A SPOKE 1

Tabla 44-C: Promedio del porcentaje de paquetes perdidos para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

PROMEDIO	IPsec	DMVPN
Datos	0,13	0,11
Voz	0,05	0,00
Video	10,38	8,67

Realizado por: Alex Jaramillo

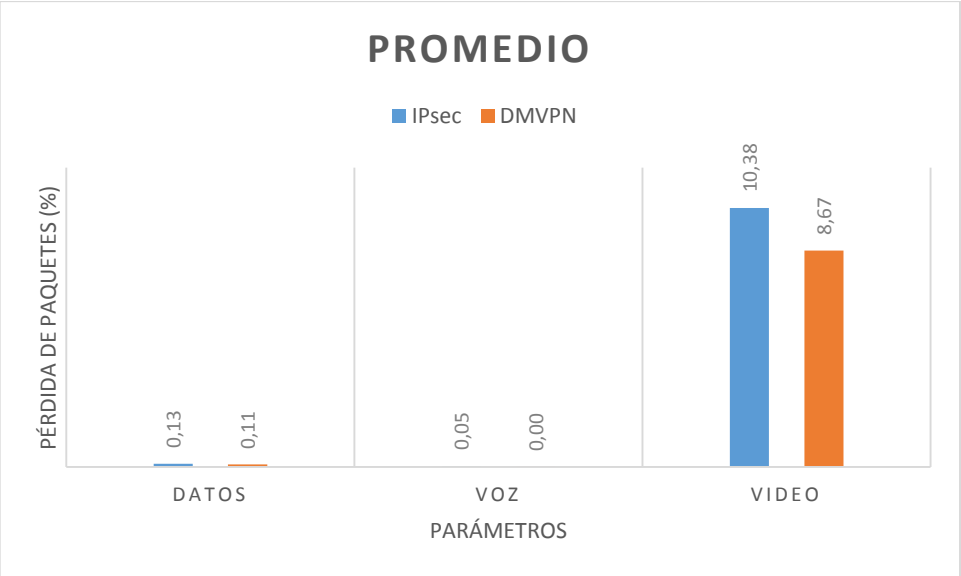

Figura 68-C: Promedio del porcentaje de paquetes perdidos para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

Tabla 45-C: Desviación estándar del porcentaje de paquetes perdidos para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

DESVIACIÓN ESTANDAR	IPsec	DMVPN
Datos	0,35	0,33
Voz	0,15	0,00
Video	1,24	2,25

Realizado por: Alex Jaramillo

Figura 69-C: Desviación estándar del porcentaje de paquetes perdidos para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

B. TUNEL SPOKE 1 A SPOKE 2

Tabla 46-C: Promedio del porcentaje de paquetes perdidos para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

PROMEDIO	IPsec	DMVPN
Datos	26,62	0,03
Voz	0,05	0,01
Video	7,42	3,39

Realizado por: Alex Jaramillo

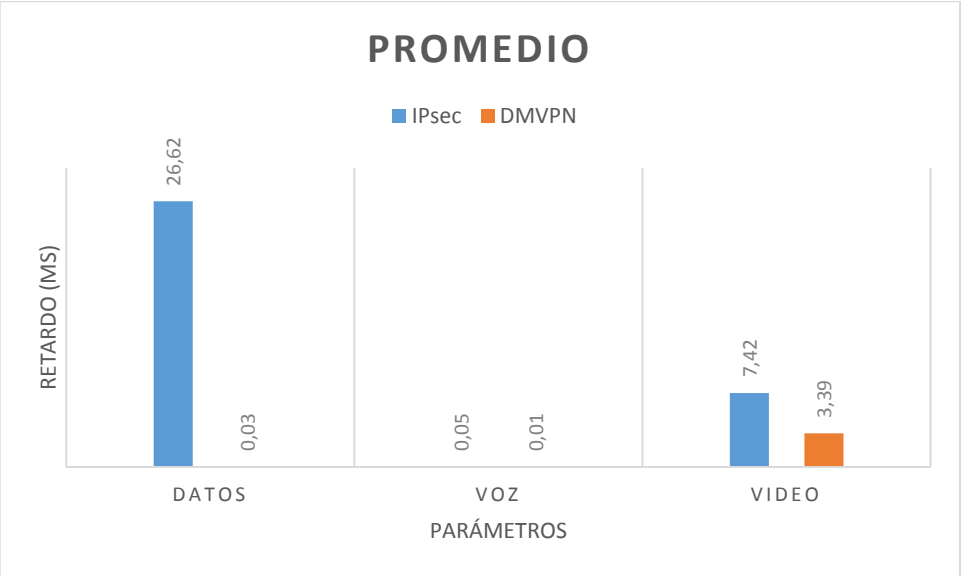

Figura 70-C: Promedio del porcentaje de paquetes perdidos para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

