UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN TELECOMUNICACIONES
MENCIÓN: GESTIÓN DE LAS TELECOMUNICACIONES

Resolución: RPC-SE-01-No.016-2020

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del trabajo:
Diseño y simulación de una red datos WAN Ethernet con túneles DMVPN y seguridad IPsec, para interconectar cinco localidades remotas de la Fuerza Aérea Ecuatoriana.
Línea de Investigación:
Telecomunicaciones y Sistemas Informáticos aplicados a la producción y a la sociedad
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autor/a:
Guzmán Flores Ángel Edison
Tutor/a:
MSc. Albarracín Guarochico Wilmer Fabian Ph.D. Parra Balza Fidel David

Quito – Ecuador

2021

APROBACIÓN DEL TUTOR

Yo, phD. Fidel David Parra Balza con C.I: 1757469950 en mi calidad de Tutor del trabajo de investigación titulado: Diseño y simulación de una red datos WAN Ethernet con túneles DMVPN y seguridad IPsec, para interconectar cinco localidades remotas de la Fuerza Aérea Ecuatoriana.

Elaborado por: Angel Edison Guzman Flores, de C.I: 1711866200, estudiante de la Maestría: en Telecomunicaciones, mención: Gestión de las Telecomunicaciones de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., 30 de septiembre de 2021

_____

Firma

APROBACIÓN DEL TUTOR

Yo, Mg. Wilmer Fabian Albarracín Guarochico con C.I: 1713341152 en mi calidad de Tutor del trabajo de investigación titulado: Diseño y simulación de una red datos WAN Ethernet con túneles DMVPN y seguridad IPsec, para interconectar cinco localidades remotas de la Fuerza Aérea Ecuatoriana.

Elaborado por: Angel Edison Guzman Flores, de C.I: 1711866200, estudiante de la Maestría: en Telecomunicaciones, mención: Gestión de las Telecomunicaciones de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., 30 de septiembre de 2021

_____

Firma

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

La Fuerza Aérea Ecuatoriana es una institución militar que opera a nivel nacional, entidad cuya misión entregada por el estado ecuatoriano, es la seguridad del espacio aéreo del país, la institución para el normal desarrollo de las actividades operativas, administrativas y logísticas cuenta con una infraestructura tecnológica de telecomunicaciones e informática, los diferentes sistemas y servicios de comunicaciones como bases de datos, portales de servicios FAE, correo electrónico institucional, comunicaciones unificadas, entre otros, los cuales se encuentran instalados en servidores virtualizados en la infraestructura de hiperconvergencia, alojados en el data center del sitio matriz y administrado por la Dirección de Tecnologías de la Información y Comunicaciones.

El presente proyecto contempla el diseño y simulación de una red WAN (*Wide Area Network*) para integrar cinco localidades de la Fuerza Aérea Ecuatoriana, con la implementación de túneles DMVPN y encriptación IPsec sobre la capa de conectividad del proveedor de servicios, basado en el uso de la tecnología Ethernet.

El proyecto tiene un enfoque orientado en el diseño de una infraestructura de red WAN, bien dimensionada en capacidad de ancho de banda de acuerdo a las necesidades institucionales, con seguridad en los enlaces y acceso al internet a través del sitio matriz, para lo cual se deberá contratar canales de datos de un proveedor de servicios privado, realizar la interconexión, configuración y pruebas a fin de garantizar el funcionamiento de la red con encriptación de los enlaces, esto debido a que la institución genera tráfico sensible y una posible desviación de la información puede atentar a la seguridad nacional.

Es importante en la actualidad el uso de la tecnología Ethernet para la interconexión de sucursales con grandes capacidades de tráfico, por lo tanto se debe aprovechar todo el desarrollo tecnológico que existe en la actualidad en el área de telecomunicaciones, la ejecución del proyecto es innovador ya que sobre la infraestructura del proveedor de servicios se implementará túneles DMVPN (*Dynamic Multipoint VPN*) con encriptación IPsec (*Internet Protocol security*), de esta manera mitigar al máximo el acceso no autorizado de la información institucional.

El presente proyecto de investigación se fundamenta en conceptos de Ethernet como una tecnología muy utilizada en la actualidad, para el transporte de información en las infraestructuras de las redes de datos, al permitir la ampliación de su utilidad, pasando de dominios LAN hacia entornos WAN beneficiando al usuario final, proveyendo un servicio de alta calidad con una tecnología de gran escalabilidad y capacidad (Avendaño, 2018).

Actualmente las infraestructuras de red LAN de cinco sitios remotos, se encuentran interconectados a través de la red WAN MPLS (*Multiprotocol Label Switching*) de Fuerzas Armadas como su proveedor de servicios, cuya capacidad de ancho de banda es relativamente baja (100 Mbps Quito – Guayaquil), considerando el incremento exponencial del desarrollo de nuevos sistemas y servicios de telecomunicaciones en la actualidad.

Al disponer de todos los servicios de telecomunicaciones de forma centralizada en el sitio matriz, el acceso a la información desde los sitios remotos se vuelve vital para el desarrollo de las actividades propias de la institución, regularmente las localidades remotas se quedan sin enlace por horas o días, debido a la falta de respuesta inmediata a la solución de los problemas de comunicaciones en la red WAN, por parte de la entidad responsable de la administración, soporte y mantenimiento de la infraestructura tecnológica que provee la conectividad a las diferentes localidades de la institución, lo cual complica y entorpece el normal desarrollo de las actividades institucionales.

Actualmente el servicio de internet se contrata de forma local en cada sitio remoto, lo cual encarece la contratación parcial del servicio y genera huecos de seguridad, debido a la interconexión de segmentos de red públicas en los equipos de networking de la institución y a la falta de equipamiento robusto de seguridad perimetral en cada lugar, y a esto se suma que no ha sido factible la adquisición de mencionados equipos por falta de asignación presupuestaria del estado, aquello hace que la infraestructura de red institucional sea vulnerable en cuanto a seguridad informática.

Por lo expuesto es importante diseñar un proyecto, que solucione los problemas planteados, una infraestructura de red bien dimensionada en capacidad, con alta seguridad, acorde a la tecnología actual y con un nivel de SLA (*service level agreement*) de 99,999 del proveedor de servicios, a fin de que se garantice la disponibilidad del servicio de conectividad a nivel nacional.

Pregunta Problémica

¿De qué manera se solucionará los continuos cortes en la conectividad, el acceso lento a los servicios y los huecos de seguridad que presenta la infraestructura de red actual de la Fuerza Aérea Ecuatoriana, con un diseño y dimensionamiento de red WAN con alta seguridad que integre las cinco localidades remotas?

Objetivo general

Desarrollar una red Ethernet a nivel WAN con túneles DMVPN y seguridad IPsec mediante simulación en un entorno controlado con la herramienta GNS3 para la Fuerza Aérea Ecuatoriana,

a través del *backbone* MPLS de un proveedor de servicios del país, para interconectar cinco sitios remotos con acceso al servicio de internet.

Objetivos específicos

- Contextualizar los fundamentos teóricos sobre las diferentes tecnologías actuales de Ethernet y protocolos de seguridad para el diseño y simulación del proyecto.
- Determinar las deficiencias en la conectividad a los diferentes servicios de comunicaciones que dispone la institución.
- Dimensionar la red Ethernet a nivel WAN que interconecte cinco localidades remotas.
- Simular la red en un ambiente controlado mediante el aplicativo GNS3 a fin de verificar su funcionamiento.
- Verificar el rendimiento de la red a través de indicadores claves de desempeño, como el *jitter*, retardo y paquetes perdidos, medidos en la red simulada según el diseño.

Beneficiarios directos:

Los beneficiarios directos con la ejecución de este proyecto, es todo el personal militar, servidores y trabajadores públicos que laboran en la institución, quienes podrán desarrollar sus actividades eficientemente al contar con una infraestructura de red que les permita acceder de forma ágil y segura a los diferentes servicios institucionales alojados en la matriz.

En el ámbito estratégico serán beneficiarios directos, las autoridades militares, quienes toman las decisiones en la conducción de las actividades operativas de la institución, con la finalidad de alcanzar los objetivos institucionales y el cumplimiento de la misión encomendada.

Como beneficiarios indirectos será toda la población civil del país, por cuanto si la institución armada se encuentra con una infraestructura de telecomunicaciones operativa y segura, la información estará disponible 24x7 para la toma de decisiones, en ese sentido la seguridad del espacio aéreo y el apoyo a la consecución de los objetivos nacionales estarán garantizados para la población.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización de fundamentos teóricos

El presente proyecto de investigación se fundamenta en las teorías y estudios realizados por un equipo de investigadores en el campo de las telecomunicaciones, en el área de redes de datos, específicamente en ambientes LAN, WAN y seguridad de la información, a fin de garantizar en todo momento la disponibilidad de la información, que sea verás y confiable.

Para el desarrollo del presente proyecto se utilizará la tecnología Ethernet como estándar para el despliegue de redes LAN y WAN, permitiendo revisar artículos científicos referentes a la tecnología Metro Ethernet donde: Guo (2010) menciona que, una red de área metropolitana (MAN) se puede construir utilizando tecnología de red de área amplia (WAN) o de área local (LAN), en ese sentido Ethernet es una tecnología que en la actualidad se ha desarrollado considerablemente, tanto que los grandes proveedores de servicio la utilizan como redes WAN, por lo tanto, se fundamenta el uso de la tecnología Ethernet como *backbone* a nivel WAN.

Así también para la ejecución del trabajo de investigación se utilizará protocolos de enrutamiento, como OSPF y EIGRP para el entorno de simulación y futura implementación en la institución, lo cual no contempla dentro del alcance de este trabajo, Ummi Fiade, Fathul & Amelia (2017) afirman que, existen protocolos de enrutamiento dinámico que se utilizan en una red WAN como OSPF, RIP, IS-IS y EIGRP, cada uno tiene sus ventajas y desventajas en el funcionamiento de una red.

Como fundamentación teórica en el desarrollo del trabajo en curso se usará el protocolo IPsec debido a que su aporte es importante en el tema de la seguridad de una comunicación de datos, el propósito de la seguridad de la red es proporcionar confidencialidad, integridad y autenticación, por lo que el protocolo de seguridad IPsec protege un tráfico muy sensible como la VoIP, videoconferencia, acceso a las bases de datos, entre otros. En el caso que el tráfico sea capturado de forma mal intencionada no podría ser desencriptado (Kolahi, Mudaliar, Zhang, & Gu, 2017).

En otro estudio científico que se fundamenta el desarrollo este trabajo de investigación, es el uso correcto de los túneles DMVPN con IPsec, en el cual se indica que una VPN tradicional no es escalable cuando el número de sucursales se incrementa, en ese sentido una solución a este problema es el uso de túneles DMVPN, lo cual ofrece una comunicación segura entre las sucursales de una compañía; la principal ventaja de la solución DMVPN consiste en la creación de enlaces privados entre sucursales sin pasar el tráfico por la matriz, es muy importante el uso del mencionado protocolo porque dentro de la red DMVPN permite ejecutar protocolos de

enrutamiento como OSPF y EIGRP (Angelescu, Puchianu, Preduscac, Circiumarescu, & Movila, 2017).

Como trabajos previos que guardan relación con el presente proyecto de investigación, luego de realizar una revisión bibliográfica se encontraron algunos estudios.

Un artículo donde se diseñó e implementó una red MPLS sobre GRE para una red de un *service provider (ISP)* usando un simulador GNS3, este artículo guarda relación con este trabajo ya que para la implementación de la red propuesta, se utilizará el software GNS3 y además también se simulará la infraestructura de red de un proveedor de servicios local para la capa de conectividad (*underlay)*, considerando que el aporte de este artículo permite establecer la factibilidad de la simulación de redes complejas como MPLS sobre túneles GRE en una herramienta muy potente como GNS3 (Tamanna & Fatema, 2017).

De la misma manera en el proceso investigativo para el desarrollo del presente trabajo se encontró un proyecto donde se implementó canales de datos utilizando MPLS con VRF (*virtual routing forwarding*), en el cual se describe que las aplicaciones útiles de MPLS son las redes privadas virtuales (VPN), que proporciona túneles de capa 2 y 3, en el que el proveedor de servicios garantiza el transporte del tráfico de forma privada y segura. En este artículo también se describe como se implementa un canal MPLS VPN usando VRF, se explica la configuración y la función de los *routers* CE (*customer edge*), PE (*provider edge*) y P(*provider*) (Mehraban, Samiullah, Komil, & Upadhyay, 2018), este estudio aporta en gran medida al proyecto, debido a que para la interconexión de las localidades remotas se hará uso de canales de datos de un proveedor local, el cual utiliza la tecnología MPLS para la entrega de los enlaces de conexión a los sitios.

Sobre el uso de los túneles DMVPN se encontró un estudio donde se realiza la evaluación del performance de DMVPN usando los protocolos de enrutamiento RIP, OSPF y EIGRP, los parámetros utilizados para este estudio fueron el *throughput, jitter* y *packet loss*, se demostró que RIP es mejor en cuanto a la tasa de rendimiento en fase 2 de DMVPN y en fase 3 tiene el más alto porcentaje de paquetes perdidos, EIGRP en DMPVN fase 2 tiene el valor más bajo en *jitter*, muchas empresas y compañías en la actualidad utilizan DMVPN para comunicarse de modo seguro sobre el internet (Siti, Khairul, Andrew, & Ristanti, 2018), este trabajo tiene un aporte significativo en el desarrollo de la simulación, por cuanto se utilizará los protocolos OSPF y EIGRP para enrutar el tráfico a través de los túneles DMVPN.

Durante la revisión bibliográfica de trabajos relacionados con el proyecto en curso se encontró un estudio comparativo entre túneles VPN con IPsec y DMVPN, con la finalidad de mejorar el rendimiento de redes privadas sobre internet, en el cual se concluye que DMVPN ofrece el mejor rendimiento en todo tipo de tráfico a través de los túneles dinámicos, VPN con

IPsec no es escalable, porque para agregar nuevos *SPOKE (sucursales)* se debe establecer una configuración adicional del peer, mientras que DMVPN es muy escalable, porque al agregar un nuevo *SPOKE* no es necesario agregar alguna configuración adicional en el *HUB,* por otro lado dentro de las evaluaciones técnicas de los dos protocolos, se resalta que DMVPN siempre tuvo los mejores valores en *jitter,* retardo y una tasa de paquetes perdidos frente a VPN con IPsec. Este estudio aporta significativamente al desarrollo de este trabajo ya que existe un análisis previo en el rendimiento del protocolo DMVPN para interconectar los sitios remotos (Jaramillo, 2018).

Finalmente, dentro de los trabajos previos realizados que guardan relación con el presente proyecto de titulación, se encontró el estudio de evaluación de la tecnología MPLS con la aplicación VPN, con el objetivo de mejorar el rendimiento de la red de datos de la Corporación Nacional de Electricidad Regional de Bolívar, en el cual el autor una vez realizada la simulación de la red en el software GNS3, concluye que el uso de MPLS con aplicación VPN permite mejorar el rendimiento en términos de *jitter* y latencia, en comparación con las VPN tradicionales basadas en IP, como se puede visualizar este trabajo presenta un gran aporte al desarrollo del proyecto de investigación, considerando que en la propuesta se utilizará la herramienta GNS3 (Usca, 2018).

1.2. Problema a resolver

Las unidades militares de Fuerzas Armadas para su funcionamiento y ejecución de las actividades operativas, administrativas y logísticas de cada institución, cuentan con sus propias infraestructuras de comunicaciones, las cuales se encuentran interconectadas por la red WAN del Comando Conjunto de las Fuerzas Armadas.

Actualmente los repartos militares de la Fuerza Aérea Ecuatoriana, se encuentran conectados entre sitios y hacia la matriz (Comandancia General FAE) a través de la red WAN de Fuerzas Armadas, con una capacidad de ancho de banda limitado, debido a que es una infraestructura muy antigua y a esto se suma que no ha existido acuerdos de nivel de servicio SLA y a menudo algunos repartos militares se quedan sin conexión a la WAN, dicha novedad es solucionado después de varias horas o incluso tarda días, por lo que es un verdadero problema para la institución quedarse sin enlace hacia la oficina matriz y por ende sin servicios de telecomunicaciones, afectando de esta manera al desarrollo normal de las actividades institucionales.

El servicio de internet en los repartos militares se encuentra provisto por un ISP de forma local en las ciudades donde están ubicadas, al ejecutar contratos en cada reparto de forma independiente, no se optimizan los valores económicos que se cancelan a los proveedores y

además el hecho de contratar mencionado servicio en cada localidad con direcciones IP públicas configuradas en los equipos de *networking* de la institución sin la protección de dispositivos de seguridad perimetral, lo que ocasiona que exista una potencial amenaza a la seguridad de la información, además aquello representa que la infraestructura tecnológica sea muy vulnerable a posibles ataques a los diferentes sistemas y servicios institucionales.

