

UNIVERSIDAD TÉCNICA DEL NORTE



UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

**TESTBED PARA EL ESTUDIO DE LA TECNOLOGÍA SD-WAN EN LA
UNIVERSIDAD TÉCNICA DEL NORTE**

AUTOR: CUAICAL REASCOS ADONIS GERMANICO

DIRECTOR: MSC. DOMINGUEZ LIMAICO HERNÁN MAURICIO

ASESOR: MSC. MAYA OLALLA EDGAR ALBERTO

IBARRA-ECUADOR

2023



UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN
A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA IDENTIDAD:	DE	0401964366	
APELLIDOS NOMBRES:	Y	Cuaical Reascos Adónis Germánico	
DIRECCIÓN:	El Ángel		
EMAIL:	agcuaicalr@utn.edu.ec		
TELÉFONO FIJO:	062978176	TELÉFONO MÓVIL:	0962639155

DATOS DE LA OBRA	
TÍTULO:	"TESTBED PARA EL ESTUDIO DE LA TECNOLOGÍA SD-WAN EN LA UNIVERSIDAD TÉCNICA DEL NORTE"
AUTOR (ES):	Cuaical Reascos Adónis Germánico
FECHA APROBACIÓN: DD/MM/AAAA	DE 12/10/2023
PROGRAMA:	X PREGRADO <input type="checkbox"/> POSGRADO
TITULO POR EL QUE OPTA:	Ingeniero en Telecomunicaciones
ASESOR /DIRECTOR:	MSc. Hernán Mauricio Dominguez Limaico

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 12 días del mes de Octubre de 2023.

EL AUTOR:



Cuaical Reascos Adónis Germánico
C.I: 0401964366



UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN:

MAGISTER HERNÁN MAURICIO DOMINGUEZ LIMAICO, CON CÉDULA DE IDENTIDAD Nro 1002379301 DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN CERTIFICA:

Que el presente trabajo de Titulación "TESTBED PARA EL ESTUDIO DE LA TECNOLOGÍA SD-WAN EN LA UNIVERSIDAD TÉCNICA DEL NORTE", ha sido desarrollado por el señor Cuaical Reascos Adónis Germánico bajo mi supervisión.

Es todo cuanto puedo certificar en honor a la verdad

Ing. Hernán Mauricio Dominguez Limaico, MSc
DIRECTOR

DEDICATORIA

Dedico con profundo agradecimiento mi trabajo de titulación a Dios, quien ha sido mi guía y fortaleza a lo largo de este camino académico. Agradezco a mi familia, en especial a mis padres, por su incondicional apoyo, aliento y sacrificio a lo largo de este largo proceso. También quiero agradecer a mis amigos, cuya compañía, ánimo y comprensión me han dado fuerzas en los momentos difíciles y han hecho de este camino una experiencia más amena.

AGRADECIMIENTOS

Agradezco de corazón a Dios, por haberme guiado y dado fuerzas durante todo este largo camino académico. A mis amados padres, Germánico y Rosa, les agradezco infinitamente por su comprensión, paciencia y apoyo incondicional en cada paso que di. Su amor y confianza fueron un pilar fundamental para mi éxito.

También quiero expresar mi profundo agradecimiento a mis queridos amigos, quienes estuvieron presentes en este camino de desarrollo personal y académico. Su apoyo, ánimo y palabras de aliento fueron un impulso esencial en los momentos de dificultad. Este logro no habría sido posible sin su respaldo inquebrantable. A todos ustedes, mi más sincero agradecimiento.

Finalmente, quiero expresar mi sincero agradecimiento a mi tutor, cuya orientación y apoyo resultaron fundamentales para la culminación exitosa de este trabajo de titulación.

ÍNDICE DE CONTENIDOS

1	CAPÍTULO I - ANTECEDENTES	1
1.1	Problema	1
1.2	Objetivos	2
1.2.1	Objetivo General	2
1.2.2	Objetivos Específicos	2
1.3	Alcance	3
1.4	Justificación	5
2	CAPITULO II - ESTADO DEL ARTE	8
2.1	Redes WAN Tradicionales	8
2.1.1	Costo elevado de Ancho de Banda.	8
2.1.2	Dependencia de Centros de Datos	9
2.1.3	Rendimiento variable en Aplicaciones	9
2.1.4	Infraestructura Compleja	10
2.2	Funcionamiento de una Red WAN	11
2.3	Tipos de Redes WAN	12
2.3.1	WAN Dedicada	12
2.3.2	WAN Conmutada	13
2.3.3	Conmutada por Circuitos	13
2.3.4	Conmutada por Paquetes	13
2.4	El Protocolo MPLS (Multiprotocol Label Switching).....	14

2.4.1	Elementos de MPLS	14
2.4.2	Label (Etiqueta)	15
2.4.3	LDP (Label Distribution Protocol)	15
2.4.4	LFIB (Label Forwarding Information Base)	15
2.4.5	LSR (Label Switching Router)	16
2.4.6	LSP (Label Switched Path).....	16
2.5	Funcionamiento de MPLS	17
2.6	Redes Definidas Por Software	18
2.6.1	Beneficios de SDN	19
2.6.2	Principios de Funcionamiento de Redes Definidas Por Software ...	20
2.6.2.1	Aplicaciones.....	20
2.6.2.2	Controladores	20
2.6.2.3	Dispositivos de Red	21
2.6.2.4	Protocolos que intervienen en Redes Definidas por Software .	21
2.7	Redes Definidas Por Software de Área Extendida SD-WAN	24
2.7.1	Conceptos de SD-WAN.....	25
2.7.2	Componentes y arquitectura	26
2.7.3	Overlay Management Protocol (OMP).....	32
2.7.4	BFD (Bi-directional forwarding Detection)	34
2.8	Ingeniería de Tráfico.....	36
2.8.1	Priorización del tráfico	37

2.8.2	Mapeo de tráfico de aplicaciones	38
2.9	GNS3 como Herramienta de Simulación de Redes	39
2.9.1	Arquitectura de GNS3	40
2.9.2	Requerimientos De Hardware Para el Despliegue de GNS3	41
3	CAPÍTULO III - Análisis e implementación de las arquitecturas de red para el uso de la tecnología SD-WAN	43
3.1	Topología MESH y HUB and SPOKE	43
3.2	Malla parcial	46
3.3	Spoke-Hub-Hub-Spoke	48
3.4	Topología SD-WAN para regiones geográficamente aisladas	50
3.5	SD-WAN Híbrida	52
3.6	Elección de la topología de red a simular	52
3.7	Elección del sistema operativo	63
3.8	Despliegue de vManage	65
3.9	Despliegue de vBond	81
3.10	Despliegue de vSmart	92
3.11	Instalación de certificados	95
3.12	Verificaciones plano de control	106
3.13	Despliegue de vEdge	114
3.14	Despliegue de red MPLS	126
3.14.1	Verificación de la RIB	134

3.14.2. Verificación de la LIB	136
3.14.1 Verificación de LFIB	141
3.15 Conexión de vEdges remotos	144
4 CAPÍTULO IV - Aplicación de ingeniería de tráfico y pruebas de funcionamiento de una red SD-WAN	156
4.1 Creación de política para topología HUB and SPOKE	156
4.2 Creación de VPN para el tráfico de datos de clientes.....	173
4.3 Uso de ingeniería de tráfico desde las políticas del vManage	181
4.4 Pruebas de funcionamiento	187
4.4.1. Verificación de Sesiones BFD en HUB's y SPOKES.....	189
4.4.2. Verificación de rutas para la VPN 1	190
4.4.3. Verificación de política enviada desde el vSmart en vEdge.....	192
4.4.1.1 Verificación de match en la política de datos	193
4.4.4. Simulación de flujos RTMP (Real Time Messaging Protocol)	194
4.4.5. Generación de tráfico RTMP (Streaming de video) y HTTP (web)	196
4.4.6. Verificación de métricas sobre la red SD-WAN	198
5 CAPÍTULO V – PRÁCTICAS DE LABORATORIO	201
5.1 Práctica de laboratorio 1: Despliegue del Plano de Control en un Clúster Centralizado para la Implementación del TESTBED SD-WAN.....	201
5.1.1 Topología de Red.....	202
5.1.2 Objetivo General:.....	202

5.1.3	Objetivos Específicos:	203
5.1.4	Desarrollo	203
5.1.5	Resultados.....	205
5.2	Práctica de laboratorio 2: Integración del plano de datos al TESTBED SD-WAN	206
5.2.1	Topología de red	206
5.2.2	Objetivo General.....	207
5.2.3	Objetivos específicos	207
5.2.4	Desarrollo	207
5.2.5	Resultados.....	209
5.3	Práctica de laboratorio 3: Manipulando el estado por defecto del TESTBED SD-WAN.....	210
5.3.1	Topología de red	210
5.3.2	Objetivo General.....	210
5.3.3	Objetivos Específicos	211
5.3.4	Desarrollo	211
5.3.5	Resultados.....	213
5.4	Práctica de laboratorio 4: Aplicación de ingeniería de tráfico sobre el TESTBED SD-WAN.....	214
5.4.1	Topología de red	214
5.4.2	Objetivo General.....	214
5.4.3	Objetivos Específicos	214

5.4.4	Desarrollo	215
5.4.5	Resultados	217
5.5	Practica de laboratorio 5: Mejorando la integración de la red MPLS y la red SD-WAN.	218
5.5.1	Objetivo General:.....	218
5.5.2	Objetivos Específicos:	218
5.5.3	Introducción	218
5.5.4	Desarrollo	219
A.	Configuración del protocolo 802.1Q.....	219
B.	Creación de vrf , asignación de interfaces y direccion ipv4.....	222
C.	Configuración de iBGP y activación de características extendidas 225	
D.	Establecimiento de eBGP entre CE y PE routers	227
E.	Resultados.....	229
	CONCLUSIONES	231
	RECOMENDACIONES	233
	BIBLIOGRAFÍA	235

