ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“MEJORAMIENTO EN EL USO DE LOS ENLACES WAN PARA CLIENTES CORPORATIVOS EN UNA EMPRESA DE TELECOMUNICACIONES USANDO LA SOLUCIÓN DE CISCO INTELLIGENT WAN.”

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGISTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

Autores:

GARCÍA VARGAS JUAN FERNANDO

NARVÁEZ ZAMBRANO GALO ERNESTO

Guayaquil – Ecuador

2018

AGRADECIMIENTO

A Dios, por enseñarme siempre a ser una mejor persona con cada obstáculo que se presente, por permitirme aprender de mis errores, y por darme la oportunidad de gozar de una vida junto a las personas que amo,

A toda mi familia, por hacerme sentir su apoyo incondicional en cada palabra de aliento y en cada oración.

A mi director de tesis M.Sc. Jorge Magallanes, por su asesoría en la elaboración de este trabajo.

A mi jefe, Andrey Arias por brindarme el apoyo en los proyectos personales de superación que he tenido.

A la Escuela Superior Politécnica del Litoral, por darme su aval para la realización de la Maestría.

Juan Fernando García Vargas

A DIOS Padre, amado que permite la vida sobre la tierra. El mismo que guía mi camino para poder ser un hombre de bien ya que sin el este esfuerzo no se podría hacer realidad.

A mis padres, por haberme ayudado a lo largo de mi vida.

A mi esposa Sofía, a mis hijos Kevin y Alejandro por ser parte de este logro.

A mis hermanos, por todos sus gestos amables.

A mi compañero Juan García y a nuestro director M.Sc Jorge Magallanes, por haber participado conmigo de este proyecto.

Galo Ernesto Narváez Zambrano

DEDICATORIA

Dedico este trabajo a mi madre María Vargas, cuyo ejemplo, consejos, amor y enseñanzas me han impulsado a ser mejor cada día y no rendirme a lo largo del camino. Mi ejemplo de vida.

A mi abuelita Targelia Garcés, que con su cariño, ternura, apoyo y oraciones me han dado la fortaleza que se necesita para avanzar y cumplir mis objetivos.

A mi enamorada María José Rendón, por estar siempre presente dándome su apoyo, consejo, ánimos, amor y comprensión, mi pilar de vida, al cual le agradezco a Dios por haber puesto en mi camino. ¡Gracias!

Juan Fernando García Vargas

Dedico mi trabajo a mi padre celestial que me permite seguir adelante día a día.

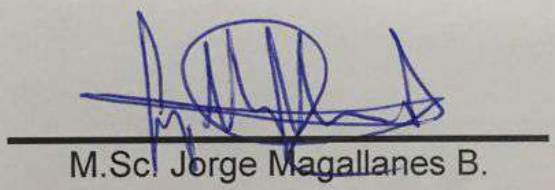
A mis padres Celina Zambrano y Galo Narváez que son un pilar fundamental en mi vida.

Galo Ernesto Narváez Zambrano

TRIBUNAL DE SUSTENTACIÓN

Mgs. Lenin Freire C.

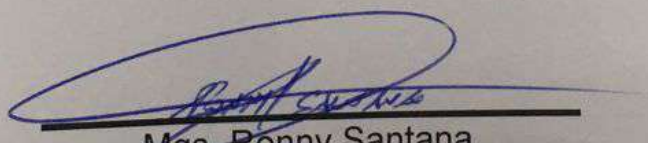
DIRECTOR MSIG



M.Sc. Jorge Magallanes B.

DIRECTOR DEL PROYECTO

DE GRADUACIÓN



Mgs. Ronny Santana.

MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL".

(Reglamento de Graduación de ESPOL)

.....

Juan Fernando García Vargas

.....

Galo Ernesto Narváez Zambrano

RESUMEN

En el presente trabajo se propone determinar el mejoramiento que pueden tener los enlaces de red de área amplia para una empresa al implementar la solución de CISCO Red de Área Amplia Inteligente. Para ello, se lleva a cabo un análisis de los componentes que son parte de la solución y cada tecnología asociada para su correcto funcionamiento.

La solución permite que empresas con enlaces de red de área amplia redundantes, puedan ser utilizados de forma activa – activa simultáneamente para el tráfico de los servicios que defina el administrador de red. Con base en umbrales de rendimiento, la solución monitorea el estado de cada enlace de red de amplia, y en caso de que un enlace no cumpla con los criterios de calidad de servicio definidos, la solución envía el tráfico por el enlace que pueda satisfacer dichas características. Adicional se provee de un mecanismo para incrementar la seguridad en el envío de paquetes entre localidades al cifrar todo el tráfico que fluye por los enlaces de red de área amplia, logrando disminuir los riesgos asociados a la perdida de la integridad, confidencialidad y disponibilidad de la información.

En el capítulo 2 de este trabajo se expone el marco teórico asociado a la arquitectura de los enlaces de red de área amplia, una reseña de los motivos que han incrementado la demanda de ancho de banda relacionado a estos enlaces, y una breve descripción de los pilares en los cuales se fundamenta la solución de iWAN. Estos pilares son importantes para determinar la forma como se debe aplicar la solución para obtener el mayor beneficio de los enlaces de red de área amplia.

En el capítulo 3 de este trabajo hacemos un análisis sobre la infraestructura de la empresa, identificando los servicios que se utilizarán para demostración de la solución, la forma de operación de los servicios y aplicaciones, así como un análisis de los riesgos asociados a la perdida en la seguridad en la información.

En el capítulo 4 se realizan los análisis asociados al diseño actual de la red de la empresa, el diseño de la solución de iWAN aplicada para el escenario piloto de pruebas, y los requerimientos que se necesita cumplir para que un enrutador soporte la implementación de las tecnologías. De la misma forma se definen los parámetros que necesita la solución para monitoreo de tráfico de servicios, y en qué condiciones la solución toma la decisión de enviar un tráfico por un enlace de red de área amplia determinado.

El capítulo 5 detalla el proceso de implementación de la solución en el escenario definido para la empresa. Se indican las consideraciones que se deben tomar para la configuración de cada tecnología asociada a la solución, así como la verificación que se encuentren operando correctamente. Se define el plan de pruebas que se tomará en consideración, y la forma de medición para los parámetros de interés en la verificación de eficiencia de la solución.

Finalmente, el Capítulo 6 presenta los resultados obtenidos por el proyecto en los ambientes de pruebas que se han definido. Es en este capítulo donde se determina la eficiencia de la solución respecto al mejoramiento en el uso de ancho de banda de los enlaces de red de área, tiempos de respuesta de las aplicaciones, y el incremento en la seguridad del tráfico que fluye por cada enlace.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

ISP:	Proveedor de servicios de internet, Internet service provider por sus siglas en ingles.
IaaS:	Infraestructura como Servicio, Infraestructure as Service por sus siglas en ingles.
MPLS:	Conmutación de etiquetas multiprotocolo, Multiprotocol Label Switching por sus siglas en ingles.
VRF:	Enrutamiento Virtual y Reenvío, Virtual Routing and Forwarding por sus siglas en ingles
PaaS:	Plataforma como servicio, Platform as a Service por sus siglas en ingles
WAN:	Red de área amplia, Wide Area Network por sus siglas en ingles
IP:	Protocolo de Internet, Internet Protocol por sus siglas en ingles
TCP:	Protocolo de Control de Transmisión , Transmission Control Protocol por sus siglas en ingles

UDP: Protocolo de Datagrama de Usuario, User Datagram Protocol por sus siglas en ingles

ICMP: Protocolo de Mensajes de Control de Internet, Internet Control Message Protocol por sus siglas en ingles

FTP: Protocolo de Transferencia de Ficheros, File Transfer Protocol por sus siglas en ingles

iWan: Red de área amplia inteligente, Inteligent Wide área network por sus siglas en ingles

DMVPN: Red privada virtual dinámica multipunto, Dynamic Multipoint Virtual Private Network por sus siglas en ingles.

PfR: Enrutamiento de rendimiento, Performance Routing por sus siglas en ingles.

IPSEC: Seguridad del protocolo de internet, Internet Protocol security Routing por sus siglas en ingles.

RTT Tiempo de retransmisión, round-trip time por sus siglas en ingles.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la actualidad las empresas requieren tener sus localidades interconectadas con la finalidad de reducir los tiempos de operación para sus actividades, al hacer uso de servicios en tiempo real que se encuentran separados geográficamente. Para interconectar dichas localidades se hace uso de los enlaces de red de área amplia. A su vez, la disponibilidad de dichos servicios y la importancia de los enlaces para establecer la conectividad llevan a la empresa a buscar la forma de adquirir varios enlaces para proveer alta disponibilidad en caso de falla de uno de los enlaces.

Tradicionalmente el esquema utilizado al brindar un servicio de alta disponibilidad se da en la forma activo-pasivo, es decir, solo un enlace es utilizado para brindar los servicios, y en caso de fallar ese enlace, otro toma su lugar. Esto nos lleva a una subutilización de los enlaces de área amplia, pero a su vez, ocasiona que, en caso de presentarse saturación del ancho de banda en el enlace principal, todos los servicios que fluyen a través de él se vean afectados. Adicional con relación a los tiempos de conmutación en caso de la caída del enlace principal, con una solución tradicional los tiempos de conmutación toman valores elevados que para una empresa con servicios críticos y que sean 24/7 no pueden permitir tener, ni afectaciones durante tiempos prolongados.

La seguridad en la forma de manejar el tráfico en una red tradicional es comúnmente derivada al proveedor de servicios, y por tal, no se toman medidas adicionales para proteger la integridad y confidencialidad de la información.

El presente trabajo es presentado como una propuesta para mejorar la utilización de los enlaces de red de área amplia a partir de la implementación de la solución de CISCO Red de Área Amplia Inteligente, generando un uso de los enlaces de forma activo-activo y a su vez, determinar qué tipo de tráfico debe atravesar un enlace de red de área amplia especifico basándose en el monitoreo del nivel de calidad de servicio que le pueda proveer. Adicional, la solución provee de su propio mecanismo para cifrar el tráfico que atraviesa los enlaces de red de área amplia, incrementando de esta forma la seguridad que se brinda a la información que maneja la empresa.

CAPÍTULO 1

GENERALIDADES

1.1 ANTECEDENTES.

El sector empresarial ha ido evolucionando de una forma rápida en los últimos años en lo que respecta a tecnologías de información. El desarrollo de aplicaciones ha permitido impulsar la productividad al resolver problemáticas específicas de varios sectores en la empresa. Dichas aplicaciones típicamente se encuentran alojadas en un servidor que procesa los requerimientos acordes a cada necesidad específica, y son los clientes los cuales se conectan a dicho servidor para hacer uso de ella. Inicialmente los servidores de aplicaciones se encontraban

físicamente dentro de la red empresarial, de tal forma que los usuarios tenían conexión a través de una red de área local y hacían uso de los servicios que necesitaban. Con el paso del tiempo, las empresas comienzan a expandir sus ubicaciones abriendo sucursales, y a su vez, abriendo un nuevo requerimiento para conectar a los usuarios hacia los servidores de aplicaciones que se encuentran remotamente en otra localidad. Para establecer dichas conexiones, las empresas hacen uso de las llamadas redes de área amplia que permiten interconectar dos localidades que se encuentran muy alejadas de forma geográfica, por lo cual, la presencia de las redes de área amplia comenzó a tomar un papel importante en mantener la calidad de los servicios que se brindan a toda la empresa en cada localidad que posea y que tenga la necesidad de interconectar.

No obstante, las demandas de ancho de banda continúan con su rápido y fuerte despliegue por la incorporación de nuevas tecnologías, como por ejemplo las aplicaciones que se encuentran en la nube, infraestructuras como servicio (Infraestructure as Service, IaaS por sus siglas en ingles), plataformas como servicio (Platform as a Service, PaaS por sus siglas en ingles), usuarios que hacen uso del teletrabajo, y es por tal motivo que se extiende la necesidad de hacer un mejor uso de los enlaces de red de

área amplia, de tal forma que podamos satisfacer las necesidades específicas de los clientes en lo que respecta a tiempos de respuesta asociados al canal, disponibilidad de las aplicaciones y seguridad en la información.

1.2 DESCRIPCIÓN DEL PROBLEMA.

El problema planteado se sitúa en una empresa de telecomunicaciones que ofrece servicio de datos a clientes corporativos. Dichos clientes requieren una conexión entre las diferentes sucursales que posean, y lo realizan a través de enlaces de datos corporativos contratados con la empresa de telecomunicaciones.

Los enlaces corporativos son realizados a través de conexiones de Red de Área Amplia (Wide Área Network o WAN por sus siglas en ingles) que son proporcionadas por el proveedor de servicios, y mediante ellas se establece la conexión: entre sucursales, o de una sucursal hacia un punto principal denominado matriz para el cliente.

Las sucursales de los clientes corporativos típicamente requieren de anchos de banda menores a 2048 Mbps, los cuales son utilizados para

los diferentes servicios que desee brindar la compañía, esto es, conectividad entre las aplicaciones de la sucursal hacia la matriz, servicios de voz y video, servicios de acceso a internet, etc. Y es justamente por la diversidad de servicios que mantienen los clientes, que dichos enlaces WAN utilizan su máximo de capacidad, llevando a la degradación de los servicios que se encuentren en ejecución. Esto a su vez lleva a los clientes a rediseñar sus servicios internos, así como implementar políticas de restricción de aplicación con la finalidad de evitar consumo excesivo de ancho de banda.

Por otro lado, el cliente confía en la seguridad brindada por el Proveedor de Servicios de Internet (ISP) en la transmisión de los datos, pero no se provee de su propio mecanismo para cifrar la información transmitida entre los diversos puntos de acceso. Esto conlleva a que las sucursales, por ser consideradas como puntos remotos, típicamente no posean un ajuste adecuado respecto a la seguridad de la información y puedan ser vulnerables a diferentes tipos de ataques, como por ejemplo, un ataque de Hombre en el Medio (Man in The Middle) que consiste en que un atacante simule ser un dispositivo válido que se encuentre en medio de la ruta del tráfico de datos, y así lograr interceptar la información que atraviesa el circuito, de manera que, al no encontrarse cifrada la información, puede ser visualizada, interpretada e incluso alterada por el

atacante, ocasionando que información sensible de la empresa o de sus clientes, sea divulgada y utilizada por terceros para generar un perjuicio económico o en su imagen corporativa.

1.3 SOLUCIÓN PROPUESTA.

La solución que se plantea consiste en analizar, diseñar e implementar una solución de CISCO llamada Red de Área Amplia Inteligente (Intelligent WAN o iWAN), la cual permitirá mantener un control de ruta de forma inteligente, un mejor rendimiento y utilización de los circuitos WAN, así como cifrado del tráfico que atraviesa los enlaces hacia cada destino. Para esto, la solución se fundamenta en tres enfoques principales:

- Lograr la independencia del transporte mediante el uso de la tecnología de Redes Privadas Virtuales Multi Punto (Dynamic Multipoint VPN o DMVPN), la cual nos permite formar túneles privados desde una localidad remota hacia un punto central o también denominado matriz, sin importar el medio de transporte que se utilice, sea Internet, una red provista por un ISP usando Conmutación de Etiquetas Multiprotocolo (MultiProtocol Label

Switching o MPLS), o incluso un acceso provisto por una red celular.

- Control de camino inteligente a través de la tecnología Enrutamiento por Rendimiento (Performance Routing o PfR), la cual nos permite monitorear el rendimiento de los enlaces WAN con base en diversos parámetros como el retardo, utilización o degradación del enlace, y en caso de presentar una congestión, el controlador maestro sea quien puede tomar decisiones basadas en criterios específicos del usuario para que el tráfico de datos sensible a retardos, pueda usar un enlace que se encuentra menos utilizado y de esta forma, evitar una degradación del servicio.
- Conectividad segura a través de un conjunto de protocolos denominado Seguridad del Protocolo de Internet (IPSec), el cual se encarga de asegurar que solo los puntos remotos que cumplan con los parámetros de autenticación con la matriz puedan levantar los túneles cifrados, y además, que el flujo de paquetes que los atraviesan no pueda ser alterado durante toda su trayectoria.

Con esta solución, se obtendrá un mejor uso del ancho de banda en cada punto del cliente, lo que, a su vez, permitirá tener un mejor rendimiento en las diversas aplicaciones que sean utilizadas, y en caso de

congestión, la solución provee un mecanismo para distribuir el tráfico con criterios de calidad de servicio, que permitan tener prioridad de cierto tráfico sobre otros que el cliente considere de menor impacto en su operación.

1.4 OBJETIVO GENERAL.

Mejorar el uso del ancho de banda y brindar mayor seguridad a los enlaces de Red de Área Amplia de los clientes corporativos en una empresa de Telecomunicaciones, usando la solución de CISCO: Red de Área Amplia Inteligente (Intelligent WAN o iWAN).

1.5 OBJETIVOS ESPECÍFICOS

- ✓ Analizar los diferentes componentes de la solución de iWAN que se pueden aplicar a una red corporativa con la finalidad de mejorar los recursos asociados a los circuitos de Red de Área Amplia de los clientes.
- ✓ Diseñar e implementar la solución de iWAN en una topología de un cliente piloto para una empresa de telecomunicaciones.
- ✓ Evaluar los resultados obtenidos luego de la implementación de la solución y verificar el mejoramiento en el uso del ancho de banda del circuito.

1.6 METODOLOGÍA

Por el lado técnico, se comenzará con el análisis de los componentes requeridos para implementar la solución, así como los requerimientos necesarios de los equipos donde se realice la configuración. Adicional se realizará una medición inicial del uso promedio del ancho de banda en cada localidad, así como las aplicaciones que serán consideradas como parte del mejoramiento. Se resaltará la importancia de asegurar la información que es compartida a través de los circuitos, haciendo un análisis de las ventajas que provee cifrar los datos mediante esta solución.

Para verificar los resultados de aplicar la solución iWan, se implementará la solución sobre una topología piloto de prueba que consiste en dos sucursales y una matriz representadas en la Figura 1.1:

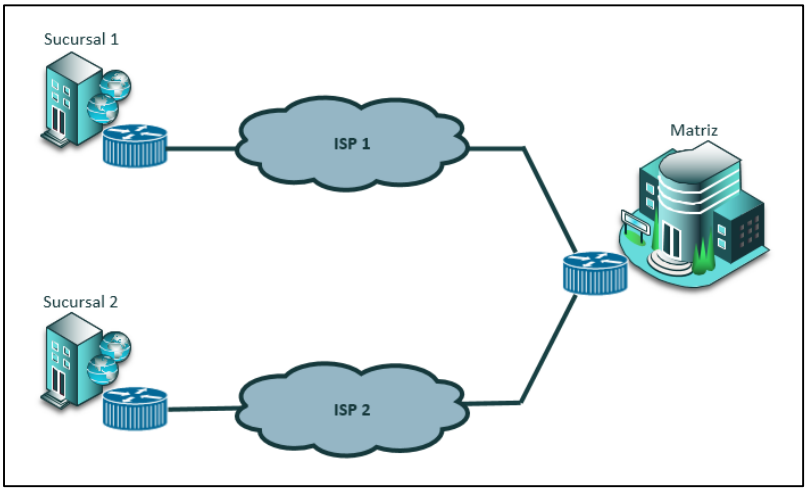


Figura 1.1 Topología de una matriz y sus sucursales

Las mediciones se realizarán sobre los servicios relevantes para la empresa, los cuales son: Servicio de Transferencia de Archivos, Servicios de Voz sobre IP, y Servicio de Comunicación entre dos dispositivos a través de un Servidor de Aplicaciones Generales, los cuales se encuentran instalados físicamente en la Matriz de Operaciones.

La toma de decisiones en los enlaces estará definida por el orden de importancia de la aplicación para la operación del usuario de la empresa. Si los usuarios de la empresa consideran que el servicio de voz es crítico para sus operaciones, se le asigna la prioridad más importante en un orden jerárquico y así, para los demás servicios de la empresa.

Los resultados que esperamos obtener nos permitirán comparar el funcionamiento y rendimiento de una red con la solución de iWAN aplicada, frente a los parámetros obtenidos en las mediciones de rendimiento de la red actual operando sin la solución, garantizando que no exista una afectación sobre los enlaces de otros clientes de la empresa. Se usará como ventaja la arquitectura de MPLS en la cual los diversos clientes se encuentran operando sobre su propia tabla de

enrutamiento independiente haciendo uso de la tecnología de Virtual Routing and Forwarding (VRF).

Con las configuraciones realizadas, se obtendrá un mejor uso del ancho de banda utilizado por los puntos del cliente, manteniendo la correcta operación de cada servicio. A su vez, se confirmará el adecuado cifrado de los datos que pasan a través del circuito, obteniendo de esa forma, un nivel mayor de seguridad en la integridad y confidencialidad de la información. Finalmente se tomará en consideración el manejo de enrutamiento inteligente al permitir que la solución, manipule el tráfico de diferentes aplicaciones a través de varios canales en caso de que el punto del cliente tenga redundancia en el circuito WAN.

El mejoramiento en el uso del ancho de banda generará liberación de tráfico interno a la empresa de telecomunicaciones, el cual, a su vez, será reutilizado para generar una mayor activación de clientes sin que deban tener tiempos extendidos de espera que estén relacionados a trabajos para incrementar la capacidad de la red. Por otro lado, el cliente obtendrá un circuito que le permita dar prioridad al manejo de tráfico en aplicaciones sensibles a pérdidas o retardos, viendo como resultado una mejor eficiencia y disponibilidad de estos, disminuyendo el riesgo asociados a ataques cibernéticos y evitar pérdidas económicas

a la compañía mediante el uso de envío de datos cifrados a través del circuito de comunicación.

Para la evaluación de eficiencia de la solución se tomarán en consideración los siguientes indicadores: Utilización del ancho de banda del circuito, Tiempo de retransmisión en caso de congestión, Tiempo de retransmisión sin congestión, Tiempo de conmutación en caso de caída de un enlace. Con estos indicadores, evaluaremos los valores antes y después de la implementación a fin de confirmar el mejoramiento en la eficiencia del uso del ancho de banda con la solución.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1 ARQUITECTURA DE REDES WAN

Las redes de los ordenadores pueden ser de varios tipos dependiendo del criterio de clasificación. Bajo el criterio de clasificación por extensión geográfica las redes pueden ser de cuatro tipos: Redes de Área Local (LAN), Redes de Área Metropolitana (MAN), Redes de Área Amplia (WAN), y Redes de Área Privada (PAN). Según se puede observar en la Figura 2.1.

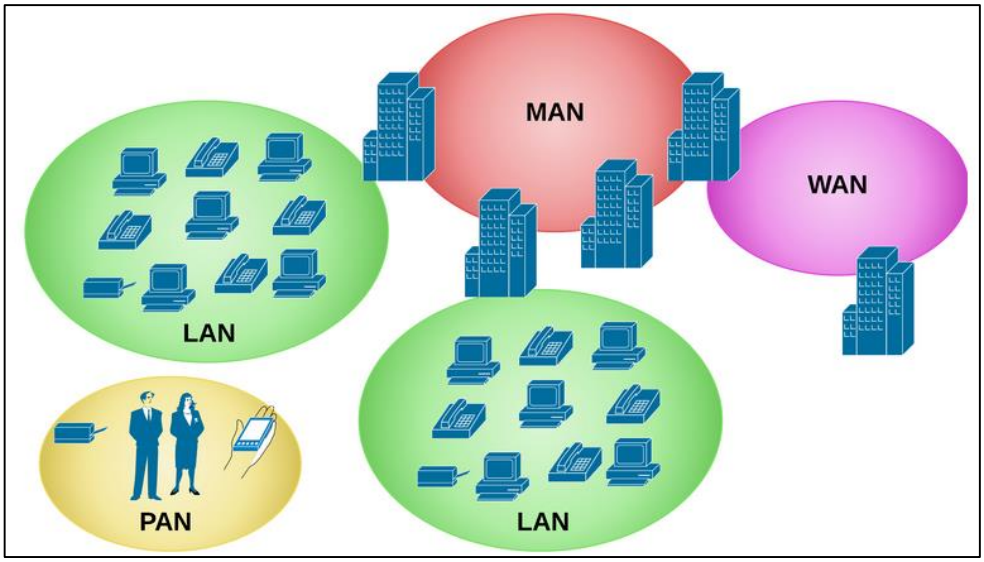


Figura 2.1 Tipo de redes basadas en el área geográfica

Las Redes de Área Local son redes que se consideran geográficamente localizadas en un área pequeña, dentro de lo cual se puede considerar una escuela, un edificio, un hospital, etc. Su principal uso se da para interconectar dispositivos de uso personal dentro de esta área, ya sea una computadora, celulares, impresoras, etc. Típicamente se considera que estas redes se encuentran limitadas en tamaño, pero esto a su vez es compensado gracias a los altos valores de ancho de banda que pueden alcanzar.

Las Redes de Área Metropolitana son redes que abarcan un área mayor que las redes de área local, pudiéndose extender hasta unos 100 Km abarcando toda un área de una organización o incluso de una ciudad.

Sin embargo, ya es concepto en desuso dado que la segmentación en bloques más pequeños de área locales produce una mejor administración de los servicios que se posean dentro de la misma, así como infraestructuras relacionadas.

Las redes de Área Amplia son redes que se extienden sobre áreas geográficas extensas, que pueden abarcar países, regiones o incluso continentes. Básicamente se componen de muchas subredes que están comunicadas por dispositivos de interconexión. Las redes de área extensa brindan la posibilidad de que las redes de áreas locales o metropolitanas, obtengan mejoras en los servicios que éstas necesiten, puesto que gracias a las redes WAN éstas pueden transmitir grandes volúmenes de información, aunque las velocidades sean menores a las de las redes de área local debido a las grandes distancias que la información debe viajar; sin embargo estas redes le han facilitado las labores a la sociedad en general, principalmente a las empresas que están en un crecimiento continuo. A pesar de que este tipo de redes se utilice para interconectar LAN distantes, al utilizar dos dispositivos WAN como los enrutadores e interconectarlos, se forma una red de área extensa en distancias limitadas, pero esa interconexión es muy costosa por esta razón es comúnmente utilizada para entrelazar redes geográficamente distantes. [1]

Las redes de Área Privada son redes que se limitan a una administración personal, y no abarca más de alrededor de cinco dispositivos.

Las redes de área amplia principalmente proveen la conectividad requerida para las redes de área local que se expanden a través de cierto espacio geográfico. El diseño y mantenimiento de las redes de área amplia puede agregar cierto grado de complejidad debido a la variedad de tecnologías de transporte existentes, limitaciones asociadas, costos y otros factores relevantes en el momento de tomar una decisión de por cual optar.

La conectividad de las redes de área amplia usa una variedad de tecnologías, pero los métodos predominantes vienen a través de los proveedores de servicio con tres soluciones principales: Circuitos arrendados, Internet, y Redes privadas virtuales basadas en Conmutación multi protocolos por etiquetas (MPLS VPNs por sus siglas en inglés). [2]

2.1.1 CIRCUITOS ARRENDADOS

Los circuitos arrendados son enlaces provistos por los proveedores de servicio para conectar dos localidades a un costo

específico. Las ventajas de estos enlaces radican en un ajuste determinado del ancho de banda solicitado por el cliente, y una seguridad implícita dado que es un enlace dedicado. Sin embargo, hay que tomar en consideración que, al ser un circuito dedicado arrendado, es la responsabilidad del cliente si obtiene el máximo uso del mismo o si tiene una subutilización del canal. Según se puede observar en la Figura 2.2.

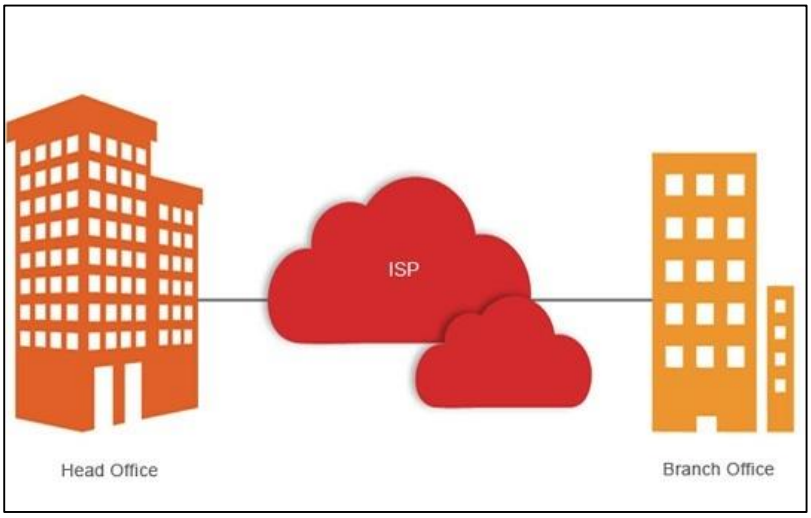


Figura 2.2 Circuitos arrendados

2.1.2 INTERNET

El Internet fue creado originalmente basado en las necesidades del departamento de defensa de los Estados Unidos, con la finalidad de permitir la comunicación incluso si un segmento de red fuese destruido. La arquitectura de Internet ha evolucionado

de tal forma que ahora puede soportar varios protocolos de red como es el caso de IPv4 e IPv6, y consiste en una red pública expandida globalmente que interconecta a múltiples proveedores de servicio. Un beneficio clave de usar el Internet como el medio de transporte de red de área amplia, es que ambas localidades no necesitan usar el mismo proveedor de servicio. Una empresa puede fácilmente establecer conectividad entre varias localidades usando diferentes proveedores de servicio. [2]

Cuando una empresa compra conectividad a través del Internet, el ancho de banda se encuentra garantizado solo para las redes bajo el control del mismo proveedor de servicio. Si el camino entre las redes atraviesa varios proveedores de servicio, el ancho de banda no es garantizado dado que el enlace de interconexión puede ser sobre subscrito dependiendo de los arreglos entre proveedores de servicio. Si existe un problema de congestión en el enlace, se puede agregar retardo o perdida de paquetes mientras se atraviesa los enlaces de interconexión. [2]

Como ejemplo podemos analizar la siguiente situación. En la Figura 2.3, podemos observar una interconexión contratada por una empresa para dos localidades (1 y 2) a través de un enlace de Internet. La empresa ha contratado un enlace de 1 Gbps con un proveedor de servicio de internet X. Observamos que dicha conexión, atraviesa dos proveedores de servicio (Y y Z) antes de llegar a su destino en la localidad 2 de la empresa. Las interconexiones entre proveedores de servicio son de 10 Gbps para conectar el proveedor de servicio X con el Y, y de 20 Gbps para conectar el proveedor de servicio Y con el Z.

Bajo condiciones normales, el tráfico de 1Gbps de la localidad 1 puede atravesar el camino indicado sin inconvenientes hasta llegar a la localidad 2, es decir, cuando no existe saturación.

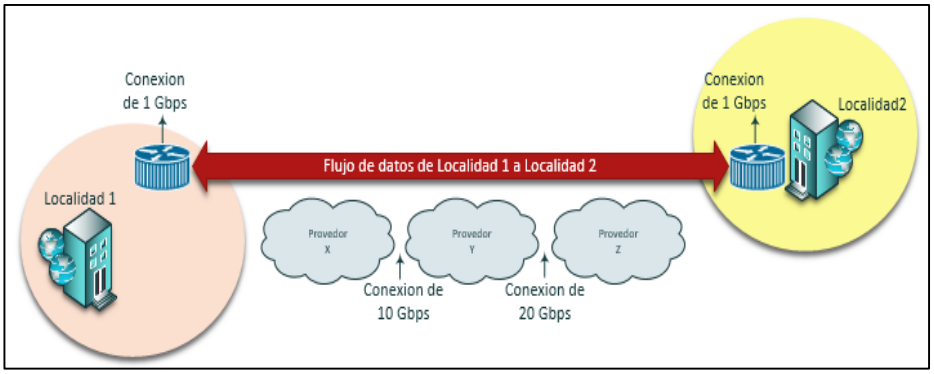


Figura 2.3 Diagrama de interconexión

En la figura 2.4, observamos un nuevo enlace contratado para que la localidad 1 se interconecte con la localidad 3, con un ancho de banda de 10Gbps. Podemos notar que esta nueva interconexión tiene que atravesar el enlace entre el proveedor de servicio X con el proveedor de servicio Y que es de 10Gbps. Es aquí cuando se presenta el problema de sobre suscripción al desear enviar más tráfico del permitido a través de un enlace. Para este caso, el enlace de 10Gbps entre proveedores de servicio necesita satisfacer la necesidad de los 11Gbps sumados que solicita la empresa, lo cual no es posible dada la actual capacidad de interconexión entre proveedores. Sin embargo, es un problema del cual, la empresa no puede tener una visión definida dado que se evidencia dentro de la infraestructura de los proveedores de servicio. Finalmente, el resultado para el cliente será evidenciar tiempos de respuesta para los paquetes enviados que son muy elevados, así como paquetes que son descartados en tránsito por los mecanismos de control de flujo de los enlaces. El ancho de banda y la latencia no pueden ser garantizados cuando los paquetes atraviesan esos enlaces de interconexión.