De no plantear y ejecutar algún proyecto para solventar las novedades expuestas, a corto plazo la institución podría ser blanco de los ciberdelincuentes, la información no estaría disponible 24x7, lo cual provocaría un verdadero problema al no poder tomar las decisiones de forma oportuna, y posiblemente atentar contra la seguridad nacional, considerando que la infraestructura tecnológica no estaría cumpliendo con las características básicas de la seguridad de la información como son la disponibilidad, integridad, confidencialidad y autenticación; el uso de recursos económicos por el servicio de internet continuaría siendo elevado con los contratos parciales en cada sitio, lo cual reflejaría una mala gestión del presupuesto asignado por el estado ecuatoriano.

Por lo expuesto se considera de vital importancia desarrollar un proyecto de telecomunicaciones, en el que se desarrolle y simule el funcionamiento de una red WAN que interconecte cinco unidades militares con un alto performance en la calidad del enlace, contratando canales de datos a un proveedor de servicios local y con acuerdos SLA donde se garantice la confiablidad del servicio, además la contratación de internet será solo en el sitio matriz desde el cual se distribuirá a los cinco repartos militares, finalmente para mitigar las amenazas de seguridad de la información en la institución militar, es necesario, sobre los canales de datos contratado levantar túneles DMVPN con IPsec, de esta manera las comunicaciones serán seguras y confiables.

1.3. Proceso de investigación

1.3.1. Metodología de la investigación

El proceso de investigación en el presente proyecto se desarrolló con un enfoque cuantitativo de carácter experimental, en vista que se estudió hechos de realidad objetiva, recopilando información de los problemas de la red actual y la percepción del usuario durante las actividades del día a día, además en la propuesta se desarrollará un diseño experimental que será simulado en la plataforma GNS3, lo cual permitirá verificar su rendimiento; según Hernandez, Fernandez, & Baptista (2014) mencionan que, “El enfoque cuantitativo utiliza la recolección de datos para probar hipótesis con base a la medición numérica y el análisis estadístico, con el fin de establecer pautas de comportamiento y probar teorías” (p.37).

1.3.2. Población, unidades de estudio y muestra

El levantamiento de información se lo realizó utilizando las técnicas e instrumentos de la investigación, en el presente proyecto se consideró una población de 45 personas, conformadas por el personal técnico, ingenieros y jefes de los departamentos TIC que laboran en las cinco localidades (Quito, Latacunga, Guayaquil, Salinas y Manta) a los cuales se aplicará el instrumento de investigación.

Para las unidades de estudio se consideró a las autoridades, jefes y personal técnico de las localidades involucradas en el proyecto

Considerando que se dispone de una población pequeña y aplicando la fórmula para calcular la muestra finita se tiene como resultado 43 personas, por lo que se tomó como muestra a toda la población (45 personas) donde intervino el personal técnico, ingenieros y jefes de los departamentos TIC de los sitios, el personal involucrado en el proceso de investigación tiene el conocimiento de la información que se detalla:

- El personal técnico, ingenieros y jefes de los departamentos TIC conocen los diferentes problemas que existen en la infraestructura de telecomunicaciones de cada localidad.
- Disponen del conocimiento del equipamiento de red que existe en el reparto
- Son los encargados de la administración de la infraestructura tecnológica de comunicaciones
- Disponen de la información sobre la capacidad de internet contratado de forma local
- Conocen la frecuencia con que se accede a los servicios institucionales
- Dan solución a los diferentes problemas de conectividad y acceso a los servicios

1.3.3. Indicadores a diagnosticar

- Corte del servicio de conectividad del proveedor hacia la intranet institucional
- Existe equipamiento de seguridad perimetral con licenciamiento actualizado
- Ancho de banda del proveedor de conectividad hacia la WAN
- Seguridad en los canales de datos
- Acceso a los servicios institucionales

1.3.4. Métodos y técnicas

Los métodos, técnicas e instrumentos utilizados para la recolección y análisis de los datos, fue la encuesta y el cuestionario, herramientas que permiten obtener la información para el análisis y tabulación de resultados.

Tabla 1

Métodos y técnicas

Técnica	A quién se aplica	Objetivo	Indicadores
Encuesta	Personal técnico, profesionales y jefes de TIC de los repartos militares	Obtener información sobre los problemas que existen con la conectividad hacia el sitio matriz.	- La conectividad hacia el sitio matriz es estable - El reparto militar dispone de un equipo o sistema de seguridad perimetral con licenciamiento actualizado - El ancho de banda asignado en el canal de datos soporta el tráfico normal del reparto - El proveedor garantiza la seguridad en las comunicaciones - Con que frecuencia se utiliza los servicios de telecomunicaciones institucionales.

Fuente: Elaboración propia

1.4. Vinculación con la sociedad

Con el desarrollo de este proyecto se estima que existirá un gran aporte al personal que labora en la institución, por ende a sus familias, por cuanto sus actividades no se verán interrumpidas por falta de la conectividad, además al disponer de canales de datos en la WAN con buenas capacidades de ancho de banda y con una disponibilidad del 99.99, se podrá establecer entrenamientos técnicos, logísticos y administrativos de forma virtual a través de videoconferencia, uso de plataforma EVA (Entorno virtual de aprendizaje), acceso a la educación superior online, es decir el recurso humano de la institución notará un cambio en el acceso a la información.

Este proyecto servirá como fuente de consulta para los futuros profesionales en el ámbito de investigación en el campo tecnológico enfocado a las telecomunicaciones, específicamente en las redes de datos con seguridad para una organización que tiene oficinas y talento humano desplazado a nivel nacional.

1.5. Indicadores de resultados

Como indicadores que evalúen el producto final se dispondrá lo siguiente:

- Frente a trabajos similares el presente proyecto agrega sobre una plataforma de conectividad de un proveedor de servicios la configuración y habilitación de una capa de seguridad como es los túneles DMVPN con encriptación IPsec.
- Este proyecto solucionará los problemas de conectividad que existe en la actualidad hacia la oficina matriz.
- El aprendizaje que deja este proyecto, en cuanto al conocimiento adquirido en el análisis de la tecnología actual para enlazar sucursales, y los modelos de seguridad cuando se utiliza infraestructura de terceros.
- Plataforma GNS3 la cual permitirá verificar el correcto funcionamiento de la red, implementado en su totalidad en cuanto al alcance del proyecto
- La implementación de este proyecto en la Fuerza Aérea, no tendría costo en cuanto al diseño, configuración y habilitación de la seguridad sobre los canales de datos contratados al proveedor de servicios.

CAPÍTULO II: PROPUESTA

2.1. Fundamentos teóricos aplicados

La propuesta de investigación consiste en el diseño y simulación de una red datos WAN Ethernet con túneles DMVPN y seguridad IPsec, para interconectar cinco localidades remotas de la Fuerza Aérea Ecuatoriana, con acceso a los servicios internos de la institución y la salida de internet a través de la oficina matriz, haciendo uso de canales de datos contratado a un proveedor de servicios local.

En la fundamentación teórica de este trabajo, se abordará las teorías y conceptualizaciones de las principales tecnologías y protocolos que se utilizará en la ejecución de la propuesta, a continuación, se desarrolla las bases teóricas donde se sustenta la investigación en curso.

2.1.1. Red de área local (LAN)

Son infraestructuras tecnológicas que cubren espacios geográficos pequeños, funcionan en un edificio, una empresa u oficina. Este tipo de redes son usadas ampliamente para interconectar dispositivos informáticos fijos o móviles, con el propósito de compartir recursos e intercambiar información, tal como se muestra en el diagrama de red de la figura 1, la capacidad en la transmisión y recepción de información en un ambiente LAN es alta comparado a los enlaces WAN (Tanenbaum & Wetherall, 2012).

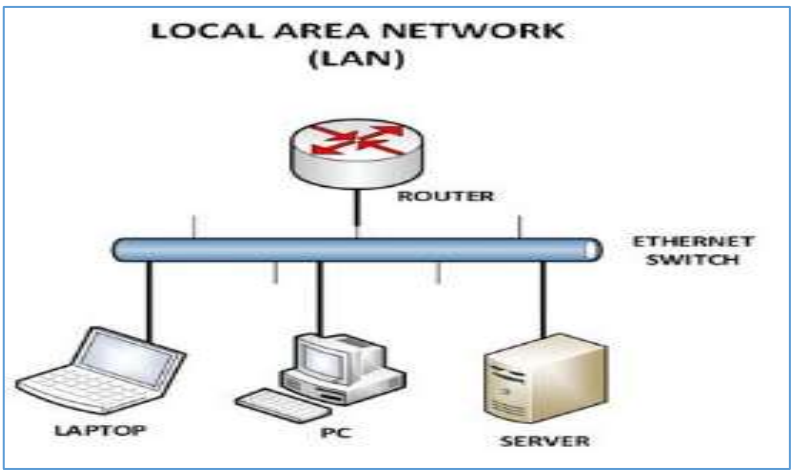

Figura 1. Red LAN (Clark, 2021)

2.1.2. Red de área amplia (WAN)

Una red WAN, es una infraestructura que abarca un área geográfica extensa, por lo general un país, continente o el mundo entero, esta conceptualización técnica se aplica en la presente propuesta donde se interconecta cinco localidades remotas de nuestro país, por lo general, una red WAN no es propiedad privada ni administrada por una sola organización, por lo que en una

infraestructura de este tipo no existe un control sobre la seguridad de información, para esto el usuario final debe emplear tecnologías y protocolos de seguridad como la implementación de VPN y IPsec (Tanenbaum & Wetherall, 2012).

Las capacidades de ancho de banda en la WAN, por lo general suelen ser menores a una LAN, van a depender siempre de los proveedores de servicio. En la figura 2 se muestra una representación gráfica de una red WAN.

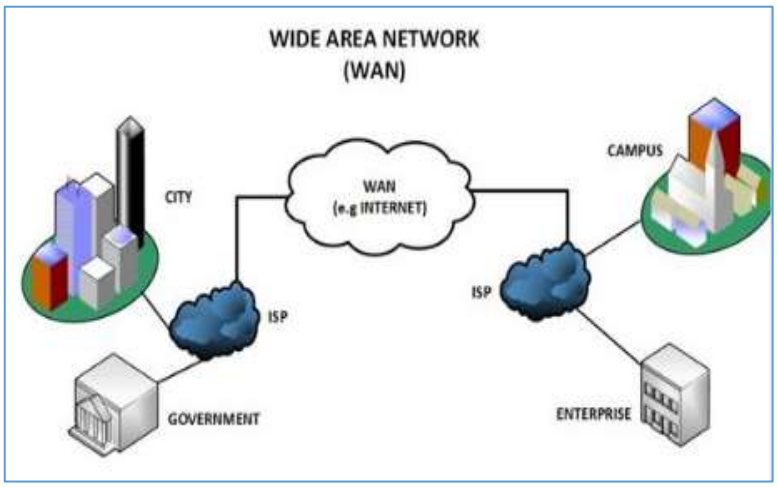

Figura 2. Red WAN (Clark, 2021)

2.1.3. Ethernet

Ethernet es un estándar para redes de datos (IEEE 802.3), cuyo inicio se dio por el año 1983, surgió para interconectar dispositivos en una red LAN o WAN por cable, lo que permite comunicarse entre sí a través de un protocolo, en la actualidad Ethernet es muy utilizado en las infraestructuras de red, desde hogares, oficinas pequeñas hasta las grandes corporaciones, Ethernet se utiliza por su alta velocidad, seguridad y fiabilidad, Ethernet pueden soportar tráficos de red hasta 400Gbps (Burke, Alissa, & Chai, 2021)

2.1.4. MPLS

MPLS es una tecnología de conmutación de etiquetas multiprotocolo, estándar desarrollado por la IETF *(Internet Engineering Task Force)* con el objetivo de solucionar los problemas que existen en el reenvió de paquetes de IP tradicional, este protocolo trabaja entre la capa dos y tres del modelo OSI, el dominio MPLS permite habilitar enlaces VPN de capa II y III para el usuario final, al ser multiprotocolo permite transportar diferentes tipos de tráficos (Huidobro & Millan, 2002).

En la figura 3, se muestra la estructura básica de una red MPLS, donde los principales elementos que intervienen son los *routers* LSR (*label switching routers*) que se encuentran internamente en el dominio MPLS y su función principal es la conmutación de etiquetas, y en el

borde de la red están los routers LER (*label Edge router*), cuya función es conmutar el tráfico de la red IP hacia el dominio MPLS y viceversa (Huawei, 2019).

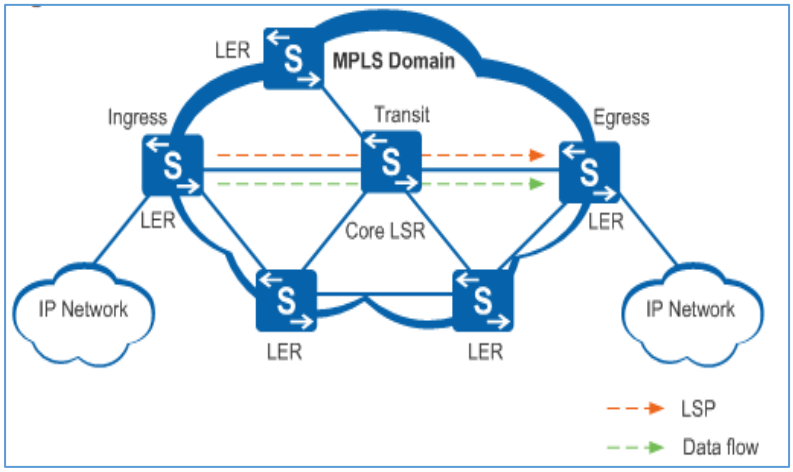

Figura 3. Estructura red MPLS (Huawei, 2019)

2.1.5. Protocolos de enrutamiento dinámico

Los protocolos de enrutamiento dinámico se encuentran estandarizados por la IEEE *(Institute of Electrical and Electronics Engineers),* se utilizan para el intercambio de información de rutas entre los *routers* en una infraestructura red, permiten a los ruteadores compartir información entre vecinos de forma dinámica sobre redes remotas y agregar esta información automáticamente en sus propias tablas de enrutamiento.

Entre las funciones principales que tienen los protocolos, es determinar la mejor ruta para el reenvió del tráfico destinado para otro equipo, en la figura 4 se muestra la clasificación de los protocolos de enrutamiento (Cisco, 2021).

	Protocolos de gateway interior			Protocolos de gateway exterior
	Protocolos de enrutamiento vector distancia	Protocolos de enrutamiento de link-state		Vector ruta
Con clase	RIP	IGRP		EGP
Sin clase	RIPv2	EIGRP	OSPFv2	IS-IS	BGPv4
IPv6	RIPng	EIGRP para IPv6	OSPFv3	IS-IS para IPv6	BGPv4 para IPv6

Figura 4. Clasificación de los protocolos de enrutamiento dinámico (Cisco, 2021)

OSPF

OSPF (*Open Shortest Path First*), es un protocolo de enrutamiento dinámico de estado de enlace, tal como se describe en la clasificación de protocolos en la Figura 4, fue creado para reemplazar al protocolo RIP, en vista que RIP no escalaba bien para redes más grandes, OSPF es muy robusto, ya que converge rápidamente y escala a redes grandes.

Es un protocolo sin clase, lo que permite la publicación de segmentos de red con mascara de longitud variable, para su funcionamiento utiliza el concepto de áreas para realizar la convergencia de la red, puede trabajar en una sola área o múltiples áreas dependiendo del tamaño de la red. En la figura 5 se muestran las características principales del protocolo de enrutamiento dinámico OSPF.

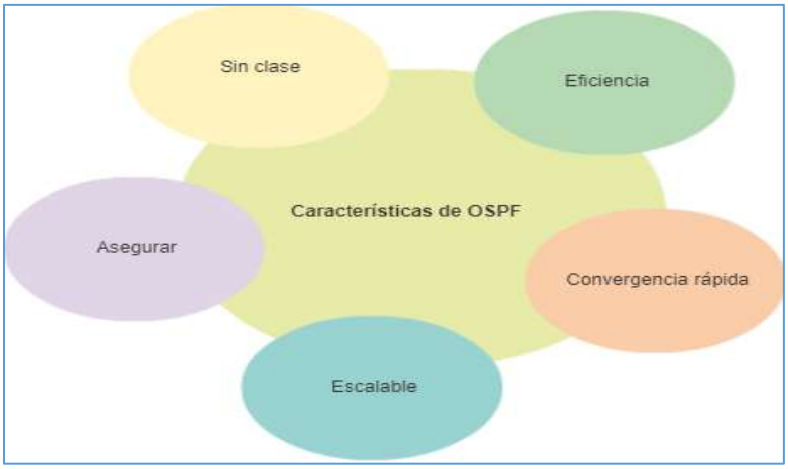

Figura 5. Características de OSPF (ITESA, s.f.)