ÍNDICE DE TABLAS

Tabla 1 Funcionamiento de GNS3	41
Tabla 2 Requerimientos recomendados.....	42
Tabla 3 Comparación Topologías SD-WAN	56
Tabla 4 Comparación diferentes soluciones SD-WAN.....	62
Tabla 5 Resumen de requerimientos de Sistemas Operativos	64
Tabla 6 Direccionamiento IPv4.....	66
Tabla 7 Rangos de etiquetas	133
Tabla 8 Resumen de ID's de equipos	157
Tabla 9 Listado de actividades cumplidas laboratorio 1	205
Tabla 10 Listado de acciones cumplidas para el laboratorio 2	209
Tabla 11 Actividades Cumplidas del laboratorio	213
Tabla 12 Acciones cumplidas laboratorio 4	217
Tabla 13 Distribución de puertos y Vlans	219
Tabla 14 Direccionamiento IPv4 MPLS-VPN para el laboratorio 5.	222

ÍNDICE DE FIGURAS

Figura 1 Topología de Red.....	5
Figura 2 Esquema Red WAN.....	11
Figura 3 Relación entre direcciones enlazadas, RIB, LIB y LFIB	18
Figura 4 Southbound y northbound	22
Figura 5 Esquema de una red SD-WAN.....	26
Figura 6 Arquitectura SD-WAN.....	28
Figura 7 Asociación de elementos de red	30
Figura 8 Esquema de conexión cisco SD-WAN.....	31
Figura 9 Colores de localizadores de transporte TLOC.....	33
Figura 10 OMP entre vEdge y vSmart.....	34

Figura 11 Esquema de funcionamiento de QoS en SD-WAN	38
Figura 12 Mapeo de aplicaciones	39
Figura 13 Funcionamiento de GNS3	40
Figura 14 (a) Topología con 1 enlace físico de transporte (b) Topología lógica Full-Mesh.....	44
Figura 15 (a) Topología con 2 enlaces físicos de transporte (b) Topología lógica Full-Mesh	45
Figura 16 Topología de Malla Parcial.....	47
Figura 17 Topología Spoke-Hub-Hub-Spoke	49
Figura 18 Topología para regiones aisladas.....	51
Figura 19 Topología propuesta.....	58
Figura 20 Topología rediseñada	61
Figura 21 Resumen de proceso de configuración de vManage	66
Figura 22 Esquema de funcionamiento del proyecto	70
Figura 23 Integración de equipos a GNS3	71
Figura 24 Configuraciones físicas vManage	72
Figura 25 Ingreso inicial vManage	73
Figura 26 Proceso de carga de vManage	74
Figura 27 Nuevo ingreso a vManage	75
Figura 28 Configuraciones iniciales vManage	76
Figura 29 Configuración de interfaz ETH0 vManage	77
Figura 30 Esquema de comunicación configuraciones iniciales	79
Figura 31 Vista de dispositivos interfaz web vista desde GNS3-cliente.....	80
Figura 32 Vista del monitor de la red vista desde GNS3-cliente	81
Figura 33 Proceso de despliegue de vBond	82
Figura 34 Configuraciones de iniciales vBond.....	83
Figura 35 Verificación de comunicación	84
Figura 36 Verificación del plano de control	85
Figura 37 Ingreso de vBond en el vManage	86
Figura 38 Configuración de interfaz vBond.....	87

Figura 39 Vista del ingreso desde la web	88
Figura 40 Creación de archivo contenedor	89
Figura 41 Contenido del fichero creado vbond.crt	89
Figura 42 Verificación de los dispositivos ingresados	90
Figura 43 Logs generados debido a la configuración	91
Figura 44 Habilitando la interfaz para la comunicación con IPsec	91
Figura 45 Conexiones del cluster de control.....	92
Figura 46 Configuraciones físicas de vSmart.....	93
Figura 47 Configuraciones iniciales del sistema de vSmart.....	94
Figura 48 Verificación de comunicación fallida	95
Figura 49 Instalación de certificados	96
Figura 50 Agregando vBond al plano de control.....	97
Figura 51 Agregando vBond al plano de control.....	97
Figura 52 Líneas de comando para la creación de certificados	98
Figura 53 Verificación de creación de certificados.....	99
Figura 54 Carga de certificado.....	100
Figura 55 Generación de firma del certificado.....	101
Figura 56 Creación de fichero para firmar el certificado	101
Figura 57 Parámetros de la firma del certificado.....	102
Figura 58 Certificado generado shell vManage	103
Figura 59 Carga del certificado firmado	104
Figura 60 Resumen de conexiones vSmart	105
Figura 61 Verificación de la comunicación con DTLS	106
Figura 62 Verificación de propiedades locales.....	107
Figura 63 Verificación de certificados instalados.....	108
Figura 64 Verificación de interfaces de los equipos.....	109
Figura 65 Verificación extendida de interfaces.....	110
Figura 66 Verificación de conexiones vManage.....	110

Figura 67 Verificación de conexiones en vBond	111
Figura 68 Verificación de LOGS desde el vBond.....	112
Figura 69 Verificación de control centralizado	113
Figura 70 Captura de paquetes en plano de control entre vManage y vSmart	114
Figura 71 Líneas de comando para configuración de vEdge desde consola	115
Figura 72 Verificación de certificados.....	116
Figura 73 Creación de archivo contenedor de la llave pública	117
Figura 74 Instalación del certificado.....	118
Figura 75 Cuenta usada para el desarrollo del trabajo	119
Figura 76 Detalles adicionales del perfil de vBond	119
Figura 77 Configuración del perfil de vBond.....	120
Figura 78 Perfiles virtuales de equipos.....	121
Figura 79 Verificación de perfiles activos	122
Figura 80 Dispositivos disponibles en el vManage	123
Figura 81 Campos de equipos provisionados	123
Figura 82 Activando la comunicación cifrada en el equipo.....	124
Figura 83 Activación del equipo	124
Figura 84 Vista desde el plano de control.....	125
Figura 85 Conexiones de vEdge.....	126
Figura 86 Topología de red para MPLS	127
Figura 87 Proceso de configuración MPLS	128
Figura 88 Ingreso de dirección IPv4 a interfaz	129
Figura 89 Creación de Loopback.....	130
Figura 90 Configuración de OSPF	131
Figura 91 Configuración de OSPF	132
Figura 92 Configuración de OSPF	134
Figura 93 Verificación de rangos de etiquetas.....	134
Figura 94 Routing Information Base (RIB) en equipo R1.....	135

Figura 95 Verificación de Neighbors.....	137
Figura 96 Verificación de LIB equipo R1	138
Figura 97 Verificación de LFIB en R1.....	142
Figura 98 Verificación etiqueta local en R3	144
Figura 99 Red, integrando vEdges remotos	145
Figura 100 Equipos activados y disponibles(Configuration->Devices).....	146
Figura 101 Equipos registrados en el plano de control (https://10.24.8.65:8443)	147
Figura 102 Estado del protocolo BFD (Monitor -> Network).....	148
Figura 103 Estado de los túneles (Monitor->Network->HUB1->Tunnels).....	149
Figura 104 Plano de orquestación con dos enlaces de transporte	150
Figura 105 (a)Consumo de recursos con un solo enlace de transporte (Monitor-> Network ->HUB2 ->Device).....	151
Figura 106 Plano de orquestación	152
Figura 107 Estadísticas de los túneles (Monitor->Network->HUB2)	152
Figura 108 Uso de las interfaces para la simulación	154
Figura 109 Sites ID de SPOKES (Monitor->Configuration->Policies->Centraliced)	158
Figura 110 Listas creadas de HUBS y SPOKES (Monitor->Configuration->Policies->Site Lists)	159
Figura 111 Asociación de política a una VPN (Monitor->Configuration->Policies->VPN service).....	160
Figura 112 Creación de política (Monitor->Configuration->Policies->Centraliced->Topology->Hub-and-Spoke)	161
Figura 113 Topología creada dentro de la política (Monitor->Configuration->Policies->Centraliced->Topology->Hub-and-Spoke)	162
Figura 114 Estado de la política.....	163
Figura 115 Activación de la política	163
Figura 116 Mensaje de estado erróneo del vSmart	163
Figura 117 Verificación del modo de vSmart	164
Figura 118 Creación del template para OMP del vSmart	165
Figura 119 Configuración de la VPN 0 para vSmart	166

Figura 120 Creación de plantillas para OMP y VPN (Monitor->Configuration->Policies->Featured Templates).....	167
Figura 121 Verificación del modo de operación de vSmart visto desde el vManage (Monitor->Devices->Controllers).....	168
Figura 122 Estado satisfactorio de la configuración remota del dispositivo	169
Figura 123 Visualización de políticas creadas desde el plano de gestión desde el plano de control ...	170
Figura 124 Sesiones BFD filtradas SPOKE 1.....	172
Figura 125 Sesiones BFD de HUB's	172
Figura 126 Interfaces asociadas a la vpn1	174
Figura 127 Configuración de OSPF.....	175
Figura 128 (a) Demostración de uso de la red MPLS	176
Figura 129 Rutas aprendidas en vpn 1 por OMP.....	179
Figura 130 TLOC con color MPLS recibido en el vSmart	180
Figura 131 Túneles establecidos en SPOKE 2.....	181
Figura 132 Aplicación de Ingeniería de Tráfico a la red SD-WAN (Monitor->Configuration->Policies->Topologia_HUB-N_SPOKE->Traffic Rules->add)	182
Figura 133 Creación de Famili List (Configuration->Policies->applications)	183
Figura 134 Emparejamiento con la familia de aplicaciones	183
Figura 135 Definir acciones para el emparejamiento	184
Figura 136 Ingreso de sitios y vpn a la política	184
Figura 137 Envío de políticas a vSmart	185
Figura 138 Verificación de logs.....	186
Figura 139 Verificación de la política de datos (show running-config policy).....	186
Figura 140 Verificación Conexiones Plano de Control	188
Figura 141 Verificación sesiones BFD SPOKE1	189
Figura 142 Verificación sesiones BFD HUB1	190
Figura 143 RIB de HUB1 para la VPN1	191
Figura 144 Política de Ingeniería de tráfico vista en SPOKE4	193