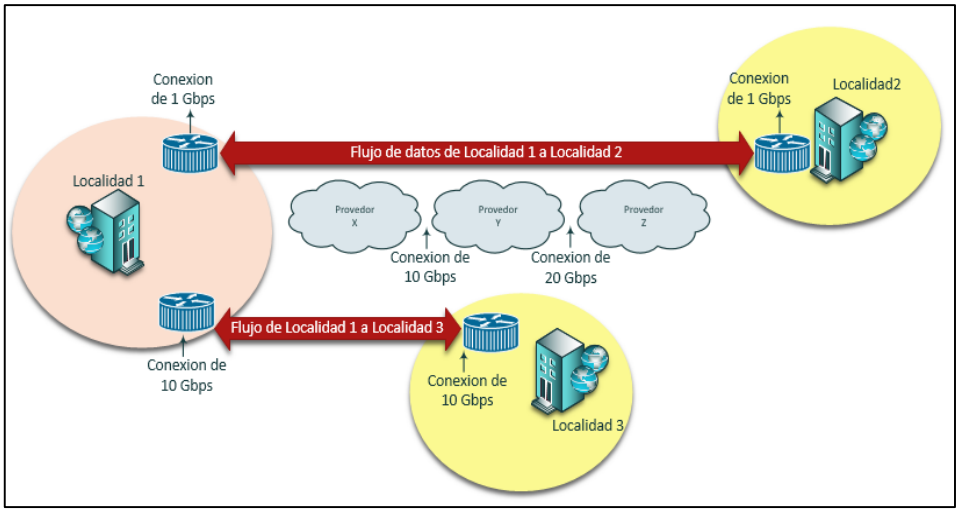


Figura 2.4 Diagrama de un nuevo enlace contratado

Los Proveedores de servicio usan Conmutación multiprotocolo por etiquetas para proveer una arquitectura escalable que permite que los paquetes sean enviados desde un enrutador a otro del proveedor de servicios, sin que cada uno deba inspeccionar el contenido del paquete, si no, tomar la decisión con base en una etiqueta agregada por el enrutador. Estos enrutadores al no tener que inspeccionar el contenido del paquete, pueden tomar una decisión de a donde enviarlo de forma más veloz al solo observar la etiqueta externa que fue insertada. Mientras el paquete atraviesa la red del proveedor de servicio, estas etiquetas pueden cambiar de enrutador a enrutador, sin que ellos tengan conocimiento de la información a nivel de IP en el paquete. Finalmente, al llegar a su destino, el

enrutador se encarga de remover cualquier etiqueta agregada en su recorrido, y entrega el paquete a su destino con el mecanismo tradicional revisando su tabla de enrutamiento, pero cabe resaltar que este proceso solo lo realizaría el ultimo enrutador que debe entregar el paquete, no los enrutadores intermedios.

2.1.3 REDES PRIVADAS VIRTUALES BASADAS EN CONMUTACIÓN MULTI PROTOCOLOS

Las redes privadas virtuales basadas en conmutación multiprotocolo por etiquetas permiten enviar tráfico de las redes de clientes a través de dos opciones que dependen de los requerimientos específicos de cada cliente: Redes privadas virtuales de capa 2 y redes privadas virtuales de capa 3.

Las redes privadas virtuales de capa 2 permiten al cliente establecer una conectividad entre los enrutadores al formar un circuito virtual entre los nodos. El proveedor de servicio emula un cable para el cliente, y no intercambia ninguna información con ellos. [2]

Las redes privadas virtuales de capa 3, permiten a los proveedores de servicio crear un contexto virtual denominado Virtual Routing Forwarding (VRF) para cada cliente. Los Proveedores de servicio proveen un método para mantener una tabla de rutas independiente para cada cliente, de tal forma que sea un ambiente seguro para interconexión entre varios puntos de la empresa. Se debe tener en consideración que el proveedor de servicios intercambia las rutas con los enrutadores del cliente que hacen frente al proveedor de servicio. El servicio de Red Virtual Privada de capa 3 permite este intercambio de paquetes IPv4 e IPv6 entre los diferentes enrutadores del proveedor de servicios. [2]

Gracias a estos servicios, el proveedor tiene las herramientas necesarias para garantizar los niveles de calidad de servicio que el cliente requiera. Dichos requerimientos por lo general son estipulados en un acuerdo en el nivel de servicio o SLA, que permite especificar diversos parámetros como el ancho de banda que requiere el cliente, el mayor retardo permitido para los paquetes, tiempos de afectación, etc. Normalmente, los precios asociados a este tipo de servicio varían dependiendo de que tanto nivel de servicio se desea obtener, y para obtener niveles

muy altos, el proveedor puede acordar implementar enlaces redundantes en su infraestructura.

2.2 INCREMENTO EN LA DEMANDA DE LA WAN EMPRESARIAL

El comportamiento de los enlaces de red de área amplia ha evolucionado desde los años 90s. Inicialmente una gran cantidad del tráfico empresarial era distribuido dentro de la red local del edificio o localidad, esto debido a que las principales aplicaciones se encontraban localizadas en ese sitio específico, no existía la necesidad de buscar los recursos fuera de dicha ubicación. Sin embargo, poco a poco fueron incorporándose más servicios y aplicaciones que cubrían necesidades específicas de la empresa, como por ejemplo el compartir archivos o documentos con los demás usuarios en otras localidades, correo electrónico con un servidor centralizado en otra localidad, etc. Podemos destacar los servicios más representativos que impulsaron el uso mayor de los enlaces de red de área amplia como los siguientes.

2.2.1 VIRTUALIZACIÓN DE SERVIDORES Y CONSOLIDACIÓN

Las CPU de los Servidores se han vuelto cada vez más rápidas, permitiéndoles realizar una mayor cantidad de procesamiento. Los departamentos de IT se dieron cuenta que al virtualizar y consolidar servidores de archivos o de correos, consumían menores recursos y bajaban los costos operacionales. Las empresas optaban por virtualizar sus servidores físicos en máquinas virtuales, las cuales se encontraban alojadas en otra localidad externa a la empresa, típicamente un Centro de Datos que permitía que se consigan los requerimientos de alta disponibilidad para dichos servidores. Esto a su vez, produjo un incremento significativo en los enlaces de área amplia, dado que, para hacer uso de esos servicios, las localidades remotas necesitan conectarse a las máquinas virtuales alojadas en el centro de datos. [2]

En la figura 2.5 podemos apreciar un esquema sencillo de virtualización que se utiliza en los centros de datos, en el cual un conjunto de varios servidores es virtualizado y alojado en un dispositivo con características de alto rendimiento que pueda soportar la capacidad de estos. A su vez la gestión de las

máquinas virtuales se realiza a través de un gestor denominado centro virtual (Virtual Center, vCenter por sus siglas en inglés).

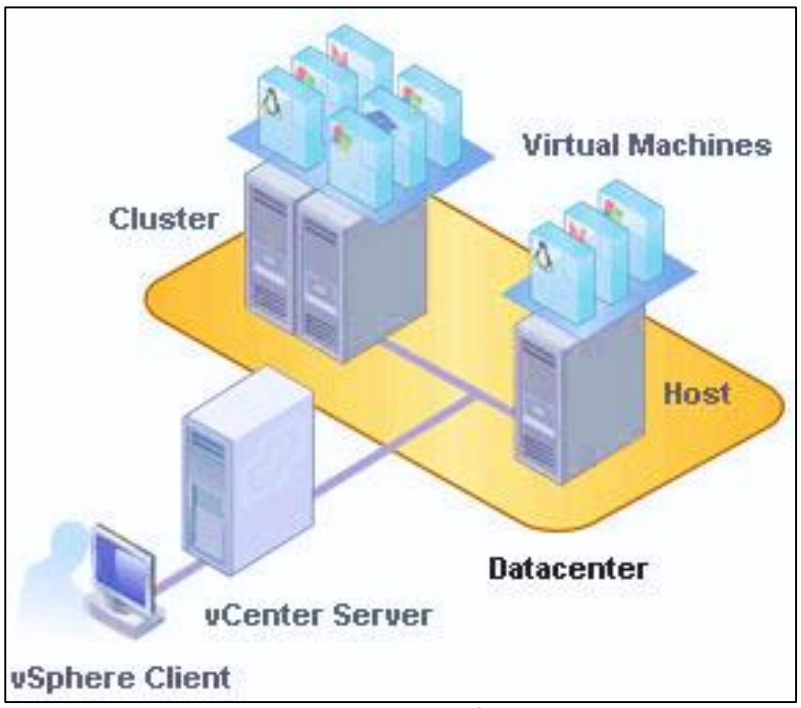


Figura 2.5 Virtualización de servidores

2.2.2 SERVICIOS BASADOS EN LA NUBE

En los últimos años, los proveedores de servicios en la Nube han tomado una importante relevancia en lo que compete a aplicaciones de negocio y la infraestructura que se encuentra relacionada. Los Proveedores de servicios en la nube, cubren con los costos asociados a recuperación en caso de desastres, licenciamiento, hardware necesario para proveer la flexibilidad a

sus clientes, y adicional, el cliente no requiere estar ligado a un único proveedor, dado que el cambio de vendedor en un modelo basado en la nube no tiene el mismo impacto financiero que implementar una aplicación dentro de la empresa con sus propios recursos. Tal como se observa en la Figura 2.6.

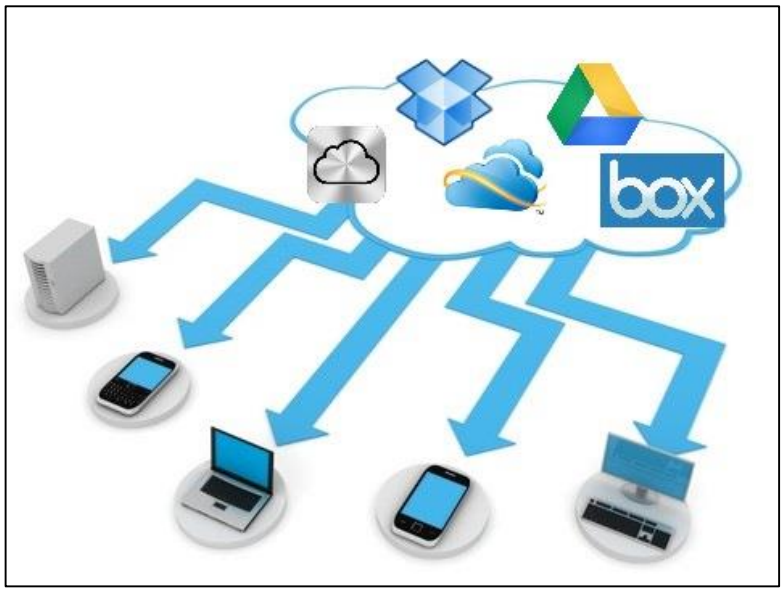


Figura 2.6 Servicios de almacenamiento de datos en la nube

La conectividad a los proveedores de servicios en la nube se establece con circuitos dedicados o a través de portales de Internet. Sea el un caso o el otro, ambos necesitan de los enlaces de área amplia para poder establecer dicha conectividad, siendo el caso del internet el que provee la ventaja adicional para el empleado de poder usar los servicios desde

cualquier localidad, sintiendo la misma experiencia como si lo hiciera en un ambiente de una red de área local.

2.2.3 SERVICIOS DE COLABORACIÓN

Las empresas han demandado desde hace varios años mantener una red para los servicios asociados a voz y datos por separado. Y con la implementación de la Voz sobre IP, los servicios de voz pasaron a ser parte de la red de datos, generando una reducción en los costos operativos para la empresa. Las llamadas entre diferentes usuarios de localidades geográficas separadas hacen uso de los enlaces de área amplia para establecer dichas llamadas de larga distancia, apartando la necesidad de circuitos de voz dedicados como los antiguos puntos de intercambio privados (PBX por sus siglas en ingles) en cada localidad. Al hacer uso de los enlaces de área amplia para el servicio de voz sobre IP, hay que tener en consideración que, si bien eliminamos los costos asociados a mantener un circuito de voz dedicado, tendremos un incremento en la utilización del enlace de área amplia por el tráfico de voz adicional que agregaremos como un nuevo servicio. En la figura 2.7 podemos observar las distintas formas de establecer un servicio de voz

sobre dos localidades, tomando en consideración que el Internet es un medio válido para establecer el servicio siempre que se tenga una conexión activa mediante un Proveedor de Servicio.

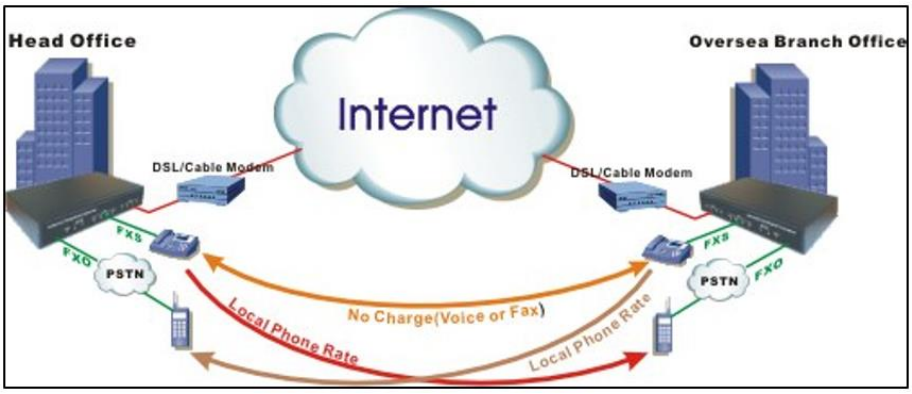


Figura 2.7 Servicio de VOIP entre dos localidades.

Incluso, siguiendo la misma línea de expansión, actualmente tenemos servicios que permiten integrar la voz y el video a través de la misma aplicación ofreciendo los servicios de video conferencia, permitiendo al usuario realizar reuniones y conferencias sin la necesidad de incurrir en costos asociados a viajes entre ciudades y costos por hospedaje entre otros, generando que las decisiones se realicen de una manera más eficiente y ágil sin la necesidad de retardos adicionales generados por la movilización del usuario.

Sin embargo, el uso de la voz y video dentro de la red requiere el uso de priorización del tráfico, debido a que la voz es más sensitiva a retardos, un canal que presente saturación en su capacidad puede generar perdida de paquetes y tiempos de respuesta muy elevados, afectando directamente a la calidad del servicio. Dado que las llamadas se realizan utilizando los enlaces de red de área amplia, se ve la necesidad de aplicar políticas de calidad de servicio que puedan aplicar adecuadamente una prioridad a este tráfico sensible, y a su vez, tener un mejor control de la utilización de dicho canal a fin de evitar posibles escenarios de saturación.

2.3 CALIDAD DE SERVICIO PARA LA WAN

Los usuarios de red esperan tiempos de respuesta adecuados para sus aplicaciones de red. La mayoría de las redes de área local proveen enlaces GigabitEthernet para las computadoras y dispositivos, de tal forma que se pueda prevenir un escenario de saturación. Para esto, las empresas e ingenieros desarrollan un plan de Políticas de calidad de servicio, con la finalidad de determinar cuál es el tráfico sensible para el cliente, y que tráfico debe tener preferencia sobre otro. A pesar de que las políticas de calidad de servicio deben desplegarse en toda la red de

la empresa, es puntualmente importante y necesaria su implementación para los enlaces de red de área amplia y su diseño asociado, dado que es aquí donde se encuentran los enlaces de menor capacidad, y mayor costo y requerimientos de disponibilidad. [2]

Por su naturaleza, las aplicaciones que hacen uso de voz y video son las más sensitivas a retardos y perdidas de paquetes, por lo cual, se considera que deban tener la prioridad más alta cuando se establecen las políticas de calidad de servicio.

Así mismo, los servicios que hacen uso de tráfico de Internet que no se encuentran relacionados con la empresa, son considerados como tráfico no relevante, y por lo cual, se les puede asignar la prioridad más baja en la política de calidad de servicio. Todos los demás servicios que se encuentren en la mitad de estas categorías se pueden distribuir aplicando una jerarquía adecuada para dichas aplicaciones, estableciendo claramente en las políticas qué aplicación es más relevante que otra, los tiempos de respuesta eficientes en una aplicación son un criterio importante para establecer una política adecuada de calidad de servicio, y estos deben promover un mejor rendimiento en la operación de la empresa, justificando de esta forma el orden de importancia para las aplicaciones que se llegue a definir.

Cuando se analizan los criterios para implementar una política de calidad de servicio, hay que tomar en consideración un aspecto importante llamado la Clasificación. Cuando se tienen identificadas las prioridades del tráfico empresarial, la Clasificación se realiza aplicando sentencias de configuración que hagan una comparación entre la información de la cabecera del paquete recibido, con las políticas que se encuentran definidas basadas en los criterios expuestos anteriormente.

En la figura 2.8 se muestra el comportamiento de dos canales de datos. En la parte superior observamos un canal de datos sin políticas de control en el cual los tres servicios involucrados se disputan todo el canal sin importar que sea voz, videos o datos. En la parte inferior en cambio observamos un canal de datos con políticas de control establecidas y cada servicio ocupa la cantidad del canal asignado según su prioridad proporcionada.

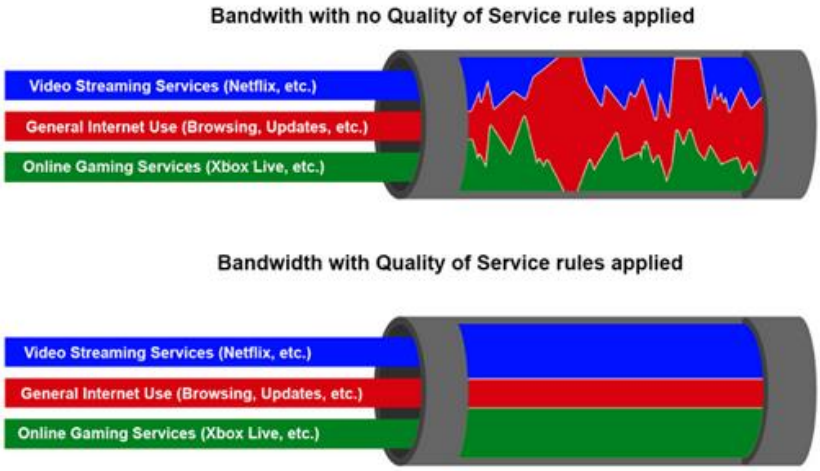


Figura 2.8 Políticas de calidad de servicio aplicadas bajo criterio de clasificación.

2.4 CONECTIVIDAD REMOTA Y SEGURIDAD

El Internet provee de múltiples formas para obtener información de todo tipo, pero así mismo, al ser una red de acceso global, se puede tener usuarios que desean obtener información de forma ilegal con la finalidad de chantajear o hacer daño a una persona o empresa. Por tal motivo, es necesario implementar las políticas de seguridad adecuadas para garantizar la integridad, confidencialidad y disponibilidad de la información para los usuarios.

Una herramienta usada en el proceso de seguridad, son los Corta Fuegos, los cuales nos permiten establecer reglas para permitir o denegar el tráfico con base en múltiples parámetros, como la fuente y destino del paquete, el tipo de protocolo utilizado, los puertos de origen o destino del segmento a nivel de aplicación, el tamaño del paquete, etc. Actualmente, la inteligencia de estas herramientas nos permite hacer una inspección dentro de la información del paquete a nivel de aplicación y así determinar si tiene contenido malicioso o fraudulento, como, por ejemplo, la búsqueda de contenido en un correo electrónico que puede contener un vínculo que lleva a una dirección utilizada para robar información digital del usuario. Además, los Corta Fuegos permiten hacer un filtrado de páginas a las cuales no se desea permitir su acceso dentro de la empresa por motivos organizacionales, ya sea evitar distracciones de los empleados en sitios de entretenimiento, o consideraciones de seguridad.

El acceso a Internet a las sucursales de la empresa puede darse de dos formas: De forma centralizada en un punto principal o también llamado matriz, o de forma distribuida en cada sucursal de tal forma que posean su propia salida a Internet.

Para la solución de acceso a Internet de forma centralizada, el tráfico de cada sucursal es direccionado hacia un punto común que será la matriz de la empresa, en la cual, se instala un Corta Fuegos para que pueda filtrar de manera adecuada dicho tráfico acorde con las políticas organizacionales de la empresa. Sin embargo, la desventaja de este modelo es que los enlaces de red de área amplia pueden llegar a ser sobre utilizados por este tráfico de Internet, y causar degradación de los demás servicios que atraviesan el mismo, tal como se observa en la Figura 2.9.

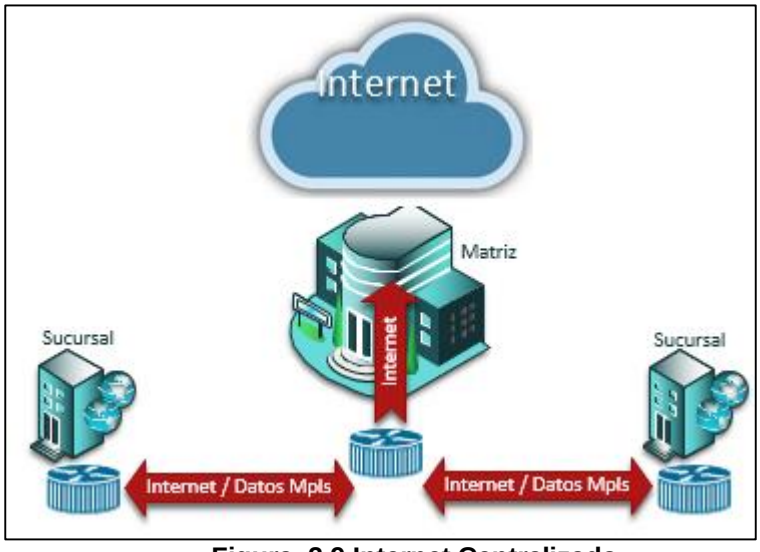


Figura 2.9 Internet Centralizado.

Para la solución de acceso a Internet de forma distribuida, cada sucursal tiene su propia salida a Internet, permitiendo que los enlaces de red de

área amplia puedan servir solo al tráfico de red interna que requiera el uso de aplicaciones en otras localidades. La desventaja de esta solución es que el aspecto de seguridad se debe llevar de forma distribuida en cada sucursal, compartiendo las políticas de la organización, pero con un dispositivo encargado de hacerla cumplir como un Corta Fuegos, tal como se observa en la Figura 2.10.

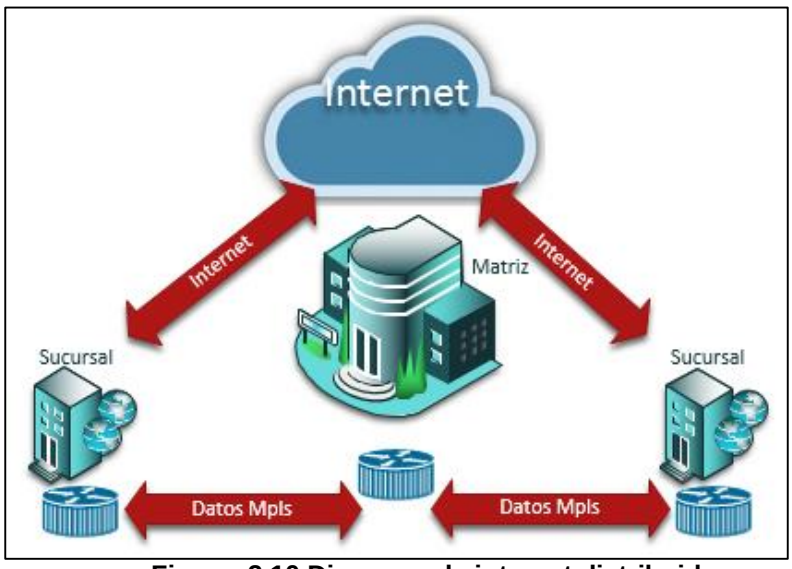


Figura 2.10 Diagrama de internet distribuido

2.5 SOLUCIÓN DE BANDA ANCHA INTELIGENTES

La arquitectura de las Redes de Área Amplia Inteligentes de CISCO permite a una organización tener la capacidad para proveer un mayor ancho de banda utilizable a un bajo costo, sin sacrificar rendimiento,

seguridad o confiabilidad. La solución se fundamenta en 4 pilares: Independencia de transporte, Control de Camino Inteligente, Optimización de aplicaciones y Conectividad Segura. [2]

2.5.1 INDEPENDENCIA DE TRANSPORTE

La solución de Red de Área Amplia Inteligente de CISCO usa la tecnología de VPN Dinámica Multipunto (DMVPN por sus siglas en ingles), para obtener la independencia en el transporte a través de un enrutamiento que trabaja sobre la infraestructura definida. Esto nos permite que podamos tener cualquier tipo de transporte intermedio como por ejemplo Internet, una red de datos MPLS, una red de acceso con tecnología GEPON, incluso una conexión provista por una red celular, y levantar una infraestructura de comunicación entre los puntos involucrados que trabaje sobre el transporte sin importar el proveedor. Con la utilización de DMVPN también favorecemos a la rápida habilitación de una nueva localidad, dado que el despliegue se realiza de forma simple y automática siempre y cuando exista conectividad hacia el punto principal o Matriz. [9]

2.5.2 CONTROL DE CAMINO INTELIGENTE

Los enrutadores toman una decisión de a donde enviar un paquete con base en la información de IP destino en su cabecera y la información que se obtiene a partir del protocolo de enrutamiento encontrada en la tabla de rutas del dispositivo. Pero hay que tener en consideración que los enrutadores toman esta decisión sin tomar en consideración otros parámetros como la utilización del enlace, retardo, degradación del canal, etc.

La tecnología llamada Enrutamiento por Rendimiento (Performance Routing - PfR por sus siglas en inglés) permite manejar un control de camino inteligente basado en las aplicaciones que se están utilizando. La tecnología monitorea el rendimiento con base en la clase de tráfico y puede tomar una decisión de por qué enlace se puede enviar un paquete bajo determinadas condiciones. Enrutamiento por Rendimiento se encarga de garantizar que el camino por el cual se vaya a enviar el paquete cumpla con las condiciones mínimas que necesita el tráfico para garantizar su rendimiento adecuado para dicha aplicación, tal como se observa en la Figura 2.11.

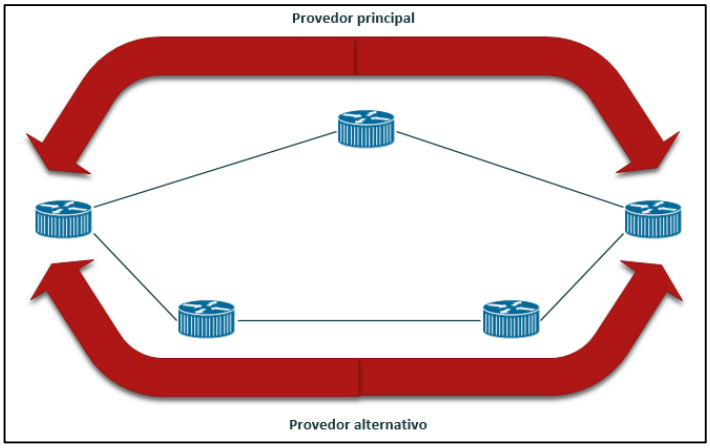


Figura 2.11 Diagrama de camino inteligente

2.5.3 OPTIMIZACIÓN DE LAS APLICACIONES

La solución de red de área amplia inteligente de CISCO permite realizar un análisis profundo de la aplicación de tal forma que se pueda determinar qué tipo de protocolos se están utilizando, y a su vez, proveer de una mejor forma de clasificación para el paquete acorde con un criterio de importancia definido por el administrador para el protocolo en uso. Una vez clasificado el paquete, el enrutador que tiene la función de Controlador Maestro puede tomar la mejor decisión del enlace a utilizar para enrutar el paquete a su destino.

2.5.4 CONECTIVIDAD SEGURA

La meta principal de un enrutador es garantizar el envío de paquetes hacia su destino. Sin embargo, se deben tomar en cuenta aspectos de seguridad relacionados a garantizar que el paquete llega sin ser alterado o garantizar que no pueda ser interpretado por ningún elemento externo a los involucrados en la comunicación. Para lograr este objetivo, el tráfico que se envía a través de los canales es cifrado de inicio a fin con algoritmos seguros de cifrado que garantizan que, solo el enrutador que recibe el paquete, lo puede desencriptar adecuadamente y entregar la información al usuario en cuestión.

CAPÍTULO 3

LEVANTAMIENTO DE INFORMACIÓN.

3.1 INFRAESTRUCTURA DE RED.

La solución de CISCO iWAN provee mejoras en la utilización de los enlaces de red de área amplia, tanto en rendimiento como en seguridad. Para las empresas esto se vería reflejado en mejores tiempos de respuesta para los servicios que utilicen los usuarios, y confiabilidad de que la información se mantiene fluyendo entre las localidades de una forma segura.

La empresa en la cual situamos el análisis se encuentra en su despliegue inicial de expansión a dos diferentes localidades. Inicialmente sus operaciones comenzaron en una ubicación que denominaremos Matriz de Operaciones, y las localidades a expandirse denominaremos Sucursales de Operaciones. Para efectos de simplicidad, tomaremos en consideración un proceso de expansión a dos localidades adicionales a la Matriz, las cuales llamaremos como Sucursal 1 y Sucursal 2. (Fig 3.1)

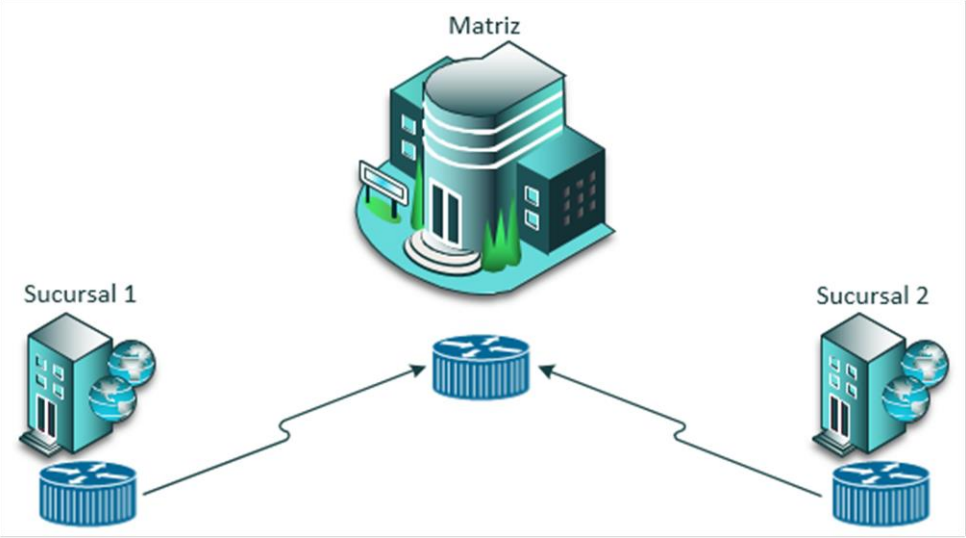


Figura 3.1 Diagrama simplificado de la matriz y sucursales.