Tabla 47-C: Desviación estándar del porcentaje de paquetes perdidos para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

DESVIACIÓN ESTANDAR	IPsec	DMVPN
Datos	3,04	0,03
Voz	0,11	0,02
Video	2,35	2,85

Realizado por: Alex Jaramillo

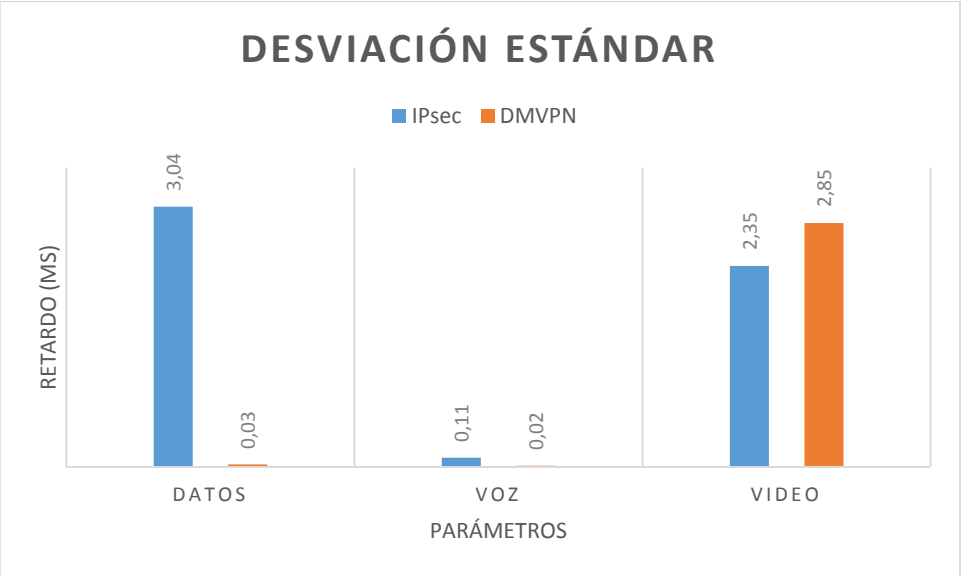

Figura 71-C: Desviación estándar del porcentaje de paquetes perdidos para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

C. TUNEL SPOKE 1 A SPOKE 3

Tabla 48-C: Promedio del porcentaje de paquetes perdidos para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

PROMEDIO	IPsec	DMVPN
Datos	7,29	0,03
Voz	0,02	0,00
Video	2,92	0,51

Realizado por: Alex Jaramillo

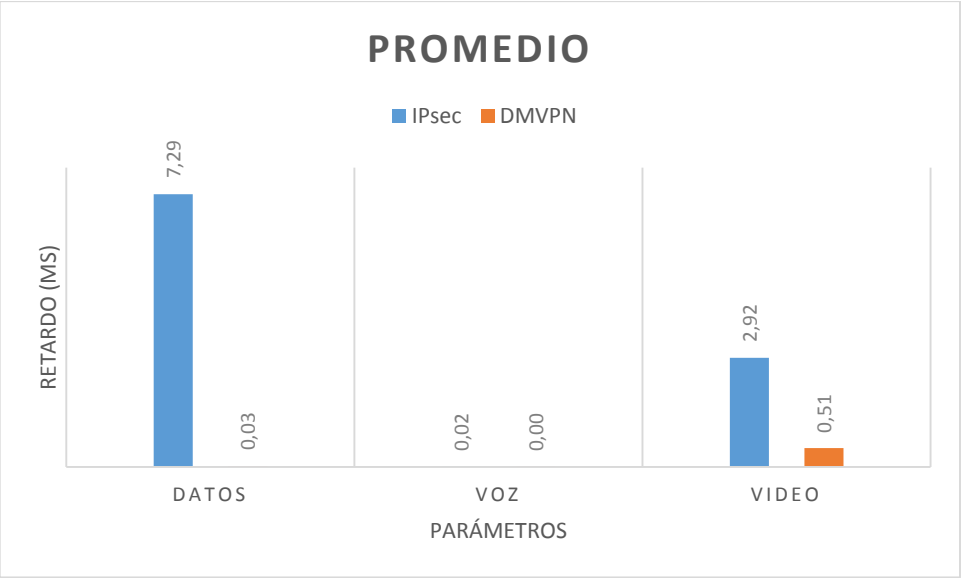

Figura 72-C: Promedio del porcentaje de paquetes perdidos para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

Tabla 49-C: Desviación estándar del porcentaje de paquetes perdidos para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