Figura 145 Flujos para la VPN1 desde SPOKE4	194
Figura 146 Simulación de Flujo RTMP (Monitor->Network->SPOKE4->Troubleshooting->Simulate Flows)	195
Figura 147 Simulación de flujo no RTMP	196
Figura 148 Ingreso al servicio web, desde SPOKE4	197
Figura 149 Inicio de transmisión con OBS	197
Figura 150 Ingreso de Streaming de video desde SPOKE-4	198
Figura 151 Métricas túnel mpls-mpls SPOKE-4	199
Figura 152 Esquema de establecimiento de túneles.....	200
Figura 153 Topología de red.....	202
Figura 154 Diagrama de flujo del despliegue del cluster central.....	203
Figura 155 Topología de red para full mesh	206
Figura 156 Diagrama de flujo para integración de vEdges al testbed SD-WAN	208
Figura 157 Diagrama de flujo para la configuración de la topología SHHS en el TESTBED SD-WAN. ...	212
Figura 158 Diagrama de flujo, para configuración de ingeniería de tráfico.....	216
Figura 159 Configuración de Vlans Switch 4	221
Figura 160 Configuración de vrf en R3.....	223
Figura 161 Asignación de interfaz a vrf redhibrida	224
Figura 162 Ingreso de interfaces a la vrf red hibrida	225
Figura 163 iBGP entre R3 y R5.....	226
Figura 164 Activación de características extendidas de BGP	227
Figura 165 Establecimiento de eBGP (configure terminal -> vpn 0)	227
Figura 166 Establecimiento de eBGP en vEdge.....	228
Figura 167 Verificación eBGP	229

RESUMEN

El presente trabajo detalla el diseño de un TESTBED para el estudio de la tecnología SD-WAN utilizando equipos de la marca CISCO. En este sentido, el enfoque del trabajo incluye el diseño de una red SD-WAN híbrida, en la cual se aplicará ingeniería de tráfico para filtrar sesiones BFD (Bidirectional Forwarding Detection), optimizando así los recursos en los nodos de acceso vEdge. Además, se llevará a cabo el mapeo de aplicaciones para redirigir paquetes selectivamente mediante la herramienta de ingeniería de tráfico proporcionada por la solución VIPTELA SD-WAN.

Para llevar a cabo este proyecto, se elige cuidadosamente el sistema operativo que servirá como base para toda la infraestructura SD-WAN. Luego, se define y despliega el software de simulación GNS3 dentro del sistema operativo elegido.

Una vez completados estos pasos, se cargan las imágenes necesarias para implementar la solución propuesta y se crean las redes virtuales y puentes para las redes de transporte correspondientes. Dado que es una red híbrida, también se despliega una red MPLS, siguiendo criterios específicos de despliegue establecidos en el presente documento.

Antes de implementar la red MPLS, se despliega un clúster de control que incluye el plano de gestión, control y orquestación. Para esta etapa, se propone un plan de direccionamiento IPv4 privado basado en el RFC1918. Luego, se asignan interfaces y direcciones IPv4 a cada uno de los nodos de la red, permitiendo el despliegue de certificados, conexiones seguras y la verificación de la comunicación entre los diferentes planos de control.

Dado que la red es reconfigurable ya que es una tecnología IaaS (Infraestructura como Servicio), se realizarán cambios en su estado inicial (FULL-MESH) para operar en el modo SHHS (Spoke-Hub-Hub-Spoke), lo cual permitirá verificar mejoras en el enrutamiento y el manejo de sesiones BFD.

Finalmente, para verificar tanto el TESTBED como la red SD-WAN híbrida, se realizarán simulaciones de flujo y se transportará tráfico en tiempo real a través de la red. Se evaluarán las métricas medidas bajo diferentes condiciones, incluyendo tráfico real en la red y su estado por defecto sin tráfico. Estas pruebas permitirán validar el funcionamiento y rendimiento de la infraestructura SD-WAN implementada.

ABSTRACT

This paper details the design of a testbed for the study of SD-WAN technology using CISCO equipment. In this sense, the focus of the work includes the design of a hybrid SD-WAN network, in which traffic engineering will be applied to filter BFD (Bidirectional Forwarding Detection) sessions, thus optimizing resources in the vEdge access nodes. In addition, application mapping will be carried out to selectively redirect packets using the traffic engineering tool provided by the VIPTELA SD-WAN solution.

To carry out this project, the operating system that will serve as the basis for the entire SD-WAN infrastructure is carefully chosen. Then, the GNS3 simulation software is defined and deployed within the chosen operating system.

Once these steps are completed, the images needed to implement the proposed solution are loaded and the virtual networks and bridges for the corresponding transport networks are created. Since it is a hybrid network, an MPLS network is also deployed, following specific deployment criteria established in this document.

Before to deploy the MPLS network, it displays a control control menu that includes the management plane, control and orchestration. For this stage, it proposes a private IPv4 addressing plan based on the RFC1918. Then, IPv4 interfaces and addresses are assigned to each of the network nodes, allowing the deployment of certificates, secure connections and the verification of communication between the different control planes.

Since the network is reconfigurable as it is an IaaS (Infrastructure as a Service) technology, changes will be made in its initial state (FULL-MESH) to operate in SHHS (Spoke-Hub-Hub-Spoke) mode, which will allow verifying improvements in routing and BFD session handling.

Finally, to verify both the testbed as the hybrid SD-WAN network, will perform flow simulation and will transport traffic in real time through the network. It will evaluate the different measures under different conditions, including real traffic in the network and its default status without traffic. These tests will allow validate the performance and performance of infrastructure SD-WAN implemented.

1 CAPÍTULO I - ANTECEDENTES

1.1 Problema

Las redes WAN tradicionales se basan en equipos distribuidos en determinados espacios físicos, en los cuales estos se encuentran conectados con enlaces WAN. Por otro lado, estas redes tienen un ancho de banda costoso ya que este depende directamente de los dispositivos usados y el protocolo de enrutamiento implementado como MPLS, lo cual dificulta la implementación y a su vez tiene grandes repercusiones en lo referente a tiempos de retardo, throughput, entre otros; además, al manejar redundancias como en MPLS, su implementación y configuración es más compleja (VMware.sf).

De igual manera las redes WAN tradicionales son dependientes de los denominados centros de datos, esto se debe a que no pueden acceder a los recursos en Internet de manera directa, lo cual implica que previo a retornar al sitio deseado debe realizar un paso por el centro de datos lo cual se traduce como afecciones en el rendimiento. Además, en caso de aplicar calidad de servicio en la red, implica que se deba configurar de manera manual en los diferentes equipos de red.

De acuerdo con el portal de VMware, una de las empresas más importantes de virtualización, la WAN tradicional incluye múltiples dispositivos de una sola función que se conectan a través de distintos enlaces de la red. Esta proliferación de la infraestructura hace que la gestión del entorno de TI (Tecnología de la Información) en las sucursales sea compleja.

En base a los problemas expuestos respecto a las redes tradicionales, la implementación de redes SD-WAN (Software Defined Wide Area Network) son una solución en cuanto al manejo del ancho de banda ya que permite superposición de redes

además de que simplifica la administración. En este sentido dentro de la Universidad Técnica del Norte (UTN) no se cuenta con un laboratorio para este tipo de redes emergentes; por lo que es necesario implementar soluciones para el acceso a este tipo de redes, ya que cada vez están tomando fuerza al igual que muchas aplicaciones en la nube, y los estudiantes de la carrera de Telecomunicaciones deben disponer de soluciones basadas en las tecnologías emergentes y no solamente en las redes tradicionales.

El implementar un laboratorio con equipamiento específico para el estudio la tecnología SD-WAN resulta excesivamente costoso, ya que los dispositivos necesarios, como controladoras, pueden llegar a costar miles de dólares, en este sentido, el presente trabajo propone realizar una guía para la elaboración de un TESTBED de manera simulada lo cual reducirá significativamente los costos para su implementación en laboratorio.

1.2 Objetivos

1.2.1 Objetivo General

Construir un TESTBED para el estudio del funcionamiento de SD-WAN mediante el despliegue de una topología de red con control de aplicativos de manera virtualizada mediante el software GNS3.

1.2.2 Objetivos Específicos

1. Establecer el estado del arte de la tecnología SD-WAN para comprender su funcionamiento, arquitectura y escalabilidad de este tipo de redes en comparación con las redes tradicionales.
2. Diseñar una topología de red en un ambiente controlado en el software GNS3 para el despliegue de control de tráfico en redes SD-WAN.

3. Realizar pruebas de funcionamiento y operación del TESBED implementado, para realizar la comparación entre las SD-WAN y las redes tradicionales.

4. Implementar prácticas de laboratorio para reforzar los conocimientos teóricos de la tecnología SD-WAN en el ambiente académico de enseñanza e investigación.

1.3 Alcance

En el presente proyecto se busca en primera instancia estudiar los fundamentos teóricos que apalancan una Red de Área Extensa Definida por Software (SD-WAN), con la finalidad de comprender su funcionamiento y comparar las mejoras que se pueden obtener con respecto a las redes de área extensa tradicionales, así como también conocer soluciones como por ejemplo la escalabilidad que proporciona SD-WAN.