En el inicio de sus operaciones, la empresa tomó en consideración que, por la criticidad en la disponibilidad de sus servicios, necesitaban tener enlaces de red de área amplia redundantes a fin de disminuir el tiempo de indisponibilidad en caso de una falla de uno de ellos. Tomaremos en

consideración a dos Proveedores de Servicio que llamaremos Proveedor de Servicio 1 (ISP-1) y Proveedor de Servicio 2 (ISP-2).

Ambos Proveedores de Servicios se dedican a brindar servicios de Internet a sus clientes, y adicional, servicios de datos para interconexión de diversas localidades a través de una red basada en Conmutación por Etiquetas Multi Protocolo (MultiProtocol Label Switching, MPLS por sus siglas en ingles), la cual se fundamenta en hacer un envío de paquetes sin analizar el campo de dirección IP destino, sino, con base en una etiqueta que colocan los enrutadores con la finalidad de hacer el envío de una manera mucho más rápida y utilizando menos recursos de cada dispositivo. Adicional, se considera que una red basada en la tecnología de MPLS es más segura que una red tradicional, dado que la tecnología tiene como pilar fundamental la separación lógica de la información de los distintos clientes que tenga un ISP gracias al uso de las llamadas Tablas de Enrutamiento Virtuales y de Envío (Virtual Routing and Forwarding, VRF por sus siglas en ingles). Las VRFs permiten que cada cliente maneje su propia tabla de rutas, independiente de otros clientes en los dispositivos del Proveedor de Servicios. Esto permite mantener la seguridad de su información y datos, garantizando que no serán compartidos con agentes externos a su infraestructura de red, o con otros clientes que compartan la infraestructura del proveedor de servicios. [10]

Cuando la empresa comience con su proceso de expansión, determinaron que cada localidad nueva, deberá contar con el mismo esquema de redundancia para sus enlaces de red de área amplia, a fin de garantizar el nivel de disponibilidad de los servicios. Por lo cual, cada nueva sucursal poseerá dos enlaces de red de área amplia, ambos usando un Servicio de Transmisión de Datos con el Proveedor de Servicios 2 dado que es considerado un ISP con mejores tiempos de respuestas ante incidencias en sus enlaces. En los casos donde el Proveedor de Servicios 2 no pueda tener presencia, se considerará el uso del Proveedor de Servicios 1, como es la situación de la Sucursal 2 en la cual, por su ubicación, solo tiene permisos de acceso el ISP-1.

En la figura 3.2 podemos observar el esquema de conexión entre la Matriz y las Sucursales, en la cual se observan los enlaces de red de área amplia tanto principal como alternativo para cada localidad.

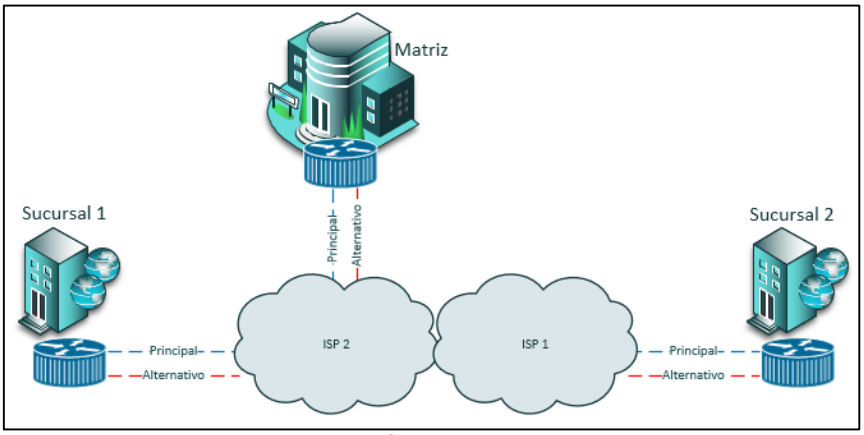


Figura 3.2 Diagrama de conexión para matriz y sucursales con el ISP.

El direccionamiento de red que utiliza la empresa se encuentra en la red clase C 192.168.0.0/16 y se encuentra distribuido acorde con lo indicado en la Tabla 1 mostrada a continuación.

Tabla 1 Información de las subredes de la empresa

Enrutador	Localización	Subred Primaria	Transporte	¿Tiene redundancia?
Matriz	Matriz de Operaciones	192.168.0.0/24	MPLS	Si
Sucursal-1	Sucursal 1	192.168.1.0/24	MPLS	Si
Sucursal-2	Sucursal 2	192.168.2.0/24	MPLS	Si

En la Tabla 2 la Matriz de Operaciones usa el direccionamiento 192.168.0.0 con mascara de subred de 24 bits. Dentro de esta subred, se alojan los servicios críticos de la empresa y sobre los cuales vamos a realizar las mediciones de rendimiento, en la figura 3.3 podemos ver cuáles son:

- ✓ Servidor de Aplicaciones Generales con IP 192.168.0.100
- ✓ Central de Voz con IP 192.168.0.110
- ✓ Servidor de Transferencia de Archivos usando FTP con IP 192.168.0.120

Tabla 2 Descripción de los servidores en Matriz

Nombre del Servidor	Localización	Dirección IP	Función
Servidor de Aplicaciones Generales	Matriz	192.168.0.100	Servidor usado para probar conectividad a nivel de respuestas ICMP.
Central de Voz	Matriz	192.168.0.110	Servidor que funciona como central de requerimientos de Voz sobre IP de los usuarios.
Servidor de Transferencia de Archivos	Matriz	192.168.0.120	Servidor utilizado por los usuarios para transferencia de archivos utilizados en la operación de la empresa.

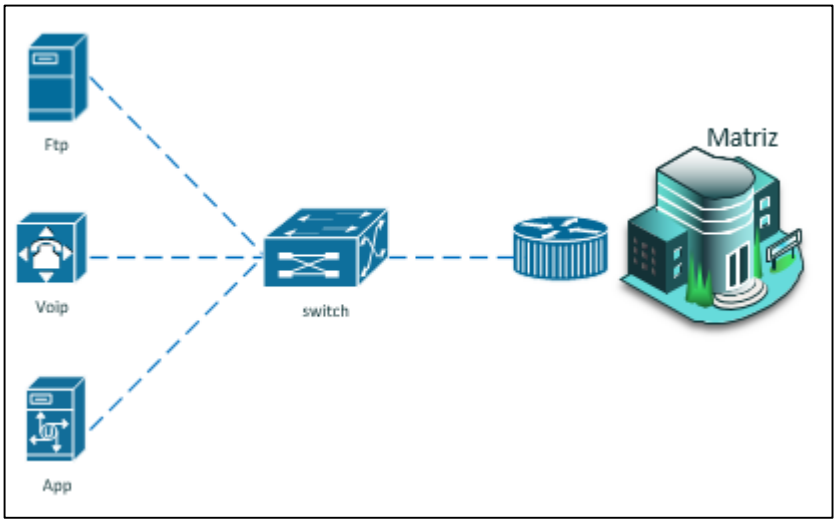


Figura 3.3 Servidores ubicados en matriz

Las sucursales solo tendrán usuarios que establecerán conexión hacia la matriz para hacer uso de los recursos que necesiten de los servicios implementados. Estos usuarios harán uso de las subredes 192.168.1.0 /24 en las Sucursal 1 y 192.168.2.0 /24 en la Sucursal 2. Debemos tener en consideración que los usuarios de las sucursales pueden tener comunicación directa entre ellos sin que el tráfico pase por la Matriz, de esta forma evitamos un consumo innecesario de ancho de banda por un enrutamiento inadecuado.

3.2 IDENTIFICACIÓN DE APLICACIONES Y SERVICIOS

La operación de la empresa se fundamenta en el uso de los servicios que se encuentran en Matriz, sin embargo, no se encuentra limitada solo al uso de ellos, por ejemplo, en la figura 3.4 se puede apreciar un reporte generado por un dispositivo colector, el cual recibe información acerca de los flujos de información que se envían de una localidad a otra. En el reporte podemos observar algunas de las aplicaciones que tienen una mayor utilización respecto del total de ancho de banda disponible.

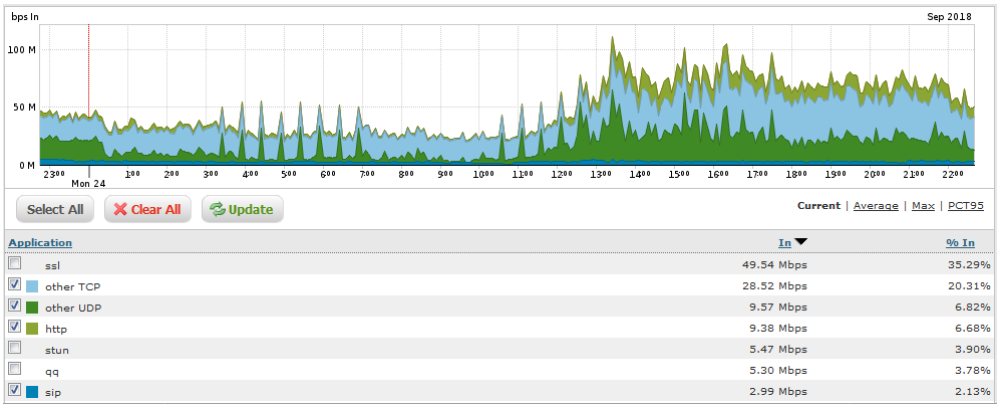


Figura 3.4 Reporte de tráfico de un dispositivo colector, en la cual se identifica algunas de las aplicaciones de mayor utilización.

Para el proceso de mejoramiento en el uso de los enlaces de red de área amplia tomaremos en consideración los tipos de tráficos principales y relevantes para los usuarios, y que podemos agrupar en 3 secciones: Tráfico de aplicaciones TCP, Tráfico de aplicaciones UDP y Tráfico restante. Los servicios para cada grupo de tráfico se han seleccionados acorde con la facilidad de reproducirlos en un ambiente de prueba, pero que a su vez puedan reflejar adecuadamente el comportamiento de la solución al identificar el tipo de tráfico que se encuentra en uso.

Cada usuario en cada localidad podrá hacer uso de los siguientes servicios:

- ✓ Servicio de Transferencia de Archivos que se encuentran almacenados en un Servidor en Matriz. Este servicio identificará

una aplicación que hace uso de tráfico TCP. En la Figura 3.5 se aprecia el esquema de operación del protocolo de FTP.

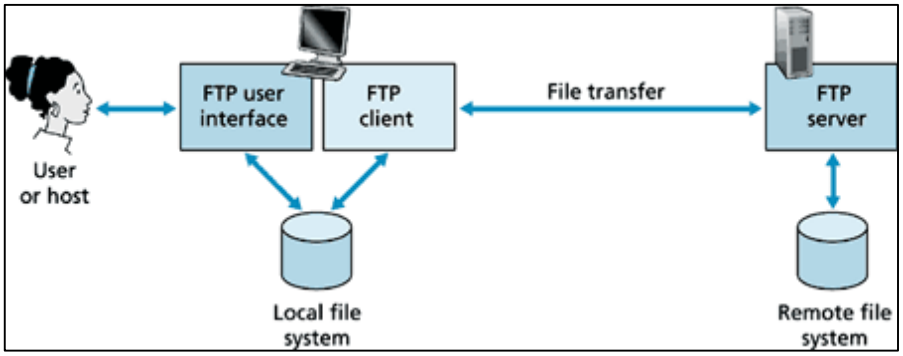


Figura 3.5 Proceso de transferencia de archivos usando FTP

- ✓ Servicio de Voz sobre IP para comunicación entre usuarios. Este servicio identificará una aplicación que hace uso de tráfico UDP. En la Figura 3.6 identificamos las diversas formas que se puede establecer una comunicación mediante VoIP.

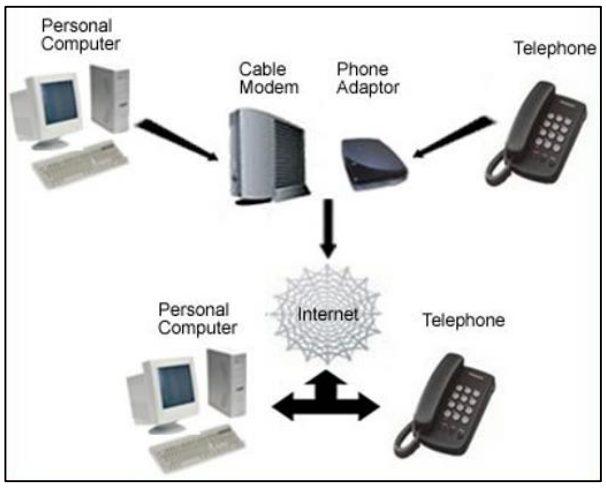


Figura 3.6 Como funciona la Voz sobre IP

- ✓ Servicio de Aplicaciones Generales centralizadas en un servidor al cual, solo se probará conectividad con paquetes de control usando el Protocolo de Control de Mensajes de Internet (Internet Message Control Protocol, ICMP por sus siglas en ingles). Este servicio identificará una aplicación que hace uso de tráfico restante que no es categorizado como TCP ni como UDP. La Figura 3.7 resume la forma de operación del protocolo ICMP entre dos dispositivos.

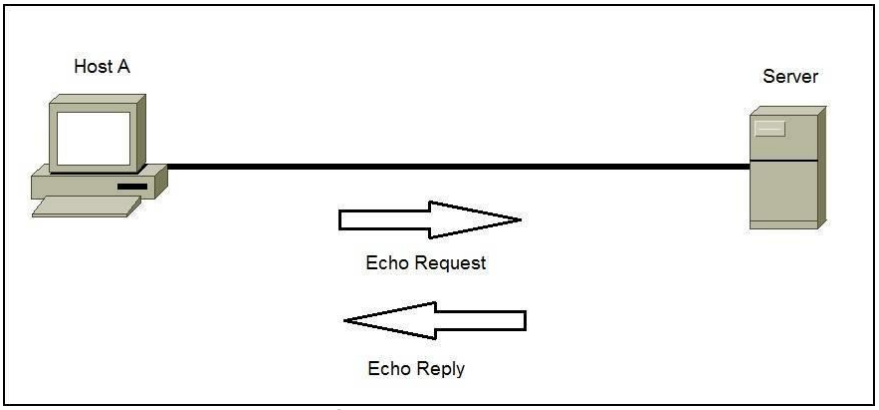


Figura 3.7 Comunicación entre dos dispositivos usando ICMP

- ✓ Servicio de Internet, el cual usaran los usuarios para los diferentes servicios que tengan permitidos acceder que no se encuentren dentro de la infraestructura de la empresa. Por considerarse contenido ajeno a la empresa, se determina que este servicio es el menos importante en un orden de prioridad para el usuario.

3.3 FUNCIONAMIENTO ACTUAL DE LAS APLICACIONES Y LOS SERVICIOS

El Servicio de Transferencia de Archivos entre usuarios se realiza mediante el uso del Protocolo de Transferencia de Archivos (File Transfer Protocol, FTP por sus siglas en ingles). FTP es un protocolo estandarizado que usa como transporte conexiones con el Protocolo de Control de Transmisión (Transmission Control Protocol, TCP por sus siglas en Ingles). FTP es un protocolo orientado a la conexión en la forma Cliente-Servidor que confía en la comunicación establecida con ambas partes a través de dos canales: un canal de control de la conversación y un canal dedicado a transmitir el contenido del archivo. En la Figura 3.8 se muestra el proceso de conexión entre dos dispositivos utilizando el protocolo de FTP. [3]

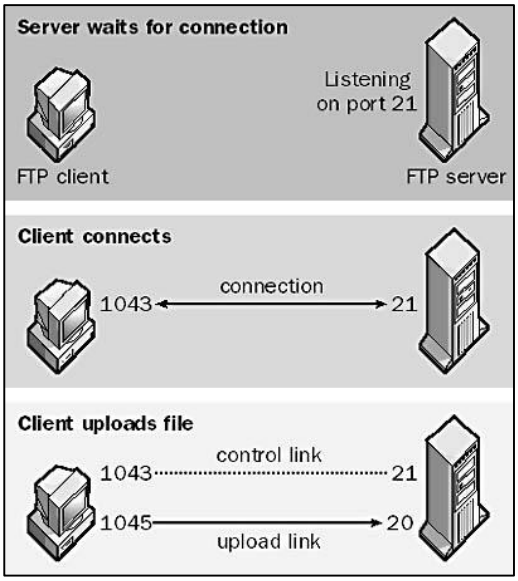


Figura 3.8 Proceso de transferencia de archivos usando FTP

Los Clientes inician la conversación con los servidores realizando una solicitud de descarga del archivo sobre el puerto TCP número 21. Haciendo uso de FTP, un cliente puede subir, descargar, renombrar, borrar, mover, o copiar archivos de un servidor.

Típicamente, un cliente para hacer uso del servicio de FTP necesita autenticarse con credenciales en el servidor, aunque es posible que el servidor permita los accesos anónimos, lo cual es conocido como un FTP Anónimo. El servidor FTP de la empresa no permite accesos anónimos, por lo cual, cada usuario que desee hacer uso del servicio de transferencia de archivos del servidor deberá autenticarse con las credenciales de acceso correspondientes. [3]

El Servicio de Voz sobre IP es un método para tomar señales de audio analógicas y convertirlas en información digital que puede ser transmitida a través del Internet como cualquier otro tipo de información. Existen varias formas de proveer un servicio de Voz sobre IP, en el caso de la empresa en cuestión, consideraremos que el servicio es brindado directamente sobre las computadoras de los usuarios para lo cual solo necesitan un software denominado softphone, un micrófono, un auricular y una conexión entre los dos usuarios a nivel de IP. [4]

Los servicios de Voz sobre IP utilizan la tecnología de conmutación por paquetes la cual se puede describir como la siguiente secuencia de pasos:

- ✓ La Computadora origen divide la información en pequeños paquetes que son enviados a los dispositivos de red correspondientes.
- ✓ Dentro de cada paquete se encuentra una carga útil, que es esa parte de la información original que se desea enviar.
- ✓ La Computadora origen envía el paquete al enrutador más cercano, y este a su vez, lo reenvía al siguiente enrutador que se encuentre más cerca hacia el destino.

- ✓ Cuando la Computadora destino recibe los paquetes, vuelve a juntar todas las partes gracias a un parámetro llamado Número de Secuencia, y así formar la información en su estado original. [4]

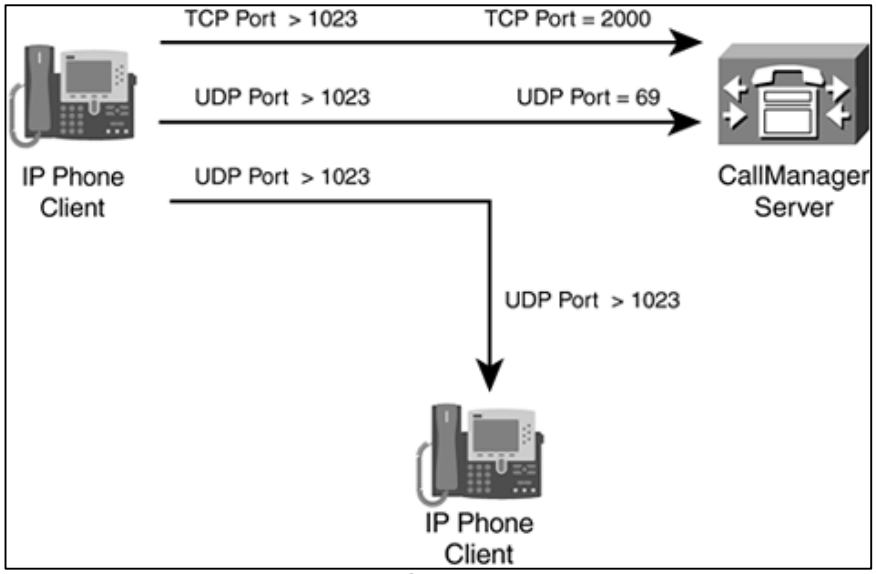


Figura 3.9 Comunicación entre dos clientes de VoIP

Debemos tener en consideración que la comunicación establecida entre dos usuarios con el servicio de VoIP se realiza a través del Protocolo de Datagrama de Usuario (User Datagram Protocol, UDP por sus siglas en inglés), el cual se caracteriza por ser un protocolo no orientado a la conexión y no confiable, pero a cambio, se garantiza un rápido procesamiento del paquete a su llegada. La aplicación de softphone en las computadoras usa los puertos UDP 5060 y 5061.

El Servicio de Aplicaciones Generales se representará mediante un proceso de verificación de conectividad entre el usuario y el servidor mediante el envío de paquetes usando el Protocolo de Control de Mensajes de Internet (ICMP). Para esto usaremos la herramienta de red llamada Ping, la cual envía un paquete ICMP hacia una dirección IP destino que contiene un mensaje de Solicitud de Eco. A su vez el dispositivo destino responde a esta solicitud con un paquete ICMP que contiene un mensaje de Respuesta de Eco. Si el dispositivo origen recibe la respuesta, se confirma que existe conectividad hacia el dispositivo destino. [10] En la Figura 3.10 se muestra la forma de operación de la herramienta de ping al utilizar paquetes ICMP en la comunicación entre dos dispositivos.

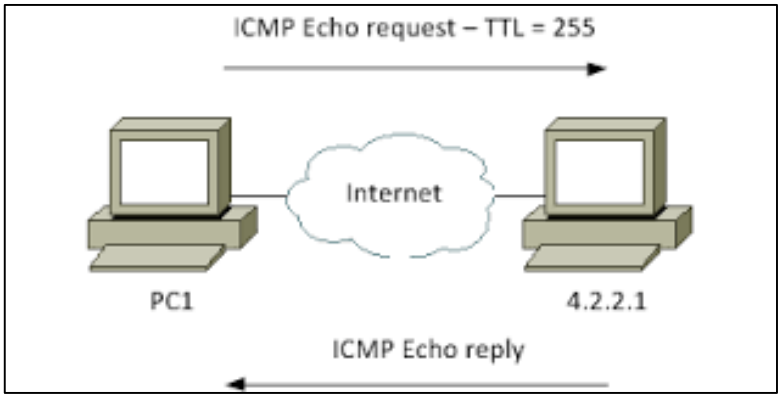


Figura 3.10 Prueba de ping entre una computadora y un servidor en el mundo con IP 4.2.2.1

A su vez la herramienta de Ping tiene parámetros que pueden ser modificados con la finalidad de lograr una mejor verificación de conectividad. Las modificaciones que podemos realizar son las siguientes:

- ✓ Definir el número de paquetes que se envían, de esta forma podemos tomar una muestra de mayor tamaño de Solicitudes/Respuestas y tomar mediciones de los tiempos que le toma a cada paquete en alcanzar a su destino.
- ✓ Incrementar el tamaño de los paquetes, lo cual nos permite enviar paquetes con una carga útil de mayor tamaño y así incrementar la utilización del enlace de comunicación.
- ✓ Definir la IP origen con la cual son enviados los paquetes, para el caso en que la respuesta deba ser enviada hacia una IP especifica que el usuario requiera.

Realizaremos esta prueba de conectividad con la finalidad de tener un servicio que se pueda medir su rendimiento sin necesidad de agregar una aplicación al proceso. Sin embargo, este servicio puede ser reemplazado por cualquier aplicación siempre que se conozca el tipo de protocolo de la capa de transporte utilizado (TCP o UDP) y el número de puerto utilizado.

La utilización del protocolo de ICMP se realiza por razones de simplicidad en el análisis del escenario de la empresa.

3.4 IDENTIFICACIÓN DE LOS RIESGOS RELACIONADOS A LA SEGURIDAD DE LA INFORMACIÓN

Las organizaciones para su operación manejan activos, los cuales son valorados de cierta manera, sin embargo, la información muchas veces no es considerada como un activo importante y en el mejor de los casos se transfiere la protección a terceros, cuando en otros casos ni siquiera se identifican los riesgos asociados a la perdida de confidencialidad, disponibilidad e integridad de la información.

La confidencialidad es la propiedad con la cual se controla quien puede tener acceso a la información, y esto puede ser: un proceso, una persona o un sistema. Por ejemplo, usuarios que necesitan tener acceso a una aplicación son definidos por un administrador, y pertenecen a un área de ventas, para lo cual, se definen credenciales de acceso con permisos orientados exclusivamente al contenido que tienen permitido visualizar o modificar. Con esta propiedad se previene la divulgación o fuga de información a entidades no autorizadas.

La integridad es la propiedad en la cual la información debe ser precisa y exacta para su uso. Por ejemplo, un balance financiero en el cual sus cifras fueron modificadas sin autorización afecta a la integridad de la información, y por lo cual, genera una afectación sobre la veracidad y confiabilidad que tienen los usuarios al hacer uso de ella.

La disponibilidad es la propiedad en la cual la información debe ser accesible para los usuarios autorizados en el momento que lo requieran. Por ejemplo, una falla en los sistemas transaccionales de un banco genera una indisponibilidad de los servicios que se ofrecen a sus clientes, afectando la operación del negocio.

La seguridad de la información busca proteger la confidencialidad, integridad y disponibilidad de esta. Esto va más allá de seguridad física de los equipos dentro de la organización, y dado que su enfoque es proteger las tres propiedades, se basa en la gestión de riesgos por lo cual es importante, analizar, evaluar y tratar los riesgos asociados a la perdida de la seguridad de la información.

Se considera un riesgo a los efectos o incertidumbres de alcanzar un objetivo y estos pueden ser positivos o negativos. Los riesgos negativos

pueden afectar o comprometer al negocio, mientras que los positivos son los que generan oportunidad para la organización.

La gestión de riesgos es un proceso que tiene dos componentes: La **Apreciación del riesgo** y los **Tratamientos de los riesgos.**

La apreciación del riesgo es un componente que consta de tres fases:

- ✓ Identificación, que consiste en la descripción del riesgo, la cual se puede basar en las amenazas, vulnerabilidades y las fuentes del riesgo, esto es, describir la causa y el efecto.
- ✓ Análisis, en la cual se estima el nivel del riesgo, la combinación de la probabilidad de ocurrencia del riesgo y sus consecuencias. Se debe tener en consideración que el método para establecer la probabilidad puede ser cualitativo o cuantitativo dependiendo del mecanismo definido por la organización.
- ✓ Evaluación es comparar el nivel de riesgo generado en la fase de Análisis con los criterios de aceptación del riesgo definidos por la organización o la empresa. Es decir, el nivel de riesgo que la organización está dispuesto a tolerar o aceptar en su negocio.

Por ejemplo, observemos la Tabla 3 en la cual, hacemos una apreciación de tres riesgos en una empresa:

Tabla 3 Ejemplo de tabla de apreciación de un riesgo.

Identificación del Riesgo	Probabilidad (P)	Consecuencia (C)	Nivel de riesgo (P*C)	Evaluación (¿El riesgo es aceptable?)
Riesgo 1	2	1	2	SI
Riesgo 2	3	2	6	NO
Riesgo 3	1	3	3	NO

Como resultado de la Evaluación de riesgos nos permite decidir si los riesgos identificados necesitan tratamiento o no, con base en los niveles aceptables por la organización. Para el ejemplo de la tabla 3, la empresa considera que un nivel de riesgo mayor a 2 no es aceptable para la empresa y, por lo tanto, necesita ser tratado.

Dentro del tratamiento se establecen acciones para disminuir el nivel de riesgo, transferirlo a un tercero, eliminar la fuente del riesgo o aceptar el riesgo.

La forma actual de operar en la empresa nos lleva a realizar una apreciación de los riesgos que están asociados a una pérdida parcial o total de las propiedades de la seguridad de la información y establecer acciones para tratarlos.

La Tabla 4 muestra la identificación de los riesgos que son considerados importantes en la empresa y que requieren un tratamiento para su prevención y ocurrencia. Los datos de probabilidades han sido tomados de una encuesta realizada por la empresa Deloitte sobre tendencias de Ciber-Riesgos y Seguridad de la Información en Latinoamérica en el 2016, sobre 89 organizaciones participantes en 13 países, y en la que se ha determinado que 4 de cada 10 organizaciones sufrieron una brecha de seguridad en los últimos 24 meses. [17] El impacto o consecuencia es un parámetro subjetivo, y determinado directamente por las consideraciones administrativas de la empresa, para nuestro caso hemos considerado que los riesgos identificados tienen un impacto alto para los activos de la empresa y por tal motivo, deben ser tratados a fin de reducir la probabilidad de ocurrencia. Para la escala relacionada a la consecuencia, se considera un impacto alto un valor de 100/100, impacto medio a un valor de 50/100 y un impacto bajo un valor de 10/100.

Tabla 4 Identificación de los riesgos a ser tratados en la empresa

Riesgo	Identificación	Descripción del Riesgo	%	Impacto	Nivel
Riesgo 1	Alteración de la información en la nube del proveedor de servicios	La información es enviada a través de los proveedores de servicio mediante una infraestructura basada en MPLS. Si bien es cierto, la tecnología se considera segura, estamos confiando en un tercero para asegurar la integridad de la información. Los enlaces pueden ser vulnerables a un ataque de suplantación de identidad o de intercepción de los datos, con lo cual, pueden ver el contenido de los paquetes mientras fluye de una localidad a otra y usarlos con la finalidad de afectar la operación de la empresa. Se considera como una brecha de seguridad interna.	27	Impacto Alto (100)	27
Riesgo 2	Suplantación de identidad en el proceso de enrutamiento	Un enrutador atacante puede intentar establecer una vecindad con un enrutador válido dentro de la empresa en el proceso de intercambio de información del protocolo de enrutamiento. De esta forma, puede inyectar información incorrecta en la tabla de rutas de los demás enrutadores con la finalidad de modificar el siguiente salto de los paquetes con una IP atacante, interceptando los paquetes que son enviados de una localidad a otra. Se considera como una brecha de seguridad interna.	27	Impacto Alto (100)	27
Riesgo 3	Degradación de los servicios por un ataque de denegación de servicio.	Un ataque de denegación de servicio está enfocado en afectar a la disponibilidad de uno o más servicios. Existen varias formas de efectuar un ataque de este estilo, sin embargo, la forma más común de producir una indisponibilidad es generando tráfico falso con la finalidad de consumir todos los recursos de un enlace, ya sea de red de área local o de área amplia. Si el enlace se encuentra saturado, todos los servicios que fluyan por el mismo se verán afectados. Se considera como una brecha de seguridad externa.	37	Impacto Alto (100)	37

La solución de CISCO iWAN se ofrece como un tratamiento para los riesgos identificados en la Tabla 4, dado su mecanismo de cifrado para los paquetes que son intercambiados entre las localidades, así como la forma de garantizar que dichos paquetes no pueden ser alterados en tránsito, preservando de esta forma la integridad y confidencialidad del servicio. A su vez, el mecanismo de enrutamiento inteligente que provee la solución permite que el tráfico que se defina como servicios de importancia para la empresa, pueda mantener su nivel de calidad alta en la transferencia de la información aun presentándose un escenario de saturación de un enlace ocasionado por un ataque de denegación de servicio, de esta forma permite garantizar la disponibilidad de este.

CAPÍTULO 4

ANÁLISIS Y DISEÑO

4.1 ANÁLISIS DE LA SITUACIÓN ACTUAL

La comunicación de las sucursales con los servicios de Matriz, se realizan a través de los enlaces de red de área amplia. La redundancia de los enlaces en cada localidad funciona en el esquema de Activo-Pasivo, lo cual indica que un solo enlace es utilizado a la vez, y el otro funciona como el enlace secundario en caso de una falla en el enlace principal. En la figura 4.1 se puede observar el esquema de redundancia para los enlaces en las localidades de la empresa.