EIGRP

EIGRP (*Enhanced Interior Gateway Routing Protocol),* es un protocolo de enrutamiento dinámico vector distancia muy utilizado en la actualidad, se desarrolló para reemplazar IGRP con mejoras en el algoritmo, estas mejoras tienen que ver con la rápida convergencia y su eficiencia operativa en redes de gran tamaño, aquello lo convierte en uno de los mejores protocolos.

EIGRP es fácil de configurar, los routers mantienen actualizada la información de las tablas de rutas y topología, con la finalidad de reaccionar ante cambios de la red, esta información se guarda en varias tablas y bases de datos (Cisco, 2005).

2.1.6. VPN

Una VPN (*virtual private network*) son redes seguras desplegadas sobre el internet, con técnicas y uso de protocolos de seguridad para levantar comunicaciones desde un lugar remoto hacia una infraestructura de red interna de una organización.

A través de la tecnología de VPN, se puede establecer conectividad con servidores que estén alojadas en la red interna de la empresa, ya que el tráfico que viaja de extremo a extremo es totalmente cifrado.

Existe diferentes aplicaciones para el uso de VPN, en la actualidad ha sido muy común el uso en teletrabajo para acceder a los recursos corporativos de la empresa desde los hogares, hoteles, etc. Otra aplicación es la conectividad de sucursales con la oficina matriz a través de proveedores de servicios con canales de datos o a través de internet, en la figura 6 se muestra una aplicación muy utilizada y la que se usará en la propuesta (Goujon, 2012).

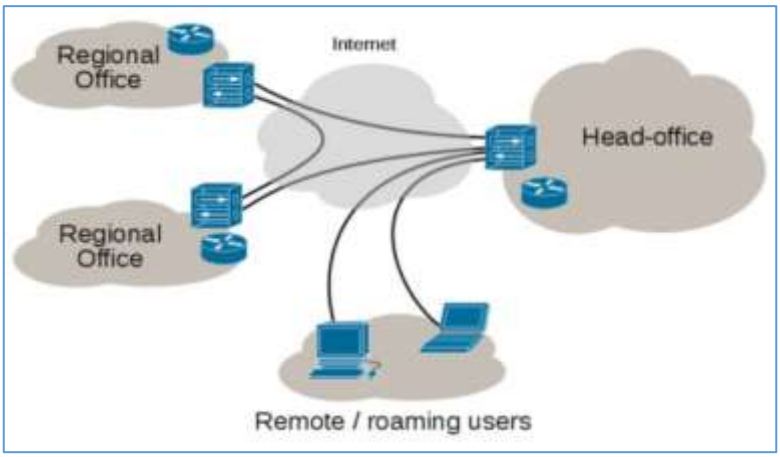

Figura 6. Uso de las conexiones VPN (Moreno, 2021)

2.1.7. DMVPN

DMVPN *(Dynamic Multipoint Virtual Private Network)* son túneles dinámicos que conectan un sitio matriz con todos los sitios remotos de forma dinámica, de esta manera un nodo puede levantar un túnel dinámico con otro nodo sin pasar el tráfico por el nodo central o Hub, para lo cual se utiliza el protocolo NHRP (*Next Hop Resolution Protocol*) el cual permite de forma dinámica que un router *Next Hop Client* (NHC) se registre en el router Next Hop Server (NHS), en el diseño de una red privada virtual multipunto dinámica, NHC es el router SPOKE y el NHS es el router HUB.

El uso de DMVPN en una red permite agregar fácilmente nuevos routers SPOKE sin modificar la configuración del router HUB, la configuración admite dos fases:

- Fase 1 permite levantar túneles HUB con SPOKE
- Fase 2 agrega la capacidad de levantar túneles SPOKE a SPOKE

DMVPN es un protocolo de CISCO para crear VPN seguras tipo punto multipunto, que se establecen en forma dinámica al momento que se requiere el envió de información, en la figura 7 se muestra la topología de túneles DMPVN de Cisco (Urra, 2019).

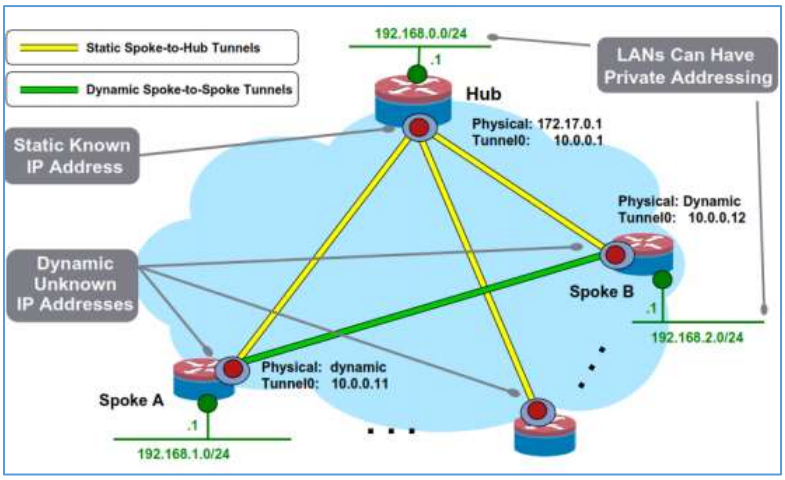

Figura 7. Topologías DMVPN (Cisco, 2005)

2.1.8. IPsec

IPsec es un protocolo de seguridad muy importante para proteger toda la información que circula a través de una red, trabaja en la capa de red del modelo de referencia OSI.

Cabe destacar que IPsec es protocolo que brinda seguridad a la capa IP, una de las funcionalidades de IPsec es la encriptación lo cual garantiza una comunicación segura entre diferentes puntos a través de Internet, IPsec se adapta perfectamente a las necesidades de VPN.

IPsec es un protocolo robusto para la seguridad de los datos, cumple con los cuatro pilares básicos de seguridad de la información como autenticación, confidencialidad, integridad y no repudio, IPsec es un estándar de seguridad para las redes de datos, en la actualidad IPsec es un componente básico en seguridad (De Luz, 2021).

2.2. Descripción de la propuesta

Luego de haber realizado la investigación y determinar que existe problemas en el acceso a los diferentes servicios de la institución, donde se justifica el diseño y ejecución de un proyecto de telecomunicaciones que resuelva las novedades expuestas a lo largo de este trabajo, en ese sentido la propuesta planteada es el “Diseño y simulación de una red datos WAN Ethernet con túneles DMVPN y seguridad IPsec, para interconectar cinco localidades remotas de la Fuerza Aérea Ecuatoriana, a través de canales de datos contratados a un proveedor de servicios local con acceso a los servicios internos de la institución y la salida de internet a través de la oficina matriz.

Se ha determinado el uso de la tecnología Ethernet para el despliegue de la red WAN en el presente proyecto, haciendo uso de la infraestructura tecnológica de telecomunicaciones de un proveedor de servicios, por su gran desarrollo que ha tenido, sus prestaciones están vigentes y sus proyecciones a futuro son grandes en términos de capacidad de ancho de banda y mínima

latencia que presenta al utilizar como medio de transmisión la fibra óptica, la cual en la actualidad es muy común en la última milla.

Con la propuesta planteada se resuelve los problemas que existe actualmente, como son los continuos cortes de servicio en la conectividad de la WAN de los repartos militares de la Fuerza Aérea, se soluciona también los problemas de ancho de banda que existe en los enlaces al sitio matriz (Quito), al contratar el servicio de internet en el sitio matriz y distribuir a los repartos a través de los canales contratados, se resuelve las potenciales amenazas de seguridad que existe al contratar el servicio en los sitios de forma local, además el presente proyecto como valor agregado garantiza la seguridad en el tráfico de la información al utilizar túneles DMVPN con encriptación IPsec.

a. Estructura general

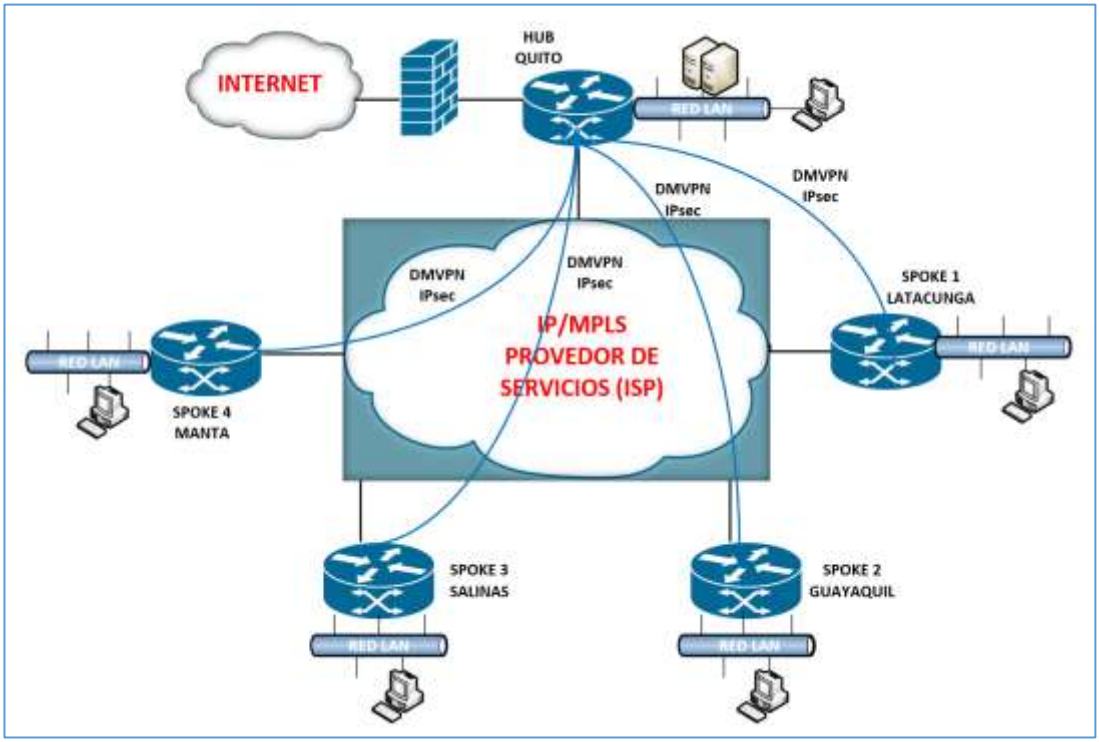

Figura 8. Estructura de la red propuesta, Elaboración propia

b. Explicación del aporte

En la figura 8 se muestra la estructura general de la red propuesta en el presente trabajo, lo cual contempla dos infraestructuras de red que se interconectan para el funcionamiento de los servicios en los cinco repartos militares para cumplir con el objetivo planteado.

En la estructura general de la propuesta, se muestran las infraestructuras de red de área local de las cinco localidades de la Fuerza Aérea Ecuatoriana (Quito, Latacunga, Guayaquil, Salinas y Manta) motivo de este estudio y en el centro la infraestructura de red del proveedor de

servicios, el cual permite la interconexión de todos los sitios a través de la provisión de canales de datos.

Para verificar el funcionamiento del diseño de la red WAN propuesta que integre las infraestructuras de red interna, se realizó la simulación en el aplicativo GNS3, herramienta que permite modelar escenarios de redes complejas. Para efectos de la simulación en los cinco repartos militares se ha utilizado *routers* Cisco modelo C3725 con un IOS de seguridad *c3725-advsecurityk9-mz.124-15.T12.bin,* el cual establece la conexión física con el equipo CE *(Customer Edge)* del proveedor, la infraestructura de red del ISP permite la interconexión entre los cinco repartos militares, a través de canales de datos L3VPN que son contratados.

Para la simulación de la red del proveedor de servicios en la plataforma GNS3, se utilizó tres *router* de la familia Cisco 7200 con un IOS c7200-advipservicesk9-mz.152-4.S5.bin, los cuales se encuentran interconectados como se muestra en la figura 9; para la conexión entre *router* se utilizó segmentos de red con direccionamiento privado en máscara de 30 bits y con la finalidad de establecer la conectividad entre los equipos se habilitó el protocolo de enrutamiento OSPF v2.

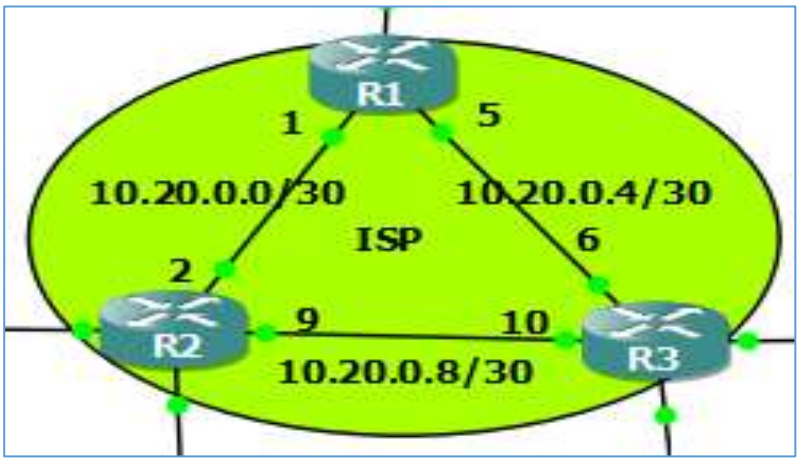

Figura 9. Red simulada proveedor de servicios, Elaboración propia

Para verificar el funcionamiento de la infraestructura de red del proveedor simulado, se realizó pruebas de diagnóstico de conectividad en los tres ruteadores, donde se pudo verificar la convergencia total de la red del proveedor, cuyo resultado se muestra en las figuras 10, 11 y 12.

```
R1#show ip route ospf

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O        10.20.0.8/30 [110/2] via 10.20.0.6, 00:03:20, GigabitEthernet1/0
                      [110/2] via 10.20.0.2, 00:03:10, GigabitEthernet0/0
      172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
O        172.16.254.4/30 [110/2] via 10.20.0.6, 00:03:20, GigabitEthernet1/0
O        172.16.254.8/30 [110/2] via 10.20.0.6, 00:03:20, GigabitEthernet1/0
O        172.16.254.12/30 [110/2] via 10.20.0.2, 00:03:10, GigabitEthernet0/0
O        172.16.254.16/30 [110/2] via 10.20.0.2, 00:03:10, GigabitEthernet0/0
```

Figura 10. Test de conectividad OSPF R1, Elaboración propia

```
R2#show ip route ospf

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O        10.20.0.4/30 [110/2] via 10.20.0.10, 00:12:01, GigabitEthernet1/0
                      [110/2] via 10.20.0.1, 00:12:11, GigabitEthernet0/0
      172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
O        172.16.254.0/30 [110/2] via 10.20.0.1, 00:12:11, GigabitEthernet0/0
O        172.16.254.4/30 [110/2] via 10.20.0.10, 00:12:01, GigabitEthernet1/0
O        172.16.254.8/30 [110/2] via 10.20.0.10, 00:12:01, GigabitEthernet1/0
```

Figura 11. Test de conectividad OSPF R2, Elaboración propia

```
R3#show ip rou ospf

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O        10.20.0.0/30 [110/2] via 10.20.0.9, 00:22:30, GigabitEthernet0/0
                      [110/2] via 10.20.0.5, 00:22:30, GigabitEthernet1/0
      172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
O        172.16.254.0/30 [110/2] via 10.20.0.5, 00:22:40, GigabitEthernet1/0
O        172.16.254.12/30 [110/2] via 10.20.0.9, 00:22:30, GigabitEthernet0/0
O        172.16.254.16/30 [110/2] via 10.20.0.9, 00:22:30, GigabitEthernet0/0
```

Figura 12. Test de conectividad OSPF R3, Elaboración propia

En la figura 13 se muestra la interconexión de los equipos de borde (*router* C3725) de los cinco repartos militares y el equipamiento de red del proveedor de servicios, en los cuales para establecer los enlaces WAN, se estableció segmentos de red con direccionamiento privado con una máscara de 30 bits.