En primera instancia se definirá el funcionamiento de MPLS (Multi Protocol Label Switching) así como el de SD-WAN, de esta manera se define un escenario de trabajo híbrido. En base al estudio del funcionamiento se definen ventajas y desventajas respectivamente lo cual implicará el realizar un análisis del trabajo de las dos tecnologías en conjunto.

A continuación, se analizará distintas arquitecturas de red para implementar SD-WAN, y de esta manera definir la adecuada de acuerdo con el entorno elegido para su simulación, es decir limitar los recursos mínimos requeridos para su implementación dentro del entorno de GNS3. En este mismo ámbito optimizar los recursos dentro del software de simulación para el correcto funcionamiento de la red a implementar.

En la siguiente etapa se plantea el diseño y simulación de una red SD-WAN híbrida, basada en equipamiento cisco, de los cuales no se cuenta con licencia por lo que

en el proceso se observarán ciertas características a las cuales no se tendrá acceso, las mismas que serán descritas en el desarrollo del trabajo de grado. Se usará la SD-WAN como una solución que es gestionada y operada mediante una vManage, vSmart y vBond alrededor de las cuales se planteará la solución. De este modo es necesario mencionar que acción desempeñará cada uno de los elementos mencionados; el vManage proporciona una interfaz gráfica, el vSmart el que gestionan la red y en la cual están implementadas tanto políticas como conectividad entre los elementos de la SD-WAN, el vBond permite la autenticación de cada uno de los elementos de la red, además de información de la topología de red.

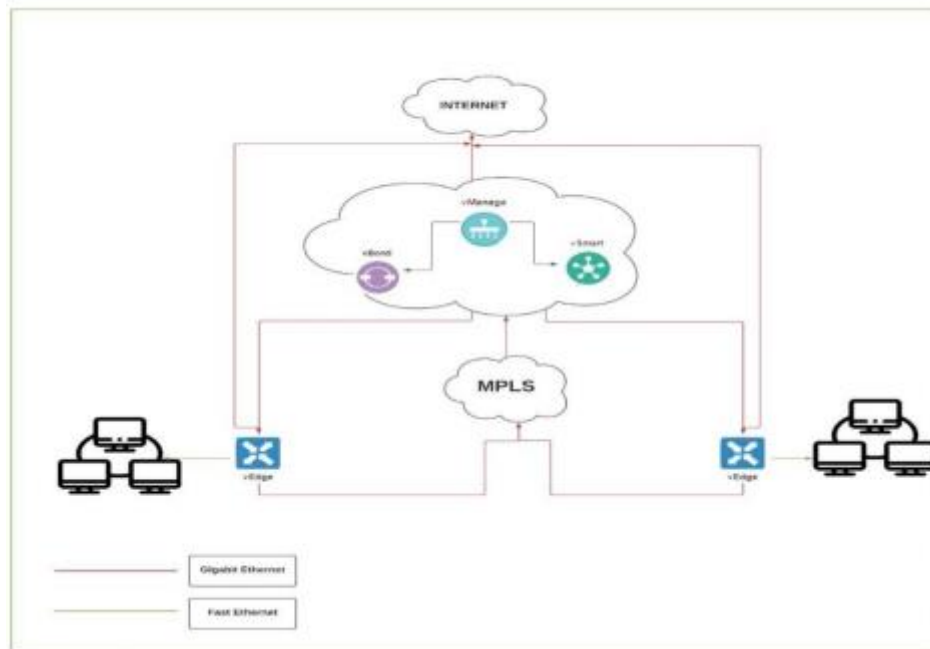
Una vez desplegada la red dentro del entorno GNS3 se realizará la implementación de ingeniería de tráfico, además de una comparativa del antes y después de su implementación, esto se lo realizará mediante las mediciones de tasas de transferencia, jitter en servicios en tiempo real y de esta manera identificar de manera clara las ventajas de la implementación de SD-WAN. Para realizar la comparativa se realizará un entorno con una red completamente MPLS y la realizada para el presente proyecto, identificados los escenarios de simulación, las pruebas de funcionamiento se las realizará con servicios en tiempo real como Voz sobre IP y streaming de video.

Definido el entorno de simulación, se aplicará el criterio de ingeniería de tráfico para una SD-WAN como son el balanceo de carga, el control de aplicativos y de esta manera realizar pruebas de funcionamiento con dichos criterios para identificar claramente las ventajas que ofrece.

Finalmente se propone 5 guías de laboratorio, así como su desarrollo, en donde se obtendrá datos para el análisis del funcionamiento de SD-WAN.

Figura 1

Topología de Red



1.4 Justificación

Al buscar métodos sencillos para implementar de manera virtualizada escenarios como el planteado permite al estudiante el acercamiento con nuevas tecnologías como las redes definidas por software que son soluciones relativamente costosas y en base a la situación socio económica del país no sería posible para los estudiantes tener un acercamiento con las mismas, analizando la situación presentada, el trabajo propuesto ayuda al estudiante y a la academia a buscar soluciones para el acceso a las nuevas tecnologías que sean realizables.

Las prácticas de laboratorio son una herramienta en el aprendizaje de los estudiantes, ya que ayudan a entender cómo funcionan las tecnologías y de esta manera construir conocimiento en base al traslado de estos a la práctica. El llevar la teoría de la mano con la práctica impulsa un interés intrínseco en los estudiantes debido a que lo

aprendido no solamente se queda como teoría puesto que se evidencian los procesos que implica generar dichos conocimientos.

Al tener acceso a nuevas tecnologías es fundamental en el desarrollo académico de un estudiante, a pesar de ello las “nuevas” tecnologías están fuera de nuestro alcance debido a los costos de los equipos para el estudio de las mismas, de este modo el pensar en alternativas que nos permitan a nosotros como estudiantes tener un acercamiento a estas tecnologías, y al realizarlo de manera simulada implica que están a nuestro alcance y de esta manera adquirir los conocimientos y competencias necesarias para la vida laboral.

Nuestro país no está en la vanguardia con respecto a este tipo de tecnologías, por lo cual las redes de área extensa definidas por software no se han visto difundidas a tal punto de tener dentro de nuestra universidad un laboratorio para poder manipularlas, de este modo el presente trabajo es un aporte importante para los estudiantes ya que tendrán noción de cómo funcionan estas redes y así implementarlas en entornos reales, en este sentido cada estudiante puede realizar prácticas en este tipo de entornos de manera más sencilla.

El tener la posibilidad de interactuar con las redes SD-WAN de manera virtualizada además de tener guías para su uso y configuración resulta beneficioso para los estudiantes ya que de esta manera evita los problemas de la falta de información o la falta de recursos para acceder a los equipos físicos propiamente dichos.

Si bien conocemos como funcionan las redes tradicionales, y algunas de las soluciones que presentan para controlar el tráfico, las soluciones que proporciona SD-WAN resultan más interesantes ya que al estar separados el plano de control y datos supone un reto debido a la estructura centralizada de la red. De este modo el aporte que

se brindará en este aspecto será realizar el análisis de las soluciones acerca del control de tráfico y el cómo implementarlas dentro de un entorno simulado además de mostrar estos resultados con las mediciones de retardo en servicios de tiempo real.

2 CAPITULO II - ESTADO DEL ARTE

2.1 Redes WAN Tradicionales

Las redes de área extendida (WAN), se encargan de interconectar redes más pequeñas como las LAN (Local Area Network), para ello utilizan protocolos de transmisión alojados en las capas 1, 2 y 3 del modelo de referencia OSI. Una red WAN, básicamente, hace uso del hardware haciendo que los paquetes se envíen de un nodo a otro hasta entregarse al dispositivo correcto, para ello se emplean los protocolos que define el modelo TCP/IP. Las redes WAN tradicionales emplean protocolos como MPLS, en el cual todos los cálculos para lograr la convergencia de la red se realizan en el dispositivo físico con lo cual, cuanto mayor tamaño tenga la red, mayor es el procesamiento requerido para lograr dicha convergencia y a su vez se traduce como un bajo desempeño de la red ante cambios de esta, esto se debe a que los cálculos para la convergencia de la red se deben realizar nuevamente.(cisco, 2023)

Por otra parte, las redes WAN presentan una serie de problemas por el propio modo de operación y gestión dentro del mismo equipo, de esta manera, de acuerdo con (vmware, 2022) los problemas que se desprenden de estas redes son: Costo elevado de Ancho de Banda, Dependencia de Centros de Datos, Rendimiento Variable en Aplicaciones e Infraestructura compleja.

2.1.1 *Costo elevado de Ancho de Banda.*

Para las redes WAN tradicionales el ancho de banda es crucial, ya que depende directamente de los enlaces físicos y su capacidad, de esta manera VMWARE, una de las empresas más grandes en cuanto a virtualización menciona:

El limitado ancho de banda de los caros circuitos de conmutación de etiquetas multiprotocolo (MPLS) o privados dificulta la implementación y repercute en el

rendimiento de las aplicaciones. Por otra parte, la redundancia privada o mediante MPLS de la red WAN resulta compleja de implementar y gestionar.(vmware, s. f.)

En este sentido, en MPLS (Multiprotocol Label Switching), al realizar o configurar redundancia, la administración y configuración de los equipos se complica debido a que dichas configuraciones se deben realizar directamente en el equipo físico, lo cual repercute directamente en el funcionamiento de las aplicaciones debido a la gestión de tráfico en base a las políticas que se manejen dentro de la misma red.

2.1.2 Dependencia de Centros de Datos

Los centros de datos son el núcleo de las redes WAN tradicionales, ya que estas redes no son capaces de tener acceso directo a los recursos de la nube, de este modo todo el tráfico generado, debe salir e ingresar por el centro de datos hasta llegar a su destino, añadiendo más retardo a los paquetes extremo a extremo.