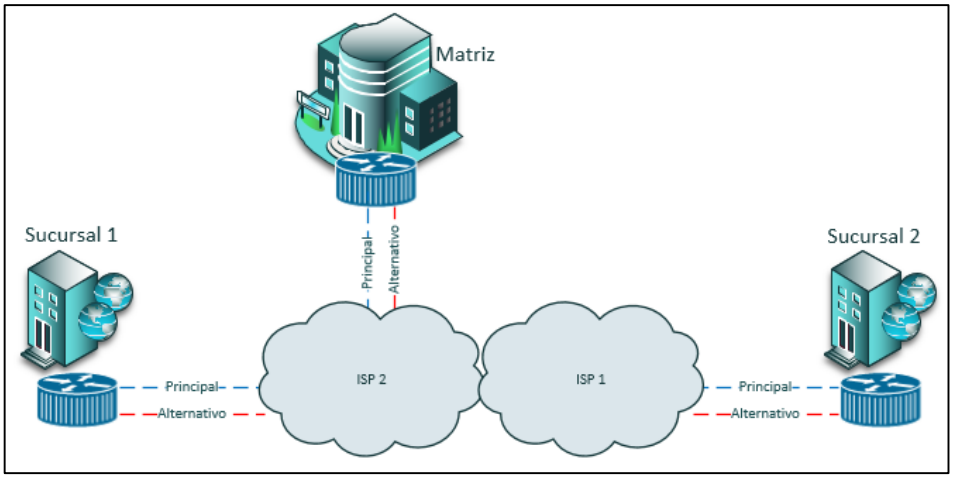


Figura 4.1 Diagrama enlaces principal y alternativo.

Bajo esta situación tenemos que considerar que un canal se encuentra inutilizado hasta el momento que un incidente afecte la disponibilidad del primer enlace. La conmutación en caso de falla es manejada por el protocolo de enrutamiento dinámico llamado Protocolo de Puerta de Enlace en el Borde (Border Gateway Protocol, BGP por sus siglas en ingles), el cual permite que las subredes de las sucursales y la matriz puedan ser intercambiadas a través de ambos enlaces principal y secundario. Al ocurrir un evento que afecta la disponibilidad del enlace principal, BGP determina que los prefijos que son intercambiados y tienen como siguiente salto la IP del enlace afectado sean considerados como inválidos y, por ende, no son considerados para reenvío de tráfico. El inconveniente se presenta por los altos tiempos de espera para conmutación del tráfico bajo un escenario normal. BGP maneja

temporizadores para determinar que existe una afectación sobre el enlace entre dos vecinos. [11]

El temporizador encargado de determinar que existió una falla en la vecindad de BGP se denomina Temporizador de Tiempo de Espera (Hold Time), el cual por defecto tiene un valor de 180 segundos o 3 veces el valor del temporizador de “Mantener Vivo” (Keepalive). El temporizador de Keepalive tiene por defecto un valor de 60 segundos, y son paquetes enviados de un vecino a otro con la finalidad de determinar que la comunicación entre vecinos se encuentra activa y sin inconvenientes. [11]

Bajo estas consideraciones, una conmutación por una falla de enlace puede tomar hasta 3 minutos para que se comience a utilizar el enlace alternativo, lo cual, para la empresa en análisis, resulta ser un tiempo que dada la criticidad en las transacciones que se realizan, desean mejorar.

La capacidad de los enlaces es de 1544 Mbps tanto el principal como el secundario, y los usuarios de las sucursales notan que durante el horario de 13h00 a 16h00 tienen una actividad mayor que la del resto de la jornada de trabajo. Durante ese intervalo, los usuarios de llamadas

telefónicas vía VoIP notan que existe un retardo o voz entre cortada que dificulta la comunicación de ambos usuarios. De la misma forma, los usuarios que hacen uso del servicio de transferencia de documentos vía el Protocolo de Transferencia de Archivos notan que los tiempos de transferencia se elevan durante el intervalo de congestión y los tiempos de respuesta de los dispositivos entre matriz y las sucursales, se elevan o incluso llegan a existir paquetes que se pierden en tránsito. Fuera del horario de congestión no existen inconvenientes de saturación en el enlace.

4.2 ANÁLISIS DEL DISEÑO PROPUESTO

La solución se basa en el uso de la Red de Área Amplia Inteligente de Cisco (iWan) para establecer un mejor uso de ambos canales en cada localidad a fin de evitar la subutilización o inutilización de estos, así como proveer una mayor seguridad en la información que fluye, gracias al mecanismo de cifrado en los paquetes, garantizando así la confidencialidad e integridad de la información.

La solución es aplicable para escenarios donde se cuenten con uno o más enlaces redundantes, de tal forma que la tecnología utilizada por la solución pueda evaluar por cual camino enviar cierto tráfico acorde a

consideraciones de calidad que se hayan estipulado. Para el escenario de la empresa, cada localidad tiene dos enlaces redundantes, por lo cual, es un candidato válido para implementación de la solución como se muestra en la figura 4.2.

La solución provee el concepto de Independencia de Transporte gracias al uso de la tecnología de Redes Privadas Virtuales Multi Punto Dinámicas (DMVPN), por lo cual, no es necesario que un solo Proveedor de Servicios ofrezca el enlace principal y alternativo, evitando un punto de falla común en caso de que todo el Proveedor de Servicios sufra una indisponibilidad. Bajo esta premisa, es importante destacar en el diseño que el enlace secundario no se contrate con el mismo Proveedor de Servicio del enlace principal, y el mismo puede ser de cualquier tipo de transporte, ya sea Internet, Transmisión de Datos por MPLS, Satelital, GEPON, 3G/4G, etc. [2]

Para el diseño propuesto, cada localidad tendrá dos enlaces de distinto tipo de transporte. En el caso de Matriz y la Sucursal-1 tenemos un enlace de Internet a través del Proveedor de Servicios 1 y un enlace de Transmisión de Datos MPLS a través del proveedor de Servicios 2. En el caso de la Sucursal-2 tenemos dos enlaces de Internet, uno a través del Proveedor de Servicios 1 con fibra óptica corporativa, y el otro con

un Proveedor de Servicios 2 con tecnología de Redes Ópticas Pasivas Gigabit Ethernet (GEPON por sus siglas en inglés) residencial.

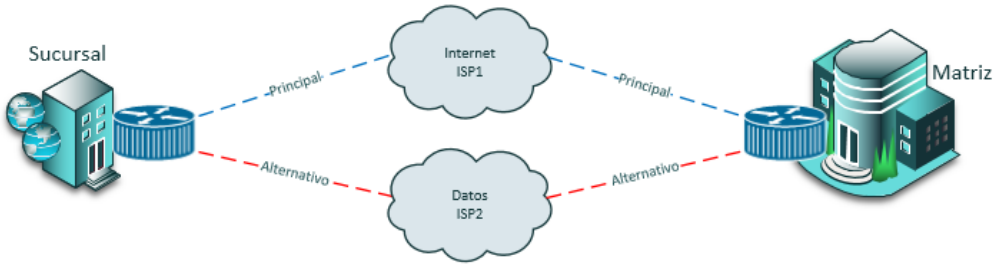


Figura 4.2 Tipos de enlaces del diseño propuesto

Con los transportes identificados y definidos, se procede a establecer la conectividad entre la Matriz y las Sucursales haciendo uso de la tecnología de DMVPN.

En el diseño de DMVPN vamos a considerar los siguientes aspectos:

- ✓ Cada transporte debe tener su propia nube de DMVPN, esto es, todas las localidades que compartan un transporte, como por ejemplo transmisión de datos MPLS, van a conectarse haciendo uso de una nube privada de DMVPN las cuales se representan como túneles multipunto que conectan las localidades a través de dicho transporte. Para el escenario de la empresa, el servicio de Internet ofrecido por el Proveedor de Servicios 1 se representa como el túnel 100. El servicio de Transmisión de Datos MPLS

ofrecido por el Proveedor de Servicios 2 se representa como el túnel 200. El servicio de Internet GEPON residencial ofrecido por el Proveedor de Servicios 2 se representa como el túnel 300. En la figura 4.3 observamos los túneles DMVPN creados entre las localidades. [6]

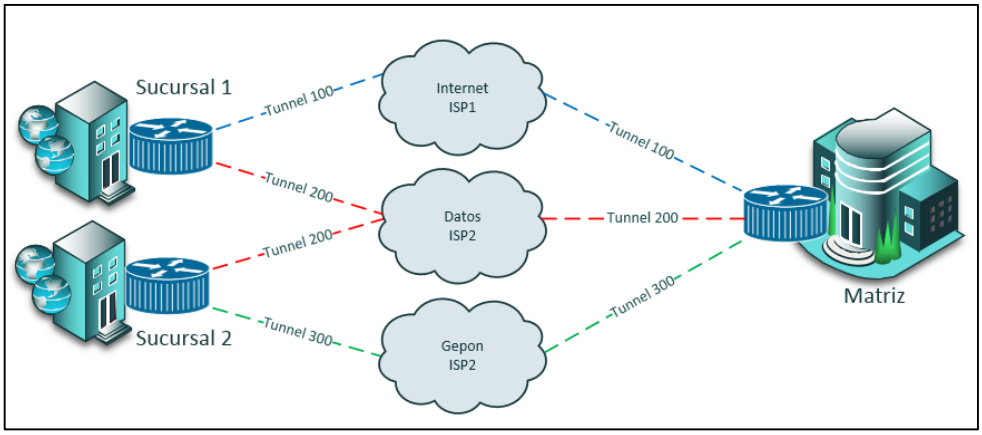


Figura 4.3 Túneles DMVPN

- ✓ Los túneles de DMVPN se centralizarán en Matriz, es decir, las sucursales deberán establecer una conexión hacia Matriz antes de poder determinar que camino es el más adecuado para reenvío de tráfico. Este esquema nos permite que la configuración inicial de una nueva sucursal se realice a través de los lineamientos definidos desde nuestra matriz centralizada. Cabe destacar que en caso de existir tráfico que sea de comunicación entre

sucursales, el tráfico de una sucursal origen no irá primero a matriz y luego a la sucursal destino dado que generaría un enrutamiento inadecuado y agotamiento de recursos del canal. El tráfico entre sucursales es instruido para que puedan ser reenviados directamente sin necesidad de pasar por la Matriz gracias al Protocolo de Redundancia del Próximo Salto (Next Hop Redundancy Protocol, NHRP por sus siglas en ingles). En la figura 4.4 mostramos el comportamiento del envío de tráfico utilizando el protocolo de NHRP. [8]

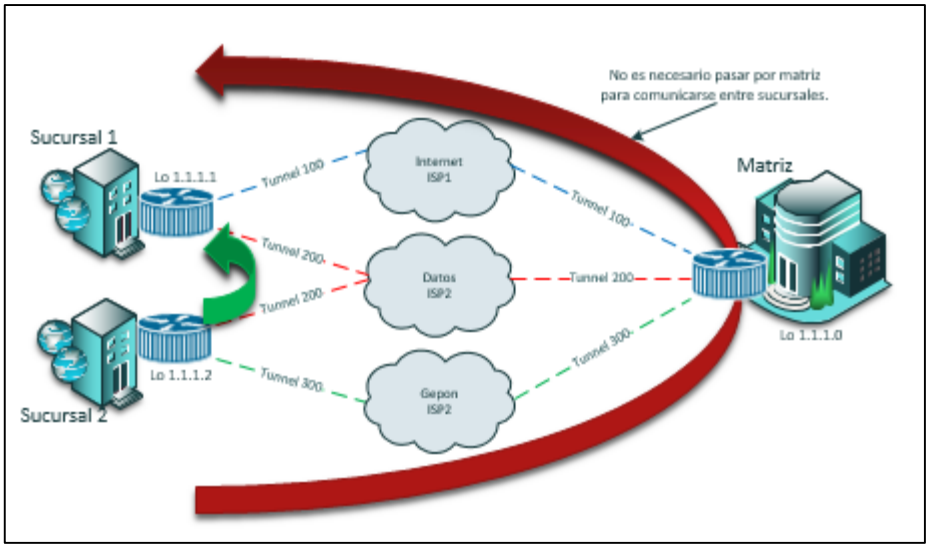


Figura 4.4 Comunicación ofrecida por el protocolo NHRP

✓ El protocolo de NHRP permite que los enrutadores puedan determinar el siguiente salto adecuado en cada nube DMVPN

que se haya definido. El procedimiento es automático en matriz, es decir, una vez configurado inicialmente, el enrutador matriz espera pasivamente que una sucursal inicie una comunicación a través de cada túnel DMVPN, y si los parámetros de comunicación coinciden en ambos extremos, se establecen sesiones entre las dos localidades que identifican a ambas como vecinos que usan el servicio de ese túnel. [8]

- ✓ Como una medida de seguridad, el protocolo de NHRP usado en los túneles DMVPN es protegido con una contraseña que prohíbe a enrutadores que no pertenecen a la empresa, establecer una conexión con los mismos y quieran participar en el proceso de resolución del siguiente salto tal como se muestra en la figura 4.5.

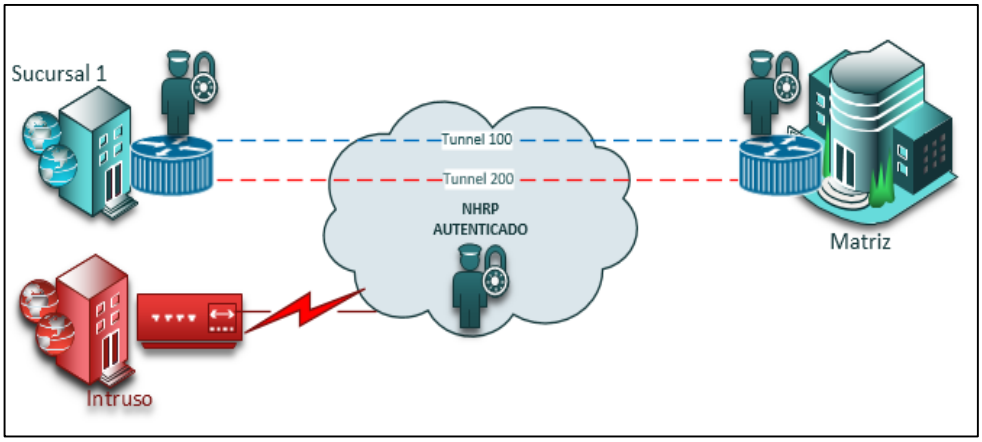


Figura 4.5 Autenticación dentro del protocolo de NHRP

- ✓ Para el caso de la Sucursal-2, tenemos dos transportes: El Servicio de Internet Corporativo y el Servicio de Internet residencial GEPON, sin embargo, al ser dos transportes de similares características (Ambos se enrutan a través del Internet), tenemos un inconveniente en el momento que el enrutador deba tomar la decisión de por qué servicio enviar un paquete. El enrutador debe tener una ruta por defecto activa a través de uno de los dos servicios, por lo cual, el otro servicio queda inutilizado hasta que el primer servicio se vea afectado. Para evitar este inconveniente y a fin de obtener el beneficio que buscamos que utilización efectiva de ambos enlaces, debemos definir en el enrutador una Instancia de Enrutamiento Virtual de Reenvío (VRF por sus siglas en inglés) mediante la cual, podamos separar los servicios brindados por cada Proveedor de Servicios y que se mantengan independientes el uno del otro. De esta forma, podemos indicar que una instancia tenga una ruta por defecto a través del Servicio de Internet Corporativo y otra instancia virtual tenga otra ruta por defecto a través del Servicio de Internet Residencial GEPON.

Con las nubes DMVPN operando y habiendo obtenido las vecindades a través de los servicios definidos, se procede a establecer el protocolo de enrutamiento dinámico que permitirá la comunicación entre las distintas subredes que tenga la empresa. La solución de Redes de Área Amplia Inteligente de Cisco sugiere el uso de dos protocolos de enrutamiento dinámicos: Protocolo de Puerta de Enlace Interior Mejorado (EIGRP por sus siglas en inglés) o Protocolo de Puerta de Enlace de Borde (BGP por sus siglas en ingles). La decisión de cuál de los dos protocolos usar está determinada por la preferencia del administrador de red, por lo cual, se ha optado por usar el protocolo de EIGRP como protocolo de enrutamiento para nuestro diseño y se resaltan las siguientes particularidades:

- ✓ Protocolo de rápida convergencia
- ✓ Envía solo una actualización cuando ocurre un cambio en la topología
- ✓ Usa paquetes de Saludo entre los vecinos a fin de mantener la vecindad y determinar una caída de enlace
- ✓ Usa el ancho de banda y el retado para hacer un cálculo de la preferencia de ruta a elegir.
- ✓ Soporta un balanceo de carga desigual

- ✓ Mantiene una tabla topológica en la cual almacena información sobre los distintos caminos disponibles. [10]

Una vez elegido el protocolo de enrutamiento dinámico EIGRP, tomaremos en consideración las siguientes recomendaciones de diseño aplicadas a la solución de Red de Área Amplia Inteligente:

- ✓ Las localidades remotas no deben reenviar las rutas aprendidas de un enrutador en matriz a otro enrutador en matriz.
- ✓ Los enrutadores en matriz deben anunciar las rutas de forma sumarizada a las sucursales a fin de que se pueda reducir el tamaño de la tabla de enrutamiento. De forma concisa esto consiste en anunciar una ruta por defecto para el caso de tráfico de Internet, los prefijos que se usan en la Matriz y los prefijos que se usan en las sucursales.
- ✓ Los enrutadores principales en cada localidad deben preferir las rutas aprendidas por los túneles asociados al mismo transporte que el otro enrutador, esto es, si un enrutador aprende una ruta a través del túnel 100 asociado al Servicio de Internet Corporativo, y también a través del túnel 300 asociado a Internet GEPON residencial, pero no posee un

transporte GEPON, entonces debe preferir reenviar tráfico por servicio de Internet Corporativo.

- ✓ Se debe manipular las métricas del protocolo de enrutamiento a fin de que el tráfico de red sea reenviado por el enlace de transporte preferencial, esto con la finalidad de que, en caso de una falla de la tecnología de Enrutamiento por Rendimiento, el tráfico siga su flujo normal por el transporte con mejor calidad.
- ✓ Se debe mantener la menor cantidad de variables de configuración a fin de que a futuro, se pueda automatizar el levantamiento de cualquier nueva sucursal. [2]

Para un mejor control de los enrutadores que forman vecindades, cada nueva vecindad se deberá autenticar contra la matriz dentro del protocolo de EIGRP utilizando el modo de autenticación más seguro que posee el protocolo Hashed Message Authentication Code-Secure Hash Algorithm-256 (HMAC-SHA-256) en el cual, se utiliza una clave secreta compartida que tiene que coincidir entre los dispositivos que deseen establecer una vecindad.

Se aseguran de que las interfaces que no deban tener habilitado el protocolo de enrutamiento dinámico se encuentren en estado pasivo,

esto es, no enviaran ni recibirán paquetes de saludo por las mismas, previniendo de esa forma cualquier intento de establecimiento de vecindad. [10]

En el diseño de la funcionalidad de Enrutamiento por Rendimiento (PFR por sus siglas en ingles), cada dispositivo debe cumplir un rol, y con ello, se procede a la definición de responsabilidades a realizar para establecer la correcta operación de este. El dominio de iWAN para la empresa está conformado por un sitio central (Matriz) y dos sitios remotos (Sucursal-1 y Sucursal-2). En cada sitio debemos definir un enrutador que debe ser el Controlador Maestro, el cual se encargará de tomar las decisiones locales y controlar a los Enrutadores de Borde en las mediciones de rendimiento y forzar la toma de un camino alternativo.

El enrutador en Matriz tendrá la función de Controlador Maestro del Sitio Central por lo cual, será el encargado de definir y distribuir las políticas de PfR para todo el dominio de iWAN. [15]

Por efectos de simplicidad, en cada Sucursal se tiene un solo enrutador, por lo cual, estos tomarán la función de Controlador Maestro del Sitio Remoto y se encargarán de mantener la sincronización con el sitio

central, así como tomar una decisión en su sitio respectivo para que un tráfico tome cierto camino, con base en las mediciones de rendimiento.

4.3 ANÁLISIS DEL ESCENARIO PILOTO PARA PRUEBAS

Las pruebas serán realizadas sobre la infraestructura operativa de la empresa, sin embargo, se deben tomar algunas consideraciones para prevenir cualquier tipo de afectación sobre los servicios funcionales en esta.

- La configuración de cada tecnología debe realizarse sobre ventanas programadas que se encuentren en un horario de bajo impacto, el cual puede ser a partir de la 01h00 en los fines de semana. Dichas ventanas de configuración deben ser notificadas a todo el personal de la localidad con la finalidad que no se agenden trabajos para ese intervalo de tiempo y minimizar cualquier impacto en la operación. Si bien la configuración no afectaría a los servicios en producción, las notificaciones se consideran una medida de minimizar cualquier riesgo en la disponibilidad los servicios de la empresa.
- Se debe generar los respaldos respectivos en la configuración de los enrutadores que van a intervenir directamente en la implementación de la solución.

- Las nuevas tecnologías de la solución pueden coexistir con las implementadas inicialmente por la empresa, por lo cual, no se eliminarán configuraciones iniciales a fin de garantizar a la empresa un rápido plan de acción en caso de requerir volver al esquema inicial.
- Al implementarse los protocolos, se debe garantizar que cada tecnología implementada haya alcanzado su estado operativo funcional y que se encuentre estable, por lo cual, no se realizará un envío de tráfico a través de la solución hasta verificar estabilidad de los protocolos durante una semana. Si posterior al periodo de verificación, se considera que la solución no ha sufrido ninguna afectación y los protocolos se han mantenido operativos, se puede planificar la ventana de migración del tráfico a través de la nueva solución.

4.4 REQUERIMIENTOS DE LOS DISPOSITIVOS PARA SOPORTE DE LA TECNOLOGÍA

La solución de Red de Área Amplia Inteligente requiere la configuración e implementación de varios protocolos y tecnologías. En la Tabla 5 se enumeran las tecnologías que serán utilizadas en la implementación de la solución en el piloto de pruebas definido. [2]

Tabla 5 Descripción de las tecnologías a utilizar en la solución.

	TECNOLOGÍA	ABREVIATURA	DESCRIPCIÓN
1	Protocolo de resolución del siguiente salto	NHRP	Protocolo encargado de identificar el dispositivo al cual se debe enviar un paquete en la subred.
2	Encapsulación de enrutamiento genérica	GRE	Protocolo de tunelización que permite encapsular la información que se desea enviar entre dos enrutadores remotos.
3	Red virtual privada dinámica multipunto	DMVPN	Solución que permite la integración entre los túneles GRE creados, haciendo uso de NHRP.
4	Protocolo de seguridad de Internet	IPSEC	Tecnología que define los protocolos de seguridad que serán utilizados en la solución
5	Protocolo de enrutamiento de puerta de enlace interior mejorado	EIGRP	Protocolo de enrutamiento dinámico que permitirá la conexión entre las subredes remotas para cada localidad.
6	Detección de envío bidireccional	BFD	Tecnología que nos permite tener una rápida detección en caso de falla de un enlace.
7	Enrutamiento por rendimiento versión 3	PfRv3	Tecnología que permite monitorear el estado de los enlaces y tomar una decisión de mejor camino para un tráfico determinado.

Los enrutadores necesitan un sistema operativo que es el encargado del correcto establecimiento y funcionamiento de dichas tecnologías, sin embargo, no todas las versiones de los sistemas operativos pueden ser soportadas por todos los modelos de enrutadores. Esto dependerá en su mayor parte de las características de rendimiento a nivel del hardware del dispositivo. El sistema operativo de los enrutadores CISCO se denomina CISCO IOS, en la Tabla 6 se muestra los requerimientos de versión de sistema operativo que indica CISCO para la implementación de la solución de Red de Área Amplia Inteligente. [5]

Tabla 6 Requerimientos de CISCO IOS para implementación de iWAN

PLATAFORMA	MODELO DE ENRUTADOR	CISCO SOFTWARE IOS
Cisco ISR-G2 Series Routers—1900 Series	ISR 1921 ISR 1941	Cisco IOS 15.7(3)M o posterior.
Cisco ISR-G2 Series Routers—2900 Series	ISR 2901 ISR 2911 ISR 2921 ISR 2951	Cisco IOS 15.7(3)M o posterior.
Cisco ISR-G2 Series Routers—3900 Series	ISR 3925 ISR 3925E ISR 3945 ISR 3945-E	Cisco IOS 15.7(3)M o posterior.

La empresa establece sus conexiones a través de enrutadores CISCO de modelo ISR 1841 perteneciente a la familia de los CISCO ISR 1800

Series, sin embargo, dicho modelo no soporta la implementación de la solución de Red de Área Amplia Inteligente, lo cual hace necesario un reemplazo de los enrutadores de cada localidad por otro modelo que soporte la solución. Para el caso del piloto de pruebas se ha tomado en consideración un reemplazo por un enrutador que pertenezca a la primera familia que pueda implementar la solución, y acorde con la Tabla 6, se toma la decisión de hacer el reemplazo por enrutadores de la familia de CISCO ISR 1900 Series.

En la Tabla 7 observamos los protocolos de enrutamiento y funcionalidades que soportan los dos modelos de la familia de CISCO ISR 1900 y adicional un valor aproximado del máximo rendimiento que puede soportar el equipo como capacidad de procesamiento total en una prueba de estrés realizada por CISCO. Dado que deseamos implementar la funcionalidad de Detección de Envío Bidireccional, es necesario que el modelo elegido sea el ISR 1941. [5]

Tabla 7 Comparación entre los modelos ISR 1921 y 1941

MODELO DE ENRUTADOR	PROTOCOLOS DE ENRUTAMIENTO	MÁXIMO RENDIMIENTO EN MBPS
ISR 1921	OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, static IP routing, IGMPv3, GRE, PIM-SSM, static IPv4 routing, static IPv6 routing, policy-based routing (PBR), MPLS	290
ISR 1941	OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, PIM-SSM, static IPv4 routing, static IPv6 routing, policy-based routing (PBR), MPLS, Bidirectional Forwarding Detection (BFD), IPv4-to-IPv6 Multicast	330

Con la decisión del modelo de enrutador a utilizar para el desarrollo de la solución, debemos tomar en consideración que las tecnologías que utilizaremos están ligadas a la activación de una licencia para su uso. La figura 4.6 muestra los cuatro paquetes existentes de licencias que se pueden activar en un enrutador CISCO de la familia ISR 1900. [5]

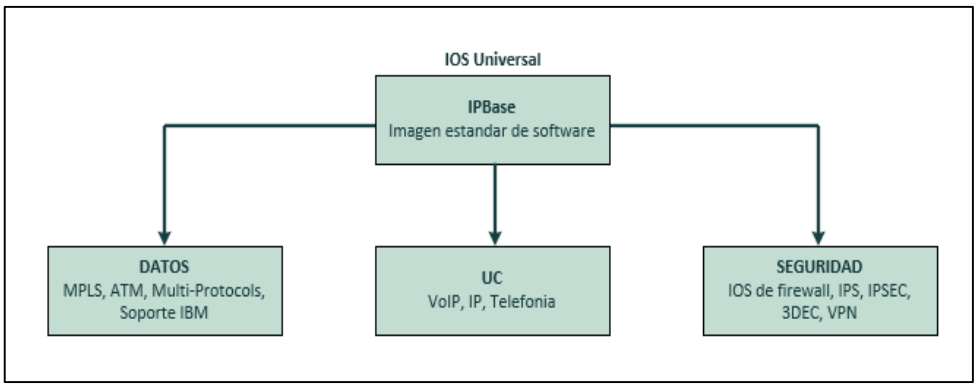


Figura 4.6 Licencias que se pueden activar en un enrutador CISCO de la familia ISR 1900

En el caso de los enrutadores de los modelos ISR 1900, el software utilizado por el enrutador debe tener habilitada la licencia asociada a las tecnologías que usaremos en la implementación de la solución, y que están descritas en la Tabla 5. Hemos realizado una correspondencia de cada tecnología a su respectiva licencia, y se muestra en la Tabla 8, con lo cual determinamos la necesidad de instalar tres licencias: IPBase, DATA y SECURITY, en cada uno de los enrutadores que se encuentran en las localidades de la empresa. La licencia IPBase es la que se encuentra implementada por defecto en los enrutadores, por lo cual, no requiere de ningún proceso de instalación. [5]

Tabla 8 Relación entre la tecnología y la licencia necesaria para su funcionamiento

	TECNOLOGÍA	ABREVIATURA	TIPO DE LICENCIA NECESARIA
1	Protocolo de resolución del siguiente salto	NHRP	IPBase
2	Encapsulación de enrutamiento genérica	GRE	IPBase
3	Red virtual privada dinámica multipunto	DMVPN	Security
4	Protocolo de seguridad de Internet	IPSEC	Security
5	Protocolo de enrutamiento de puerta de enlace interior mejorado	EIGRP	IPBase
6	Detección de envío bidireccional	BFD	DATA
7	Enrutamiento por rendimiento versión 3	PfRv3	DATA

Los enrutadores de modelo CISCO 1941 tienen un costo aproximado en el mercado de $375, mientras que las licencias que se requieren tienen un costo de $302 la licencia de SECURITY y $158 la licencia de DATA. Se considera un costo aproximado de $835 el proveer a un enrutador con la capacidad de soporte para la implementación de la solución de iWAN. [5]

4.5 DEFINICIÓN DE CAMINOS REDUNDANTES PARA EL TRÁFICO

Cada localidad de la empresa posee dos enlaces de red de área amplia de tal forma que genera una alta disponibilidad de los servicios en caso de afectación de un enlace. En el análisis del diseño propuesto identificamos cada enlace como un Túnel que se forma entre las distintas localidades, y dentro de la configuración del dominio de iWAN, estos caminos deben ser definidos formalmente con una etiqueta que los identifica a lo largo de toda la implementación.

En las Tablas 9 y 10 podemos identificar los enlaces en cada localidad, con la etiqueta que se ha asignado para esta implementación. Se debe tener en consideración que la etiqueta en el dominio de iWAN debe tener un máximo de 7 caracteres. [15]

Tabla 9 Definición de los enlaces para Matriz y Sucursal-1

LOCALIDAD MATRIZ / SUCURSAL-1	PROVEEDOR DE SERVICIO	TIPO DE ENLACE	TÚNEL ASOCIADO AL ENLACE	ETIQUETA EN EL DOMINIO DE IWAN
Enlace principal	ISP 2	Datos con MPLS por Fibra óptica	Túnel 200	MPLS
Enlace alternativo	ISP 1	Internet corporativo por Fibra óptica	Túnel 100	INETCRP

Tabla 10 Definición de los enlaces para Sucursal-2

LOCALIDAD SUCURSAL-2	PROVEEDOR DE SERVICIO	TIPO DE ENLACE	TÚNEL ASOCIADO AL ENLACE	ETIQUETA EN EL DOMINIO DE IWAN
Enlace principal	ISP 1	Internet corporativo por Fibra óptica	Túnel 100	INETCRP
Enlace alternativo	ISP 2	Internet residencial con tecnología GEPON	Túnel 300	INETGPN

Las etiquetas definidas proveen a la solución de la forma de identificar cada enlace, y esta información es consistente en todo el dominio de iWAN, es decir, de todos los enrutadores que formen parte de la solución. En la figura 4.7 se puede observar la definición de los caminos redundantes desde la perspectiva de la solución, finalmente la forma de llamar a los caminos dentro de la solución es definida por la etiqueta estipulada y que se configura en el Controlador Maestro.