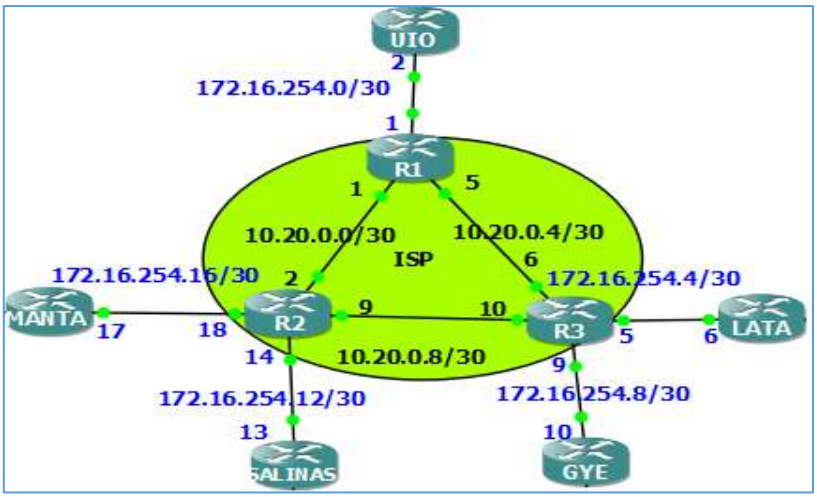

Figura 13. Interconexión de los router de la institución, Elaboración propia

Una vez que se ha realizado la configuración de los enlaces punto a punto y se ha establecido el enrutamiento IP en los ruteadores del proveedor como los del cliente, es necesario verificar la conectividad entre las localidades remotas a nivel de la capa *underlay,* lo cual se muestra en la figura 14.

```
UIO#ping 172.16.254.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.254.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/134/144 ms
UIO#ping 172.16.254.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.254.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 132/148/172 ms
UIO#ping 172.16.254.13

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.254.13, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 136/166/240 ms
UIO#ping 172.16.254.17

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.254.17, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/132/204 ms
```

Figura 14. Test de conectividad entre sitios remotos (SPOKE), Elaboración propia

*C*on la finalidad de cumplir con el objetivo de la propuesta, mitigando al máximo posibles desvíos del tráfico de información institucional, en los router de borde se encuentran configurados túneles DMVPN sobre la capa de conectividad del proveedor, en la figura 15 se

muestra cuatro túneles dinámicos levantados desde la matriz (HUB) hacia las localidades remotas (SPOKE).

```
UIO#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incompletea
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer

Tunnel0, Type:Hub, NHRP Peers:4,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1   172.16.254.6       10.10.0.2    UP    never D
     1   172.16.254.10      10.10.0.3    UP    never D
     1   172.16.254.13      10.10.0.4    UP    never D
     1   172.16.254.17      10.10.0.5    UP    never D
```

Figura 15. Túneles DMVPN mostrados en el HUB, Elaboración propia

Al disponer de una nueva capa de conectividad *overlay* (túneles DMVPN) entre los *routers* C3725, se habilitó el protocolo de enrutamiento dinámico EIGRP para enrutar los enlaces WAN y LAN de los repartos militares a nivel de los túneles DMVPN, cuyo direccionamiento IP se encuentra detallado en la tabla 5, el funcionamiento del enrutamiento dinámico se muestra en la figura 16, donde se puede visualizar que el aprendizaje de los segmentos de red de las LAN de los repartos es a través de las interfaces túnel 0.

```
GYE#show ip rou eigrp
D    192.168.30.0/24 [90/310070016] via 10.10.0.4, 00:22:57, Tunnel0
D    192.168.10.0/24 [90/310070016] via 10.10.0.5, 00:22:50, Tunnel0
D    192.168.20.0/24 [90/310070016] via 10.10.0.2, 00:22:57, Tunnel0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.0.0.0/8 is a summary, 00:23:20, Null0
D    192.168.0.0/24 [90/297270016] via 10.10.0.1, 00:22:57, Tunnel0
D*EX 0.0.0.0/0 [170/297372416] via 10.10.0.1, 00:22:58, Tunnel0
```

Figura 16. Rutas EIGRP sobre los túneles DMVPN, Elaboración propia

Luego de verificar el funcionamiento de la conectividad entre los sitios remotos y la matriz a través de los túneles dinámicos y con el objetivo de precautelar la seguridad de la información de la institución militar, garantizando la autenticación, confidencialidad, integridad y no repudio, se encuentra levantado IPsec sobre los túneles DMVPN, de esta manera se logra encriptar el tráfico que circula por la capa de conectividad *overlay*, en la figura 17 se muestra una captura del test de funcionamiento de IPsec ejecutado desde el router matriz (HUB).

```
UIO#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
172.16.254.2    172.16.254.17   QM_IDLE           1004    0 ACTIVE
172.16.254.2    172.16.254.13   QM_IDLE           1003    0 ACTIVE
172.16.254.2    172.16.254.10   QM_IDLE           1002    0 ACTIVE
172.16.254.2    172.16.254.6    QM_IDLE           1001    0 ACTIVE
```

Figura 17. Asociaciones de seguridad de la matriz con los SPOKE, Elaboración propia

Una de las pruebas realizadas para verificar que el tráfico de la red LAN de los repartos militares dirigidos hacia la matriz o entre sucursales (SPOKE) circula a través de los túneles DMVPN, se realizó un tracert desde la pc de Guayaquil hacia la LAN de la matriz, lo cual se muestra en la figura 18 y la simulación hacia internet verificando la conectividad hacia la IP pública 190.152.214.1 alojada en la matriz, ejecutado desde la misma pc se muestra en la figura 19.

```
PC_GYE> tracer 192.168.0.10
trace to 192.168.0.10, 8 hops max, press Ctrl+C to stop
 1   192.168.40.254   14.824 ms  15.049 ms  14.986 ms
 2   10.10.0.1   104.722 ms  104.866 ms  104.555 ms
 3   *192.168.0.10   105.417 ms (ICMP type:3, code:3, Destination port unreachable)
```

Figura 18. Test de verificación del recorrido del tráfico, Elaboración propia

```
PC_GYE> ping 190.152.214.1
84 bytes from 190.152.214.1 icmp_seq=1 ttl=254 time=104.825 ms
84 bytes from 190.152.214.1 icmp_seq=2 ttl=254 time=104.908 ms
84 bytes from 190.152.214.1 icmp_seq=3 ttl=254 time=104.845 ms
84 bytes from 190.152.214.1 icmp_seq=4 ttl=254 time=105.369 ms
84 bytes from 190.152.214.1 icmp_seq=5 ttl=254 time=105.590 ms
```

Figura 19. Test de verificación de la conectividad hacia el internet, Elaboración propia

Finalmente, para verificar que todo el tráfico que circula por los túneles dinámicos está siendo encriptados en el origen y desencriptados en el destino, se realizó una prueba de *troubleshooting* sobre IPsec, lo cual se muestra en la figura 20, donde se visualiza el funcionamiento de IPsec.

```
GYE#show crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 172.16.254.10

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.254.10/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.254.2/255.255.255.255/47/0)
   current_peer 172.16.254.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 523, #pkts encrypt: 523, #pkts digest: 523
    #pkts decaps: 531, #pkts decrypt: 531, #pkts verify: 531
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 7, #recv errors 0
```

*Figura 20. V*erificación de encriptación y desencriptación del tráfico, Elaboración propia

c. Estrategias y/o técnicas

Para el desarrollo de la propuesta, se utilizó varios insumos que dispone la institución en su infraestructura de telecomunicaciones actual, a esto se suma la información disponible en los portales web de los fabricantes de equipos de *networking* donde se encontró las especificaciones técnicas de los equipos propuestos, también fue necesario consultar los costos actuales de los canales de datos que se comercializa en el país y costos de los equipos de *networking.*

Con el objetivo de poder dimensionar el ancho de banda de los canales de datos que deberán ser contratados, se realizó una revisión del consumo actual del servicio de internet en cada reparto militar que son parte del presente estudio, para lo cual se utilizó capturas del monitoreo a través de la herramienta Cacti, como se muestra en las figuras 21 al 25.

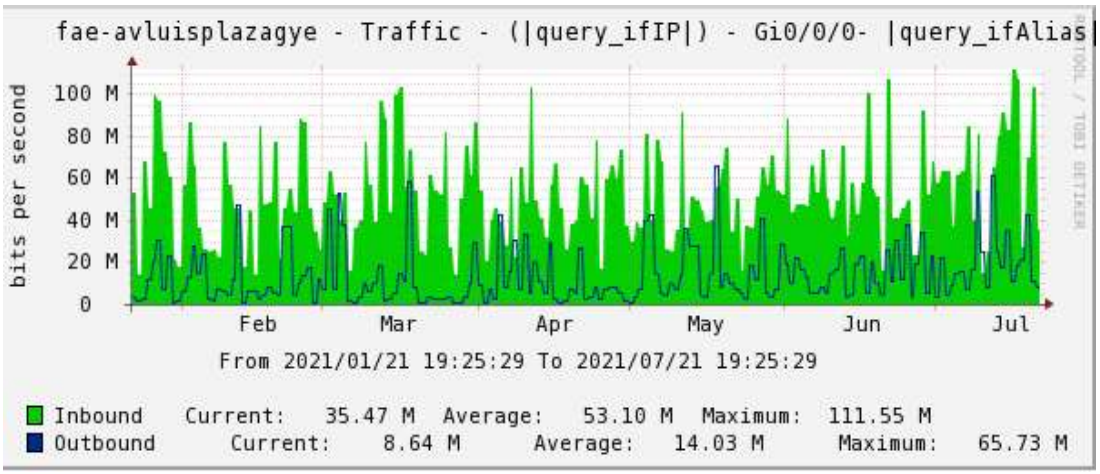

Figura 21. Consumo internet Guayaquil, Elaboración propia

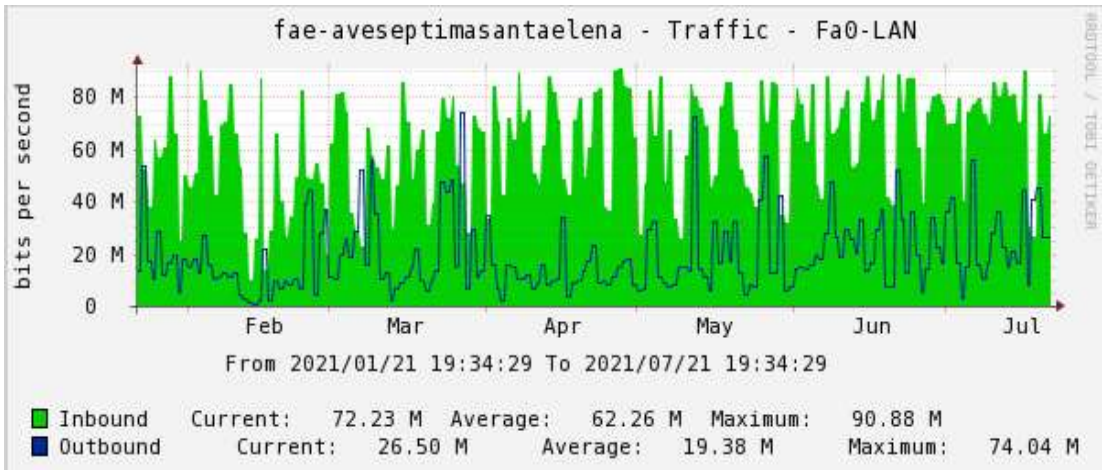

Figura 22. Consumo internet Salinas, Elaboración propia

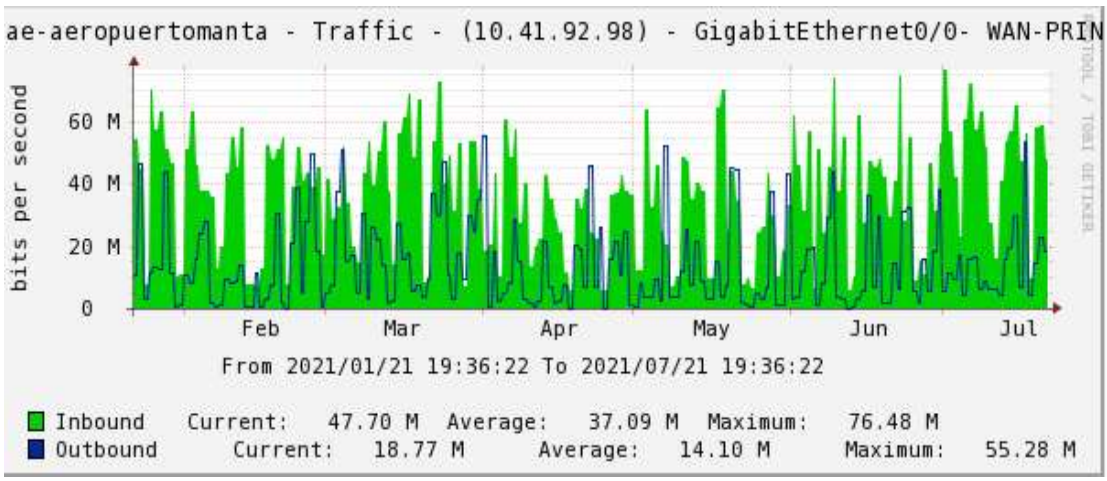

Figura 23. Consumo internet Manta, Elaboración propia

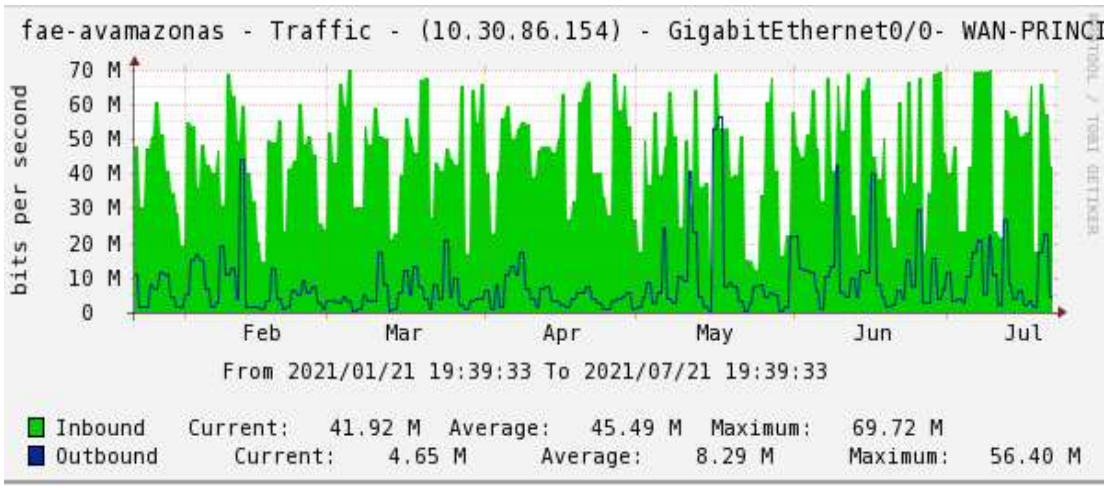

Figura 24. Consumo internet Latacunga, Elaboración propia

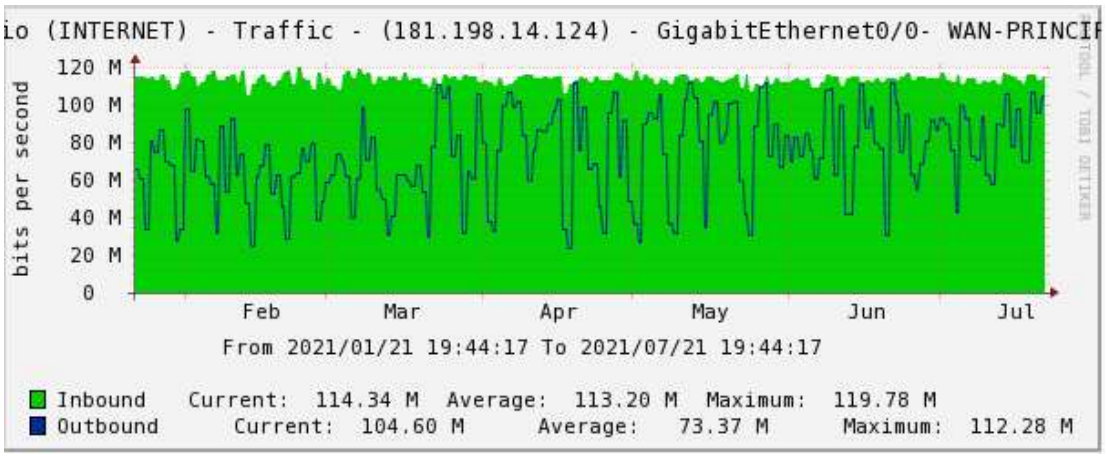

Figura 25. Consumo internet Quito, Elaboración propia

Una vez que ya se disponía de los insumos necesarios, se realizó el análisis correspondiente y se planteó un diseño de red con el dimensionamiento apropiado, lo siguiente fue hacer uso de la plataforma GNS3 para simular el funcionamiento de la red WAN interconectando las cinco localidades, a través de canales de datos contratado a un proveedor de servicios local, a fin de garantizar la seguridad de la información, considerando el tipo de información que genera y procesa la institución militar, se utilizó protocolos de seguridad como la configuración de túneles DMVPN y encriptar los canales virtuales con IPsec.