Al no disponer de acceso directo a los recursos de la nube desde la sucursal debido a un arcaico diseño radial de la red, el tráfico retorna a través del centro de datos de la empresa con importantes problemas de rendimiento.(vmware, s. f.)

Este problema incluye problemas adicionales para la empresa ya que hace necesario adquirir, gestionar y mantener el centro de datos lo cual se traduce como gastos adicionales en la contratación de personal calificado.

2.1.3 Rendimiento variable en Aplicaciones

Con la capacidad de “controlar el tráfico” asignando niveles de servicio para clasificar el mismo pueden ocurrir problemas en base a que dichas configuraciones deben realizarse en toda la red lo cual incurre en problemas de disponibilidad ya que deben deshabilitar los equipos en el transcurso de la configuración. La diferenciación de servicio

puede hacer que ciertos paquetes sean eliminados con lo cual las aplicaciones tendrán problemas en funcionamiento si no se contempla en tráfico de manera adecuada.

El tráfico de las aplicaciones en los enlaces de Internet carece de un acuerdo de nivel de servicio que permita predecir su rendimiento. Cada uno de los cambios en la calidad de servicio de la aplicación requiere modificaciones manuales en las sucursales y en el centro de datos.(vmware, s. f.)

Las modificaciones que se realicen en un solo equipo como el cambio de las políticas de tráfico puede hacer que falle toda la red ya que las marcas o priorizaciones que se da al tráfico no serán iguales en todos los equipos con lo cual no se dará el resultado esperado.

2.1.4 *Infraestructura Compleja*

Con el propio hecho de adquirir un centro de datos, el manejo del área tecnológica se complica de tal manera que se debe tener personal especializado para esta área, nótese que la gestión se complica a medida que el tamaño de la red crece.

La WAN tradicional incluye múltiples dispositivos de una sola función que se conectan a través de distintos enlaces de la red WAN. Esta proliferación de la infraestructura hace que la gestión del entorno de TI en las sucursales sea compleja.(vmware, s. f.)

Este crecimiento de la red implica que el manejo del área tecnológica se complica con lo cual incurre en gastos adicionales a la empresa ya que se necesita personal especializado para el manejo de esta área.

2.2 Funcionamiento de una Red WAN

Una red WAN por definición es una red que conecta nodos diferentes, para ello se vale de otras infraestructuras para lograr su objetivo, las cuales no se encuentran bajo el control de la misma entidad. Para desempeñar el trabajo requerido la red necesita dispositivos como enrutadores y conmutadores para cursar el tráfico de un lugar a otro.

El funcionamiento de una red WAN es interconectar una gran cantidad de redes de menor tamaño mediante un medio de transmisión, para lo cual se requiere dispositivos como enrutadores, conmutadores. La función principal es cursar una gran cantidad de información.

Las operaciones de WAN se enfocan principalmente en la capa física (capa 1 de OSI) y la capa de enlace de datos (capa 2 de OSI). Los estándares de acceso a WAN suelen describir tanto los métodos de entrega de la capa física como los requisitos de la capa de enlace de datos. Los requisitos de la capa de enlace de datos incluyen direccionamiento físico, control de flujo y encapsulación. (Cisco Press, 2017)

Figura 2

Esquema Red WAN



Nota. Imagen tomada de (RF Wireless World, 2012)

En la Figura 2 se muestra un esquema de cómo funciona una red WAN tradicional, se observa el denominado centro de datos, el medio de transporte y los routers usados para cursar el tráfico de un lado a otro, la capa física puede ser de cualquier naturaleza como se observa en el bloque de los medios de transporte.

2.3 Tipos de Redes WAN

La clasificación de las redes WAN se la realiza en base a que, si usa o no circuitos dedicados, considerando que un circuito dedicado es aquel en el cual la conexión con el medio físico está siempre abierta, y uno no dedicado, es decir el conmutado, debe realizar las conexiones en distintos canales físicos.

2.3.1 WAN Dedicada

Una WAN dedicada puede entenderse como una conexión privada entre dos puntos, es generalmente usada por empresas para conectar sucursales, en esencia para transportar datos de un punto a otro.

Se utiliza un enlace punto a punto para proporcionar una ruta de comunicaciones WAN preestablecida desde las instalaciones del cliente hasta la red del proveedor.

Por lo general, un proveedor de servicios arrienda las líneas punto a punto, que se llaman «líneas arrendadas. (CCNA, s.f.)

Las líneas arrendadas es una forma de comunicar dos puntos sin necesidad de contar con un medio físico para realizar la transmisión, ya que se alquila cierta capacidad para poder realizar la conexión deseada, la infraestructura del medio físico es administrada por otra empresa.

2.3.2 *WAN Conmutada*

Una WAN conmutada se encarga de realizar, mantener y finalizar la conexión física para realizar la transmisión de datos, este tipo de enlaces es ofrecido por compañías de telecomunicaciones.

2.3.3 *Conmutada por Circuitos*

La comunicación por conmutación de circuitos involucra tres etapas que consisten en: crear el camino (o circuito) entre los extremos, transmitir la información y llevar a cabo la desconexión del circuito. Una vez establecida la ruta de conexión queda reservado un ancho de banda fijo durante el tiempo en el cual dure la sesión. (Universidad Internacional de Valencia, 2016)

La conmutación de circuitos se lo realiza físicamente generando los caminos, es decir el medio de transmisión existe físicamente mientras se lo esté usando. La ventaja de este tipo de red es que no se necesita enlaces físicos para comunicar cada uno de los puntos de red deseados.

2.3.4 *Conmutada por Paquetes*

La conmutación por paquetes es un método de conmutación WAN en el que los dispositivos de red comparten un circuito virtual permanente (PVC), que es similar al enlace punto a punto para transportar paquetes desde un origen hasta un destino a través de una red portadora.(CCNA, s. f.)

A diferencia de la WAN conmutada y dedicada se tiene que se generan enlaces **virtuales permanentes**, con lo cual el medio de transmisión esta siempre disponible en cada uno de los nodos sin necesidad de dedicar líneas y tampoco conmutarlas.

2.4 El Protocolo MPLS (Multiprotocol Label Switching)

MPLS, es un protocolo para transmitir datos usando etiquetas, este protocolo nació gracias a la necesidad de unificar cualquier tipo de datos para ser transmitidos por la misma red y no afectar al rendimiento de esta. Este protocolo tiene un costo elevado de implementación, sin embargo, proporciona beneficios a la red WAN y a la creación de VPN (Virtual Private Networks).

En el caso de MPLS se separa la información de control necesaria para la retransmisión de paquetes en la red de datos. En el enrutamiento IP clásico, cuando se envía un paquete de un enrutador a otro, cada enrutador selecciona de forma independiente el siguiente salto para el paquete, analizando la información del encabezado del paquete y algún algoritmo de enrutamiento. Los encabezados contienen mucha más información de la necesaria para la selección de una ruta o el próximo salto. En la tecnología MPLS, la elección de la ruta más adecuada se determina una sola vez a la entrada de la red MPLS. (Nadyalkov & Giorgiev, 2021).

En el protocolo MPLS de cierta manera se separan los planos de control y datos ya que el procesamiento de las rutas y la conmutación de paquetes se lo realiza en planos diferentes en el mismo equipo, de esta manera se logra que los datos viajen con mayor eficiencia, esto se explica gracias a que los paquetes no deben subir hasta la capa 3 para ser enrutados.

2.4.1 Elementos de MPLS

MPLS usa dispositivos de capa 3 los cuales reciben diferentes denominaciones de acuerdo con la función que desempeñan, es decir si ingresan, cambian o quitan las etiquetas, además se vale de un protocolo de enrutamiento interior como OSPF o IS-IS

para tener una vista general de toda la red, de esta manera se encuentran los siguientes elementos.

2.4.2 *Label (Etiqueta)*

Una etiqueta en MPLS se coloca entre las capas 2 y 3, esta etiqueta asocia la dirección de capa 3 con la interfaz de salida por la cual puede alcanzar el destino del paquete, con lo cual no es necesario subir hasta capa 3 para conocer por donde se debe enviar este, las etiquetas pueden ser quitadas, cambiadas y retiradas del paquete dependiendo de la estructura de la red.

2.4.3 *LDP (Label Distribution Protocol)*

El protocolo de distribución de etiquetas (LDP) es un protocolo para distribuir etiquetas en aplicaciones sin ingeniería de tráfico. LDP permite a los enrutadores establecer rutas de acceso conmutadas por etiqueta (LSP) a través de una red mediante la asignación directa de información de enrutamiento de capa de red a rutas de acceso conmutadas de capa de vínculo de datos. (Juniper Networks, 2022).

El protocolo LDP permite compartir las etiquetas a los vecinos del router, para de esta manera conocer con que etiqueta se ha asociado determinado prefijo y de esta manera ser capaz de conmutar dicha etiqueta dentro de toda la red, este protocolo se ayuda de la base de datos de enrutamiento para poder asociar las etiquetas a los prefijos.

2.4.4 *LFIB (Label Forwarding Information Base)*

La LFIB es la tabla utilizada para reenviar paquetes etiquetados. Se llena con los entrantes y etiquetas salientes para los LSP. La etiqueta entrante es la etiqueta del enlace local en el LSR particular. La etiqueta saliente es la etiqueta del enlace remoto elegido por el LSR de todos los enlaces remotos posibles. Todos estos

enlaces remotos se encuentran en la LIB. La LFIB elige solo una de las posibles etiquetas salientes de todos los enlaces remotos posibles en la LIB y lo instala en la LFIB. La etiqueta remota elegida depende de qué ruta es la mejor ruta encontrada en la tabla de enrutamiento. (Cisco Press, 2007)

2.4.5 LSR (*Label Switching Router*)

CISCO, uno de los fabricantes más importantes de equipamiento de red define que los LSR son enrutadores compatibles con MPLS y estos son capaces de comprender las etiquetas MPLS, es decir son capaces de recibir y retransmitir un paquete que ha sido etiquetado (Cisco Press, 2007).