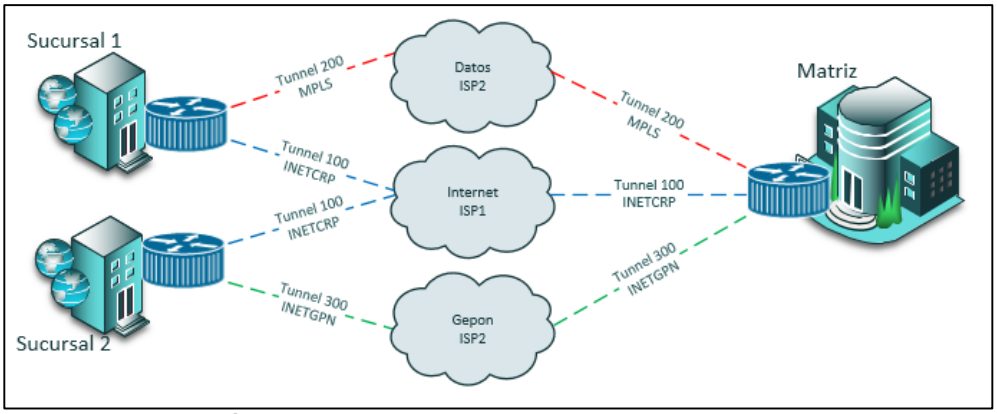


Figura 4.7 Definición de los caminos redundantes con sus respectivas etiquetas de la solución de iWAN

4.6 DEFINICIÓN DE PRIORIDAD DE TRÁFICO PARA LOS SERVICIOS

En el capítulo 3 se realizó la identificación de los servicios que hacen uso los usuarios de la empresa. Para el piloto de pruebas, se ha definido en la Tabla 11 el nivel de prioridad asignado para cada servicio. Se debe tener en consideración que la asignación de prioridades se ha realizado con base en la criticidad de los servicios para el usuario, sin embargo, la misma no es estática y puede cambiar acorde con las necesidades del usuario o la incorporación de nuevos servicios. Adicional, es necesario identificar cada servicio de una forma que la solución pueda interpretar y tomar una decisión adecuada de cómo tratar dicho tráfico del servicio, para esto, se utilizarán los criterios de calidad de servicio que consisten en marcar y clasificar el tráfico de red que fluye de una localidad a otra. Para marcar el tráfico necesitamos un criterio que se pueda cumplir, por

lo cual, usaremos como criterio de marcado los protocolos que usa cada servicio. El marcado se realiza a través del campo en la cabecera IP del paquete denominado Punto de Código de Servicios Diferenciados (Differentiated Service Code Point, DSCP por sus siglas en ingles), básicamente nos permite etiquetar el tráfico para que la solución pueda tomar identificar adecuadamente el tráfico de los servicios. [14] La marca será insertada por el enrutador en cada localidad al enviar el tráfico de su localidad hacia otra, con base en los criterios definidos en la Tabla 11.

Tabla 11 Identificación de prioridades para los servicios y marcado de los paquetes

SERVICIO	TIPO DE PROTOCOLO	PUERTO UTILIZADO	MARCA DSCP (AF)	PRIORIDAD
Voz	UDP	5060 / 5061	46 (EF)	Alta
Transferencia de archivos	TCP	21	26 (AF31)	Media
Aplicaciones generales	ICMP	0	18 (AF21)	Baja
Internet	TCP o UDP	0 - 65535	0	Último esfuerzo

El orden de importancia en la columna de prioridad se tomará de la siguiente forma:

Alta > Media > Baja > Último esfuerzo

Al servicio de Internet no se colocará ninguna marca por considerarse un servicio de muy baja importancia, será tratado como un servicio sin categorización pudiendo estar sujeto a políticas de último recurso que implica alta cantidad de retardos o paquetes perdidos.

4.7 DEFINICIÓN EN EL NIVEL DE SEGURIDAD A APLICAR PARA EL TRÁFICO

La solución de iWAN debe contener el componente de seguridad necesario para garantizar la integridad, confidencialidad y disponibilidad de la información. Se coloca un cierto nivel de confianza en el proveedor de servicios para mantener a integridad y la confidencialidad, pero debemos habilitar la seguridad necesaria en el lado de la organización para proteger el tráfico que fluye a través de los túneles. La protección será desplegada en las distintas fases del desarrollo de la solución.

Durante la implementación de los túneles, el establecimiento se realiza de forma dinámica, lo cual, puede causar que un enrutador intruso pueda establecer un túnel valido con un enrutador de la empresa. Para evitar un establecimiento indebido de un túnel, se usará una forma de autenticación sencilla que implementa la tecnología, basada en un número de llave que debe coincidir en ambos enrutadores que deseen establecer la conectividad. En la Tabla 12 observamos la llave definida

para el establecimiento de cada túnel en la implementación de la solución. La llave puede ser un número entero en el rango de 0 a 4294967295 y no es necesario que coincida con la numeración del túnel, pero por simplicidad en el desarrollo de la solución se ha definido que coincidan dichos valores. [12]

Tabla 12 Seguridad en el establecimiento de los túneles

Número de Túnel	Tipo de enlace	Número de llave
100	Internet corporativo por Fibra óptica	100
200	Datos con MPLS por Fibra óptica	200
300	Internet residencial con tecnología GEPON	300

Una vez establecido el túnel, se continúa con el proceso para levantar el Protocolo de resolución del siguiente salto (NHRP), el cual, nos permite agregar una seguridad en el protocolo a través del establecimiento de una cadena de caracteres como medida de autenticación. Solo los enrutadores configurados con la misma cadena de caracteres pueden comunicarse haciendo uso de NHRP, por lo cual, si el esquema de autenticación es usado, es necesario que la misma cadena de caracteres sea configurada en todos los dispositivos que hagan uso del protocolo. La solución recomienda el uso de la cadena de autenticación, pero hay que tener en consideración que la cadena de caracteres no es enviada de forma cifrada, por lo cual, no debe ser usada como único

mecanismo de autenticación para los enrutadores. La cadena de caracteres que utilizamos en todos los enrutadores de la solución es “iwan2018”. [12]

Con el protocolo de resolución del siguiente salto operativo, se debe configurar el protocolo de enrutamiento de EIGRP entre los enrutadores que deseen compartir la información de las subredes que van a utilizar. Los enrutadores deben establecer las vecindades dinámicamente con los enrutadores conectados en una subred común haciendo uso de paquetes “Hello” enviados periódicamente por cada enrutador. Se recomienda que los paquetes de hello sean autenticados en el intercambio entre dos vecinos, de manera que se asegure que un dispositivo acepte solo los paquetes que conozcan una llave pre compartida de autenticación. [10]

EIGRP soporta dos tipos de autenticación, a través del algoritmo de MD5 y a través del Algoritmo de Hash Seguro (Secure Hash algorithm, SHA por sus siglas en ingles). Se considera un algoritmo más seguro si su longitud de hash es mayor. Para el caso de los algoritmos soportados, MD5 tiene una longitud de hash de 128 bits mientras que SHA posee una longitud de hash de 256 bits, por lo cual, se implementará la autenticación con base en el algoritmo de SHA. Se debe tomar en

consideración que el algoritmo de SHA es solo soportado si el modo de operación de EIGRP es el modo extendido o nombrado, dado que el modo clásico de operación no soporta el algoritmo. Al igual que en la autenticación de NHRP, la llave pre compartida debe coincidir entre los enrutadores que deseen establecer una vecindad. Cada enrutador al recibir un paquete de hello hace una comparación entre el hash que se obtiene con su llave pre compartida y el hash enviado por el enrutador remoto, si no coincide entonces el paquete es descartado y no es procesado por el enrutador. La llave pre compartida utilizada en el desarrollo de la solución para el establecimiento de las vecindades en EIGRP es “P4ssw0rd41grp”. En la figura 4.8 se muestra un diagrama de flujo para el proceso de autenticación del protocolo de EIGRP. [10]

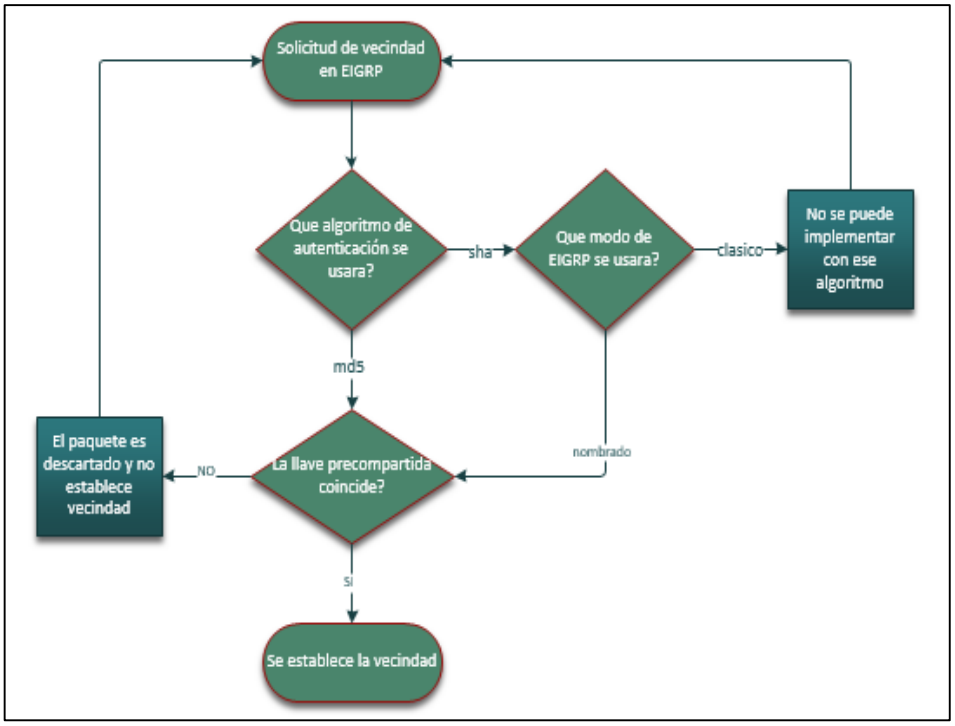


Figura 4.8 Diagrama de flujo para la seguridad aplicada al protocolo de EIGRP mediante autenticación de paquetes

Con la comunicación establecida entre las localidades, podemos realizar el cifrado del tráfico que fluye a través de los túneles. Los túneles DMVPN por defecto no cifran el tráfico que los atraviesa, pero si pueden ser cifrados utilizando IPSec. IPSec provee cifrado a través de una seguridad criptográfica y que fue diseñada con la perspectiva de interoperabilidad entre múltiples plataformas o vendedores. Cuando se integra IPSec con los túneles de DMVPN, los túneles cifrados proveen una red segura sobre cualquier transporte con las siguientes funciones:

- ✓ Autenticación de origen: Se logra a través del establecimiento de una llave pre compartida entre los enrutadores.
- ✓ Confidencialidad de la información: Se logra a través del establecimiento del algoritmo de cifrado entre dos enrutadores.
- ✓ Integridad de la información: Se logra a través del algoritmo de Hash y es encargado de asegurar que los paquetes no sean modificados en tránsito.
- ✓ Detección de reproducción: El cifrado de los túneles garantiza que un atacante intentando capturar el tráfico, no puedo insertar tráfico inválido en la red.
- ✓ Regeneración de clave de forma periódica: Cada cierto tiempo, se crean nuevas llaves de seguridad entre los enrutadores con la finalidad forzar un nuevo establecimiento de las asociaciones sin afectar al tráfico que se encuentra cursando por un túnel determinado.

Para lograr el cifrado de los paquetes, IPSec hace uso del protocolo de Encapsulamiento de seguridad en la carga útil (Encapsulation Security Payload, ESP por sus siglas en ingles), el cual se asegura que la información original mantiene la confidencialidad al cifrar la carga útil del paquete mientras se transporta a través de una red pública. A su vez,

se debe definir cuál será el algoritmo utilizado para cifrar y autenticar por el protocolo de ESP. En el anexo 3 se pueden apreciar las diferentes variantes que pueden tener el algoritmo de cifrado y el de autenticación en ESP. La diferencia se presenta fundamentalmente en la cantidad de bits que usa el algoritmo, recordando que mientras más alto sea el valor, más seguro es el algoritmo, pero a costo de mayor cantidad de procesamiento del equipo. [13]

CISCO recomienda usar en el desarrollo de la solución de iWAN los siguientes algoritmos, por ser la mejor combinación de alta seguridad con un consumo adecuado de recursos de procesamiento del enrutador:

- ✓ Para el cifrado en ESP: Estándar de Cifrado Avanzado de 128 bits (Advanced Encryption Standard, AES por sus siglas en ingles)
- ✓ Para la autenticación en ESP: Algoritmo de Hash Seguro (SHA) de 256 bits

Para la autenticación, se debe definir una llave pre compartida para el protocolo de seguridad y que debe coincidir entre los enrutadores que deseen cifrar el tráfico. Esta cadena de caracteres puede ser configurada para que sea diferente dependiendo de la dirección IP

remota con la cual se desee establecer la asociación de seguridad. Para efectos de la solución, se utilizará la llave pre compartida “3sp0l1w4n” para cualquier dirección IP se la cual provenga la solicitud, es decir, la dirección “0.0.0.0” que hace referencia a toda dirección IP. [13]

4.8 DEFINICIÓN DE UMBRALES PARA APLICAR EN LA TOMA DE DECISIÓN RESPECTO A LOS DIVERSOS CAMINOS

El controlador maestro es el dispositivo encargado de tomar una decisión con base en un criterio determinado dependiendo del tráfico de interés. La solución de iWAN posee plantillas con umbrales predeterminados con base en diversos parámetros. En el anexo 4 se observan las diferentes plantillas predefinidas que vienen por defecto en los enrutadores para la implementación de la solución de iWAN

En la implementación de la solución vamos a tomar en consideración las siguientes plantillas predefinidas de la Tabla 13 y 14 para los servicios definidos en la empresa. Solo para el caso del tráfico del servicio de Aplicaciones Generales se definirá sus propios umbrales válidos para el tráfico, y así poder confirmar que las políticas pueden ser personalizadas acorde con una necesidad. [15]

Tabla 13 Definición de umbrales para las localidades de Matriz y Sucursal-1

Servicio	Plantilla predefinida	Definición de umbrales	Camino principal	Camino Alternativo
Voz	Voice	Prioridad 1: retardo de una vía menor a 150ms Prioridad 2: Perdida de paquetes menor al 1% Prioridad 3: Variación menor a 30ms	MPLS	INETCRP
Transferencia de archivos	Low-latency-data	Prioridad 1: Retardo de una vía menor a 100ms Prioridad 2: Perdida de paquetes menor al 5%	MPLS	INETCRP
Aplicaciones generales	Personalizada	Prioridad 1: Retardo de una vía menor a 500 ms	INETCRP	MPLS
Internet	Sin Plantilla	Sin umbral definido	INETCRP	MPLS

Tabla 14 Definición de umbrales para Sucursal-2

Servicio	Plantilla predefinida	Definición de umbrales	Camino principal	Camino Alternativo
Voz	Voice	Prioridad 1: retardo de una vía menor a 150ms Prioridad 2: Perdida de paquetes menor al 1% Prioridad 3: Variación menor a 30ms	INETCRP	INETGPN
Transferencia de archivos	Low-latency-data	Prioridad 1: Retardo de una vía menor a 100ms Prioridad 2: Perdida de paquetes menor al 5%	INETCRP	INETGPN
Aplicaciones generales	Personalizada	Prioridad 1: Retardo de una vía menor a 500 ms	INETGPN	INETCRP
Internet	Sin Plantilla	Sin umbral definido	INETGPN	INETCRP

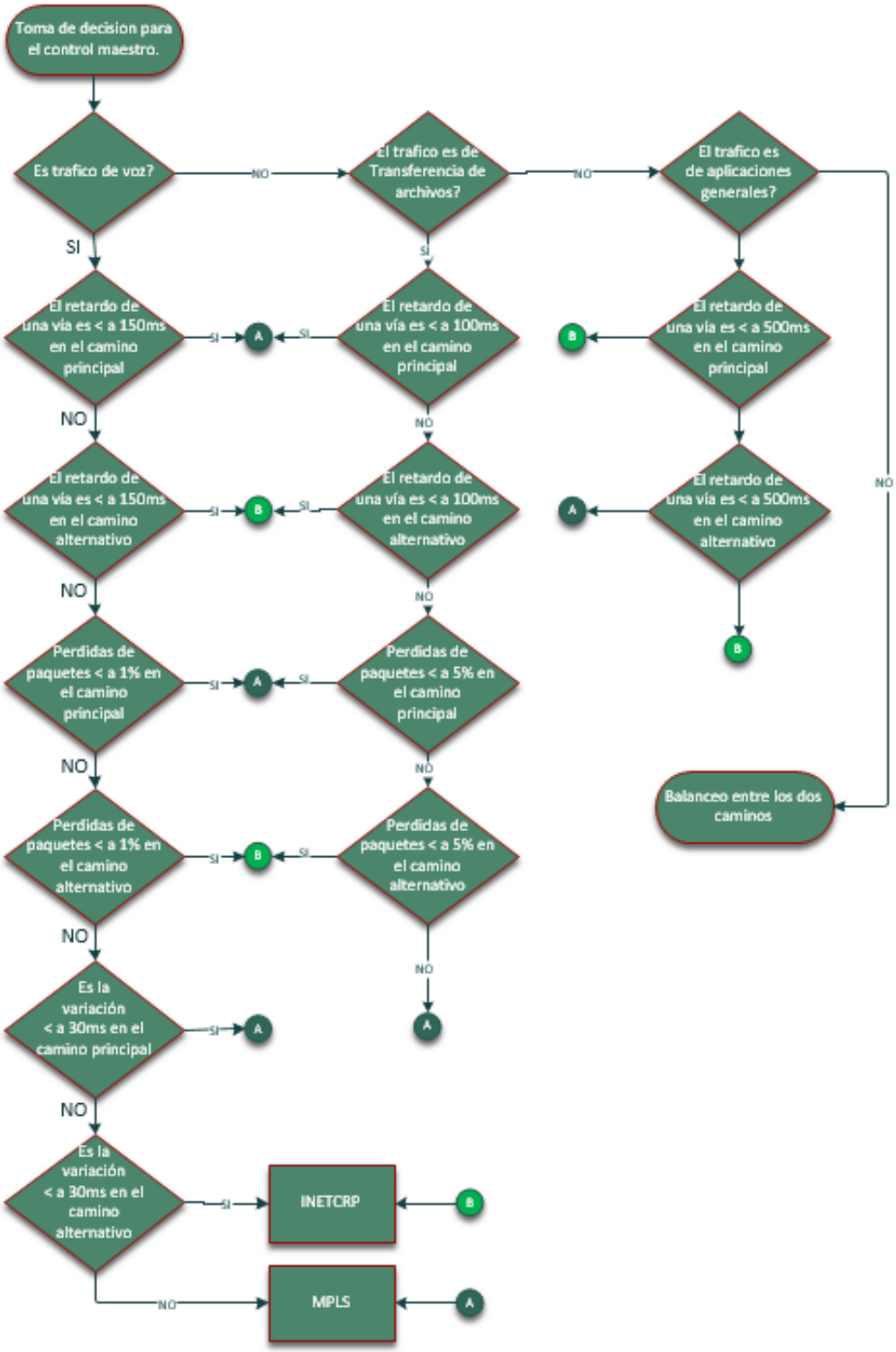


Figura 4.9 Diagrama toma de decisión Matriz / Sucursal1

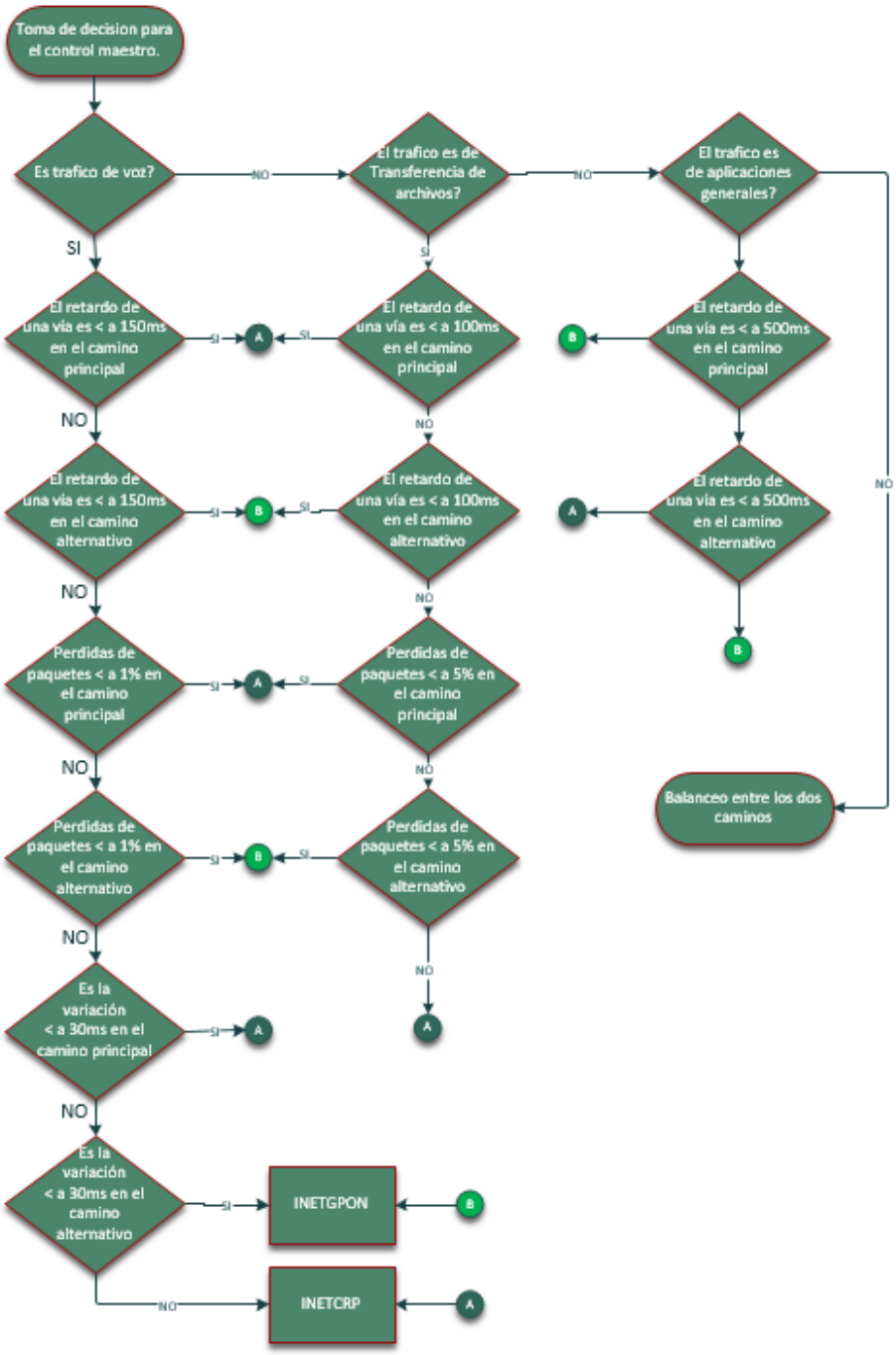


Figura 4.10 Diagrama toma de decisión Sucursal2

La definición del umbral se debe interpretar como el máximo valor permitido en el parámetro de medición para poder utilizar un camino por la solución como el camino principal. Si la medición del parámetro analizado excede el umbral definido, la solución interpreta el camino como un camino no apto para utilizar en el envío del tráfico para el servicio asociado y por ende procede a utilizar el camino alternativo siempre que este cumpla con los criterios de aceptación para el parámetro analizado. En el caso que ambos caminos no cumplan con el primer criterio de decisión, la solución consulta si existen otros parámetros de medición a considerar, los cuales son definidos como prioridades dentro de un mismo criterio. Las mediciones se realizan tomando en consideración el menor orden de prioridad, es decir, el criterio de prioridad 1 se evalúa antes que el criterio de prioridad 2, y así sucesivamente. En las figuras 4.9 y 4.10 se muestra el diagrama de flujo asociado al proceso de decisión del controlador maestro con base en las mediciones de los parámetros de calidad definidos. [15]

Tomaremos en consideración el siguiente ejemplo para entender la forma de tomar la decisión del controlador maestro para un servicio. Si analizamos el tráfico del servicio de Voz en Matriz, la plantilla predefinida posee 3 criterios de evaluación:

- ✓ Prioridad 1: Retardo de una vía menor a 150ms
- ✓ Prioridad 2: Perdida de paquetes menor al 1%
- ✓ Prioridad 3: Variación menor a 30ms

El controlador maestro se encuentra evaluando constantemente los 3 parámetros identificados en la definición. El primer parámetro evaluado es el retardo de una vía para un paquete, es decir, el tiempo que toma un paquete en ir desde el origen hacia su destino y debe ser menor a 150 milisegundos. Siempre que este parámetro sea menor a 150 ms, el tráfico del servicio de voz tomará el camino a través de la red MPLS del Proveedor de Servicios 2. En el momento que la medición da como resultado un retardo de una vía mayor a 150 ms, el controlador maestro marca el camino principal como un camino no valido para envío de tráfico del servicio de voz, y verifica si el camino alternativo cumple con el criterio de prioridad 1 definido, y si cumple con el criterio, se convierte en el nuevo camino utilizado para envío del tráfico de voz. Si el camino alternativo no cumple con el criterio de prioridad 1, entonces el controlador maestro procede a evaluar el criterio de prioridad 2 que realiza una medición sobre el porcentaje de paquetes perdidos que tiene el enlace. Si la cantidad de porcentaje de paquetes perdidos es menor al 1%, el enlace principal continúa como el enlace válido para envío de

tráfico de voz, pero si es mayor al 1%, el controlador maestro realiza la evaluación sobre el enlace alternativo y verifica si cumple con el criterio de prioridad 2. El criterio de prioridad 3 realiza una medición del parámetro llamado Variación, el cual hace referencia a la variación en el tiempo de retardo que tiene un paquete, por ejemplo, si un paquete demora en una primera medición 100 ms en ir desde el origen a su destino, y en una segunda medición demora 130 ms, la variación es 30 ms. La variación puede afectar a diversas aplicaciones y servicios entre las cuales se encuentra la voz, dado que una variación muy elevada puede causar el efecto de voz desfasada o entrecortada. Si se llega a evaluar todos los criterios definidos para el servicio, y no se cumple ninguno en ningún enlace, entonces la solución prefiere enviar el tráfico por el enlace que haya sido definido inicialmente como principal.

CAPÍTULO 5

IMPLEMENTACIÓN Y PRUEBAS

5.1 IMPLEMENTACIÓN DEL ESCENARIO PILOTO

En el análisis de requerimientos para dar soporte a la solución de iWAN realizados en el capítulo 4 se determinó que la implementación de las distintas tecnologías demanda un cambio de enrutador por motivo de soporte de sistema operativo necesario para el correcto funcionamiento de la solución. El enrutador seleccionado fue el CISCO ISR 1941 que se puede apreciar en la figura 5.1.

Figura 5.1 Enrutador modelo CISCO 1941

Las pruebas de eficiencia de la solución se realizarán en dos ambientes, un ambiente en producción y uno no productivo, durante los cuales se tomarán las mediciones asociadas a los parámetros a analizar. Para realizar las mediciones asociadas al ambiente en producción con la solución de iWAN, debemos realizar el cambio de enrutadores necesario para soporte de la tecnología en cada localidad de la empresa.

Dada la forma de operación de la empresa, es necesario coordinar con los usuarios una ventana de mantenimiento para hacer el reemplazo de los enrutadores, durante la cual se tendría afectación de cualquier servicio que se requiera en la respectiva localidad. En la Tabla 15 podemos observar un cronograma adecuado para realizar el reemplazo de los enrutadores en cada localidad con las respectivas fechas de

notificación teniendo en consideración que deben realizarse con al menos una semana de anticipación.

Tabla 15 Cronograma para mantenimiento de los enrutadores en las localidades

	Fecha de notificación	Fecha de mantenimiento	Hora de inicio	Hora de finalización
Sucursal-1	Semana 0	Sábado – Semana 1	01h00	04h00
Sucursal-2	Semana 1	Sábado – Semana 2	01h00	04h00
Matriz	Semana 2	Sábado – Semana 3	01h00	04h00

Durante la ventana de mantenimiento se debe tener en consideración el siguiente plan de acción para el reemplazo de los enrutadores en cada localidad.

1. Inicio de la ventana de mantenimiento.
2. Verificación de servicios operando correctamente, y enlaces de red de área amplia operativos.
3. Obtención del respaldo de la configuración del enrutador a ser reemplazado.
4. Instalación física del nuevo enrutador en una posición cercana al anterior.
5. Actualización del sistema operativo del nuevo enrutador a la versión de CISCO IOS 15.7(3)M recomendada por CISCO para la implementación de la solución.

6. Instalación de las licencias DATA y SECURITY en el enrutador para soporte de las tecnologías.
7. Configuración del nuevo enrutador con el respaldo obtenido del enrutador anterior.
8. Notificar el inicio del cambio de enrutador y comienzo de la afectación de los servicios.
9. Desconexión de los enlaces de red de área amplia del enrutador anterior.
10. Conexión de los enlaces de red de área amplia en el nuevo enrutador.
11. Verificación de conectividad al nuevo enrutador a través de los enlaces de red de área amplia migrados.
12. Desconexión de los enlaces de red área local del enrutador anterior.
13. Conexión de los enlaces de red de área local en el nuevo enrutador.
14. Verificación de conectividad hacia las redes de área local de las otras localidades.
15. Verificación de los servicios operando correctamente.
16. Finalización de la ventana de mantenimiento.

Finalizada la ventana de mantenimiento debemos confirmar en cada enrutador de cada localidad que se encuentre operando con el sistema operativo sugerido, y las licencias respectivas instaladas adecuadamente como se observa en la figura 5.2 5.3 y 5.4. El comando "show version" nos permite identificar el sistema operativo que se encuentra corriendo en el dispositivo y las licencias activas con su respectivo tipo de funcionamiento, ya sea una licencia permanente o una con periodo de evaluación. Para la implementación se han utilizado licencias con un periodo de prueba de 3 meses que son las que ofrece CISCO de forma gratuita para prueba de tecnologías. En las figuras 5.5 5.6 y 5.7 podemos observar las licencias habilitadas en los enrutadores que son requeridas para la implementación, para esto usamos el comando "show license feature". [10]

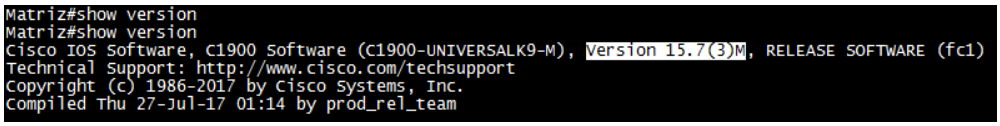


Figura 5.2 Enrutador en Matriz con el IOS 15.7(3)M

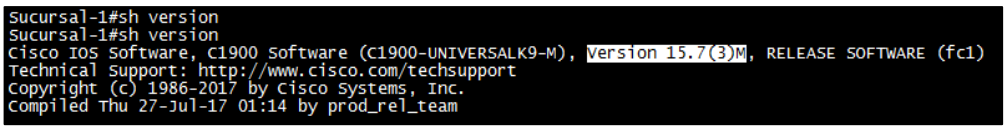


Figura 5.3 Enrutador en Sucursal-1 con el IOS 15.7(3)M

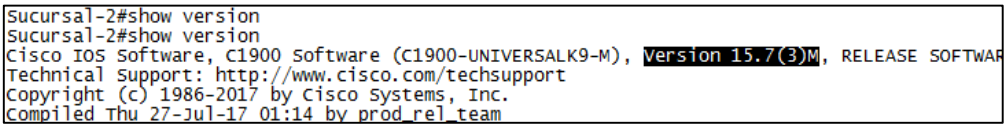


Figura 5.4 Enrutador en Sucursal-2 con el IOS 15.7(3)M

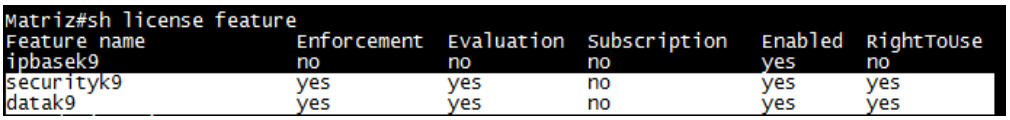


Figura 5.5 Enrutador en Matriz con las licencias de DATA y SECURITY habilitadas

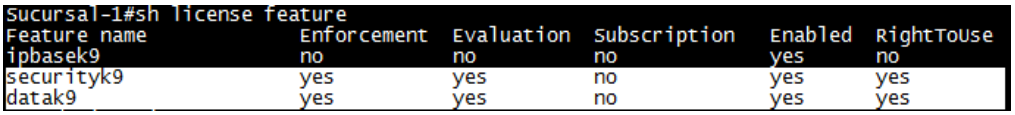


Figura 5.6 Enrutador en Sucurasl-1 con las licencias de DATA y SECURITY habilitadas

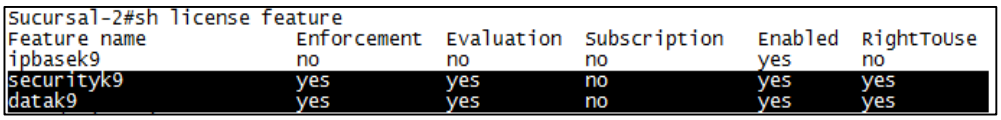


Figura 5.7 Enrutador en Sucursal-2 con las licencias de DATA y SECURITY habilitadas

Con la finalización de la ventana de mantenimiento en las tres localidades y con los enrutadores funcionando con el sistema operativo IOS versión 15.7(3)M con sus respectivas licencias, podemos confirmar que el escenario se encuentra listo para la implementación de la solución de CISCO iWAN.