Dentro del proceso de simulación en la plataforma GNS3, se diseñó un esquema de direccionamiento IPv4 para la configuración del equipamiento planteado en la red WAN y LAN, conforme se muestra en la tabla 5.

d. Desarrollo de la propuesta

Para el desarrollo de la propuesta fue necesario estructurarla con cada uno de los objetivos específicos formulados en este trabajo, para lo cual se utilizaron cinco (5) fases, las cuales consisten en:

Fase uno

Consiste en contextualizar los fundamentos teóricos sobre las diferentes tecnologías actuales de Ethernet, y protocolos de seguridad para el diseño y simulación del proyecto, en esta fase se realizó una investigación de las principales teorías en las que se fundamenta la propuesta, en ese sentido se articuló las principales tecnologías y protocolos que se encuentran descritos en el item fundamentos teóricos aplicados de este trabajo, iniciando con una contextualización y desarrollo de la importancia en el uso de la tecnología Ethernet en las redes actuales, la cual se determinó para el desarrollo de la propuesta, debido a que ofrece grandes prestaciones para el usuario final en términos de confiabilidad, disponibilidad, gran ancho de banda y bajo retardo

en las comunicaciones de datos, se revisó también protocolos de seguridad como DMVPN e IPsec los cuales contemplan su uso en este proyecto.

Fase dos

Determinar las deficiencias en la conectividad a los diferentes servicios de comunicaciones que dispone la institución, dentro del proceso metodológico de investigación se aplicó una encuesta al personal técnico, profesionales del área y jefes de los departamentos TIC de las localidades que son parte del presente estudio, como resultados se obtuvo:

1. *¿Con qué frecuencia su reparto militar accede a los servicios institucionales (videoconferencia, telefonía MODE, portales FAE, correo institucional, etc.)?*

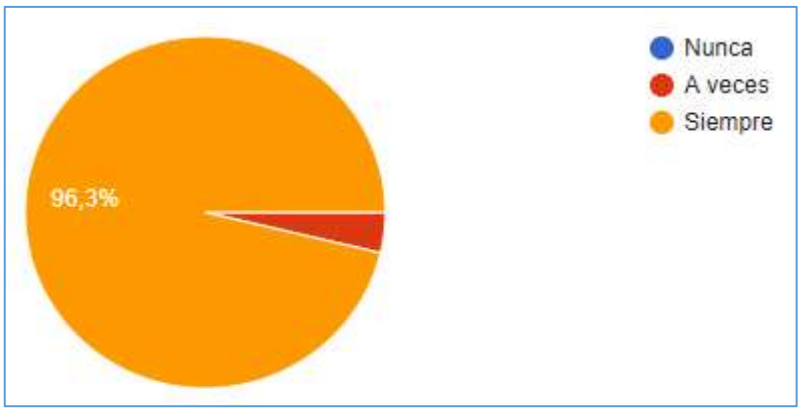

Figura 26. Acceso a los servicios institucionales, Elaboración propia

Análisis: como se visualiza en la figura 26, el 96,3% del personal encuestado respondió que siempre accede a los servicios institucionales alojados en la matriz y el 3.7% afirma que a veces

Interpretación: Se determina que casi todos los usuarios acceden a los servicios institucionales alojados en el sitio matriz.

2. *¿A menudo su reparto se queda sin enlace a la red WAN (COMACO/MODE)?*

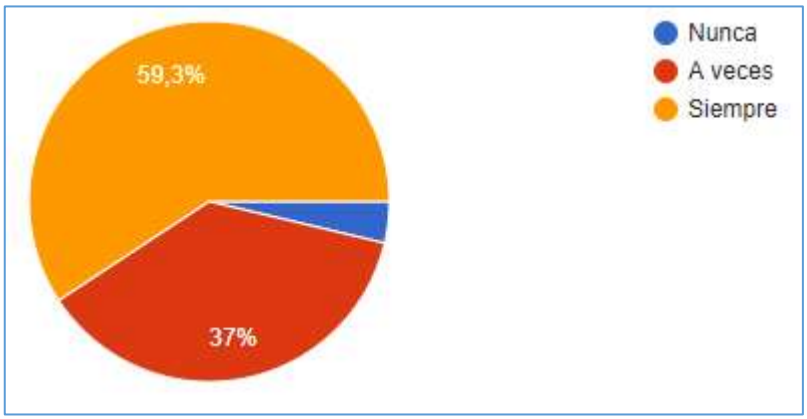

Figura 27. Porcentaje sin enlace a la WAN, Elaboración propia

Análisis: En la figura 27 se visualiza que, el 59,3% del personal encuestado respondió que siempre se queda sin enlace a la WAN, el 37% responde que a veces y el 3.7% afirma que nunca se queda sin enlace

Interpretación: En base a los resultados se interpreta que regularmente los repartos militares se quedan sin enlace a la WAN y por ende sin servicios de la intranet FAE.

3. *Cuándo existe fallas en la red MODE y su reparto se queda sin servicios, ¿El problema es solucionado de forma inmediata)?*

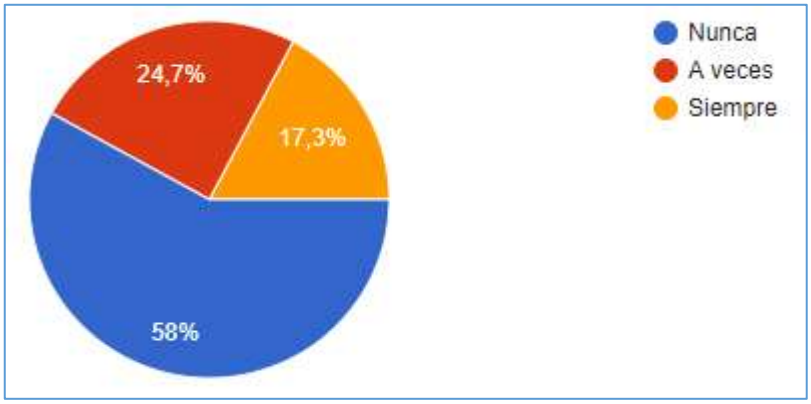

Figura 28. Los fallos en la red son solucionados de forma inmediata, Elaboración propia

Análisis: En la figura 28 se visualiza que, el 58% del personal encuestado respondió que nunca se soluciona las fallas en la WAN de forma inmediata, el 24,7% a veces se soluciona y el 17,3 informa que siempre se soluciona inmediatamente.

Interpretación: Se determina que en la gran mayoría de los casos de falla no es solucionado de forma inmediata, un porcentaje menor afirma que a veces si se soluciona de forma inmediata.

4. *¿Su proveedor de servicios en la red WAN (COMACO) dispone de una mesa de ayuda 24x7 para un eficiente soporte técnico?*

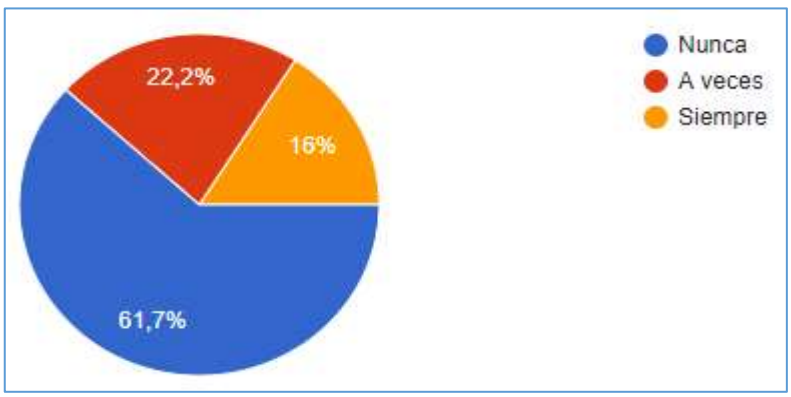

Figura 29. Mesa de ayuda 24x7 para un eficiente soporte técnico, Elaboración propia

Análisis: En la figura 29 se visualiza que, el 61.7% del personal encuestado respondió que nunca el proveedor de la WAN dispone de una mesa de ayuda para el soporte técnico, el 22% responde que a veces y el 16% manifiesta que siempre existe una mesa de ayuda con soporte técnico.

Interpretación: Se determina que no existe soporte técnico 24x7 en el proveedor de la WAN, a fin de que se puedan solventar fallas en la conectividad.

5. *¿Considera usted que la capacidad de ancho de banda asignado por el proveedor de la WAN (COMACO), abastece los requerimientos del reparto?*

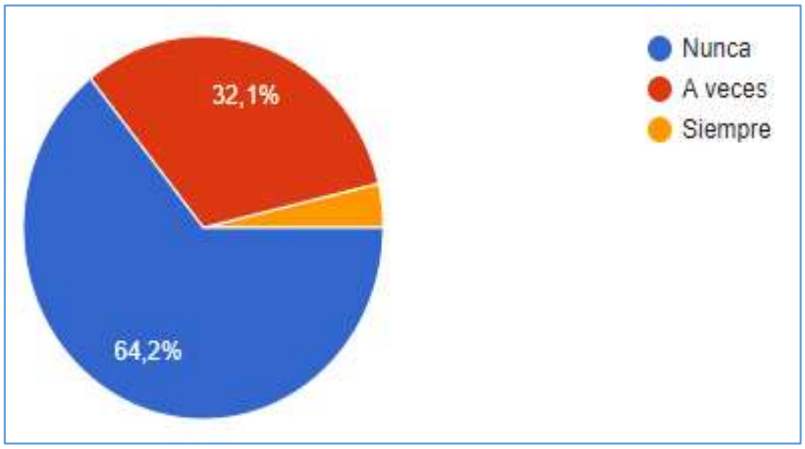

Figura 30. La capacidad asignada en la WAN abastece los requerimientos del reparto, Elaboración propia

Análisis: En la figura 30 se muestra que, el 64.2% del personal encuestado respondió que la capacidad asignada no abastece a los requerimientos del reparto, un 32,1% afirma que a veces abastece y un 3,7% que si abastece.

Interpretación: La capacidad de ancho de banda asignado por el proveedor de la WAN, no cumple con los requerimientos del reparto militar.

6. *¿Su reparto dispone de un equipo o sistema de seguridad perimetral acorde a la tecnología actual, con licenciamiento vigente que garantice la seguridad de la información?*

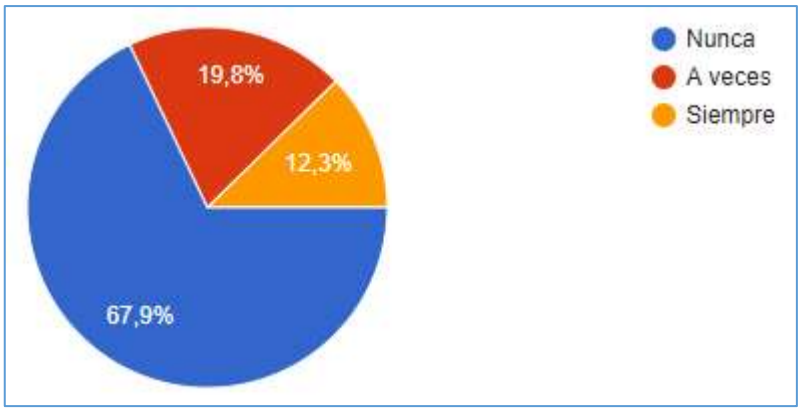

Figura 31. El reparto dispone sistema de seguridad perimetral actualizado, Elaboración propia

Análisis: En la figura 31 se muestra que, el 67.9% del personal encuestado respondió que el reparto no dispone de un sistema de seguridad perimetral acorde a la tecnología actual, un 19,8% afirma que a veces existe y un 12,3% que existe.

Interpretación: Se determina que, en los repartos militares, donde se realiza el estudio no existe un sistema de seguridad perimetral acorde a la tecnología actual y con licenciamiento vigente.

7. *El proveedor de servicios en la WAN (COMACO) garantiza la seguridad de la información en sus enlaces*

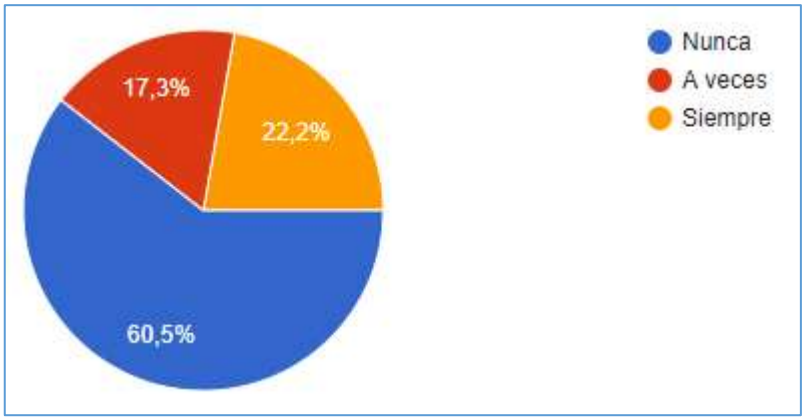

Figura 32. El proveedor de servicios garantiza la seguridad en los enlaces, Elaboración propia

Análisis: En la figura 32 se muestra que, el 60.5% del personal encuestado respondió que el proveedor no garantiza la seguridad en sus enlaces, un 22.2% afirma que si garantiza la seguridad y un 17,3% que a veces garantiza la seguridad.

Interpretación: El personal encuestado en su gran mayoría afirma que el proveedor de la WAN no garantiza la seguridad de la información en sus enlaces.

8. *Considera una amenaza de seguridad el hecho de contratar internet de forma local en su reparto, tomando en cuenta que no se dispone de equipamiento de seguridad actualizado.*

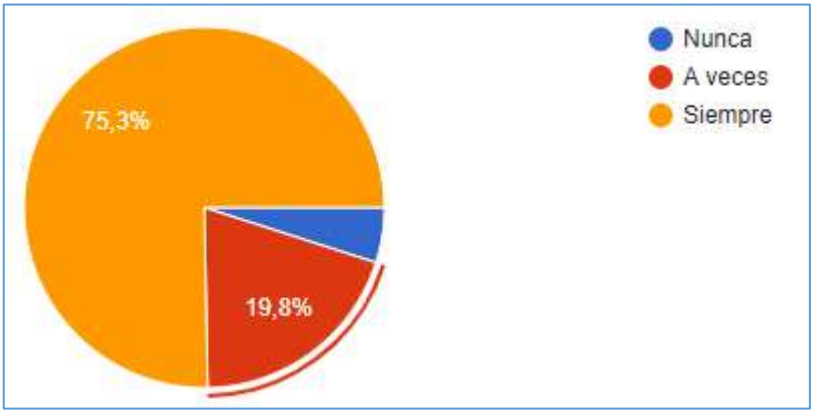

Figura 33. Amenaza de seguridad si se contrata internet local, Elaboración propia

Análisis: En la figura 33 se visualiza que, el 75,3% del personal encuestado respondió que la contratación de internet de forma local es una amenaza de seguridad, el 19,8% responde que a veces es una amenaza y 4,9% menciona que no es una amenaza.

Interpretación: La gran mayoría del personal encuestado afirma que la contratación de internet de forma local en los repartos es una amenaza de seguridad a la infraestructura tecnológica de la institución.

- *Resumen del diagnóstico*

Luego de haber realizado el análisis y tabulación de los datos recolectados en el proceso de investigación, se ha llegado a las siguientes puntualizaciones:

La gran mayoría del personal encuestado de los repartos militares, manifiestan que todo el tiempo acceden a los servicios institucionales alojados en el data center del sitio matriz, así como también indican que los enlaces del proveedor WAN a menudo se cortan y no son reparados de forma inmediata.

En el análisis, también se puedo determinar que el ancho de banda asignada en la WAN no responde a los requerimientos de los repartos militares, no existe una mesa de ayuda 24x7 para soporte técnico por parte del proveedor y el proveedor de la WAN no garantiza la seguridad de la información en sus enlaces.

Otro tema importante que se puede concluir del proceso de estudio es el hecho de que en los repartos no existe equipamiento robusto de seguridad perimetral acorde a la tecnología actual y con licenciamiento actualizado, por lo que en su gran mayoría del personal encuestado

informa que contratar internet de forma local es una amenaza de seguridad a la infraestructura interna de los repartos.

Con el instrumento aplicado en el proceso de investigación, la revisión de la documentación institucional y el análisis realizado a los datos se determinó que existen las falencias en la conectividad hacia los servicios provistos desde la matriz.

Fase tres

Dimensionar la red Ethernet a nivel WAN que interconecte cinco localidades remotas de la Fuerza Aérea Ecuatoriana, en esta fase se realizó varias actividades con la finalidad de alcanzar el desarrollo la propuesta planteada.

Dimensionamiento

Para establecer la capacidad de los canales de datos que se debe contratar al proveedor de servicios, partimos como base, el análisis realizado al registro estadístico de consumo de internet de los últimos seis meses en cada uno de los repartos militares, reflejado en la herramienta de monitoreo Cacti, tal como se muestran en las figuras del 13 al 17.

Con el objetivo de utilizar los canales de datos contratados, con el servicio de internet, además tráfico de aplicaciones y servicios propios de la institución se planificó un 20% adicional de la capacidad que registra la herramienta de monitoreo, los cálculos realizados se presentan en la tabla 2.