Los LSR pueden ser tanto de frontera como pertenecer totalmente al dominio MPLS, de esta manera los de frontera también se les conoce como LER (Label Edge Router), este elemento se encarga de colocar y retirar etiquetas, por lo contrario, los LSR dentro del dominio MPLS solamente conmutan las etiquetas ya que sus vecinos de igual manera entienden las etiquetas.

2.4.6 LSP (*Label Switched Path*)

Una ruta conmutada por etiquetas es una secuencia de LSR's que transmiten un paquete por un dominio MPLS. Específicamente LSP es la ruta por la cual un paquete es encaminado, de esta manera se tiene los LSR que colocan la etiqueta por primera vez dentro de la red y los que se encargan de retirarla, estos también son conocidos como LER (Cisco Press, 2007).

El LSP al ser el camino dentro del dominio MPLS, es decir comprende todo el camino en donde se conmutan etiquetas hasta llegar al destino, para llegar de un prefijo a otro se coloca por primera vez una etiqueta y posteriormente se cambian dichas etiquetas,

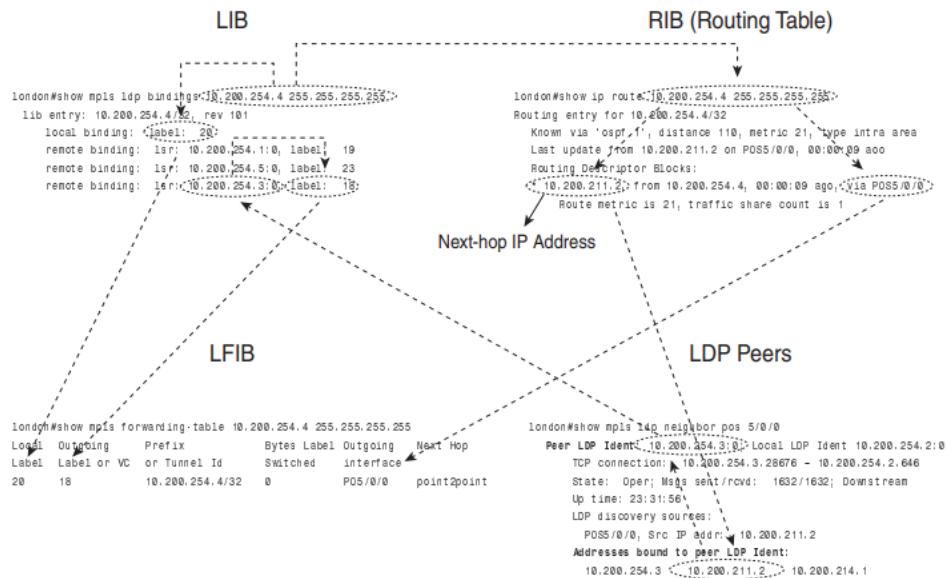
un salto previo a alcanzar el prefijo se retira las mismas para hacer más eficiente la conmutación.

2.5 Funcionamiento de MPLS

El funcionamiento de MPLS no resulta del todo complejo si entendemos cómo funciona la participación de cada una de las bases de datos generadas por los diferentes protocolos. En este sentido la Figura 3 resume el funcionamiento de MPLS, en primera instancia se genera la Routing Information Base (RIB), la cual se genera gracias a OSPF o IS-IS los cuales proporcionan una vista general de toda la red, una vez se tiene convergencia en toda la red, se construye la LIB que contiene o asocia las etiquetas locales con los prefijos proporcionados por la RIB, una vez se ha asociado los prefijos con etiquetas locales, con ayuda del protocolo de distribución de etiquetas se comparten las etiquetas locales con los vecinos, con lo cual las etiquetas locales se convierten en remotas y se forma la base de datos denominada LFIB, en esta instancia ya es posible realizar el envío de paquetes mediante la conmutación de etiquetas ya que se tiene asociados los prefijos con las etiquetas locales y remotas además de las interfaces por las cuales debe conmutar.

Figura 3

Relación entre direcciones enlazadas, RIB, LIB y LFIB



Nota. Imagen tomada de Cisco Press 2017

2.6 Redes Definidas Por Software

Las redes definidas por software (SDN: Software Defined Networks) representan un enfoque en el que las redes utilizan controladores basados en software o interfaces de programación de aplicaciones (API) para dirigir el tráfico en la red y comunicarse con la infraestructura de hardware subyacente. Este enfoque es distinto al de las redes tradicionales, que utilizan dispositivos de hardware dedicados (enrutadores y conmutadores) para controlar el tráfico de la red. Una SDN puede crear y controlar una red virtual o controlar una red de hardware tradicional mediante el software. (vmware, 2022)

Las redes definidas por software proporcionan una nueva solución para controlar el enrutamiento de manera centralizada, esto quiere decir que, en las SDN a diferencia de las tradicionales, el enrutamiento se lo maneja de manera remota mas no dentro del mismo

dispositivo de red, con lo cual dichos dispositivos se encargarán solamente del reenvío de los paquetes.

2.6.1 Beneficios de SDN

Las SDN presentan grandes beneficios respecto a las redes tradicionales, esto se debe a que al ser una red centralizada y reconfigurable presenta mayor flexibilidad al momento de escalar la red, lo cual se traduce en mayor velocidad en su despliegue. A continuación, se presentan los principales beneficios de SDN.

- Mayor control con velocidad y flexibilidad

El mayor control, velocidad y flexibilidad se debe a que en lugar de configurar manualmente cada uno de los dispositivos de red en el hardware, es posible controlar el tráfico que fluye sobre una red con un solo programa basado en software denominado controlador, gracias a esta estructura de red es posible conectar y centralizar cualquier cantidad de dispositivos.

- Infraestructura de red reconfigurable

Al ser una red centralizada, los operadores de red son capaces de reconfigurar los servicios y a su vez asignar recursos de manera virtualizada para de esta manera cambiar la infraestructura en “tiempo real”, esto posibilita dar prioridad a tráfico de aplicaciones deseadas.

- Mayor seguridad

De igual manera al ser una red centralizada proporciona la capacidad de una visión general de esta, lo cual permite generar zonas de acuerdo con el nivel de seguridad requerido, de igual manera definir que dispositivos son peligrosos para la red y aislarlos de manera oportuna.

2.6.2 Principios de Funcionamiento de Redes Definidas Por Software

El principio de funcionamiento es sencillo, ya que se basa en separar el hardware del software, es decir se tiene dos planos, el de control y el plano de datos, el primero se encarga de las funciones de procesamiento para el cálculo de rutas, por otro lado, el de datos que se lleva a cabo por el hardware solamente reenvía el tráfico. En pocas palabras la administración de este tipo de redes es centralizado ya que desde un solo dispositivo es posible controlar y reconfigurar toda la red.

Dentro de la arquitectura SDN se encuentran elementos como aplicaciones, controladores y dispositivos de red los cuales se describen a continuación:

2.6.2.1 Aplicaciones

Vmware, una de las empresas dedicadas a la virtualización menciona que las aplicaciones dentro de SDN son las que se encargan de comunicar y enviar solicitudes de recursos o información a la red (vmware, 2022).

Las aplicaciones se encargan de descubrir los dispositivos de red, de igual manera estas permiten un fácil acceso a los datos. Dichas aplicaciones permiten a los administradores observar la red de manera general sin necesidad de acudir a cada nodo a verificar su correcto funcionamiento.

2.6.2.2 Controladores

De acuerdo con (vmware, 2022) los controladores son aquellos que utilizan la información proporcionada por las aplicaciones para realizar los cálculos de rutas y de esta manera conocer como enrutar un paquete. Así mismo CISCO menciona que una controladora SDN se puede entender como el cerebro de la red, esto se debe a que estos elementos ofrecen la centralización de esta.

2.6.2.3 Dispositivos de Red

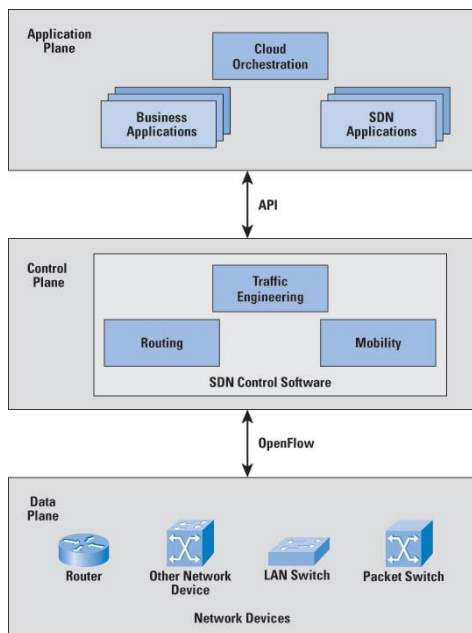
Los dispositivos de red son los elementos que reciben la información proveniente del controlador acerca de las rutas que deben tomar los paquetes (vmware, 2022). En este sentido, se puede entender a los dispositivos de red como los encargados de realizar la conmutación de paquetes en base a la información recibida por el controlador, con lo cual estos dispositivos no necesitan mucho procesamiento ya que solamente se encargan de realizar el reenvío de paquetes dentro de la red.

2.6.2.4 Protocolos que intervienen en Redes Definidas por Software

Las interfaces asociadas con SDN, se pueden definir como northbound y southbound son interfaces programadas para trabajar entre los planos de control, datos y aplicación. Las interfaces **southbound**, son las que interactúan con el plano de datos, más conocido como el plano de reenvío, cabe recalcar que estas interfaces varían de acuerdo con los cambios de la red. Por otro lado, las interfaces **northbound** definen como se debe comunicar la controladora SDN con el plano de aplicación, dichas definiciones se resumen dentro de la Figura 4.