5.2 INSTALACIÓN DE LA SOLUCIÓN PROPUESTA EN EL DISEÑO

La solución de CISCO iWAN requiere la configuración de varias tecnologías, las cuales mantienen dependencia entre ellas, no es posible configurar una tecnología sin haber configurado su dependencia anterior, por lo cual, en la Figura 5.8 se identifica el proceso de configuración para cada tecnología que se tomará en consideración en la instalación de la solución en cada enrutador de la empresa. [2]

Figura 5.8 Proceso de configuración para cada tecnología de la solución de iWAN.

5.3 CONFIGURACIÓN DE LOS COMPONENTES DE LA NUEVA INFRAESTRUCTURA

La primera fase de configuración corresponde al levantamiento de los túneles DMVPN entre las tres localidades. En la figura 5.9 se muestra un diagrama con información más específica sobre las IP que tienen los enlaces en cada localidad.

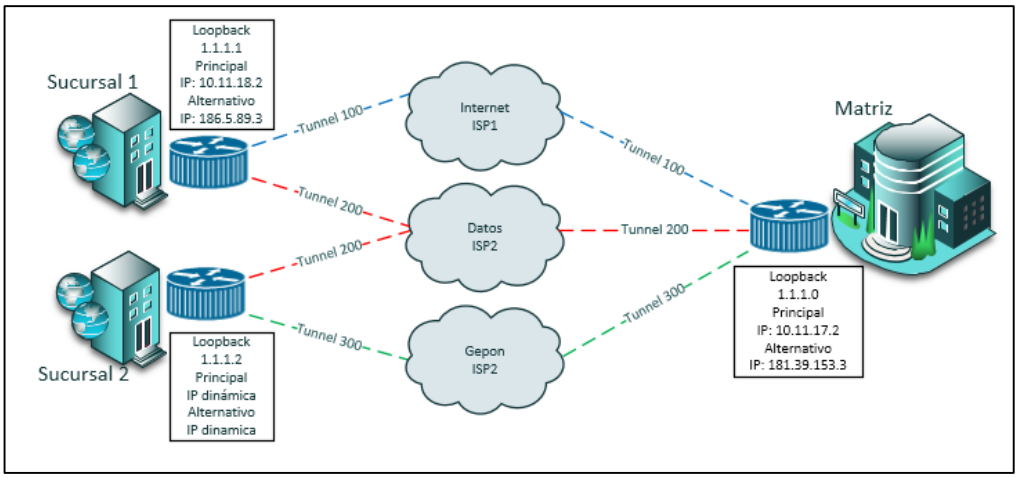


Figura 5.9 Diagrama con el direccionamiento IP en las localidades.

La información del direccionamiento IP para las redes de área amplia en las tres localidades se resume en la Tabla 16 y será de utilidad para el levantamiento de los túneles DMVPN.

Tabla 16 Direccionamiento IP en las tres localidades

	IP de loopback	Subred de red de área local	IP de enlace principal	IP del enlace alternativo
Matriz	1.1.1.0	192.168.0.0/24	10.11.17.2	181.39.153.3
Sucursal-1	1.1.1.1	192.168.1.0/24	10.11.18.2	186.5.89.3
Sucursal-2	1.1.1.2	192.168.2.0/24	Dinámica a través del ISP1	Dinámica a través del ISP2

La configuración de los túneles DMVPN representa una interconexión lógica entre las distintas localidades y por tal motivo, debe tener un direccionamiento IP asignado a estos nuevos enlaces. En la Tabla 17 se asigna el direccionamiento lógico para cada túnel en cada localidad.

Tabla 17 Direccionamiento IP para los túneles DMVPN en las tres localidades

	Túnel principal	IP del túnel principal	Túnel alternativo	IP del túnel alternativo
Matriz	Túnel 200 – ISP2	200.200.200.1	Túnel 100 – ISP1	100.100.100.1
Sucursal-1	Túnel 200 – ISP2	200.200.200.11	Túnel 100 – ISP1	100.100.100.11
Sucursal-2	Túnel 100 – ISP1	100.100.100.22	Túnel 300 – ISP2	30.30.30.22

Identificado el direccionamiento a asignar para cada túnel, la configuración del túnel exige se identifique cuál será la interfaz física con la que será originada la conexión lógica del túnel en consideración. En la Tabla 18 se observa la interfaz asociada a cada túnel para establecimiento de la conexión.

Tabla 18 Definición de interfaces asociadas a los túneles DMVPN en las tres localidades

	Túnel principal	**Interfaz del túnel principal**	**Túnel alternativo**	**Interfaz del túnel alternativo**
Matriz	Túnel 200 – ISP2	GigabitEthernet0/0/0	Túnel 100 – ISP1	GigabitEthernet0/0
Sucursal-1	Túnel 200 – ISP2	GigabitEthernet0/1	Túnel 100 – ISP1	GigabitEthernet0/0
Sucursal-2	Túnel 100 – ISP1	GigabitEthernet0/0	Túnel 300 – ISP2	GigabitEthernet0/1

Para el establecimiento de los túneles DMVPN, se utilizará el modo de tunelización a través del protocolo de Encapsulación de Enrutamiento Genérica (GRE), y acorde a lo establecido por la solución y la naturaleza de descubrimiento automático de localidades remotas, será establecida de la forma GRE multipunto. [7] Esto nos permite que, a través del mismo enlace lógico, se puedan descubrir las diferentes localidades sin tener que crear un enlace lógico para cada una. En el anexo 1 se indican las configuraciones necesarias para levantar los túneles lógicos DMVPN en cada localidad. Como resultado, debemos confirmar que el estado de los túneles se encuentre en un estado “UP” con la dirección IP definida en la Tabla 17 y el modo de operación como “multi-GRE” que representa el modo GRE multipunto, y se puede observar su verificación en la Figura 5.10

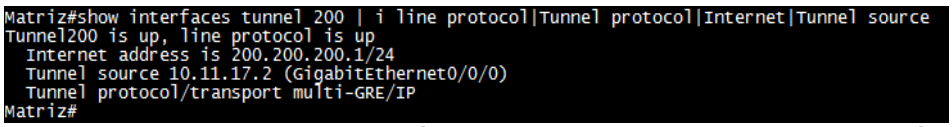


Figura 5.10 Ejemplo de verificación en Matriz para el levantamiento del túnel 200.

Levantados los túneles DMVPN en las tres localidades, se procede a la siguiente fase de configuración asociada al protocolo de resolución del siguiente salto (NHRP). En el anexo 1 se muestran las configuraciones asociadas al protocolo, se debe tener en consideración que las configuraciones son diferentes para el enrutador central y para los enrutadores remotos. Principalmente esto se debe al modelo de la solución en el cual, el enrutador central es el encargado de escuchar las nuevas conexiones que se generen remotamente y validar si es factible que puedan establecer una conexión contra él. Desde el aspecto de configuración esto se ve reflejado en lo siguiente:

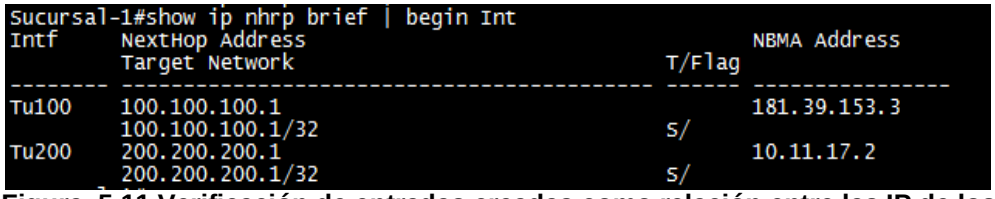
- Todos los túneles en el enrutador en la matriz escuchan los paquetes de NHRP y los ingresan a una tabla que permite ir formando la relación con los enrutadores remotos que vaya descubriendo. Esto se realiza con el uso del comando “ip nhrp map multicast dynamic”. [8]
- Los enrutadores remotos deben dirigir los paquetes de NHRP directamente hacia el enrutador principal en la matriz, por lo

cual, necesitan asociar cual es la IP que tiene la interfaz en el enrutador principal por el cual recibirá el paquete, y, además, cual es la IP que tiene asignada el túnel de la interfaz correspondiente. Por ejemplo, si el paquete se recibe en matriz por el enlace de datos MPLS con el ISP 2, esto será el túnel 200 que tiene asignada la IP 200.200.200.1, y a su vez, utiliza la interfaz GigabitEthernet0/0/0 con IP 10.11.17.2, por lo tanto, la relación sería (200.200.200.1 10.11.17.2) y es expresada en configuración como “ip nhrp map 200.200.200.1 10.11.17.2”.

- Los enrutadores remotos adicionales, deben declarar explícitamente la IP del túnel en el enrutador principal. al cual dirigen los paquetes, y lleva el nombre de Servidor de Siguiente Salto (Next Hop Server, NHS por sus siglas en ingles), y es expresado con el comando: “ip nhrp nhs”, en el ejemplo anterior el NHS sería “ip nhrp nhs 200.200.200.1”. [8]

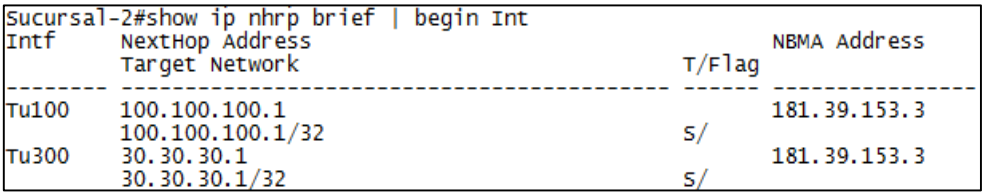
Como resultado de esta fase, cada enrutador debe llenar una tabla con las entradas creadas por el protocolo, en la cual, hace referencia a la IP del túnel con la IP de la interfaz. En el caso de los enrutadores de las sucursales, cada uno debe tener dos entradas creadas en la tabla, que

hacen referencia a las IP que tiene en la conexión por cada enlace hacia la matriz como se observa en la Figura 5.11 y 5.12. [8]



```
Sucursal-1#show ip nhrp brief | begin Int
Intf     NextHop Address                                NBMA Address
         Target Network                          T/Flag
-------- ---------------------------------------- ------ ----------------
Tu100    100.100.100.1                                  181.39.153.3
         100.100.100.1/32                        S/
Tu200    200.200.200.1                                  10.11.17.2
         200.200.200.1/32                        S/
```

Figura 5.11 Verificación de entradas creadas como relación entre las IP de los enlaces en Sucursal-1



```
Sucursal-2#show ip nhrp brief | begin Int
Intf     NextHop Address                                NBMA Address
         Target Network                          T/Flag
-------- ---------------------------------------- ------ ----------------
Tu100    100.100.100.1                                  181.39.153.3
         100.100.100.1/32                        S/
Tu300    30.30.30.1                                     181.39.153.3
         30.30.30.1/32                           S/
```

Figura 5.12 Verificación de entradas creadas como relación entre las IP de los enlaces en Sucursal-2

Con el protocolo de NHRP y las entradas en su tabla correctamente identificadas, procedemos a agregar los parámetros de seguridad asociados al cifrado del túnel. Los algoritmos utilizados para el cifrado fueron definidos en el capítulo 4, y su configuración se adjunta en el anexo 1. Es importante destacar los siguientes aspectos de configuración:

- Los algoritmos deben coincidir en todos los enrutadores que deseen cifrar el tráfico que fluye a través de ellos. Si un

algoritmo no coincide, la protección falla y, por ende, el túnel pierde conectividad. [13]

- El enrutador principal en Matriz debe recibir las conexiones de forma dinámica, por lo cual, él debe indicar en su configuración que espera recibir los paquetes desde cualquier IP, representado con “0.0.0.0” en el comando: “crypto isakmp key 3sp0l1w4n address 0.0.0.0” [13]
- Las sucursales deben indicar explícitamente la IP de las interfaces en Matriz contra las cuales se deben autenticar, por ejemplo, en el caso de Sucursal-1, debe indicar que realizará la autenticación contra la IP 10.11.17.2 asociada al enlace de datos MPLS, y contra la IP 181.39.153.3 asociada al enlace de internet corporativo.

Como resultado se debe observar que las asociaciones de seguridad se hayan creado adecuadamente y se encuentren en un estado “ACTIVE” como se muestra en la figura 5.13 y 5.14. En este punto el enrutador de Matriz debe probar conectividad con la IP de los túneles de los enrutadores en las sucursales y debe ser exitosa antes de proceder con la fase de configuración del protocolo de enrutamiento. Se adjuntan resultados de conectividad en el anexo 2. [13]

```
Sucursal-1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.11.17.2      10.11.18.2      QM_IDLE           1139 ACTIVE
186.5.89.3      181.39.153.3    QM_IDLE           1140 ACTIVE
```

Figura 5.13 Verificación de asociaciones de seguridad activas entre la Sucursal-1 y Matriz

```
Sucursal-2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
181.39.153.3    100.67.18.182   QM_IDLE           1026 ACTIVE
181.39.153.3    192.168.100.50  QM_IDLE           1025 ACTIVE
```

Figura 5.14 Verificación de asociaciones de seguridad activas entre la Sucursal-2 y Matriz

Con la conectividad exitosa entre los túneles de Matriz y las sucursales, procedemos a la fase de levantamiento del protocolo de enrutamiento entre los enrutadores de las localidades. El protocolo de enrutamiento es EIGRP, y se debe tener especial cuidado en su configuración en ambientes de producción, dado que puede afectar al enrutamiento que usa la empresa. Esto depende del protocolo de enrutamiento que use inicialmente, dado que cada protocolo de enrutamiento tiene una medida de preferencia que ayuda a determinar que protocolo tiene más preferencia sobre otro, y es denominada Distancia Administrativa. En el caso de la empresa en análisis, inicialmente usa el protocolo de BGP con sesiones externas, las cuales usan una distancia administrativa con un valor de 20, y el protocolo de EIGRP usa una distancia administrativa de 90, por lo cual, se considera como un protocolo de enrutamiento como

mejor o preferido si su distancia administrativa es menor (20 de BGP < 90 de EIGRP). [10] Bajo esta consideración, se procede a configurar el protocolo de enrutamiento sin riesgo de afectar al enrutamiento actual de la empresa. En el anexo 1 se adjuntan las configuraciones relacionadas al protocolo de EIGRP, y adicional, durante el proceso de configuración se ha agregado la parte relacionada a la autenticación del protocolo de tal forma que no puedan establecer vecindades dos enrutadores cuyas llaves pre compartidas no coinciden.

Como resultado se debe verificar que cada enrutador en las sucursales deba establecer dos vecindades con Matriz, una a través de cada enlace como se observa en la figura 5.15 y 5.16. [10]

```
Sucursal-1#show eigrp address-family ipv4 neighbors
EIGRP-IPv4 VR(IWAN) Address-Family Neighbors for AS(10)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
1   100.100.100.1           Tu100                    12 4w0d        9   234  0  553
0   200.200.200.1           Tu200                    14 4w0d        1   216  0  552
```

Figura 5.15 Verificación de vecindades en Sucursal-1 con Matriz

```
Sucursal-2#show eigrp address-family ipv4 neighbors
EIGRP-IPv4 VR(IWAN) Address-Family Neighbors for AS(10)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
1   100.100.100.1           Tu100                    10 1d11h       4  1398  0  553
0   30.30.30.1              Tu300                    10 1d11h       3  1398  0  551
```

Figura 5.16 Verificación de vecindades en Sucursal-2 con Matriz

Con las vecindades establecidas en el protocolo de enrutamiento, podemos configurar la funcionalidad de detección de envío bidireccional (BFD) con la finalidad de una rápida convergencia de los enlaces en caso de una falla sobre alguno. BFD actúa directamente sobre el protocolo de enrutamiento proveyendo una alerta en el caso que se detecte una pérdida de paquetes de control enviados por el protocolo. Si tres paquetes de control en BFD no llegan a su destino, la tecnología asume que existe una falla en el enlace, y envía una alerta al protocolo de enrutamiento, EIGRP en este caso, para que elimine cualquier vecindad que se haya levantado sobre dicho enlace, de esta forma, se evita que paquetes sigan siendo enviados por un enlace que ha presentado una falla, y cuya detección se ha logrado en tiempos de milisegundos. Se adjunta en el anexo 1 las configuraciones relacionadas a la tecnología de BFD, y en la figura 5.17 y 5.18 se observa el resultado de las configuraciones en la cual, se establecen también vecindades entre dos enrutadores que han recibido paquetes de control de BFD y están censando el estado de estos. [10]

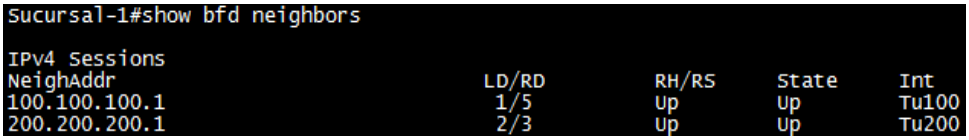


Figura 5.17 Verificación de vecindades BFD en Sucursal-1 con Matriz

```
Sucursal-2#show bfd neighbors

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
30.30.30.1                             2/6           Up        Up        Tu300
100.100.100.1                          1/4           Up        Up        Tu100
```

Figura 5.18 Verificación de vecindades BFD en Sucursal-2 con Matriz

La última fase de configuración corresponde al levantamiento de la configuración asociada a la tecnología de Enrutamiento por Rendimiento (PfRv3). El enrutador en Matriz ha sido definido como el Controlador Maestro del sitio central, es decir, el enrutador principal encargado de sincronizar las políticas e información del estado de los caminos a los demás enrutadores en las sucursales remotas. Con esta consideración, el mayor detalle de configuración se encuentra en este Controlador Maestro, mientras que los enrutadores de las sucursales se limitan a establecer conectividad contra él, y recibir las políticas y definiciones que en él se disponga. [15]

Se deben tener las siguientes consideraciones en el proceso de configuración de PfRv3.

- Existen dos listas de prefijos que deben ser definidas y estipuladas en la configuración. Una se denomina lista de prefijos del sitio, y otra lista de prefijos de la empresa. Dentro de ellas deben contener información acerca de las subredes

que se usan en la red empresarial y que serán monitoreadas para toma de decisión del controlador maestro respecto a que enlace de red de área amplia utilizar. La lista de prefijos de la empresa es la que debe contener a todos los prefijos usados en la topología, por tal motivo, debe también contener los prefijos que se definan en la lista de prefijos del sitio que serían las sucursales.

- En este proceso cada túnel debe recibir la etiqueta en el dominio de iWAN que se definió en las Tablas 9 y 10. Esta etiqueta será la forma que tiene la solución para identificar cada enlace de red de área amplia. Esta etiqueta se define en los túneles de Matriz, mientras que las sucursales solo reciben esta información automáticamente dependiendo del túnel por el cual establezcan la conexión.
- La opción de balanceo de carga se configura con el comando “load-balance” y solo funciona sobre el tráfico que no sea definido en ninguna clase de tráfico, es decir, tráfico que no se encuentra monitoreado. [15]
- En el proceso de configuración se ha agregado la sentencia de autenticación para la tecnología, de tal forma que solo los enrutadores que compartan la misma clave puedan recibir información del controlador maestro.

Como resultado de la configuración, es importante verificar que cada enrutador en las sucursales reciba información del controlador maestro del sitio central. En las figuras 5.19 y 5.20 se puede apreciar los estados operacionales y funcionales en los enrutadores de las sucursales, así como información de las etiquetas que ha asignado el controlador maestro en Matriz, la cual ha sido recibido de forma automática por cada túnel respectivo. [15]

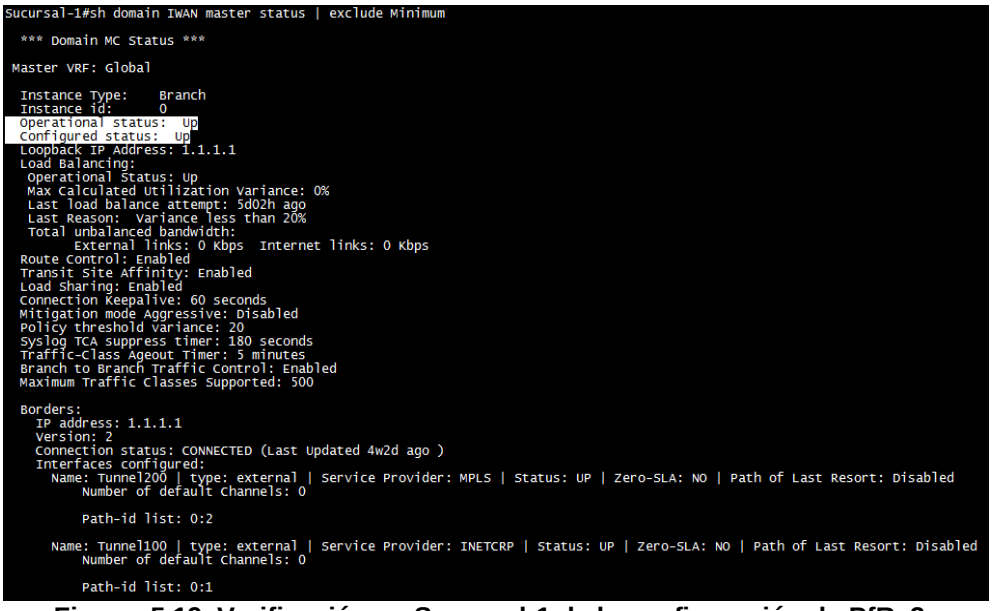


Figura 5.19 Verificación en Sucursal-1 de la configuración de PfRv3

```
Sucursal-2#show domain IWAN master status | exclude Minimum

  *** Domain MC Status ***

 Master VRF: Global

  Instance Type:    Branch
  Instance id:      0
  Operational status:  Up
  Configured status:  Up
  Loopback IP Address: 1.1.1.2
  Load Balancing:
   Operational Status: Up
   Max Calculated Utilization Variance: 0%
   Last load balance attempt: never
   Last Reason:  Variance less than 20%
   Total unbalanced bandwidth:
         External links: 0 Kbps  Internet links: 0 Kbps
  Route Control: Enabled
  Transit Site Affinity: Enabled
  Load Sharing: Enabled
  Connection Keepalive: 60 seconds
  Mitigation mode Aggressive: Disabled
  Policy threshold variance: 20
  Syslog TCA suppress timer: 180 seconds
  Traffic-Class Ageout Timer: 5 minutes
  Branch to Branch Traffic Control: Enabled
  Maximum Traffic Classes Supported: 500

  Borders:
    IP address: 1.1.1.2
    Version: 2
    Connection status: CONNECTED (Last Updated 09:48:06 ago )
    Interfaces configured:
      Name: Tunnel100 | type: external | Service Provider: INETCRP | Status: UP | Zero-SLA: NO | Path of Last Resort: Disabled
          Number of default Channels: 0

          Path-id list: 0:1

      Name: Tunnel300 | type: external | Service Provider: INETGPN | Status: UP | Zero-SLA: NO | Path of Last Resort: Disabled
          Number of default Channels: 0

          Path-id list: 0:3
```

Figura 5.20 Verificación en Sucursal-2 de la configuración de PfRv3

Por ejemplo, en la figura 5.20 podemos observar el estado de PfRv3 en la Sucursal-2, y de especial atención es observar la sección relacionada a los enrutadores de borde “Borders” en la cual se pueda apreciar que a través del túnel local 100, he recibido información de un proveedor de servicios con una etiqueta “INETCRP” la cual conocemos se encuentra asociada al servicio de internet corporativo ofrecido por el ISP-1. Así mismo, en el túnel local 300 recibimos la etiqueta del proveedor de servicio “INETGPN” que se encuentra asociada al servicio de internet residencial con tecnología GEPON ofrecido por el ISP-2.

5.4 PLAN DE PRUEBAS

El escenario piloto se ha levantado sobre los enrutadores en producción, de tal forma que el tráfico normal de la empresa continúa funcionando como antes de aplicar las configuraciones de la solución de iWAN. Para la evaluación de la eficiencia de la solución se tomaron en consideración la medición de los siguientes indicadores: Utilización del ancho de banda del circuito, Tiempo de retransmisión en caso de congestión, Tiempo de retransmisión sin congestión, Tiempo de conmutación en caso de caída de un enlace. El levantamiento de esta información consistirá principalmente en dos etapas:

- En ambientes no productivos, en el cual la red de la empresa continúa operando acorde a su funcionamiento inicial, sin que la solución de iWAN esté afectando el tráfico de los enlaces.
- En ambientes de producción, para lo cual, se debe dar dominancia al protocolo de enrutamiento que maneja la solución de iWAN (EIGRP) a fin de que se pueda tener el monitoreo del rendimiento de los enlaces y se pueda tomar una decisión acorde a los umbrales estipulados.

5.5 PRUEBAS EN AMBIENTES NO PRODUCTIVOS

Durante las pruebas en ambientes no productivos debemos validar inicialmente que exista conectividad entre las localidades, y que los servicios funcionen de forma adecuada.

En la figura 5.21 observamos una computadora que realiza las pruebas de conectividad desde la red de área local en la Sucursal-2 con dirección IP 192.168.2.2 y mediante un envío de paquetes ICMP usando la herramienta de ping, podemos confirmar que existe conexión hacia el servidor de aplicaciones generales con en Matriz con IP 192.168.0.100.

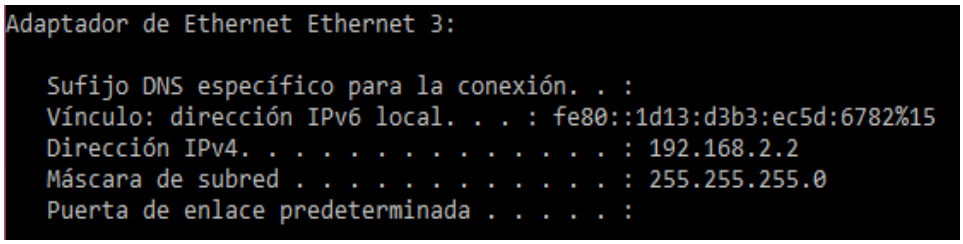


Figura 5.21 Dispositivo con dirección IP 192.168.2.2 conectado en Sucursal-2

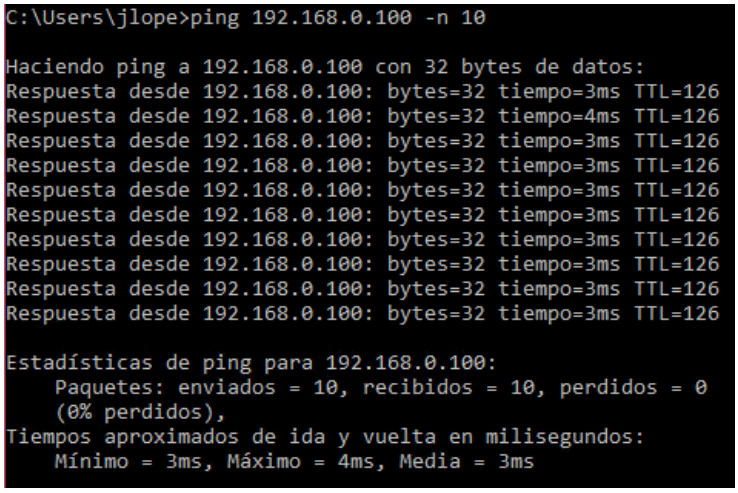


Figura 5.22 Prueba de conectividad con ICMP hacia el servidor de aplicaciones generales con IP 192.168.0.100

El servicio de transferencia de archivos se prueba mediante una conexión FTP realizada hacia el servidor de transferencia de archivos con IP 192.168.0.120 ubicado en Matriz. En la figura 5.23 se observa una conexión establecida exitosamente contra el servidor FTP, y una transferencia en curso de un archivo ubicado en Matriz hacia la computadora ubicada en la Sucursal-2.

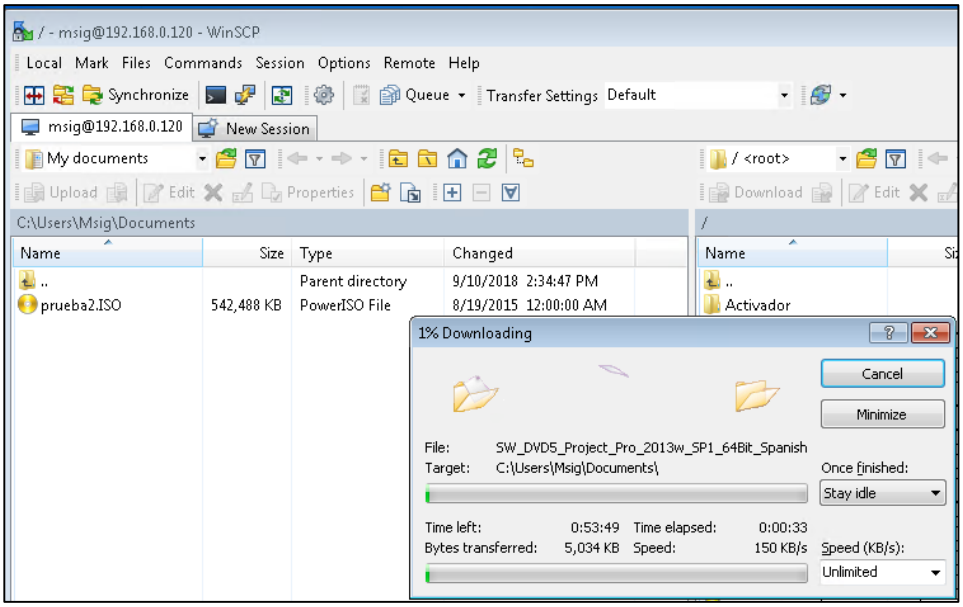


Figura 5.23 Verificación de funcionamiento del servicio de FTP haciendo una transferencia desde el servidor con IP 192.168.0.120

Para verificar la correcta operación del servicio de voz, se establece una llamada mediante VoIP entre la computadora y el servidor que funciona como central de voz con dirección IP 192.168.0.110 utilizando un software gratuito llamado X-TEN Softphone. Según como se observa en la Figura 5.24

Figura 5.24 Verificación del servicio de voz en la cual se puede apreciar el establecimiento de una llamada mediante VoIP hacia el Servidor con IP 192.168.0.110

Con la finalidad de verificar que los datos viajan en la infraestructura de los proveedores de servicio en texto plano, es decir, sin cifrar, se realiza una captura de los paquetes enviados por el enrutador en la Sucursal-1 cuando realiza una conexión al servidor FTP en Matriz. En la figura 5.25 se puede observar el contenido de un paquete haciendo uso del servicio, y la información contenida dentro del paquete donde podemos identificar que la contraseña utilizada para establecer conexión con el servidor es

enviada en texto plano (PASS msig) y cualquier atacante que logre interceptar la comunicación, puede ver y obtener esta información.

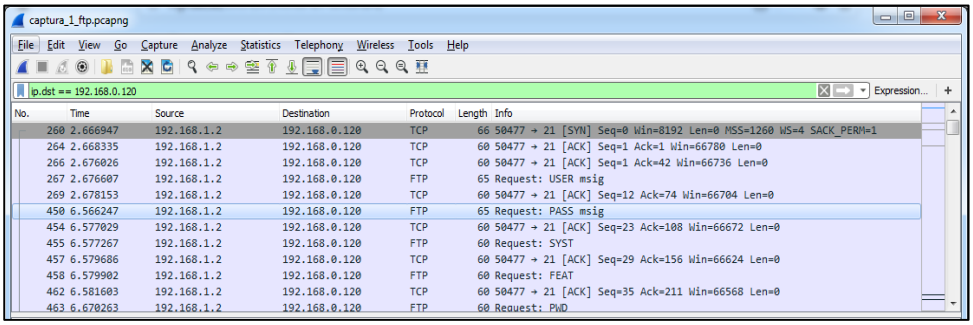


Figura 5.25 Captura de tráfico mediante Wireshark donde se aprecia la comunicación entre el dispositivo 192.168.1.2 con el servidor FTP 192.168.0.120. Se aprecia el contenido del usuario y la contraseña en texto plano.