Tabla 2

Cálculo del ancho de banda de los canales de datos

Ord.	Localidad	Actual (Mbps)	Máximo (Mbps)	Promedio (Mbps)	Crecimiento 20% (Mbps)	Total (Mbps)
1	Matriz Quito	114.34	119.78	117.06		
2	Latacunga	41.92	69.72	55.82	11.16	66.9
3	Guayaquil	35.47	111.55	73.51	14.70	88.2
4	Salinas	72.23	90.88	81.55	16.31	97.8
5	Manta	47.7	76.48	62.09	12.41	74.5
			Total	390.035	54.59	327.57

Nota. Cálculo realizado en base a la medición de tráfico del servicio de internet, utilizando la herramienta de monitoreo Cacti, Elaboración propia.

En el proceso de dimensionamiento de la capacidad de ancho de banda de los canales de datos que se muestran en la tabla 2, se calculó un promedio (columna cinco) entre los valores consumo actual y el pico máximo que se registra en los últimos seis (6) meses (tercera y cuarta columna) en cada reparto militar, para efectos de un crecimiento futuro y el uso del canal de

datos para tráfico institucional, al valor promedio se le agregó un 20% de capacidad adicional (columna seis), de esta forma se estableció la capacidad total que debe ser contratado; en vista que todo el tráfico se concentra en el sitio matriz, se tiene una capacidad que es igual a la suma de las capacidades de todos los sitios.

A fin de poder determinar un *router* que se encuentre en vigencia tecnológica en el mercado, se ajuste a los requerimientos institucionales y al cumplimiento de los objetivos planteados en este proyecto, se realizó la comparación de las especificaciones técnicas de cinco modelos de ruteadores Cisco, se selecciona esta marca debido a la calidad, soporte y además la institución dispone equipamiento de esta marca. Actualmente el equipamiento existente se encuentra descontinuado por ser modelos muy antiguos, en la tabla 3 se muestra la matriz comparativa de las principales especificaciones técnicas de los modelos citados.

Tabla 3

Matriz comparativa router Cisco

Especificaciones técnicas	**ISR 4461**	**ISR 4451**	**ISR 4431**	**ISR 4351**	**ISR 4331**
Rendimiento predeterminado	1.5 Gbps	1Gbps	500 Mbps	200Mbps	100Mbps
Rendimiento con licencia	3Gbps	2Gbps	1Gbps	400Mbps	300Mbps
Puertos WAN o LAN 10/100/1000	4	4	4	3	3
Puertos RJ45	4	4	4	3	2
Puertos SFP	4	4	4	3	2
Memoria Flash	8GB	8GB	8GB	4GB	4GB
Potencia máxima	1000W	450W	250W	430W	250W
Protocolos	IPv4, IPv6, rutas estáticas, RIPv2, OSPF, IGRP, EIGRP, BGP, IS-IS, IGMPv3, PIM SM, PIM (SSM), RSVP, ACL, DHCP, HSRP, RADIUS, AAA, DVMRP, IPv4-to-IPv6 *Multicast*, MPLS, *capa* 2 y *capa* 3 VPN, IPsec, L2TPv3, IEEE 802.1ag e IEEE 802.3ah.				
Encapsulaciones	Ethernet, VLAN 802.1q. PPP, MLPPP, HDLC, serie (RS-232, RS-449, X.21, V.35 y EIA-530) y PPP sobre Ethernet (PPPoE)				
Gestión de tráfico	QoS, CBWFQ, WRED, PBR y NBAR.				
Algoritmos criptográficos	Cifrado: DES, 3DES, AES -128 o AES-256 Autenticación: RSA (748/1024/2048 bit), ECDSA (256/384 bit) Integridad (MD5, SHA, SHA-256, SHA-384, SHA-512)				

Fuente: ***(Cisco, 2021)***

Del análisis comparativo realizado a los diferentes modelos de *router*, se determinó el uso de dos modelos para este proyecto, el ISR 4431 para el sitio matriz y el ISR 4331 para los sitios remotos cuyas imágenes se muestran en las figuras 34 y 35, la diferencia entre los dos modelos, básicamente está en la capacidad de tráfico que pueden procesar (rendimiento), el modelo ISR

4431 con la licencia base su rendimiento es de 500Mbps y con una licencia adicional se puede ampliar hasta 1Gbps, mientras que el modelo ISR 4331 por defecto su rendimiento es 100Mbps y con una licencia adicional se puede ampliar hasta 300Mbps; en el HUB o sitio matriz circulará un tráfico total de 327.5 Mbps considerando la suma de los tráficos de los cinco sitios, por lo que es necesario la implementación del ISR 4431, además cuyo rendimiento permitirá a futuro la integración de algunos sitios adicionales.

Figura 34. Router ISR 4431 (Cisco, 2021)

Figura 35. Router ISR 4331 (Cisco, 2021)

Costos

Tabla 4

Costo de servicios internet y canales de datos

Ord.	Localidad	Servicio	Ancho de banda (Mbps)	Medio de transmisión	Valor instalación	Valor mensual
1	Quito	Internet dedicado (1:1)	390	Fibra óptica	$6.50	$2,535.00
2	Quito	Concentrador	328	Fibra óptica		
3	Latacunga	L3 MPLS	67	Fibra óptica	$13.85	$927.95
4	Guayaquil	L3 MPLS	88	Fibra óptica	$13.85	$1,218.80
5	Salinas	L3 MPLS	98	Fibra óptica	$13.85	$1,357.30
6	Manta	L3 MPLS	75	Fibra óptica	$13.85	$1,038.75
					Subtotal mensual	$7,077.80
					Subtotal anual	$84,933.60
					Iva 12%	$10,192.03
					Total	$95,125.63

Fuente: Elaboración propia

Los costos de los servicios de telecomunicaciones mostrados en la tabla 4, son referenciales tomados de la oferta comercial entregada por la empresa pública CNT-EP, al ser un documento

confidencial no es factible el anexo de dicho documento; en referencia a los valores de los equipos de *networking*, en la tabla 5 se muestran los precios de lista, entregados por una empresa local *partner* de la empresa Cisco.

Tabla 5

Costo del equipamiento de networking

Ord	Modelo	Cantidad	Precio de lista	Total
1	ISR4431	1	$24,860.08	$24,860.08
2	ISR4331	4	$9,208.71	$36,834.84
			Subtotal	$61,694.92
			Iva	$7,403.39
			Total	$69,098.31

Fuente: Elaboración propia

En la tabla 6 se muestra el resumen total de los costos del proyecto, considerando la adquisición de un nuevo equipamiento de *networking* debido a que los equipos que existen actualmente se encuentran descontinuados y sin soporte del fabricante por ser muy antiguos.

Tabla 6

Resumen de costos del proyecto

Ord	Descripción	Valor
1	Servicio de internet y canales datos	$95,125.63
2	Equipamiento de *networking*	$69,098.31
	Valor total del proyecto	$164,223.94

Fuente: Elaboración propia

Fase cuatro

Simular la red en un ambiente controlado mediante el aplicativo GNS3 a fin de verificar su funcionamiento, en esta fase se realizó la simulación de la red propuesta, en donde se verificó el funcionamiento de las infraestructuras de red, tanto la del proveedor de servicios como la de la institución, además se confirmó la convergencia de los protocolos de enrutamiento como OSPF y EIGRP, permitiendo la conectividad entre los sitios remotos con la matriz mediante el uso de los túneles DMVPN y finalmente con el objetivo de garantizar la seguridad de la información institucional, se verificó el funcionamiento del protocolo IPsec. En el proceso de simulación fue necesario realizar las siguientes actividades.

Elaboración del diagrama lógico de conexión

Luego del análisis de las deficiencias que existen en la institución relacionado con la conectividad a la matriz y por ende el acceso a los diferentes servicios institucionales alojados en el data center de la Comandancia General FAE y una vez que se tiene definido la estructura general de la propuesta, donde claramente se define una conexión física que es provista por el proveedor de servicios y sobre aquello se levantan túneles virtuales del tipo punto multipunto, sobre este esquema se diseña e implementa una topología de red en GNS3, en la figura 36, se presenta el diseño del diagrama de red lógico de la red WAN Ethernet, la cual integra las redes LAN de los sitios involucrados en el presente estudio.

El diagrama de red contempla la interconexión de todos los routers de la institución con los equipos del proveedor, asimismo se encuentra el esquema de direccionamiento IP, tanto para los enlaces WAN como para las infraestructuras de red LAN, cada equipo con sus respectivos interfaces.

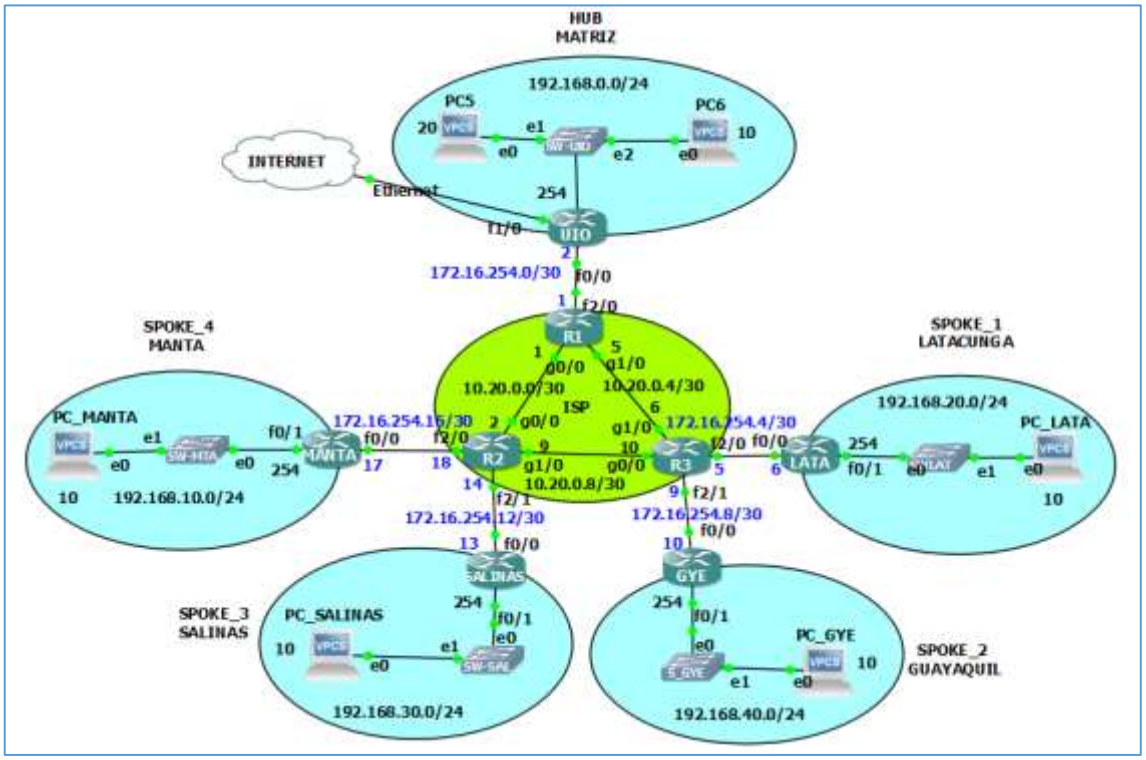

Figura 36. Diagrama lógico de conexión, Elaboración propia

Planificación del esquema de direccionamiento IPv4

Una vez que se disponía el diagrama de red lógico a nivel WAN y LAN, para proceder con la configuración de las interfaces de los equipos, tanto del proveedor como de la institución, fue

necesario el diseño de un esquema de direccionamiento IPv4 que cumpla con las necesidades del diseño planteado, lo cual se muestra en la tabla 5.

Tabla 7

Esquema de direccionamiento IPv4

Dispositivo	Interface	Dirección IP	Prefijo máscara	Gateway
ISP R1	G0/0	10.20.0.1	/30	N/A
	G1/0	10.20.0.5	/30	N/A
	F2/0	172.16.254.1	/30	N/A
ISP R2	G0/0	10.20.0.2	/30	N/A
	G1/0	10.20.0.9	/30	N/A
	F2/0	172.16.254.18	/30	N/A
	F2/1	172.16.254.14	/30	N/A
ISP R3	G0/0	10.20.0.10	/30	N/A
	G1/0	10.20.0.6	/30	N/A
	F2/0	172.16.254.5	/30	N/A
	F2/1	172.16.254.9	/30	N/A
R Quito HUB	F0/0	172.16.254.2	/30	N/A
	F0/1	192.168.0.254	/24	N/A
	L0	190.152.214.1	/32	N/A
	TUN 0	10.10.0.1	/27	N/A
R Latacunga SPOKE_1	F0/0	172.16.254.6	/30	N/A
	F0/1	192.168.20.254	/24	N/A
	TUN 0	10.10.0.2	/27	N/A
R Guayaquil SPOKE_2	F0/0	172.16.254.10	/30	N/A
	F0/1	192.168.40.254	/24	N/A
	TUN 0	10.10.0.3	/27	N/A
R Salinas SPOKE_3	F0/0	172.16.254.13	/30	N/A
	F0/1	192.168.30.254	/24	N/A
	TUN 0	10.10.0.4	/27	N/A
R Manta SPOKE_4	F0/0	172.16.254.17	/30	N/A
	F0/1	192.168.10.254	/24	N/A
	TUN 0	10.10.0.5	/27	N/A
PC1 Quito	E0	192.168.0.10	/24	192.168.0.254

Dispositivo	Interface	Dirección IP	Prefijo máscara	Gateway
PC2 Quito	E0	192.168.0.20	/24	192.168.0.254
PC Latacunga	E0	192.168.20.10	/24	192.168.20.254
PC Guayaquil	E0	192.168.40.10	/24	192.168.40.254
PC Salinas	E0	192.168.30.10	/24	192.168.30.254
PC Manta	E0	192.168.10.10	/24	192.168.10.254

Fuente: Elaboración propia

Simulación

En la propuesta se ejecutó la simulación de la red planteada, para lo cual se utilizó como plataforma de simulación, la aplicación GNS3 versión 2.2.22 ultima disponible en el portal de citada herramienta, GNS3 es un software muy robusto que permite desarrollar topologías de red complejas y verificar el funcionamiento utilizando comandos de diagnóstico de red.

Durante la fase de simulación se realizó la configuración de los equipos del ISP, donde se configuró las interfaces y luego de verificar la conectividad entre los equipos, se habilitó el protocolo de enrutamiento OSPF v2 que permita la interconectividad entre ellos.

En los equipos de borde de los diferentes localidades (CE), se realizó la configuración de las interfaces WAN que se enlazan al proveedor y las interfaces internas que interconectan la red de los repartos, en estos equipos se verificó que exista conectividad al sitio matriz y con los otros sitios remotos a nivel de la capa de conectividad *underlay*, con la finalidad de garantizar la seguridad de la información y de acuerdo a lo planteado en la propuesta se levantó túneles DMVPN entre los sitios *SPOKE* y *HUB,* se verificó la conectividad entre los sitos a nivel de la conectividad de VPN conocido como conectividad *overlay*.

Al disponer de una capa de conectividad *overlay* a través de los túneles DMVPN, fue necesario la implementación del protocolo EIGRP para enrutar de forma dinámica el tráfico institucional a través de los túneles y para finalizar se habilitó IPsec sobre los túneles DMVPN; las capturas de los archivos de configuración de los *routers* del ISP como los del cliente en encuentran en los anexos.

Una vez que se terminaron las tareas para la ejecución de la simulación, se verificó el funcionamiento de la red propuesta, se realizaron diferentes pruebas de conectividad y uso de comandos de *troubleshooting* a fin de verificar el funcionamiento de los diferentes protocolos configurados.

e. Resultados

En la etapa de análisis de resultados, en lo que respecta a la fase uno se puede mencionar que dentro de la investigación bibliográfica realizada se obtuvo, la información técnica sobre las teorías y protocolos de comunicaciones que fundamentan el presente trabajo de investigación, se revisó y se analizó el estándar Ethernet como tecnología que permite el despliegue de infraestructuras de red a nivel LAN y WAN, luego de haber utilizado esta tecnología en la simulación de la red y verificado su funcionamiento, se puede indicar que tiene un alto rendimiento en ambientes LAN como WAN; las redes MPLS con sus servicios de VPN de capa II y III permiten la conectividad entre dos sucursales de una organización, finalmente se verificó el funcionamiento de los túneles DMVPN y IPsec, a fin de garantizar la integridad y confiabilidad de la información del usuario.