Figura 4

Southbound y northbound



Nota. Imagen tomada de (Joe, 2019)

Los protocolos usados en las interfaces southbound son los usados en el plano de datos, dichos protocolos se resumen a continuación:

- ForCES

La separación del plano de datos y control define una pila de protocolos en su arquitectura para el intercambio de información entre los dos planos. El protocolo ForCES es el predecesor de OpenFlow ya que tienen la misma visión para la separación de los planos en una red.

El funcionamiento de ForCES se basa en una arquitectura maestro-esclavo donde los elementos de reenvío (FE) son esclavo y permiten que el elemento de control maestro (CE) los controle. Esto quiere decir, que FE está a cargo de procesar y manejar los paquetes, mientras que CE se encarga de la administración y ejecución del enrutamiento de los paquetes. (Guacho & Celleri, 2020)

- BGP

Se lo clasifica como protocolo de ruta vectorial o un protocolo de vector de distancia. Se basa en su tabla de enrutamiento con las direcciones que se puede alcanzar, y se las van asociando a una métrica de costo (valor que representa la conexión a cada router). (Guacho & Celleri, 2020)

- OpenFlow

Considerado en muchas aplicaciones para protocolos hacia el sur. Es un protocolo a través del cual un controlador lógicamente centralizado puede controlar un Switch OpenFlow. El enrutamiento de los paquetes se basa en las tablas de flujo de cada conmutador OpenFlow. (Guacho & Celleri, 2020)

De acuerdo con el artículo realizado por Basheer Mohammed y Bassan Estabrak, OpenFlow trabaja con tres tipos de mensajes los cuales son usados para la comunicación entre controlador y el conmutador OpenFlow, dicha comunicación se realiza mediante una conexión TCP entre los dos elementos mencionados. Los mensajes son clasificados como: mensajes entre la controladora y el switch, mensajes asíncronos los cuales son de switch a controlador, y finalmente mensajes simétricos. Los mensajes desde el controlador al switch son usados para afirmar el control del switch, lo realiza leyendo el estado del switch y modificando los mismos, esto implica que las tablas de flujo deben ser modificadas. Los mensajes desde el switch a la controladora son usados para informar de un nuevo flujo entrante, o para informar el cambio de estado de este, o simplemente para requerir la modificación de un flujo. Los mensajes simétricos pueden ser iniciados ya sea por la controladora o por el conmutador, estos mensajes son de reconocimiento, de eco o de error.

- OVSDB

Según Guacho y Celleri, autores del artículo denominado Análisis Comparativo de Protocolos de Comunicación para Redes definidas por Software, definen que, el protocolo de administración OVSDB usa un JSON¹. Permite que las aplicaciones se conecten a la base de datos Open vSwitch², en donde se encuentra la configuración (Guacho & Celleri, 2020).

- NetConf

Es un protocolo que proporciona mecanismos para instalar, manipular y eliminar la configuración de los dispositivos de red. Emplean el lenguaje XML, para los datos de configuración y los mensajes de protocolo. Tienen como objetivo la reducción de la complejidad y mejora del rendimiento de red. (Guacho & Celleri, 2020).

2.7 Redes Definidas Por Software de Área Extendida SD-WAN

SD-WAN tiene una perspectiva definida por software para la administración de una red WAN. Dentro de las principales ventajas de esta tecnología se tiene:

- Bajo costo independientemente de la red de acceso, ya sea mediante MPLS u otras tecnologías.
- Se mejora el rendimiento y la flexibilidad de las aplicaciones, debido a su uso eficiente ancho de banda ya que presenta incluso beneficios en la seguridad.

¹ JSON. JSON (Notación de objetos de JavaScript) es un formato ligero de intercambio de datos. Es fácil para los humanos leer y escribir. Es fácil para las máquinas analizar y generar.

² Open vSwitch: Es un switch virtual el cual; está diseñado para permitir la automatización masiva de la red a través de la extensión programática

- Simplifica las operaciones basándose en automatización debido a la gestión en la nube.

2.7.1 Conceptos de SD-WAN

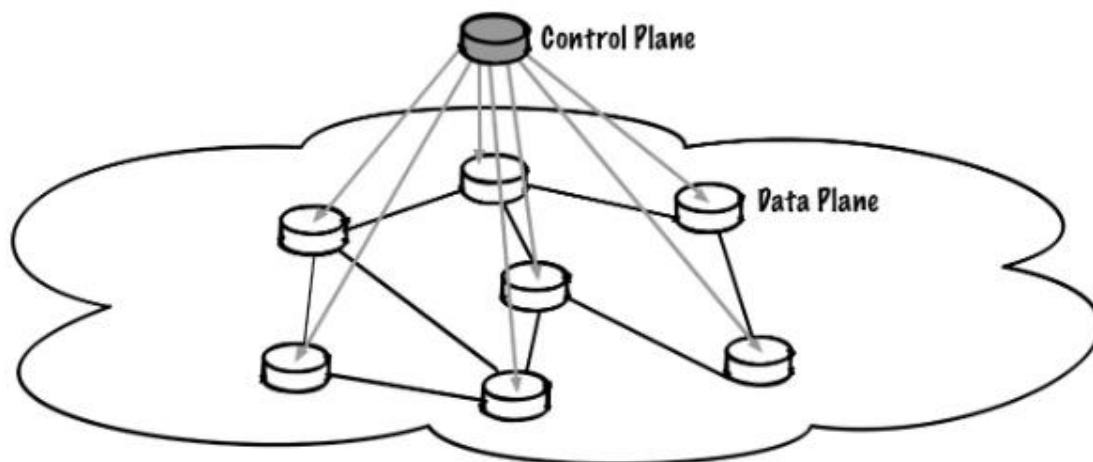
SD-WAN presenta un enfoque de red, arquitectura, implementación y objetivos diferentes a una red WAN tradicional, todos estos enfoques son dirigidos a mejorar las prestaciones de la red WAN. De manera resumida SD-WAN hace que la WAN sea más flexible ante el crecimiento de la red, además de programable e inteligente.

Los enfoques mencionados facilitan que nuevas funciones sean introducidas así mismo como la mejora de la prestación de servicios además de reducir los costos. De igual manera SD-WAN ha presentado un avance en los modelos para gestionar la red, así como la supervisión y seguridad de esta.

SD-WAN presenta una nueva interfaz o plataforma que influye o proporciona funciones y características de WAN. Todo, desde la orquestación, las operaciones y el control de paquetes de bajo nivel, puede ser impulsado por esta nueva (y a menudo centralizada) plataforma de software. (JuniperNETWORKS, 2022).

Figura 5

Esquema de una red SD-WAN



Nota. Imagen tomada de (JuniperNETWORKS, 2022)

En la Figura 5 se muestra una descripción gráfica del funcionamiento SD-WAN, con ello, se desea separar los planos de control y de datos, siendo el plano de control ubicado fuera de la red, incluso puede ser basado en la nube.

Para simplificar, unificar y proteger múltiples tipos de acceso, ya sean sucursales, campus, centros de datos o de otro tipo, las soluciones SD-WAN prometen una mayor resistencia, agilidad y seguridad en todas las formas de factores y modelos de negocio. Al evaluar las soluciones SD-WAN, las organizaciones deben tener claras sus motivaciones, requisitos y resultados deseados, no sólo en el día 0 (diseño), sino durante el día 1 (implementación), el día 2 (operaciones) y más allá. (JuniperNETWORKS, 2022).

2.7.2 Componentes y arquitectura

La solución SD-WAN de CISCO es una arquitectura de superposición WAN que se basa en la nube, extiende los principios de las redes definidas por software (SDN) a la

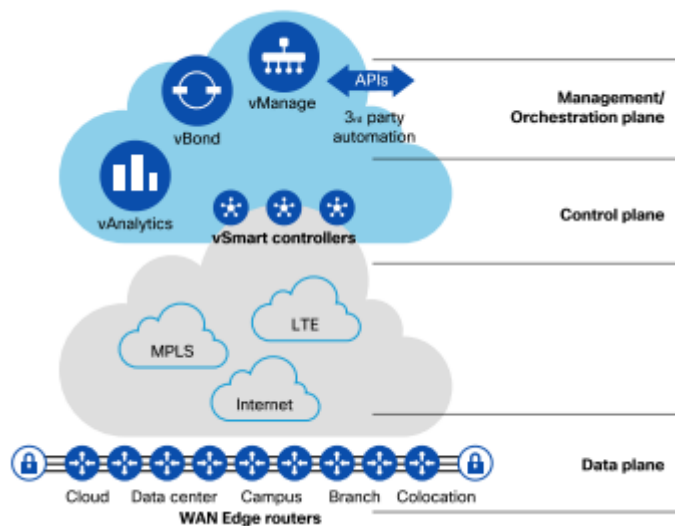
WAN. La solución de este fabricante se divide en cuatro planos: Datos, Control, Gestión y Orquestación.

En la Figura 6 se muestran los planos propuestos por CISCO para una SD-WAN, en el nivel más bajo se tiene el plano de datos, el cual se encarga de entregar los paquetes a un nodo específico ya que está ubicado directamente en un punto o sucursal deseada, en el segundo nivel se observa el plano de control, este plano se encarga de generar políticas para el tráfico además de encargarse de la seguridad del sistema, ya que este se comunica directamente con el plano de datos; en el tercer nivel se muestra el plano de gestión, el cual es el encargado de centralizar la red, provee un vistazo del tráfico de la red de manera centralizada, en vista de que todos los dispositivos deben conectarse a este; finalmente se observa el plano de orquestación, este plano es el encargado de la autenticación de cada uno de los nodos existentes, también se encarga de descubrir nuevos nodos y mantenerlos unidos a la red.