Confirmada la conectividad y los servicios operativos, se procede a realizar las mediciones de los indicadores. Para esto, mediremos los tiempos de retransmisión de los paquetes en diferentes utilizaciones del ancho de banda del circuito. La utilización es el resultado del uso de los servicios por parte de los usuarios, siendo el mayor valor de utilización durante el horario de 13h00 a 16h00 en el cual la utilización alcanza el máximo valor de ancho de banda que tiene contratado la empresa, 1544 Mbps. La medición se realiza a través de prueba de ping directamente entre los enrutadores de dos localidades, esto con la finalidad de no agregar retardo hacia los dispositivos finales, sino solo medir el tiempo

de retransmisión entre un enrutador y el enlace de red de área amplia que lo conecta hacia la otra localidad.

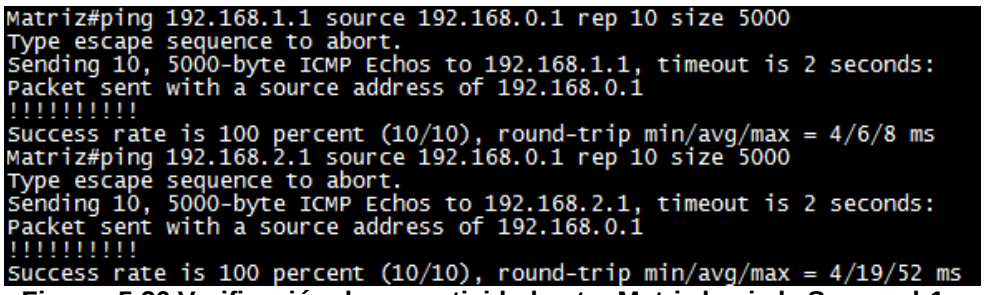


Figura 5.26 Verificación de conectividad entre Matriz hacia la Sucursal-1 y Sucursal-2

Adicionalmente, se verifica el tiempo que le toma a un enrutador en conmutar el tráfico por el enlace alternativo en caso de falla sobre el enlace principal. Para esto procedemos a desconectar físicamente la fibra del enlace principal y medimos el tiempo que demora en que volvamos a tener conectividad entre la localidad afectada y una localidad remota con una prueba de ping. En la figura 5.27 observamos que la desconexión del enlace principal en Matriz se realiza a las 20:28:29, sin embargo, BGP determina que el vecino no es alcanzable a las 20:31:15 luego que el temporizador de Hold Time ha expirado, solo luego que la sesión se identifique como invalida o caída, el tráfico puede conmutar adecuadamente por el enlace alternativo.

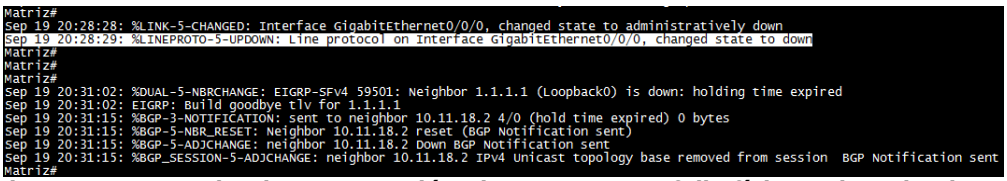


Figura 5.27 Prueba de conmutación al provocar una falla física sobre el enlace principal, se verifica que aproximadamente luego de 3 minutos del temporizador de tiempo de espera, la sesión se declara como inválida

En las tablas 19, 20 y 21 se indican los resultados de las mediciones sobre el escenario sin la solución de iWAN aplicada a los enlaces.

Tabla 19 Medición de indicadores en Matriz sin la solución de iWAN

Uso en Kbps del enlace de red de área local	Uso en Kbps del enlace principal	% de uso del enlace principal	% de uso del enlace alternativo	RTT hacia Suc-1	RRT hacia Suc-2	Tiempo de conmutación ante la caída del enlace principal
154	158	10.2	0	8 ms	4 ms	166 seg
772	776	50.25	0	16 ms	8 ms	170 seg
1544	1550	100.3	0	36 ms	64 ms	162 seg

Tabla 20 Medición de indicadores en Sucursal-1 sin la solución de iWAN

Uso en Kbps del enlace de red de área local	Uso en Kbps del enlace principal	% de uso del enlace principal	% de uso del enlace alternativo	RTT hacia Suc-1	RRT hacia Suc-2	Tiempo de conmutación ante la caída del enlace principal
154	158	10.2	0	8 ms	4 ms	166 seg
772	776	50.25	0	16 ms	16 ms	170 seg
1544	1550	100.3	0	36 ms	30 ms	162 seg

Tabla 21 Medición de indicadores en Sucursal-2 sin la solución de iWAN

Uso en Kbps del enlace de red de área local	Uso en Kbps del enlace principal	% de uso del enlace principal	% de uso del enlace alternativo	RTT hacia Suc-1	RRT hacia Suc-2	Tiempo de conmutación ante la caída del enlace principal
154	158	10.2	0	4 ms	4 ms	166 seg
772	776	50.25	0	8 ms	16 ms	170 seg
1544	1550	100.3	0	64 ms	30 ms	162 seg

5.6 PLANIFICACIÓN DE IMPLEMENTACIÓN PARA AMBIENTES DE PRODUCCIÓN.

La solución de iWAN es configurada sobre el ambiente de producción de la empresa, sin embargo, hay que tomar algunas consideraciones para ponerla en producción.

- La solución de iWAN debe entrar en producción sobre una ventana programada de trabajo, notificada a los usuarios de la empresa, en un horario de bajo impacto.
- Durante la ventana, antes de iniciar cualquier configuración, se debe guardar las configuraciones actuales y ejecutar un reinicio automático en 20 minutos. Esto garantiza que en caso de efectuarse una configuración incorrecta que no nos permita acceder al dispositivo, este se reinicie luego de 20 minutos con la configuración inicial. [16]

- Para migrar el tráfico del protocolo de enrutamiento inicial BGP al nuevo que maneja la solución EIGRP, debemos indicar en la configuración de BGP de los enrutadores, que la distancia administrativa para el protocolo tenga un valor mayor que el de EIGRP (90). Para esto, configuraremos un valor de 250 a la distancia administrativa de BGP con el comando: “distance bgp 250 250 250”, esto nos garantiza que EIGRP será el nuevo protocolo de enrutamiento preferido para la red de la empresa. [10]
- Si luego de la configuración no existen inconvenientes relacionados al acceso de los dispositivos, se procede a cancelar el reinicio automático y se graba la configuración.
- Se debe verificar correcta conectividad entre las localidades, y los servicios que usan los usuarios.
- Se puede dejar configurado el protocolo de BGP solo como medida preventiva en caso de necesitar realizar un reverso de la configuración en un corto plazo. Si luego de una semana no se presentan inconvenientes, se puede proceder al retiro de la configuración de BGP dado que ya no se utilizaría en la red de la empresa. [16]

5.7 PRUEBAS EN AMBIENTES DE PRODUCCION.

Al habilitar el protocolo de enrutamiento EIGRP como protocolo principal en la topología, permitimos que la solución iWAN entre en funcionamiento con todas las características descritas anteriormente, esto es, realizar la medición de parámetros y verificación de umbrales definidos, para con esto, tomar una decisión del enlace de red de área amplia que debe utilizar. Una vez confirmada la conectividad y los servicios por parte de los usuarios, procedemos a tomar una captura del tráfico que fluye a través de un enlace de red de área amplia a fin de verificar el cifrado del tráfico que cursa por él.

En la figura 5.28 observamos el contenido de un paquete haciendo uso del servicio de FTP similar a la prueba realizada previo a poner en producción la solución. En toda la captura de paquetes no se observa ningún paquete con dirección IP fuente de la subred 192.168.1.2 como en la anterior situación, sino solamente paquetes enviados entre dispositivos con dirección IP 10.11.17.2 y 10.11.18.2. Revisando la Tabla 16, podemos confirmar que dichas direcciones corresponden a las que tienen asignadas las interfaces de red de área amplia usando el servicio de datos MPLS del ISP-2. Esto se da por la forma de operación de la solución, al levantar los túneles DMVPN entre las localidades,

dichos túneles son levantados tomando como origen la dirección IP de los enlaces de red de área amplia asociados a las interfaces, por lo cual, el tráfico de los usuarios que se encuentra en las subredes 192.168.1.0 necesita ser encapsulado al requerir atravesar los túneles DMVPN, y es en el proceso de encapsulación, donde se agrega la nueva información relacionada a la dirección fuente y destino del paquete. Adicional a esto, si examinamos el contenido de los paquetes con más detalle, observamos que el protocolo utilizado es ESP tal cual fue definido en las configuraciones de seguridad, y en el contenido del paquete, encontramos un campo llamado ESP SPI, el cual hace referencia a un indexador de parámetro de seguridad, encargado de ayudar a identificar qué tipo de flujo de tráfico existe entre dos dispositivos. [13] El enrutador remoto al recibir este paquete usa el SPI para identificar como debe descifrar el contenido del tráfico, y de esta forma entregarlo a su destino original, en este caso el servidor FTP con dirección 192.168.0.120.

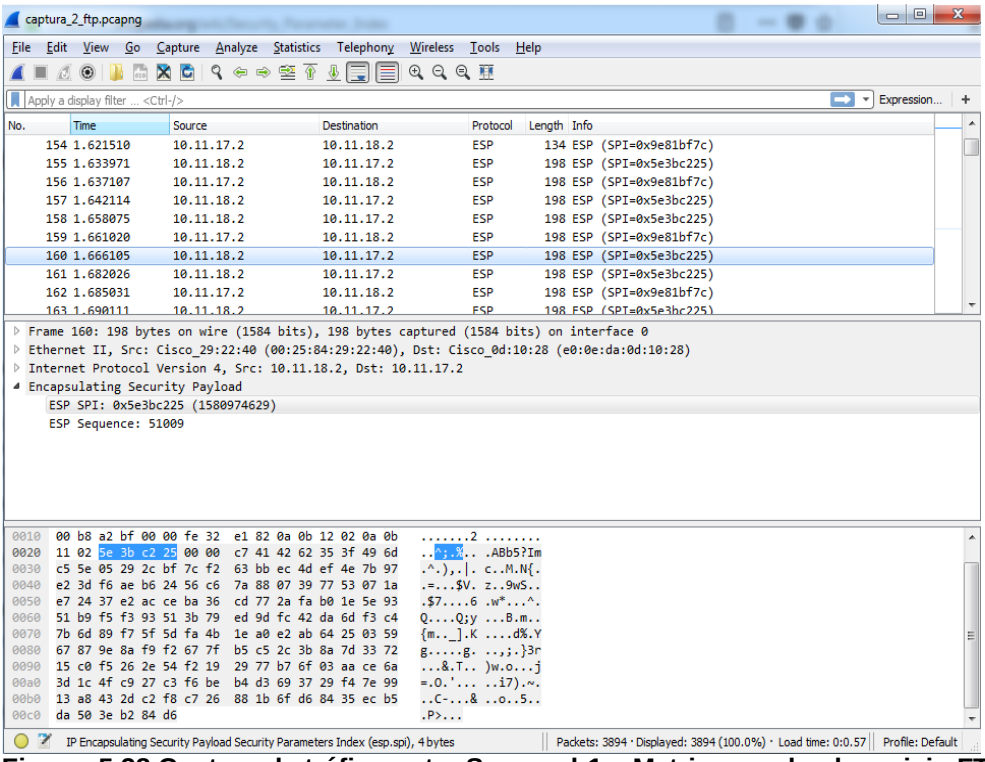


Figura 5.28 Captura de tráfico entre Sucursal-1 y Matriz usando el servicio FTP con la solución de iWAN aplicada. Se observa que los paquetes usan el protocolo ESP en su comunicación, y el contenido es indescifrable para un atacante que intercepte el paquete.

En las tablas 22, 23 y 24 se muestran los resultados de las mediciones bajo las mismas condiciones que se tomaron antes de realizar la habilitación de la solución de iWAN en la topología.

Tabla 22 Medición de indicadores en Matriz con la solución de iWAN

Uso en Kbps del enlace de red de área local	Uso en Kbps del enlace principal	Uso en % del enlace principal	Uso en % del enlace alternativo	RTT hacia Suc-1	RTT hacia Suc-2	Tiempo de conmutación ante la caída del enlace principal
154	245	15.86	12.62	3 ms	4 ms	0 seg
772	829	53.75	16.51	3 ms	4 ms	0 seg
1544	1297	84	37.1	3 ms	4 ms	0 seg

Tabla 23 Medición de indicadores en Sucursal-1 sin la solución de iWAN

Uso en Kbps del enlace de red de área local	Uso en Kbps del enlace principal	Uso en % del enlace principal	Uso en %del enlace alternativo	RTT hacia Matriz	RTT hacia Suc-2	Tiempo de conmutación ante la caída del enlace principal
154	245	15.86	12.62	3 ms	2 ms	0 seg
772	829	53.75	16.51	3 ms	2 ms	0 seg
1544	1297	84	37.1	3 ms	2 ms	0 seg

Tabla 24 Medición de indicadores en Sucursal-2 sin la solución de iWAN

Uso en Kbps del enlace de red de área local	Uso en Kbps del enlace principal	Uso en % del enlace principal	Uso en % del enlace alternativo	RTT hacia Matriz	RTT hacia Suc-1	Tiempo de conmutación ante la caída del enlace principal
154	245	15.86	12.62	4 ms	2 ms	0 seg
772	829	53.75	16.51	4 ms	2 ms	0 seg
1544	1297	84	37.1	4 ms	2 ms	0 seg

CAPÍTULO 6

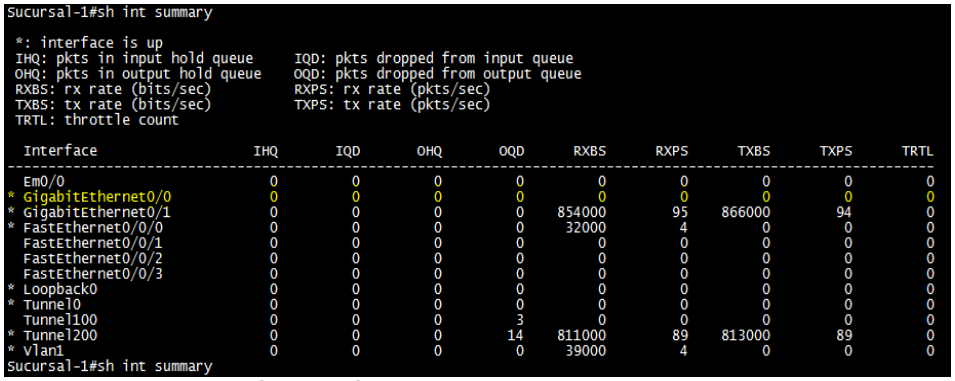
ANÁLISIS DE RESULTADOS

6.1 ANÁLISIS DE LAS MÉTRICAS DE EVALUACIÓN.

Las mediciones de los indicadores nos permiten observar cómo ha cambiado el comportamiento del tráfico antes y después de aplicar la solución de iWAN.

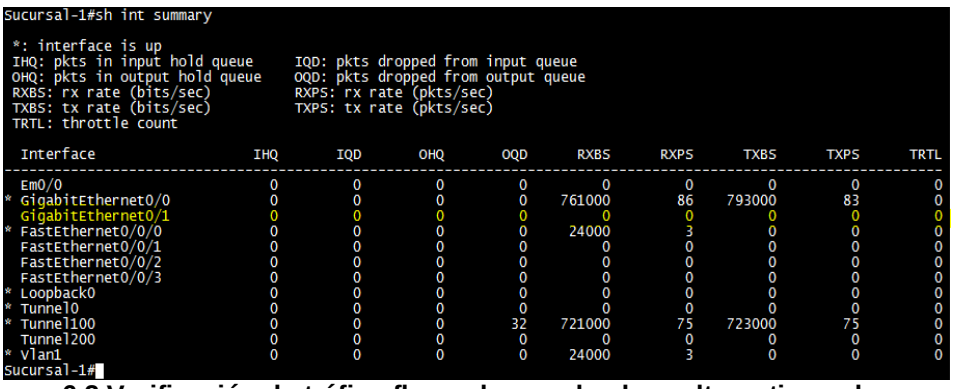
En el escenario inicial de pruebas en ambientes no productivos podemos determinar las siguientes situaciones respecto a la medición de los indicadores:

- Si ambos enlaces de red de área amplia se encontraban operativos y funcionales, entonces solo se usaba el enlace principal para hacer envío del tráfico. En enlace alternativo solo entraba en funcionamiento cuando simulábamos el corte del enlace principal, según se puede observar en la figura 6.1 y figura 6.2.



```
Sucursal-1#sh int summary

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface                IHQ       IQD       OHQ       OQD       RXBS       RXPS       TXBS       TXPS       TRTL
-----------------------------------------------------------------------------------------------------------------------
  Em0/0                      0         0         0         0          0          0          0          0          0
* GigabitEthernet0/0         0         0         0         0          0          0          0          0          0
* GigabitEthernet0/1         0         0         0         0     854000         95     866000         94          0
* FastEthernet0/0/0          0         0         0         0      32000          4          0          0          0
  FastEthernet0/0/1          0         0         0         0          0          0          0          0          0
  FastEthernet0/0/2          0         0         0         0          0          0          0          0          0
  FastEthernet0/0/3          0         0         0         0          0          0          0          0          0
* Loopback0                  0         0         0         0          0          0          0          0          0
* Tunnel0                    0         0         0         0          0          0          0          0          0
  Tunnel100                  0         0         0         3          0          0          0          0          0
* Tunnel200                  0         0         0        14     811000         89     813000         89          0
* Vlan1                      0         0         0         0      39000          4          0          0          0
Sucursal-1#sh int summary
```

Figura 6.1 Verificación de tráfico fluyendo solo por el enlace principal, aun estando los dos enlaces operativos.



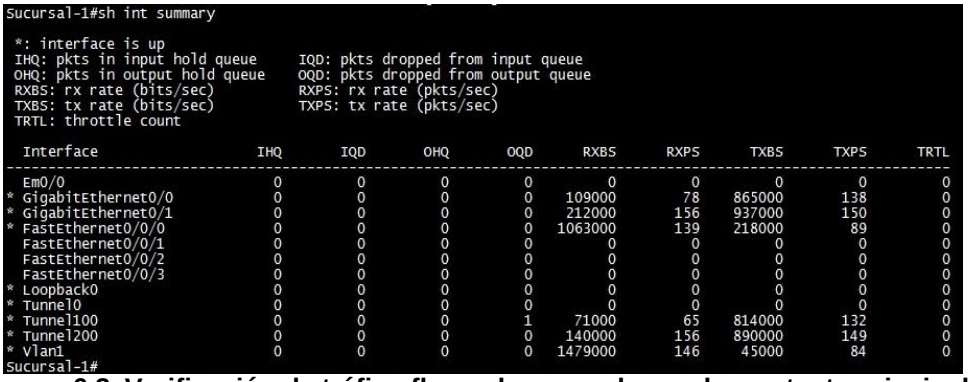
```
Sucursal-1#sh int summary

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface                IHQ       IQD       OHQ       OQD       RXBS       RXPS       TXBS       TXPS       TRTL
-----------------------------------------------------------------------------------------------------------------------
  Em0/0                      0         0         0         0          0          0          0          0          0
* GigabitEthernet0/0         0         0         0         0     761000         86     793000         83          0
  GigabitEthernet0/1         0         0         0         0          0          0          0          0          0
* FastEthernet0/0/0          0         0         0         0      24000          3          0          0          0
  FastEthernet0/0/1          0         0         0         0          0          0          0          0          0
  FastEthernet0/0/2          0         0         0         0          0          0          0          0          0
  FastEthernet0/0/3          0         0         0         0          0          0          0          0          0
* Loopback0                  0         0         0         0          0          0          0          0          0
* Tunnel0                    0         0         0         0          0          0          0          0          0
* Tunnel100                  0         0         0        32     721000         75     723000         75          0
  Tunnel200                  0         0         0         0          0          0          0          0          0
* Vlan1                      0         0         0         0      24000          3          0          0          0
Sucursal-1#
```

Figura 6.2 Verificación de tráfico fluyendo por el enlace alternativo solo cuando ocurrió una falla en el enlace principal

- El tráfico de datos que fluye a través de cualquier de los enlaces de red de área amplia no es cifrado, es enviado en texto plano.
- Los tiempos de conmutación ante la caída del enlace principal, se encuentran en un valor alrededor de 166 segundos. Esto se debe a la forma de operación del protocolo de BGP, y sus temporizadores de tiempo de espera que validan que un enrutador vecino se encuentre operativo o inalcanzable.
- El tiempo de retransmisión aumenta acorde con la utilización del canal, si mayor es la utilización entonces mayor es el tiempo de retransmisión.

Al entrar en operación la solución de iWAN, observamos la medición de los indicadores y podemos determinar las siguientes situaciones:

- Se observa utilización de ambos enlaces de red de área amplia sin importar la utilización del enlace principal, esto gracias a la funcionalidad de balanceo de carga para el tráfico que no se haya categorizado en ninguna clase, es decir, tráfico de internet, tal como se observa en la figura 6.3.



```
Sucursal-1#sh int summary

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface                 IHQ       IQD       OHQ       OQD      RXBS      RXPS      TXBS      TXPS      TRTL
------------------------------------------------------------------------------------------------------------------
  Em0/0                       0         0         0         0         0         0         0         0         0
* GigabitEthernet0/0          0         0         0         0    109000        78    865000       138         0
* GigabitEthernet0/1          0         0         0         0    212000       156    937000       150         0
* FastEthernet0/0/0           0         0         0         0   1063000       139    218000        89         0
  FastEthernet0/0/1           0         0         0         0         0         0         0         0         0
  FastEthernet0/0/2           0         0         0         0         0         0         0         0         0
  FastEthernet0/0/3           0         0         0         0         0         0         0         0         0
* Loopback0                   0         0         0         0         0         0         0         0         0
* Tunnel0                     0         0         0         0         0         0         0         0         0
* Tunnel100                   0         0         0         1     71000        65    814000       132         0
* Tunnel200                   0         0         0         0    140000       156    890000       149         0
* Vlan1                       0         0         0         0   1479000       146     45000        84         0
Sucursal-1#
```

Figura 6.3 Verificación de tráfico fluyendo por ambos enlaces, tanto principal como alternativo

- El tráfico de datos que fluye a través de cualquiera de los enlaces de red de área amplia se encuentra cifrado y su contenido no es posible visualizarlo al interceptar un paquete en tránsito de una localidad a otra.
- Al realizar una simulación de caída del enlace principal, observamos que los tiempos de conmutación son imperceptibles para el usuario dado que ambos enlaces ya se encuentran funcionando simultáneamente y listos para hacer envío de todo el tráfico de cualquier localidad.
- Observamos una utilización mayor de los enlaces de red de área amplia, comparados con la utilización del enlace de red de área local. Esto se debe principalmente a los nuevos protocolos que han entrado en funcionamiento en la solución de iWAN. Los paquetes enviados por cada protocolo para

establecimiento de conexión entre dos localidades, o mantenimiento de la vecindad generan un consumo adicional de tráfico en los enlaces, y dicho consumo es necesario para garantizar el correcto comportamiento de la solución. Podemos obtener el valor aproximado de consumo por parte de los protocolos de la solución al sumar el consumo simultaneo del enlace de red de área amplia principal con el alternativo, y al resultado restar el consumo del enlace de red de área local. En la Tabla 25 observamos el cálculo del consumo de tráfico realizado por los protocolos habilitados en la solución de iWAN.

A: Consumo aproximado de los protocolos habilitados en la solución de iWAN.
X: Porcentaje de utilización del enlace principal
Y: Porcentaje de utilización del enlace alternativo
BW: Ancho de banda de los enlaces de red de área amplia en kbps. 1544 kbps para este escenario.
U: Consumo del enlace de red de área local en kbps

$$\mathbf{A=}[(X+Y) *BW]/100 - U$$

Tabla 25 Cálculo del consumo aproximado de los protocolos habilitados en la solución de iWAN.

	Cálculo del consumo de los protocolos en la solución de iWAN	Consumo aproximado de los protocolos habilitados en la solución de iWAN en kbps
154	[(15.86+12.62) *1544]/100 - 154	286
772	[(53.75+16.51) *1544]/100 – 772	313
1544	[(84+37.1) *1544]/100 - 1544	326
Promedio		308

- Los tiempos de retransmisión para cada caso se mantenían en promedio en valores bajos cercanos a los 4 ms, esto gracias al manejo inteligente de los paquetes por parte de la solución. Al no generarse saturación en los enlaces, se tiene holgura en la utilización, y esto garantiza que no existan los comportamientos de tiempos altos de retardo o paquetes perdidos que suelen presentarse por la congestión. De la misma forma, si llega a existir congestión en un enlace, los paquetes son enrutados adecuadamente por el enlace que garantice los parámetros de confiabilidad estipulados en la configuración.

6.2 EVALUACIÓN DE EFICIENCIA DE LA SOLUCIÓN.

Para el cálculo de la eficiencia de la solución de iWAN, tomaremos en consideración los indicadores antes y después de la implementación. La eficiencia será evaluada acorde con el porcentaje de reducción en los tiempos de retransmisión para cada situación de ancho de banda utilizado, el porcentaje de reducción en la utilización del enlace principal, y el porcentaje de reducción en el tiempo de conmutación en caso de una falla del enlace principal.

Para el caso de la evaluación en la variación de los tiempos de retransmisión, en la Tabla 26 observamos cómo ha variado el indicador en ambas situaciones.

Tabla 26 Evaluación de eficiencia en los tiempos de retransmisión

Uso en Kbps del enlace de red de área local	RTT hacia Sucursal-1 antes de la solución	RTT hacia Sucursal-1 después de la solución	RTT hacia Sucursal-2 antes de la solución	RTT hacia Sucursal-2 después de la solución	Variación entre los tiempos de RTT
154	8 ms	3 ms	4 ms	4 ms	Hacia Sucursal-1 existe una reducción del 62.5% Hacia Sucursal-2 no existe reducción
772	16 ms	3 ms	8 ms	4 ms	Hacia Sucursal-1 existe una reducción del 81.25% Hacia Sucursal-2 existe una reducción del 50%
1544	36 ms	3 ms	64 ms	4 ms	Hacia Sucursal-1 existe una reducción del 91.67% Hacia Sucursal-2 existe una reducción del 93.75%

En el caso de la evaluación de utilización para el enlace principal, observamos en la Tabla 27 el resultado de la comparación en cada situación. Para los dos primeros casos en los que el consumo se encuentra en valores bajos y moderados, existe un aumento en la utilización del enlace principal debido al incremento ocasionado por el

consumo de tráfico de los protocolos de la solución de iWAN. Mientras mayor es el tráfico y se acerca a los escenarios de saturación, el controlador maestro ordena al enrutador adecuado que derive tráfico por el enlace alternativo, y de esta forma garantizar la entrega de los paquetes cumpliendo con los estándares del tráfico que fluye por el enlace.

Tabla 27 Evaluación de eficiencia en la utilización del enlace principal

Uso en Kbps del enlace de red de área local	Uso en Kbps del enlace principal antes de la solución	Uso en Kbps del enlace principal después de la solución	Variación en la utilización del enlace principal
154	158	245	Aumento del 35.5%
772	776	829	Aumento del 6.4%
1544	1550	1297	Reducción del 16.3%

Para el caso de la evaluación en la variación de los tiempos de conmutación en caso de falla de un enlace, en la Tabla 28 observamos cómo ha variado el indicador en cada situación. La reducción del 100% en el tiempo de conmutación se da por la forma de operación en esquema activo-activo de la solución de iWAN, lo cual implica que ambos enlaces están enviando tráfico simultáneamente.

Tabla 28 Evaluación de eficiencia en el tiempo de conmutación ante caída del enlace principal

Uso en Kbps del enlace de red de área local	Tiempo de conmutación ante la caída del enlace principal antes de la solución	Tiempo de conmutación ante la caída del enlace principal después de la solución	Variación en el tiempo de conmutación ante la caída del enlace principal
154	166 seg	930 ms	Reducción del 99.44%
772	170 seg	820 ms	Reducción del 99.52%
1544	162 seg	910 ms	Reducción del 99.44%

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. La elaboración del diseño nos permitió realizar un análisis adecuado de cada componente que brinda la solución, logrando identificar las oportunidades de mejora para el escenario actual de la empresa respecto al manejo de tráfico y seguridad en sus enlaces de red de área amplia, y además los requerimientos que necesita cumplir la empresa para poder implementar la solución en sus enrutadores de cada localidad.
2. De acuerdo con el análisis de los indicadores, se observa un uso simultaneo de los enlaces de red de área amplia para las localidades,

lo cual contribuye a generar una reducción en la utilización del ancho de banda del enlace principal en un promedio de 19.4% para los tres casos de utilización de ancho de banda tomados en consideración. El uso simultáneo es generado gracias al envío de tráfico inteligente de la solución por el enlace de red de área amplia que se defina como el mejor camino para el servicio identificado.

3. De acuerdo con el análisis de los tiempos de conmutación ante la caída del enlace principal, se puede observar una mejora en la variación al lograr reducir el tiempo a 887 milisegundos en promedio para los tres casos de utilización de ancho de banda tomados en consideración, haciendo casi imperceptible la caída de un enlace para los servicios que utilicen los usuarios de la empresa. El protocolo de enrutamiento EIGRP que utiliza la solución es el encargado de proveer esta característica al tener visibilidad del estado de ambos enlaces, y mantener dentro de su tabla topológica los parámetros asociados a direcciones IP de siguiente salto para el tráfico identificado. [10]
4. De acuerdo con el análisis realizado en las capturas obtenidas de tráfico que atraviesa los enlaces de red de área amplia, podemos confirmar un mayor nivel de seguridad para los paquetes que son intercambiados en las localidades gracias al cifrado que realizan los enrutadores con la solución de iWAN aplicada sobre ellos. Con los paquetes cifrados podemos garantizar que reducimos la probabilidad de ocurrencia para

los riesgos identificados en el análisis de riesgos, contribuyendo a generar un mayor nivel en la integridad y confidencialidad de la información.

5. Con la solución de CISCO iWAN aplicada a la infraestructura de la empresa, observamos una disminución en los tiempos de retransmisión entre las diferentes localidades. La reducción se genera acorde a la utilización del enlace, presentándose un mayor valor de reducción cuando realizamos el análisis sobre una utilización de 100% del enlace de red de área local, es decir un valor de 1544 Mbps. Al no presentar saturación del enlace principal, los paquetes pueden ser encaminados de una mejor manera a través de los enlaces de red de área amplia, y al tener holgura, los tiempos de retransmisiones se mantienen en valores bajos comparados a los presentados antes de aplicar la solución, logrando de esta forma un mejor uso del ancho de banda de la empresa.
6. De acuerdo con el análisis de los indicadores, se ha determinado que existe una utilización adicional de los enlaces de red de área amplia que no se presentaba antes de aplicar la solución de iWAN. Este tráfico adicional es generado por los nuevos protocolos que utiliza la solución, y su comportamiento de envío periódico de paquetes de control para verificación de un correcto establecimiento de estos. Se ha determinado un consumo promedio de 308 Kbps asociado al tráfico de protocolos de

control de la solución, el cual debe ser considerado en el dimensionamiento de los enlaces de red de área amplia.