En la fase dos mediante la investigación realizada se pudo determinar las deficiencias que existe actualmente en la institución, relacionado con los continuos cortes en la conectividad hacia la matriz, se obtuvo que el 59.3% del personal encuestado manifestó que siempre se quedan sin acceso a la WAN y el 37% a veces; el 58% manifiesta que las fallas en la red WAN no son solucionados de forma inmediata, en referencia a los problemas de seguridad debido a la contratación del servicio de internet de forma local en los repartos militares, el resultado fue que el 75,3% manifestó que siempre es una amenaza de seguridad, relacionado a la capacidad en la WAN el 64.2% manifestó que la capacidad asignada en la WAN no abastece los requerimientos del reparto y finalmente el 60.5% manifestó que el actual proveedor no garantiza la seguridad de la información en su infraestructura.

En relación a la fase tres, luego del análisis a la problemática institucional y a los requerimientos, se obtuvo un diseño de red WAN con un dimensionamiento técnico de la capacidad de ancho de banda de los canales de datos que deberá proveer un ISP, en el cual se tomó como base el actual consumo del servicio de internet en las locaciones y se consideró un 20% de capacidad adicional del registrado con la finalidad de utilizar para tráfico institucional, se realizó el análisis comparativo de las especificaciones técnicas entre algunos modelos de *router* Cisco, determinándose de acuerdo a la realidad del proyecto dos modelos el ISR 4431 para la matriz y ISR 4331 para las sucursales, se escogió estos modelos en función de su rendimiento.

Los resultados en la fase cuatro relacionado con la simulación de la red en un ambiente controlado mediante el aplicativo GNS3, fueron exitosos porque se logró verificar el funcionamiento de la estructura de la red propuesta, el funcionamiento del estándar Ethernet

tanto en los enlaces WAN como en las LAN de las locaciones, se realizaron pruebas exitosas de conectividad entre el *HUB* y los *SPOKE* a nivel de la capa *underlay* y posterior con el uso de los túneles DMVPN se verificó la conectividad en la capa *overlay*, con los comandos de *troubleshooting* se pudo verificar el funcionamiento de los protocolos de enrutamiento dinámico como OSPF y EIGRP en cada dominio de red, finalmente se realizaron pruebas de conectividad desde usuarios de la LAN de forma simulada a través de los canales de datos encriptados por medio del protocolo IPsec.

Con respecto a la fase cinco relacionado a verificar el rendimiento de la red a través de indicadores claves de desempeño, como el *jitter*, retardo y paquetes perdidos, medidos en la red simulada según el diseño, se puede mencionar que los factores negativos que existen en un tráfico de red como el jitter en la red simulada no se presenta variaciones significativas en el retardo, como se muestra en la figura 38, los tiempos de retardo dentro de las diferentes pruebas de tráfico realizadas se presentaron de forma normal como se indica en la figura 37, lo cual es un buen indicador sobre el funcionamiento de la red, finalmente cuando se evaluó las pérdidas de paquetes o *packet lo*ss, no hubo una taza de paquetes perdidos, para lo cual se muestra la figura 37.

```
SALINAS#ping
Protocol [ip]:
Target IP address: 10.10.0.1
Repeat count [5]: 500
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 500, 100-byte ICMP Echos to 10.10.0.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
Success rate is 100 percent (500/500), round-trip min/avg/max = 36/99/212 ms
```

Figura 37 Prueba sin paquetes perdidos, Elaboración propia

```
PC_GYE> ping 10.10.0.1 -t
84 bytes from 10.10.0.1 icmp_seq=1 ttl=254 time=106.326 ms
84 bytes from 10.10.0.1 icmp_seq=2 ttl=254 time=104.822 ms
84 bytes from 10.10.0.1 icmp_seq=3 ttl=254 time=106.167 ms
84 bytes from 10.10.0.1 icmp_seq=4 ttl=254 time=105.427 ms
84 bytes from 10.10.0.1 icmp_seq=5 ttl=254 time=105.904 ms
84 bytes from 10.10.0.1 icmp_seq=6 ttl=254 time=105.309 ms
84 bytes from 10.10.0.1 icmp_seq=7 ttl=254 time=90.641 ms
84 bytes from 10.10.0.1 icmp_seq=8 ttl=254 time=90.065 ms
84 bytes from 10.10.0.1 icmp_seq=9 ttl=254 time=106.046 ms
84 bytes from 10.10.0.1 icmp_seq=10 ttl=254 time=105.682 ms
84 bytes from 10.10.0.1 icmp_seq=11 ttl=254 time=104.778 ms
84 bytes from 10.10.0.1 icmp_seq=12 ttl=254 time=104.541 ms
84 bytes from 10.10.0.1 icmp_seq=13 ttl=254 time=105.477 ms
84 bytes from 10.10.0.1 icmp_seq=14 ttl=254 time=104.882 ms
84 bytes from 10.10.0.1 icmp_seq=15 ttl=254 time=105.392 ms
```

Figura 38 Prueba de retardo, Elaboración propia

2.3. Matriz de articulación

En la presente matriz se resume la articulación del trabajo realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 8

Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	CLASIFICACIÓN TIC
Dimensionamiento de la red propuesta	Se trabajó con los fundamentos teóricos: Ethernet ya que permite la conectividad en la WAN y la LAN. Monitoreo tráfico servicio de internet Especificaciones técnicas router Cisco	Investigación bibliográfica. Análisis de los resultados del consumo de internet registrados en la aplicación de monitoreo Cacti Comparación de las especificaciones técnicas de los router ISR4431 e ISR4331	Investigación en libros, documentos físicos y en la WEB Uso de la herramienta de monitoreo Cacti	Diseño del diagrama de red lógico. Dimensionamiento de los canales de datos del ISP Selección del equipamiento a utilizar en la red	Se trabajó con una laptop Se emplearon herramientas como Visio, lo cual permite realizar el diagrama de red Internet
Simulación de la red	Ethernet como tecnología que permite la interconexión de redes	Verificación del funcionamiento de la red. Ejecución de las pruebas de *troubleshooting* para	Plataforma de simulación GNS3 versión 2.2.222	Verificación del funcionamiento de la red. Pruebas de conectividad entre los sitios parte de este estudio.	Laptop y aplicativo GNS3 el cual permite la simulación de entornos de red.

	Protocolos de enrutamiento dinámico OSPF y EIGRP Túneles DMVPN IPsec, lo cual permitirá la encriptación de los enlaces Uso del software GNS3	verificar el funcionamiento de los protocolos Ethernet, OSPF, EIGRP, DMVPN e IPsec.			
Verificación del rendimiento de la red	Fundamentación teórica sobre jitter, retardo y perdida de paquetes.	Uso de herramientas de análisis de la red. Pruebas de conectividad y análisis de jitter, retardo y perdida de paquetes	Ping Ping sostenido Ping con alteración del tamaño del paquete ICMP	Verificación del funcionamiento de la red, a través de pruebas de conectividad	Laptop Herramienta de simulación GNS3

Fuente: Elaboración propia

CONCLUSIONES

Una vez que se ha realizado el análisis y discusión de los resultados obtenidos en el presente trabajo, a continuación, se presentan las conclusiones, las cuales permiten visualizar los hallazgos más importantes referidos al "Diseño y simulación de una red datos WAN Ethernet con túneles DMVPN y seguridad IPsec, para interconectar cinco localidades remotas de la Fuerza Aérea Ecuatoriana", las mismas que se detallan en base a los objetivos específicos que se formularon para la investigación.

Con relación a la contextualización de los fundamentos teóricos sobre las diferentes tecnologías actuales de Ethernet y protocolos de seguridad para el diseño y simulación del proyecto, se concluye que la tecnología Ethernet es muy utilizada en el despliegue de redes WAN y LAN debido a su continuo desarrollo tecnológico, en la actualidad encontramos capacidades de Ethernet de hasta 400Gbps; por otro lado, con la finalidad de asegurar el tráfico sobre la red se verificó que la tecnología DMVPN funciona correctamente ya que permite levantar conexiones virtuales sobre una conectividad física y finalmente el uso del protocolo IPsec permite encriptar el tráfico, por lo tanto se cumplió con la contextualización de la fundamentación teórica utilizado en este trabajo.

En referencia a determinar las deficiencias en la conectividad a los diferentes servicios de comunicaciones que dispone la institución, se cumplió con el objetivo formulado debido a que se realizó un proceso de investigación, con una revisión de documentación bibliográfica donde se informa los cortes de servicio, adicional se aplicó la técnica de la encuesta al personal que labora en los departamentos TIC de las locaciones que fueron parte del presente estudio, luego del análisis realizado a los datos obtenidos, se determinó que existe deficiencias en la conectividad a la WAN.

En lo pertinente a dimensionar la red Ethernet a nivel WAN que interconecte cinco localidades remotas de la Fuerza Aérea Ecuatoriana, se concluye que esta fase fue cumplida, porque se estableció la tabla 2, donde se indican los cálculos realizados para alcanzar el dimensionamiento de la capacidad los canales de datos que se deberán contratar a un ISP con la finalidad de interconectar todas las locaciones que son parte de este proyecto, así también se realizó la comparación de las especificaciones técnicas de cuatro modelos de router donde se determinó el uso del ISR4431 y el ISR4331 para uso del proyecto, finalmente se diseñó un diagrama de red lógico donde se recoge los requerimientos institucionales.

En relación a la simulación de la red en un ambiente controlado mediante el aplicativo GNS3, a fin de verificar su funcionamiento, se concluye que la red propuesta funciona correctamente,

en razón que se realizó varias pruebas de conectividad con éxito, tanto en la infraestructura de red del proveedor de servicios como en la red de los sitios que son parte de este trabajo, se verificó el funcionamiento de Ethernet utilizando comandos de diagnóstico en las interfaces de red, se revisó el funcionamiento de los protocolos de enrutamiento dinámico OSPF y EIGRP ejecutando comandos para verificar las tablas de enrutamiento en los routers y para terminar con esta fase se verificó el funcionamiento de los túneles DMVPN con IPsec generando tráfico desde los SPOKE hacia el HUB, por lo que se cumplió con este objetivo formulado.

Finalmente con respecto a verificar el rendimiento de la red a través de indicadores de desempeño, se verificó el funcionamiento correcto de la red debido a que se estableció diferentes pruebas de diagnóstico, realizando el análisis de los tiempos de retardo a los paquetes ICMP enviados desde un SPOKE hacia el HUB o entre SPOKE, se analizó el comportamiento de la red en términos de jitter, donde se visualizó que no existe variaciones considerables en la latencia de la red y para terminar se revisó si existe paquetes perdidos en las diferentes pruebas de conectividad, donde los resultados fueron exitosos al no encontrar paquetes perdidos en la red.

RECOMENDACIONES

De acuerdo a las conclusiones expuestas en el presente trabajo de investigación, a continuación, se plantean una serie de recomendaciones pertinentes para el "Diseño y simulación de una red datos WAN Ethernet con túneles DMVPN y seguridad IPsec, para interconectar cinco localidades remotas de la Fuerza Aérea Ecuatoriana", las cuales, habiendo sido diseñadas por objetivos, redundan en beneficio de la institución.

En ese sentido frente a nuevas tecnologías y estándares utilizados para el despliegue de redes WAN de alta capacidad que permitan la integración de las infraestructuras de red de área local de sitios remotos, se recomienda se realice un estudio y análisis de la tecnología SD-WAN para la interconexión de sucursales con un sitio matriz, se revise en términos de capacidad, seguridad, confiabilidad, monitoreo y aprovisionamiento de servicios de la red.

Asimismo, se sugiere la instalación de aplicaciones gestores de red utilizando el protocolo SNMP en todos los repartos militares, a fin de que se pueda realizar el monitoreo de los elementos de red en tiempo real y se facilite el análisis estadístico del acceso a los diferentes servicios institucionales, lo cual también servirá para la toma de decisiones frente un crecimiento de las capacidades en la red WAN y tiempos de corte de servicio si lo amerita.

En cuanto al diseño y el dimensionamiento de la red, se sugiere se realice el análisis detallado costo – beneficio, de levantar enlaces redundantes hacia el equipo de red del proveedor de servicios, con la finalidad de garantizar una disponibilidad de la información en todo momento para la institución, aquello permitiría disponer una alta disponibilidad en el acceso a los servicios institucionales alojados en la matriz.

En relación a la simulación de la red en un ambiente controlado mediante el aplicativo GNS3 y en vista que es una plataforma de uso libre, se recomienda realizar simulaciones en plataformas licenciadas como OPNET Modeler, el cual permitirá evaluar rendimientos de una red bajo diversas condiciones planteadas para el estudio, y en su momento también se pueda comparar con la simulación en GNS3.

En lo correspondiente a verificar el rendimiento de la red, se sugiere realizar el análisis de los parámetros que afectan al funcionamiento correcto de la red, haciendo uso de software diseñados para dicho análisis, lo cual permitiría disponer de información estadística en el análisis de los factores a afectan en un momento dado a la red.

BIBLIOGRAFÍA

Angelescu, N., Puchianu, D., Preduscac, G., Circiumarescu, L., & Movila, G. (2017). DMVPN simulation in GNS3 network. *ECAI 2017 - International Conference – 9th Edition.* Targoviste, Romania.

Avendaño, G. M. (2 de febrero de 2018). *http://repositorio.ucsg.edu.ec/.* Obtenido de http://repositorio.ucsg.edu.ec/bitstream/3317/9765/1/T-UCSG-POS-MTEL-90.pdf

Brockners, F. F. (2003). Metro Ethernet - Deploying the Extended Campus Using Ethernet Technology. *Proceedings - Conference on Local Computer Networks, LCN. Vols. 2003-Janua*, (págs. 594-604).

Burke, J., Alissa, I., & Chai, W. (Mayo de 2021). *TechTarget.* Obtenido de https://searchdatacenter.techtarget.com/es/definicion/Ethernet

Cisco. (10 de Agosto de 2005). Obtenido de https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/13669-1.html#eigrp

Cisco. (29 de Agosto de 2005). Obtenido de https://www.cisco.com/c/en/us/support/security/dynamic-multipoint-vpn-dmvpn/series.html

Cisco. (1 de Junio de 2021). Obtenido de https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/data_sheet-c78-732542.html

Cisco. (2021). *CCNA Introducción a los protocolos de enrutamiento dinamico.* Obtenido de https://www.academia.edu/10248775/1_CCNA_Introduccion_a_los_protocolos_de_enrutamiento_dinamico?auto=download

Clark, C. (20 de Enero de 2021). *Copyriright Purple 2021.* Obtenido de https://purple.ai/es/blogs/cual-es-la-diferencia-entre-una-lan-y-una-wan/

De Luz, S. (10 de Junio de 2021). *RZ redes zone.* Obtenido de https://www.redeszone.net/tutoriales/vpn/ipsec-que-es-como-funciona/

Goujon, A. (10 de Septiembre de 2012). *Welivesecurity by eset.* Obtenido de https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/

Guo, L. (2010). Reliability Study of Metro Ethernet. *5th international Conference on Computer Science and Education, Final program and Book of Abstracts.*, (págs. 1024-27).

Hernandez, R., Fernandez, C., & Baptista, P. (2014). *Metodología de la Investigación.* México: McGrawHill.

Huawei. (15 de Noviembre de 2019). *Comunidad Huawei Enterprise.* Obtenido de https://forum.huawei.com/enterprise/es/conociendo-la-arquitectura-b%C3%A1sica-de-una-red-mpls/thread/582304-100237

Huidobro, J., & Millan, R. (2002). *Consultoria Estrtégica en Tecnologías de la Información y Comunicaciones.* Obtenido de https://www.ramonmillan.com/tutoriales/mpls.php#conceptompls

ITESA. (s.f.). *Cisco Networking Academy ITESA*. Obtenido de https://www.itesa.edu.mx/netacad/switching/course/module8/8.1.1.2/8.1.1.2.html

Jaramillo, A. (Noviembre de 2018). *Escuela Politecnica Superior de Chimborazo.* Obtenido de http://dspace.espoch.edu.ec/handle/123456789/9301

Kolahi, S., Mudaliar, K., Zhang, C., & Gu, Z. (2017). Impact of IPSec security on VoIP in different environments. *Ninth International Conference on Ubiquitous and Future Networs*, (pág. 1).

Mehraban, Samiullah, Komil, B. V., & Upadhyay, D. (2018). Deploy Multi Protocol label Switching (MPLS) Using Virtual and Forwarding (VRF). *Proceedings of the 2nd International Conference on Trends in Electronics and informatics, ICOEI 2018. IEEE.*, (págs. 543-48).

Moreno, J. (14 de jULIO de 2021). *OKCLUB.* Obtenido de https://okdiario.com/curiosidades/que-conexion-vpn-que-sirve-1938966

Oña Piña, G. D. (24 de Febrero de 2016). *Repositorio Digital - EPN Facultad de Ingeniería Eléctrica y Electrónica (FIEE)*. Obtenido de http://bibdigital.epn.edu.ec/handle/15000/14922

Peterkin, R., & D., I. (2006). A Hardware Implementation of Layer 2 Mpls. 2.

Siti, U. M., Khairul, P. W., Andrew, F., & Ristanti, I. J. (2018). Performance Evaluation DMVPN Using Routing. *The 6th International Conference on Cyber and IT Service Management (CITSM 2018)*, (pág. 1). Jakarta, Indonesia.