DESVIACIÓN ESTANDAR	IPsec	DMVPN
Datos	13,51	0,11
Voz	0,02	0,00
Video	2,92	0,39

Realizado por: Alex Jaramillo

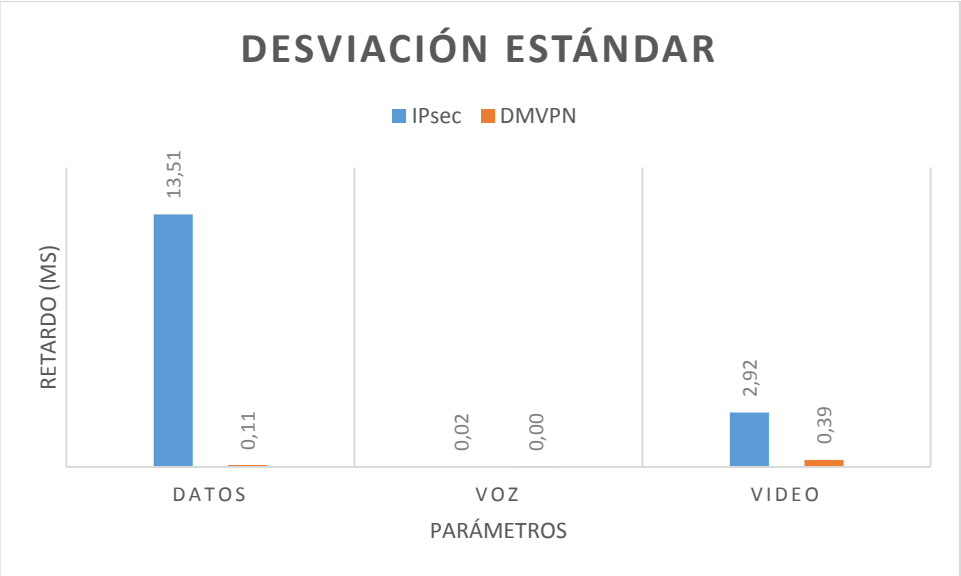

Figura 73-C: Desviación estándar del porcentaje de paquetes perdidos para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

D. TUNEL SPOKE 1 A SPOKE 4

Tabla 50-C: Promedio del porcentaje de paquetes perdidos para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

PROMEDIO	IPsec	DMVPN
Datos	8,83	0,05
Voz	0,02	0,00
Video	1,30	1,08

Realizado por: Alex Jaramillo

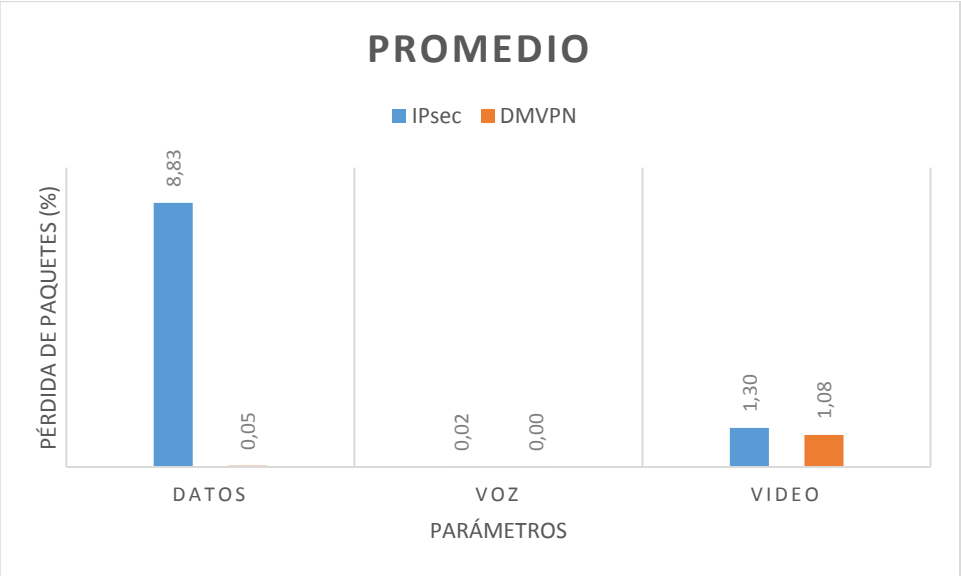

Figura 74-C: Promedio del porcentaje de paquetes perdidos para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo

Tabla 51-C: Desviación estándar del porcentaje de paquetes perdidos para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

DESVIACIÓN ESTANDAR	IPsec	DMVPN
Datos	17,55	0,16
Voz	0,11	0,00
Video	1,37	2,70

Realizado por: Alex Jaramillo

Figura 75-C: Desviación estándar del porcentaje de paquetes perdidos para los paquetes de datos, voz y video de los escenarios IPsec y DMVPN

Realizado por: Alex Jaramillo