RECOMENDACIONES

1. Se recomienda que la empresa contrate los enlaces de red de área amplia con distintos proveedores de servicio, dado que la implementación de la solución se fundamenta en la independencia de transporte, la empresa puede cotizar el proveedor que considere adecuado para garantizar la entrega de sus servicios a los usuarios que lo dispongan. De la misma forma, la empresa debe realizar un análisis de que tecnología de transporte puede utilizar para obtener como red de área amplia, siempre teniendo en consideración que los servicios corporativos conllevan a una mejor atención y resolución de problemas que un enlace residencial en caso de que se presente una falla física sobre el enlace.
2. Se recomienda instalar licencias de DATA y SECURITY con un periodo de prueba para el desarrollo de la implementación de la solución. De esta forma se puede evaluar en un ambiente controlado cómo funciona la tecnología y no es necesario incurrir en gastos por las licencias hasta confirmar que no existan inconvenientes relacionados a la operación. Desde el portal de CISCO https://tools.cisco.com/SWIFT/LicensingUI/Home se puede obtener las

licencias de pruebas previo registro con un usuario y contraseña. Para esto se necesita el modelo del enrutador, así como el número de serie que lo identifica.

3. Un diseño de red adecuado requiere que exista una documentación completa a disposición del ingeniero, relacionada a la topología de la empresa. Esta documentación debe contener diagramas sobre los enlaces físicos y lógicos para cada enlace de red de área local y red de área amplia. La topología en análisis es una empresa pequeña de tres localidades y tres enrutadores, pero esta información es esencial independiente del tamaño de la red. Adicional un inventario adecuado de los enrutadores identificando los modelos, versiones de sistema operativo y licencias activas, ayuda a identificar de forma adecuada las necesidades que se deben cubrir previo a la implementación de la solución de iWAN.
4. Con el objetivo de facilitar cualquier proceso de reverso de configuraciones a un estado inicial, se recomienda mantener una documentación adecuada de las configuraciones antes y después de cada ventana de mantenimiento. Adicional, gracias a la flexibilidad de migración entre dos protocolos de enrutamiento, es recomendable mantener el protocolo de enrutamiento anterior al despliegue de la solución, pero con una distancia administrativa mayor que el protocolo de enrutamiento de la solución de iWAN.

5. Se recomienda utilizar dos enrutadores en el sitio central, de tal forma que se separen las funciones de Controlador Maestro y Enrutador de borde que recibe los enlaces de red de área amplia. En una red de pocas localidades, un solo enrutador puede tener las dos funciones sin que esto impacte significativamente a su capacidad de procesamiento, sin embargo, mientras más crece la cantidad de enrutadores que intervienen en la operación, o mientras más subredes se agreguen para ser monitoreadas por la solución, esto genera un consumo adicional de recursos en el Controlador Maestro, por lo cual, es recomendable que se maneje un enrutador dedicado a la función de monitoreo de rendimiento de los enlaces. [16]

BIBLIOGRAFÍA

[1] Arleidi Martinez y Adriana Castro., *Diseño y arquitectura de redes wan,* Universidad Tecnologica de Bolivar, 2008.

[2] Brad Edgeworth y David Prall, *CISCO Intelligent WAN (IWAN),* CISCO Press 1st Ed, 2017.

[3] Bhushan, Abhay, "A File Transfer Protocol", RFC 114 (NIC 5823), MIT-Project MAC, 16 April 1971.

[4] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[5] CISCO, ISR G2 Licensing and Packaging White Paper, https://www.cisco.com/c/en/us/products/collateral/cloud-systems management/software-activation-on-integrated-services-routers isr/white_paper_c11_556985.html, 2012.

[6] Detienne, F., M. Kumar, and M. Sullenberger. Informational RFC, “Flexible Dynamic Mesh VPN.” IETF, December 2013. http://tools.ietf.org/html/draft-detienne-dmvpn-01.

[7] Hanks, S., T. Lee, D. Farianacci, and P. Traina. RFC 1702, “Generic Routing Encapsulation over IPv4 Networks.” IETF, October 2004. http://tools.ietf.org/html/rfc1702.

[8] Luciani, J., D. Katz, D. Piscitello, B. Cole, and N. Doraswamy. RFC 2332, “NBMA Next Hop Resolution Protocol (NHRP).” IETF, April 1998. http://tools.ietf.org/html/rfc2332.

[9] Sullenberger, Mike. “Advanced Concepts of DMVPN (Dynamic Multipoint VPN).” Presented at Cisco Live, San Diego, 2015.

[10] Edgeworth, Brad, Aaron Foss, and Ramiro Garza Rios. IP Routing on Cisco IOS, IOS XE, and IOS XR. Indianapolis: Cisco Press, 2014.

[11] Rekhter, Y., T. Li, and S. Hares. RFC 4271. “A Border Gateway Protocol 4 (BGP-4).” IETF, January 2006. http://tools.ietf.org/html/rfc4271.

[12] Kent, S., and R. Atkinson. RFC 2401, “Security Architecture for the Internet Protocol.” IETF, November 1998. http://tools.ietf.org/html/rfc2401.

[13] Huang, G., S. Beaulieu, and D. Rochefort. RFC 3706, “A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers.” IETF, February 2004. http://tools.ietf.org/html/rfc3706

[14] Babiarz, J., K. Chan, and F. Baker. RFC 4594, “Configuration Guidelines for DiffServ Service Classes.” IETF, August 2006. https://tools.ietf.org/html/rfc4594.

[15] Cisco. “Performance Routing Version 3.” www.cisco.com/go/pfr.

[16] Edgeworth, Brad, and Mani Ganesan. “Migrating Your Existing WAN to Cisco’s IWAN.” Presented at Cisco Live, Berlin, 2016.

[17] Deloitte, *La Evolución de la Gestión de Ciber - Riesgos y Seguridad de la Información,* https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Deloitte%202016%20Cyber%20Risk%20%20Information%20Security%20Study%20-%20Latinoam%C3%A9rica%20-%20Resultados%20Generales%20vf%20(Per%C3%BA).pdf, 2016.

ANEXO I

CONFIGURACION ROUTER MATRIZ

```
Matriz#sh run
Building configuration...


Current configuration : 7797 bytes
!
! Last configuration change at 15:19:57 ECT Wed Sep 26 2018 by automatico
! NVRAM config last updated at 15:20:23 ECT Wed Sep 26 2018 by automatico
!
version 15.7
no service pad
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
no service dhcp
!
hostname Matriz
!
boot-start-marker
boot system flash:c1900-universalk9-mz.SPA.157-3.M.bin
boot-end-marker
!
logging buffered 104096
no logging console
enable secret 5 $1$H0sk$zUk2E6mgIG0Jnz3UrwJq21
!
no aaa new-model
clock timezone ECT -5 0
!
no ip domain lookup
ip domain name iwan
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
```

```
!
!
#######  Configuración de PfR v3  ###############
!
domain IWAN
 vrf default
  border
   source-interface Loopback0
   master local
   password 7 097C483B485744315A1F077A
  master hub
   source-interface Loopback0
   site-prefixes prefix-list PREFIJOS_SUCURSALES
   password 7 15220D3E5578780779203672
   monitor-interval 2 dscp af21
   monitor-interval 2 dscp af31
   monitor-interval 2 dscp ef
   load-balance
   enterprise-prefix  prefix-list PREFIJOS_MATRIZ
   class VOZ sequence 10
    match dscp ef policy voice
    path-preference MPLS fallback INETCRP
   class TRANSFERENCIA_DE_ARCHIVOS sequence 20
    match dscp af31 policy low-latency-data
    path-preference MPLS fallback INETCRP
   class APLICACIONES_GENERALES sequence 30
    match dscp af21 policy custom
      priority 1 one-way-delay threshold 500
     path-preference INETCRP fallback MPLS
cts logging verbose
!
!
license udi pid CISCO1941/K9 sn FGL20162410
license boot module c1900 technology-package securityk9
license boot module c1900 technology-package datak9
!
username automatico privilege 15 secret 5
$1$PMwv$0uVR1C8Xhocbfa.v34o0F0
!
redundancy
!
!
no cdp run
!
```

```
!
####### Políticas de marcado ###############
!
class-map                                                    match-any
CLASIFICACION_TRANSFERENCIA_ARCHIVOS
 match access-group name FTP
class-map                                                    match-any
CLASIFICACION_APLICACIONES_GENERALES
 match access-group name ICMP
class-map match-any CLASIFICACION_VOZ
 match access-group name VOZ
!
policy-map MARCADO_PAQUETES
 class CLASIFICACION_VOZ
  set dscp ef
 class CLASIFICACION_TRANSFERENCIA_ARCHIVOS
  set dscp af31
 class CLASIFICACION_APLICACIONES_GENERALES
  set dscp af21
!
!
####### Configuracion de IPSec ###############

crypto isakmp policy 10
 encr aes
 hash sha256
 authentication pre-share
 group 21
crypto isakmp key 3sp0l1w4n address 0.0.0.0
!
!
crypto ipsec transform-set T-SET-IWAN esp-aes esp-sha-hmac
 mode transport
!
crypto ipsec profile PROTECCION-ISP1
 set transform-set T-SET-IWAN
!
crypto ipsec profile PROTECCION-ISP2
 set transform-set T-SET-IWAN
!
!
!
!
!
```

```
interface Loopback0
 ip address 1.1.1.0 255.255.255.255
!
!
####### Configuración Túneles dmvpn ###############
!
!
interface Tunnel100
 bandwidth 1546
 ip address 100.100.100.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication iwan2018
 ip nhrp network-id 1000
 ip nhrp redirect
 ip tcp adjust-mss 1360
 load-interval 30
 delay 200
 bfd interval 250 min_rx 250 multiplier 4
 no bfd echo
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile PROTECCION-ISP1 shared
 domain IWAN path INETCRP path-id 1
!
interface Tunnel200
 bandwidth 1546
 ip address 200.200.200.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication iwan2018
 ip nhrp network-id 1000
 ip nhrp redirect
 ip tcp adjust-mss 1360
 load-interval 30
 delay 100
 bfd interval 250 min_rx 250 multiplier 4
 tunnel source GigabitEthernet0/0/0
 tunnel mode gre multipoint
 tunnel key 200
 tunnel protection ipsec profile PROTECCION-ISP2
 domain IWAN path MPLS path-id 2
!
```

```
interface Tunnel300
 bandwidth 1546
 ip address 30.30.30.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication iwan2018
 ip nhrp network-id 1000
 ip nhrp redirect
 ip tcp adjust-mss 1360
 load-interval 30
 delay 300
 bfd interval 250 min_rx 250 multiplier 4
 no bfd echo
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 300
 tunnel protection ipsec profile PROTECCION-ISP1 shared
 domain IWAN path INETGPN path-id 3
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description Enlace_Alternativo_Internet
 ip address 181.39.153.3 255.255.255.128
 no ip redirects
 no ip proxy-arp
 load-interval 30
 duplex auto
 speed auto
 no cdp enable
!
interface GigabitEthernet0/1
 description Red_de_Area_Local
 ip address 192.168.0.1 255.255.255.0
 load-interval 30
 duplex auto
 speed auto
 service-policy input MARCADO_PAQUETES
!
interface GigabitEthernet0/0/0
 description Enlace_Principal_MPLS
 ip address 10.11.17.2 255.255.255.252
```

```
 no ip redirects
 no ip proxy-arp
 load-interval 30
 negotiation auto
 no cdp enable
!
####### Configuración de eigrp ###############

router eigrp IWAN
 !
 address-family ipv4 unicast autonomous-system 10
  !
  af-interface default
   authentication mode hmac-sha-256 7
00344715174C5B140B751D491B09
   bfd
   passive-interface
   no split-horizon
  exit-af-interface
  !
  af-interface Tunnel100
   no passive-interface
  exit-af-interface
  !
  af-interface Tunnel200
   no passive-interface
  exit-af-interface
  !
  af-interface Tunnel300
   no passive-interface
  exit-af-interface
  !
  topology base
  exit-af-topology
  network 1.1.1.0 0.0.0.0
  network 30.30.30.1 0.0.0.0
  network 100.100.100.1 0.0.0.0
  network 192.168.0.1 0.0.0.0
  network 200.200.200.1 0.0.0.0
 exit-address-family
!
####### Configuración de BGP ###############
!
router bgp 10
```

```
 bgp router-id 1.1.1.0
 bgp log-neighbor-changes
 bgp listen range 181.199.0.0/16 peer-group INTERNET
 bgp listen limit 5
 no bgp default ipv4-unicast
 neighbor INTERNET peer-group
 neighbor INTERNET remote-as 10
 neighbor INTERNET update-source GigabitEthernet0/0
 neighbor 10.11.17.1 remote-as 27947
 neighbor 186.5.89.3 remote-as 10
 neighbor 186.5.89.3 update-source GigabitEthernet0/0
 !
 address-family ipv4
  network 192.168.0.0
  neighbor INTERNET activate
  neighbor 10.11.17.1 activate
  neighbor 186.5.89.3 activate
  distance bgp 250 250 250
 exit-address-family
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 181.39.153.1
!
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!
ip access-list extended FTP
 permit tcp any any eq ftp
 permit tcp any eq ftp any
 permit tcp any eq ftp-data any
 permit tcp any any eq ftp-data
 permit tcp any any eq 1024
 permit tcp any eq 1024 any
ip access-list extended ICMP
 permit icmp any any
ip access-list extended VOZ
 permit udp any any eq 5060
 permit udp any any eq 5061
 permit udp any eq 5060 any
 permit udp any eq 5061 any
```

```
 permit udp any any eq 9099
 permit udp any eq 9099 any
!
!
ip prefix-list PREFIJOS_MATRIZ seq 10 permit 192.168.0.0/16 le 24
!
ip prefix-list PREFIJOS_SUCURSALES seq 5 permit 192.168.0.0/24
ip prefix-list PREFIJOS_SUCURSALES seq 10 permit 192.168.1.0/24
ip prefix-list PREFIJOS_SUCURSALES seq 20 permit 192.168.2.0/24
no service-routing capabilities-manager
ipv6 ioam timestamp
!
control-plane
!
!
 vstack
banner login ^CCC
**************************************************
Acceso Restringido a Personal autorizado
**************************************************
Violaciones a  este  sistema estan  penalizadas en
la Ley de Comercio Electronico Ecuatoriana y demas
Leyes Internacionales.
^C
!
line con 0
 login local
line aux 0
 login local
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 privilege level 15
 login local
 transport input ssh
!
scheduler max-task-time 5000
scheduler allocate 20000 1000
!
end
```

CONFIGURACION ROUTER SUCURSAL 1

```
Sucursal-1#sh run
Building configuration...


Current configuration : 6256 bytes
!
! Last configuration change at 15:22:10 ECT Wed Sep 26 2018 by automatico
! NVRAM config last updated at 15:23:31 ECT Wed Sep 26 2018 by automatico
!
version 15.7
no service pad
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
no service dhcp
!
hostname Sucursal-1
!
boot-start-marker
boot system flash:c1900-universalk9-mz.SPA.157-3.M.bin
boot-end-marker
!
!
logging buffered 1004096
no logging console
enable secret 5 $1$H0sk$zUk2E6mgIG0Jnz3UrwJq21
!
no aaa new-model
clock timezone ECT -5 0
!
!
!
!
!
no ip domain lookup
ip domain name iwan
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
```

```
!
!
####### Configuración de PfR v3 ###############
!
domain IWAN
 vrf default
  border
   source-interface Loopback0
   master local
   password 7 012300360A59552C705F4D59
  master branch
   source-interface Loopback0
   password 7 133511205A5E57097A372B63
   hub 1.1.1.0
!
!
license udi pid CISCO1941/K9 sn FTX163986J6
license boot module c1900 technology-package securityk9
!
!
username automatico privilege 15 secret 5
$1$PMwv$0uVR1C8Xhocbfa.v34o0F0
!
redundancy
!
!
no cdp run
!
####### Políticas de marcado ###############
!
class-map match-any
CLASIFICACION_TRANSFERENCIA_ARCHIVOS
 match access-group name FTP
class-map match-any
CLASIFICACION_APLICACIONES_GENERALES
 match access-group name ICMP
class-map match-any CLASIFICACION_VOZ
 match access-group name VOZ
!
policy-map MARCADO_PAQUETES
 class CLASIFICACION_VOZ
  set dscp ef
 class CLASIFICACION_TRANSFERENCIA_ARCHIVOS
  set dscp af31
```

```
 class CLASIFICACION_APLICACIONES_GENERALES
  set dscp af21
!
!
####### Configuración de IPSec ###############
!
crypto isakmp policy 10
 encr aes
 hash sha256
 authentication pre-share
 group 21
crypto isakmp key 3sp0l1w4n address 181.39.153.3
crypto isakmp key 3sp0l1w4n address 10.11.17.2
!
!
crypto ipsec transform-set T-SET-IWAN esp-aes esp-sha-hmac
 mode transport
!
crypto ipsec profile PROTECCION-ISP1
 set transform-set T-SET-IWAN
!
crypto ipsec profile PROTECCION-ISP2
 set transform-set T-SET-IWAN
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
####### Configuración Túneles dmvpn ##############
!
interface Tunnel100
 bandwidth 1546
 ip address 100.100.100.11 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication iwan2018
 ip nhrp map 100.100.100.1 181.39.153.3
 ip nhrp map multicast 181.39.153.3
 ip nhrp network-id 1000
 ip nhrp nhs 100.100.100.1
 ip tcp adjust-mss 1360
 load-interval 30
 delay 200
 if-state nhrp
```

```
 bfd interval 250 min_rx 250 multiplier 4
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile PROTECCION-ISP1
!
interface Tunnel200
 bandwidth 1546
 ip address 200.200.200.11 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication iwan2018
 ip nhrp map 200.200.200.1 10.11.17.2
 ip nhrp map multicast 10.11.17.2
 ip nhrp network-id 1000
 ip nhrp nhs 200.200.200.1
 ip tcp adjust-mss 1360
 load-interval 30
 delay 100
 bfd interval 250 min_rx 250 multiplier 4
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
 tunnel key 200
 tunnel protection ipsec profile PROTECCION-ISP2
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description Enlace_Alternativo_Internet
 ip address 186.5.89.3 255.255.255.128
 no ip redirects
 no ip proxy-arp
 load-interval 30
 duplex auto
 speed auto
 no cdp enable
!
interface GigabitEthernet0/1
 description Enlace_Principal_MPLS
 ip address 10.11.18.2 255.255.255.252
 no ip redirects
 no ip proxy-arp
```

```
 load-interval 30
 duplex auto
 speed auto
 no cdp enable
!
interface FastEthernet0/0/0
 no ip address
!
interface FastEthernet0/0/1
 no ip address
!
interface FastEthernet0/0/2
 no ip address
!
interface FastEthernet0/0/3
 no ip address
!
interface Vlan1
 description Red_De_Area_Local
 ip address 192.168.1.1 255.255.255.0
 load-interval 30
 service-policy input MARCADO_PAQUETES
!
####### Configuración de eigrp ###############
!
router eigrp IWAN
 !
 address-family ipv4 unicast autonomous-system 10
  !
  af-interface default
   authentication mode hmac-sha-256 7
00344715174C5B140B751D491B09
   bfd
   passive-interface
  exit-af-interface
  !
  af-interface Tunnel100
   no passive-interface
  exit-af-interface
  !
  af-interface Tunnel200
   no passive-interface
  exit-af-interface
  !
```

```
  topology base
  exit-af-topology
  network 1.1.1.1 0.0.0.0
  network 100.100.100.11 0.0.0.0
  network 192.168.1.1 0.0.0.0
  network 200.200.200.11 0.0.0.0
 exit-address-family
!
####### Configuración de bgp ###############
!
router bgp 10
 bgp router-id 1.1.1.1
 bgp log-neighbor-changes
 network 192.168.1.0
 neighbor 10.11.18.1 remote-as 27947
 neighbor 10.11.18.5 remote-as 27947
 neighbor 181.39.153.3 remote-as 10
 neighbor 181.39.153.3 update-source GigabitEthernet0/0
 distance bgp 250 250 250
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 186.5.89.1
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!
ip access-list extended FTP
 permit tcp any any eq ftp
 permit tcp any eq ftp any
 permit tcp any any eq ftp-data
 permit tcp any eq ftp-data any
 permit tcp any any eq 1024
 permit tcp any eq 1024 any
ip access-list extended ICMP
 permit icmp any any
ip access-list extended VOZ
 permit udp any any eq 5060
 permit udp any any eq 5061
 permit udp any eq 5060 any
 permit udp any eq 5061 any
 permit udp any any eq 9099
```

```
 permit udp any eq 9099 any
!
no service-routing capabilities-manager
ipv6 ioam timestamp
!
!
!
control-plane
!
!
 vstack
banner login ^CCCC
**************************************************
Acceso Restringido a Personal autorizado
**************************************************
Violaciones a  este  sistema estan  penalizadas en
la Ley de Comercio Electronico Ecuatoriana y demas
Leyes Internacionales.
^C
!
line con 0
 login local
line aux 0
 login local
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 privilege level 15
 login local
 transport input ssh
!
scheduler max-task-time 5000
scheduler allocate 20000 1000
!

end
```

CONFIGURACION ROUTER SUCURSAL 2

```
Sucursal-2#sh run
Building configuration...
```

```
Current configuration : 5499 bytes
!
! Last configuration change at 15:37:44 ECT Wed Sep 26 2018 by
automatico
! NVRAM config last updated at 15:38:04 ECT Wed Sep 26 2018 by
automatico
!
version 15.7
no service pad
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
no service dhcp
!
hostname Sucursal-2
!
boot-start-marker
boot system flash:c1900-universalk9-mz.SPA.157-3.M.bin
boot-end-marker
!
!
logging buffered 1004096
enable secret 5 $1$H0sk$zUk2E6mgIG0Jnz3UrwJq21
!
no aaa new-model
clock timezone ECT -5 0
!
!
!
ip vrf ISP-2
 rd 2:2
!
!
!
no ip domain lookup
ip domain name iwan
ip cef
ipv6 unicast-routing
no ipv6 cef
!
multilink bundle-name authenticated
!
####### Configuración de PfR v3 ###############
```

```
!
domain IWAN
 vrf default
  border
   source-interface Loopback0
   master local
   password 7 012300360A59552C705F4D59
  master branch
   source-interface Loopback0
   password 7 133511205A5E57097A372B63
   hub 1.1.1.0
!
!
license udi pid CISCO1941/K9 sn FTX181684EU
license boot module c1900 technology-package datak9
!
!
username automatico privilege 15 secret 5
$1$PMwv$0uVR1C8Xhocbfa.v34o0F0
!
redundancy
!
!
!
!
no cdp run
!
####### Políticas de marcado ###############
!
class-map match-any
CLASIFICACION_TRANSFERENCIA_ARCHIVOS
 match access-group name FTP
class-map match-any
CLASIFICACION_APLICACIONES_GENERALES
 match access-group name ICMP
class-map match-any CLASIFICACION_VOZ
 match access-group name VOZ
!
policy-map MARCADO_PAQUETES
 class CLASIFICACION_VOZ
  set dscp ef
 class CLASIFICACION_TRANSFERENCIA_ARCHIVOS
  set dscp af31
 class CLASIFICACION_APLICACIONES_GENERALES
```

```
  set dscp af21
!
####### Configuración de IPSec ###############

!
crypto keyring ISP-2 vrf ISP-2
  pre-shared-key address 181.39.153.3 key 3sp0l1w4n
!
crypto isakmp policy 10
 encr aes
 hash sha256
 authentication pre-share
 group 21
crypto isakmp key 3sp0l1w4n address 181.39.153.3
!
!
crypto ipsec transform-set T-SET-IWAN esp-aes esp-sha-hmac
 mode transport
!
crypto ipsec profile PROTECCION-ISP1
 set transform-set T-SET-IWAN
!
crypto ipsec profile PROTECCION-ISP2
 set transform-set T-SET-IWAN
!
!
!
interface Loopback0
 ip address 1.1.1.2 255.255.255.255
!
interface Loopback255
 ip vrf forwarding ISP-2
 ip address 192.168.2.1 255.255.255.0
!
####### Configuración Túneles dmvpn ###############

!
interface Tunnel100
 ip address 100.100.100.22 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication iwan2018
 ip nhrp map 100.100.100.1 181.39.153.3
 ip nhrp map multicast 181.39.153.3
```

```
 ip nhrp network-id 1000
 ip nhrp nhs 100.100.100.1
 ip tcp adjust-mss 1360
 load-interval 30
 if-state nhrp
 bfd interval 250 min_rx 250 multiplier 4
 no bfd echo
 tunnel source GigabitEthernet0/0
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile PROTECCION-ISP1
!
interface Tunnel300
 ip address 30.30.30.22 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication iwan2018
 ip nhrp map multicast 181.39.153.3
 ip nhrp map 30.30.30.1 181.39.153.3
 ip nhrp network-id 1000
 ip nhrp nhs 30.30.30.1
 ip tcp adjust-mss 1360
 load-interval 30
 if-state nhrp
 bfd interval 250 min_rx 250 multiplier 4
 no bfd echo
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
 tunnel key 300
 tunnel vrf ISP-2
 tunnel protection ipsec profile PROTECCION-ISP2 shared
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description Enlace_Principal_Internet_Corporativo
 ip address dhcp
 no ip redirects
 no ip proxy-arp
 load-interval 30
 duplex auto
 speed auto
```

```
 ipv6 address dhcp
 ipv6 address autoconfig default
 no cdp enable
!
interface GigabitEthernet0/1
 description Enlace_Alternativo_Internet_Residencial
 ip vrf forwarding ISP-2
 ip address dhcp
 no ip redirects
 no ip proxy-arp
 load-interval 30
 duplex auto
 speed auto
 ipv6 address dhcp
 no cdp enable
!
interface FastEthernet0/0/0
 no ip address
!
interface FastEthernet0/0/1
 no ip address
!
interface FastEthernet0/0/2
 no ip address
!
interface FastEthernet0/0/3
 no ip address
!
interface Vlan1
 description Red_de_Area_Local
 ip address 192.168.2.1 255.255.255.0
!
####### Configuración de eigrp ###############

!
router eigrp IWAN
 !
 address-family ipv4 unicast autonomous-system 10
  !
  af-interface default
   authentication mode hmac-sha-256 7
13354301181B54382F7079342732
   bfd
   passive-interface
```

```
  exit-af-interface
  !
  af-interface Tunnel100
   no passive-interface
  exit-af-interface
  !
  af-interface Tunnel300
   no passive-interface
  exit-af-interface
  !
  topology base
  exit-af-topology
  network 1.1.1.2 0.0.0.0
  network 30.30.30.22 0.0.0.0
  network 100.100.100.22 0.0.0.0
  network 192.168.2.1 0.0.0.0
 exit-address-family
!
####### Configuración de eigrp ###############
!
router bgp 10
 bgp router-id 1.1.1.2
 bgp log-neighbor-changes
 neighbor 181.39.153.3 remote-as 10
 !
 address-family ipv4
  network 192.168.2.0
  neighbor 181.39.153.3 activate
 exit-address-family
 !
 address-family ipv4 vrf ISP-2
  network 192.168.2.0
  neighbor 181.39.153.3 remote-as 10
  neighbor 181.39.153.3 activate
 exit-address-family
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 181.39.153.3 255.255.255.255 192.168.100.1
ip route vrf ISP-2 181.39.153.3 255.255.255.255 100.67.18.1
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
```

```
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!
ip access-list extended FTP
 permit tcp any any eq ftp
 permit tcp any eq ftp any
 permit tcp any any eq ftp-data
 permit tcp any eq ftp-data any
 permit tcp any any eq 1024
 permit tcp any eq 1024 any
ip access-list extended ICMP
 permit icmp any any
ip access-list extended VOZ
 permit udp any any eq 5060
 permit udp any any eq 5061
 permit udp any eq 5060 any
 permit udp any eq 5061 any
 permit udp any any eq 9099
 permit udp any eq 9099 any
!
no service-routing capabilities-manager
ipv6 ioam timestamp
!
!
!
control-plane
!
!
 vstack
banner login ^CCCCC
**************************************************
Acceso Restringido a Personal autorizado
**************************************************
Violaciones a  este  sistema estan  penalizadas en
la Ley de Comercio Electronico Ecuatoriana y demas
Leyes Internacionales.
^C
!
line con 0
 login local
line aux 0
 login local
line 2
 no activation-character
 no exec
```

```
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 privilege level 15
 login local
 transport input ssh
!
scheduler max-task-time 5000
scheduler allocate 20000 1000
!
!
end
```

ANEXO II

Prueba de conectividad desde la red de área local en Matriz hacia Sucursal-1

```
Matriz#ping 192.168.1.1 source 192.168.0.1 rep 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.0.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/4 ms
```

Prueba de conectividad desde la red de área local en Matriz hacia Sucursal-2

```
Matriz#ping 192.168.2.1 source 192.168.0.1 rep 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.0.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/4/24 ms
```

Prueba de conectividad desde la red de área local en Sucursal-1 hacia Sucursal-2

```
Sucursal-1#ping 192.168.2.1 source 192.168.1.1 rep 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 4/4/8 ms
```

ANEXO III

Variantes de algoritmo para cifrado y autenticación en ESP.		
Tipo de Transformación	**Transformación**	**Descripción**
Algoritmo de Cifrado ESP	esp-aes 128	Algoritmo de cifrado ESP de 128 bits con estándar de cifrado avanzado (AES)
	esp-aes 192	Algoritmo de cifrado ESP de 192 bits con estándar de cifrado avanzado (AES)
	esp-aes 256	Algoritmo de cifrado ESP de 256 bits con estándar de cifrado avanzado (AES)
	esp-gcm 128	Transformación ESP usando cifrado 128 bits con Modo de Contador de Galois (GCM)
	esp-gcm 192	Transformación ESP usando cifrado 192 bits con Modo de Contador de Galois (GCM)
	esp-gcm 256	Transformación ESP usando cifrado 256 bits con Modo de Contador de Galois (GCM)
Algoritmo de Autenticación ESP	esp-sha-hmac	Algoritmo de autenticación ESP con algoritmo de hash seguro (SHA) y (variante HMAC)
	esp-sha256-hmac	Algoritmo de autenticación ESP de 256 bit con algoritmo de hash seguro (SHA) y (variante HMAC)
	esp-sha384-hmac	Algoritmo de autenticación ESP de 384 bit con algoritmo de hash seguro (SHA) y (variante HMAC)
	esp-sha512-hmac	Algoritmo de autenticación ESP de 512 bit con algoritmo de hash seguro (SHA) y (variante HMAC)

ANEXO IV

Plantillas predefinidas en la solución de CISCO iWAN		
Plantilla Predefinida	**Definición del umbral**	**Descripción**
Voice	Prioridad 1: Retardo de una vía menor a 150ms Prioridad 2: Perdida de paquetes menor a 1% Prioridad 3: Variación menor a 30ms	Plantilla orientada a trafico de voz que sea sensible a afectación del enlace o tiempos elevados.
Real-time-video	Prioridad 1: Perdida de paquetes menor a 1% Prioridad 2: Retardo de una vía menor a 150ms Prioridad 3: Variación menor a 20ms	Plantilla orientada a servicios de videoconferencia en los cuales es prioritario garantizar la entrega de los paquetes sin perdidas.
Low-latency-data	Prioridad 1: Retardo de una vía menor a 100ms Prioridad 2: Perdida de paquetes menor a 5%	Plantilla orientada a servicios de bajo tiempo de retardo en el paquete desde el origen a su destino.
Bulk-data	Prioridad 1: Retardo de una vía menor a 300ms Prioridad 2: perdida de paquetes menor a 5%	Plantilla orientada al manejo de tráfico en cantidades grandes, en las cuales se puede dar más holgura a los tiempos de respuesta y porcentaje de paquetes perdidos.
Best-effort	Prioridad 1: Retardo de una vía menor a 500ms Prioridad 2: Perdida de paquetes menor al 10%	Plantilla similar a la de manejo de tráfico en grandes cantidades, pero brinda más holgura en la medición de los parámetros. Orientada a servicios de menor esfuerzo.
Scavenger	Prioridad 1: Retardo de una vía menor al 500ms Prioridad 2: Perdida de paquetes menor al 50%	Plantilla orientada a garantizar un retardo aceptable pero no garantiza que el paquete sea entregado adecuadamente a su destino.
Custom	Definición personalizada de los umbrales que el usuario requiera	Plantilla personalizada acorde con las necesidades de manejo para el tráfico.