Tamanna, T., & Fatema, T. (2017). MPLS VPN Over mGRE Design and Implementation for a Service Provider's Network Using GNS3 Simulator. *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, (págs. 1-4).

Tanenbaum, A., & Wetherall, D. (2012). *Redes de computadoras.* Mexico: PEARSON EDUCACIÓN.

Ummi, S., Fiade, A., Fathul, M., & Amelia. (2017). Performance Evaluation of Routing Protocol RIPv2, OSPF, EIGRP With BGP. *International Conference on innovative and creative Information Technology*, (pág. 1). Masruroh.

Urra, G. (3 de Enero de 2019). *CCIE: DMVPN.* Obtenido de https://es.linkedin.com/pulse/mis-apuntes-ccie-dmvpn-gabriel-urra-varas

Usca, R. (Febrero de 2018). *Escuela Politecnica de Chimborazo.* Obtenido de http://dspace.espoch.edu.ec/handle/123456789/8112

ANEXOS

Anexo No. 1

Configuración del equipamiento de red, tanto del proveedor como de la institución.

RED DEL PROVEEDOR ISP

Router R1

```
Building configuration...
Current configuration : 1338 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
ip tcp synwait-time 5
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 description #ENLACE WAN R2#
 ip address 10.20.0.1 255.255.255.252
 media-type gbic
 speed 1000
 duplex full
 negotiation auto
!
interface GigabitEthernet1/0
 description #ENLACE WAN R3#
 ip address 10.20.0.5 255.255.255.252
 negotiation auto
!
interface FastEthernet2/0
 description #ENLACE WAN FAE QUITO#
```

```
 ip address 172.16.254.1 255.255.255.252
 speed auto
 duplex auto
!
interface FastEthernet2/1
 no ip address
 shutdown
 speed auto
 duplex auto
!
router ospf 1
 router-id 1.1.1.1
 network 10.20.0.0 0.0.0.3 area 0
 network 10.20.0.4 0.0.0.3 area 0
 network 172.16.254.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
no cdp run
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
End
```

Router R2

```
Building configuration...
Current configuration : 1435 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname R2
!
boot-start-marker
```

```
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
ip tcp synwait-time 5
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 description #ENLACE WAN R1#,
 ip address 10.20.0.2 255.255.255.252
 media-type gbic
 speed 1000
 duplex full
 negotiation auto
!
interface GigabitEthernet1/0
 description #ENLACE WAN R3#,
 ip address 10.20.0.9 255.255.255.252
 negotiation auto
!
interface FastEthernet2/0
 description #ENLACE WAN FAE MANTA#
 ip address 172.16.254.18 255.255.255.252
 speed auto
 duplex full
!
interface FastEthernet2/1
 description #ENLACE WAN FAE SALINAS#
 ip address 172.16.254.14 255.255.255.252
 speed auto
 duplex full
!
router ospf 1
 router-id 2.2.2.2
 network 10.20.0.0 0.0.0.3 area 0
 network 10.20.0.8 0.0.0.3 area 0
 network 172.16.254.12 0.0.0.3 area 0
 network 172.16.254.16 0.0.0.3 area 0
!
ip forward-protocol nd
!
```

no ip http server
no ip http secure-server
!
no cdp run
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
End

Router R3

Building configuration...

Current configuration : 1431 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname R3
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
ip tcp synwait-time 5
!
interface Ethernet0/0
no ip address
shutdown
duplex auto

```
!
interface GigabitEthernet0/0
 description #ENLACE WAN R2#
 ip address 10.20.0.10 255.255.255.252
 media-type gbic
 speed 1000
 duplex full
 negotiation auto
!
interface GigabitEthernet1/0
 description #ENLACE WAN R1#
 ip address 10.20.0.6 255.255.255.252
 negotiation auto
!
interface FastEthernet2/0
 description #ENLACE WAN FAE LATA#
 ip address 172.16.254.5 255.255.255.252
 speed auto
 duplex auto
!
interface FastEthernet2/1
 description #ENLACE WAN FAE GUAYAQUIL#
 ip address 172.16.254.9 255.255.255.252
 speed auto
 duplex auto
!
router ospf 1
 router-id 3.3.3.3
 network 10.20.0.4 0.0.0.3 area 0
 network 10.20.0.8 0.0.0.3 area 0
 network 172.16.254.4 0.0.0.3 area 0
 network 172.16.254.8 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
no cdp run
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
```

```
line vty 0 4
 login
!
End
```

EQUIPAMIENTO DE RED INSTITUCIONAL

Router Quito (HUB)

```
Building configuration...
Current configuration : 1987 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname UIO
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key 6 proyfae address 0.0.0.0 0.0.0.0
!
crypto IPsec transform-set FAE esp-aes 256 esp-sha-hmac
!
crypto IPsec profile proyfae_ma
 set transform-set FAE
!
ip tcp synwait-time 5
!
interface Loopback0
 ip address 190.152.214.1 255.255.255.0
!
```

```
interface Tunnel0
 ip address 10.10.0.1 255.255.255.224
 no ip redirects
 ip mtu 1400
 no ip next-hop-self eigrp 1
 ip nhrp authentication CISCOFAE
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp holdtime 60
 ip nhrp redirect
 ip tcp adjust-mss 1360
 no ip split-horizon eigrp 1
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel protection IPsec profile proyfae_ma
!
interface FastEthernet0/0
 description #ENLACE WAN R1#
 ip address 172.16.254.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description #LAN QUITO#
 ip address 192.168.0.254 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
router eigrp 1
 redistribute static
 network 10.10.0.1 0.0.0.0
 network 192.168.0.0
 auto-summary
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 Loopback0
ip route 172.16.254.0 255.255.255.0 172.16.254.1
!
no ip http server
no ip http secure-server
!
```

```
no cdp log mismatch duplex
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
End
```

Router Latacunga (SPOKE_1)

```
Building configuration...
Current configuration : 1892 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname LATA
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key 6 proyfae address 0.0.0.0 0.0.0.0
!
```

```
crypto IPsec transform-set FAE esp-aes 256 esp-sha-hmac
!
crypto IPsec profile proyfae_ma
 set transform-set FAE
!
ip tcp synwait-time 5
!
interface Tunnel0
 ip address 10.10.0.2 255.255.255.224
 no ip redirects
 ip mtu 1400
 ip nhrp authentication CISCOFAE
 ip nhrp map 10.10.0.1 172.16.254.2
 ip nhrp map multicast 172.16.254.2
 ip nhrp network-id 1
 ip nhrp holdtime 60
 ip nhrp nhs 10.10.0.1
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel protection IPsec profile proyfae_ma
!
interface FastEthernet0/0
 description #ENLACE WAN R3#
 ip address 172.16.254.6 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description #LAN LATACUNGA#
 ip address 192.168.20.254 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
router eigrp 1
 network 10.10.0.2 0.0.0.0
 network 192.168.20.0
 auto-summary
!
```

```
ip forward-protocol nd
ip route 172.16.254.0 255.255.255.0 172.16.254.5
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
End
```

Router Guayaquil (SPOKE_2)

```
Building configuration...
Current configuration : 1892 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GYE
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
crypto isakmp policy 10
```

```
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key 6 proyfae address 0.0.0.0 0.0.0.0
!
crypto IPsec transform-set FAE esp-aes 256 esp-sha-hmac
!
crypto IPsec profile proyfae_ma
 set transform-set FAE
!
ip tcp synwait-time 5
!
interface Tunnel0
 ip address 10.10.0.3 255.255.255.224
 no ip redirects
 ip mtu 1400
 ip nhrp authentication CISCOFAE
 ip nhrp map 10.10.0.1 172.16.254.2
 ip nhrp map multicast 172.16.254.2
 ip nhrp network-id 1
 ip nhrp holdtime 60
 ip nhrp nhs 10.10.0.1
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel protection IPsec profile proyfae_ma
!
interface FastEthernet0/0
 description #ENLACE WAN R3#
 ip address 172.16.254.10 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description #LAN GUAYAQUIL#
 ip address 192.168.40.254 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
```

```
!
router eigrp 1
 network 10.10.0.3 0.0.0.0
 network 192.168.40.0
 auto-summary
!
ip forward-protocol nd
ip route 172.16.254.0 255.255.255.0 172.16.254.9
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
End
```

Router Salinas (SPOKE_3)

```
Building configuration...
Current configuration : 1895 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SALINAS
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
!
multilink bundle-name authenticated
```

```
!
archive
 log config
  hidekeys
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key 6 proyfae address 0.0.0.0 0.0.0.0
!
crypto IPsec transform-set FAE esp-aes 256 esp-sha-hmac
!
crypto IPsec profile proyfae_ma
 set transform-set FAE
!
ip tcp synwait-time 5
!
interface Tunnel0
 ip address 10.10.0.4 255.255.255.224
 no ip redirects
 ip mtu 1400
 ip nhrp authentication CISCOFAE
 ip nhrp map 10.10.0.1 172.16.254.2
 ip nhrp map multicast 172.16.254.2
 ip nhrp network-id 1
 ip nhrp holdtime 60
 ip nhrp nhs 10.10.0.1
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel protection IPsec profile proyfae_ma
!
interface FastEthernet0/0
 description #ENLACE WAN R2#
 ip address 172.16.254.13 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description #LAN SALINAS#
 ip address 192.168.30.254 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
```

```
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
router eigrp 1
 network 10.10.0.4 0.0.0.0
 network 192.168.30.0
 auto-summary
!
ip forward-protocol nd
ip route 172.16.254.0 255.255.255.0 172.16.254.14
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
End
```

Router Manta (SPOKE_4)

```
Building configuration...
Current configuration : 1891 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname MANTA
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
```

```
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key 6 proyfae address 0.0.0.0 0.0.0.0
!
crypto IPsec transform-set FAE esp-aes 256 esp-sha-hmac
!
crypto IPsec profile proyfae_ma
 set transform-set FAE
!
ip tcp synwait-time 5
!
interface Tunnel0
 ip address 10.10.0.5 255.255.255.224
 no ip redirects
 ip mtu 1400
 ip nhrp authentication CISCOFAE
 ip nhrp map 10.10.0.1 172.16.254.2
 ip nhrp map multicast 172.16.254.2
 ip nhrp network-id 1
 ip nhrp holdtime 60
 ip nhrp nhs 10.10.0.1
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel protection IPsec profile proyfae_ma
!
interface FastEthernet0/0
 description #ENLACE WAN R2#
 ip address 172.16.254.17 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description #LAN MANTA#
 ip address 192.168.10.254 255.255.255.0
 duplex auto
 speed auto
```

```
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
router eigrp 1
 network 10.10.0.5 0.0.0.0
 network 192.168.10.0
 auto-summary
!
ip forward-protocol nd
ip route 172.16.254.0 255.255.255.0 172.16.254.18
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
end
```

Anexo No. 2
Encuesta

UNIVERSIDAD TECNOLÓGICA ISRAEL

MAESTRÍA EN GESTIÓN DE LAS TELECOMUNICACIONES

ENCUESTA AL PERSONAL TECNICO DE LOS DEPARTAMENTOS TIC DE LOS REPARTOS QUITO, GUAYAQUIL, LATACUNGA, SALINAS Y MANTA

Estimados oficiales/aerotécnicos:

Se está desarrollando una investigación sobre la calidad en los enlaces WAN (MODE), seguridad en los enlaces de datos y el acceso a los servicios institucionales, por lo que solicito contestar la siguiente encuesta de una manera honesta, pues sus resultados ayudarán a plantear una solución al problema.

Marque con una X la respuesta que considere correcta.

N°	PREGUNTA	SIEMPRE	A VECES	NUNCA
1	¿Con qué frecuencia su reparto militar accede a los servicios institucionales (videoconferencia, telefonía MODE, portales FAE, correo institucional, etc.)?			
2	¿A menudo su reparto se queda sin enlace a la red WAN (COMACO/MODE)?			
3	Cuándo existe fallas en la red MODE y su reparto se queda sin servicios, ¿El problema es solucionado de forma inmediata)?			
4	¿Su proveedor de servicios en la red WAN (COMACO) dispone de una mesa de ayuda 24x7 para un eficiente soporte técnico?			
5	¿Considera usted que la capacidad de ancho de banda asignado por el proveedor de la WAN (COMACO), abastece los requerimientos del reparto?			
6	¿Su reparto dispone de un equipo o sistema de seguridad perimetral acorde a la tecnología actual, con licenciamiento vigente que garantice la seguridad de la información?			
7	El proveedor de servicios en la WAN (COMACO) garantiza la seguridad de la información en sus enlaces			
8	Considera una amenaza de seguridad el hecho de contratar internet de forma local en su reparto, tomando en cuenta que no se dispone de equipamiento de seguridad actualizado			

Gracias por la colaboración

Anexo 3

Validación del instrumento de investigación por especialistas

UNIVERSIDAD TECNOLÓGICA ISRAEL

MAESTRÍA EN GESTIÓN DE LAS TELECOMUNICACIONES

FORMATO PARA LA VALIDACIÓN DE ESPECIALISTAS

Nombres: Raúl Alfredo
Apellidos: Hernández Viteri
Cedula: 0909733651
Título profesional (cuarto nivel) : Conectividad y Redes de Telecomunicaciones
Fecha: 23/08/2021
Entrevistador: Angel Edison Guzmán Flores

No.	Pregunta	Pertinente	No pertinente
Determinar problemas de conectividad hacia el sitio matriz			
1	¿Con qué frecuencia su reparto militar accede a los servicios institucionales (videoconferencia, telefonía MODE, portales FAE, correo institucional, etc.)?	X	
2	¿A menudo su reparto se queda sin enlace a la red WAN (COMACO/MODE)?	X	
3	Cuándo existe fallas en la red MODE y su reparto se queda sin servicios, ¿El problema es solucionado de forma inmediata)?	X	
4	¿Su proveedor de servicios en la red WAN (COMACO) dispone de una mesa de ayuda 24x7 para un eficiente soporte técnico?	X	
Determinar problemas de ancho de banda asignado por el proveedor de servicios			
5	¿Considera usted que la capacidad de ancho de banda asignado por el proveedor de la WAN (COMACO), abastece los requerimientos del reparto?	X	
Determinar las falencias en cuanto a la seguridad de la información			
6	¿Su reparto dispone de un equipo o sistema de seguridad perimetral acorde a la tecnología actual, con licenciamiento vigente que garantice la seguridad de la información?	X	
7	El proveedor de servicios en la WAN (COMACO) garantiza la seguridad de la información en sus enlaces	X	
8	Considera una amenaza de seguridad el hecho de contratar internet de forma local en su reparto, tomando en cuenta que no se dispone de equipamiento de seguridad actualizado	X	

Observación: Las preguntas establecidas son pertinentes para el caso de estudio en curso.

RAUL ALFREDO HERNANDEZ VITERI

Firma

UNIVERSIDAD TECNOLÓGICA ISRAEL

MAESTRÍA EN GESTIÓN DE LAS TELECOMUNICACIONES

FORMATO PARA LA VALIDACIÓN DE ESPECIALISTAS

Nombres: César Marcelo

Apellidos: Erazo Llamatumbi

Cedula: 1714745716

Título profesional (cuarto nivel) : Magister en Redes de Información y Conectividad

Fecha: 23 de agosto de 2021

Entrevistador: Angel Edison Guzmán Flores

No.	Pregunta	Pertinente	No pertinente
Determinar problemas de conectividad hacia el sitio matriz			
1	**¿**Con qué frecuencia su reparto militar accede a los servicios institucionales (videoconferencia, telefonía MODE, portales FAE, correo institucional, etc.)**?**	X	
2	¿A menudo su reparto se queda sin enlace a la red WAN (COMACO/MODE)?	X	
3	Cuándo existe fallas en la red MODE y su reparto se queda sin servicios, ¿El problema es solucionado de forma inmediata)?	X	
4	¿Su proveedor de servicios en la red WAN (COMACO) dispone de una mesa de ayuda 24x7 para un eficiente soporte técnico?	X	
Determinar problemas de ancho de banda asignado por el proveedor de servicios			
5	¿Considera usted que la capacidad de ancho de banda asignado por el proveedor de la WAN (COMACO), abastece los requerimientos del reparto?	X	
Determinar las falencias en cuanto a la seguridad de la información			
6	¿Su reparto dispone de un equipo o sistema de seguridad perimetral acorde a la tecnología actual, con licenciamiento vigente que garantice la seguridad de la información?	X	
7	El proveedor de servicios en la WAN (COMACO) garantiza la seguridad de la información en sus enlaces	X	
8	Considera una amenaza de seguridad el hecho de contratar internet de forma local en su reparto, tomando en cuenta que no se dispone de equipamiento de seguridad actualizado	X	

Observación:
Las preguntas son aplicables de acuerdo a los indicadores que se va a investigar.

Firma