Adicionalmente la Figura 6 muestra que los planos mencionados contienen diferentes equipamientos de red, en el plano de datos se encuentra el **vEdge**, en el plano de control el **vSmart** y en el plano de gestión y orquestación **vManage** además del **vBond**, elementos que son descritos a continuación.

Figura 6

Arquitectura SD-WAN



Nota. Tomado de Cisco SD-WAN, Cloud Scale Architecture

- **Cisco vManage**

Este elemento es usado a nivel de gestión, cisco vManage es la interfaz de usuario, en este equipo los administradores y operadores de red realizan actividades de configuración, solución de problemas y supervisión. Dentro de las tareas de supervisión se tiene la recopilación de datos acerca de la conexión de los dispositivos vEdge, con lo cual es posible alertar acerca de eventos no deseados sobre la red.

- **Cisco vBond**

Este dispositivo se encuentra a nivel centralizado, los controladores vBond son los principales responsables de brindar servicios de autenticación, ya que se encargan de autenticar a los vSmart y vEdge, además coordina la comunicación entre estos; de igual manera distribuye los mensajes control entre el vSmart y vEdge mediante el uso del protocolo OMP que será descrito posteriormente. Otra de las funciones del vBond es

manejar las traducciones del protocolo NAT (Network Address Translation), ya que este debe ser ubicado en una zona desmilitarizada (DMZ) y debe tener una IP pública para que todos los dispositivos vEdge puedan alcanzarlo por medio del transporte que estén usando. Cuando el vBond se pone en marcha por primera vez en un estado no configurado, es decir que se lo ha ingresado por primera vez a la red SD-WAN, con lo cual este dispositivo por defecto se encargará de integrar dispositivos en la SD-WAN de forma mallada, lo cual quiere decir que integrará todos los dispositivos disponibles y les brindará comunicación. El papel del vBond en resumen es entender cómo se construye la red para posteriormente pasar la información a otros elementos de esta.

- **Cisco vSmart**

Es el cerebro de la red, está situado en el plano de control, este mantiene una tabla y política de enrutamiento centralizada, con lo cual el vSmart es el único encargado de calcular y distribuir las rutas al resto de la red. Las políticas para el enrutamiento se crean en el vManage, este envía dichas políticas al vSmart y este se encarga de centralizar la ejecución de estas. La información de enrutamiento se intercambia entre el controlador vSmart y los routers vEdge, con lo cual no existe la necesidad de comunicarse con otras controladoras, para realizar dicha comunicación hace uso del protocolo OMP (Overlay Management Protocol) el cual se encarga de comunicar los diferentes nodos de manera segura.

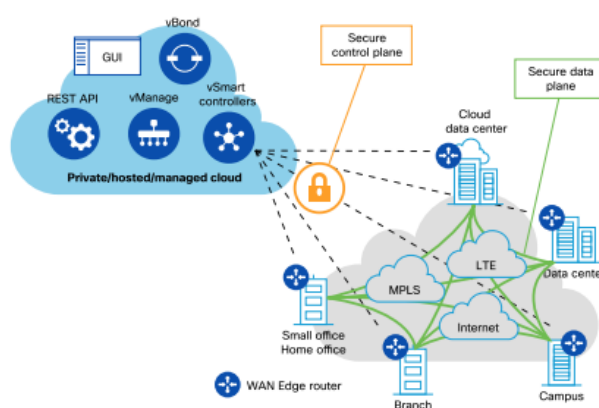
- **Cisco vEdge**

Los routers de borde WAN de Cisco, son responsables de crear las conexiones de red y supervisar el tráfico, estos pueden ser de distintas formas, ya sean físicos o virtuales. De la misma manera son los encargados de la función de asignación de recursos para determinada conexión, por ejemplo, asigna un ancho de banda para un lugar en concreto.

Este dispositivo es capaz de realizar análisis de seguridad y solucionar los mismos, además al estar más cerca de los sitios remotos mejora la disponibilidad de la red ante errores en base a que puede realizar conexiones directas con internet sin necesidad de realizarlo por el plano de control.

Figura 7

Asociación de elementos de red



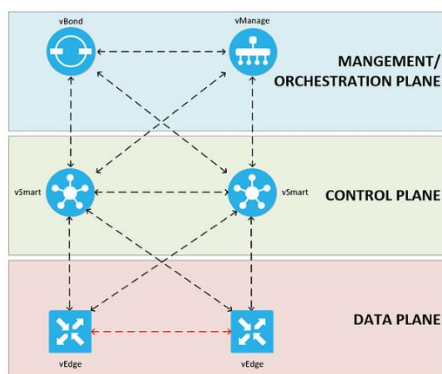
Nota. Tomado de Cisco SD-WAN, Cloud Scale Architecture

En la Figura 7 se muestra cómo los elementos que conforman la solución SD-WAN son distribuidos, de esta manera se observa que la mayoría de los elementos de la solución pueden ser ubicados en la nube³. Si bien en la Figura 7 se muestra a los vEdge como elementos desplegados en diferentes lugares estos pueden ubicarse en la nube de manera simulada siendo los proveedores de servicio de internet los que posibilitan la comunicación con este sin necesidad de desplegar físicamente dichos elementos en cada uno de los puntos requeridos.

³ Nube: No es una entidad física, es una red de servidores remotos distribuidos por todo el mundo, conectados para funcionar como una sola entidad.

Figura 8

Esquema de conexión cisco SD-WAN



Nota. Tomado de Cisco SD-WAN, Cloud Scale Architecture.

De la misma manera que en la Figura 7, en la Figura 8 se evidencia como los equipos están distribuidos en la red, de esta manera se muestran las conexiones de los dispositivos y en que plano de la red operan, en este sentido se tiene que tanto el vBond como el vManage operan en el plano de administración y orquestación, el vSmart trabaja directamente en el plano de orquestación y es el encargado de conectar al plano de control y datos, siendo este último conformado por los vEdges. Los routers vEdge forman túneles de Seguridad de Protocolo de Internet (Ipsec) entre sí, de esta manera forman la superposición de la red SD-WAN; de igual manera se establece canales de control entre los routers vEdge y los elementos de control como se muestra en la Figura 8. En este sentido, por dicho canal de control se recibe información de configuración, y enrutamiento. Nótese que el tráfico del plano de datos no se reenvía al plano de orquestación ni administración puesto que no existe conexión directa con dichos planos, de acuerdo con (CISCO,2022) en su libro denominado “cloud scale architecture”, cada uno de los planos puede tener su propia salida a internet con lo cual no tiene dependencia directa con el plano superior ya que, en caso de fallas de conexión entre estos, todos son

capaces de funcionar independientemente hasta que se reestablezca la comunicación entre los mismos.

2.7.3 *Overlay Management Protocol (OMP)*

Este protocolo gestiona la red superpuesta SD-WAN, se ejecuta entre los controladores vSmart y los routers vEdge en donde toda la información del plano de control se intercambia con el plano de datos de manera segura. Este protocolo opera en base a políticas establecidas por el vManage, en caso de no definirse ninguna política, el comportamiento de OMP es permitir una topología de malla completa donde cada router vEdge puede conectarse directamente con sus pares. Este protocolo realiza tres operaciones básicas que son:

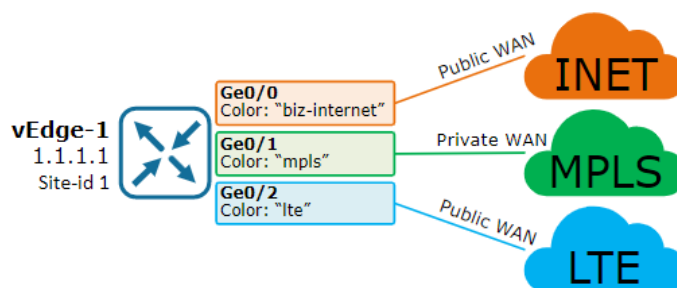
- Las rutas OMP son prefijos que se aprenden de manera local, los prefijos son distribuidos por este protocolo para que puedan ser transportados a través de la superposición de la red SD-WAN. OMP anuncia atributos dentro de los cuales se incluye; información de ubicación del transporte (TLOC), que es similar a la dirección IP del siguiente salto de BGP y otros atributos como el origen, la fuente, la preferencia, el ID del sitio, la etiqueta de VPN. **Una ruta OMP sólo se instala en la tabla de reenvío si TLOC al que apunta está activo.**
- **TLOC**, son los puntos lógicos de terminación del túnel VPN en los routers vEdge que se conectan a una red de transporte. Una ruta TLOC está identificada por tres parámetros, la dirección IP del sistema, el color del enlace y la encapsulación.⁴ De esta manera, en la Figura 9 se muestra un

⁴ TLOC color: Es una abstracción lógica para identificar un transporte WAN que se conecta a un vEdge.

ejemplo de cómo se asocian los colores con el tipo de red de transporte, estos colores se configuran dentro de del vEdge identificando claramente la interfaz y el tipo de conexión que está tiene.

Figura 9

Colores de localizadores de transporte TLOC



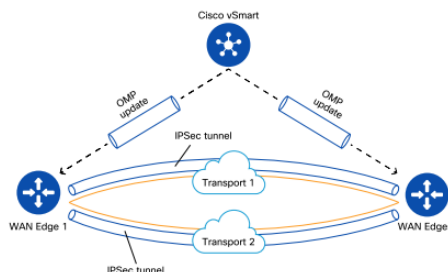
Nota. Imagen tomada de Networ Academy, TLOC Color and Carrier

- El servicio de rutas representa servicios (firewall, IPS⁵, optimización de aplicaciones) que se conectan a la red del vEdge del sitio local y son disponibles para otros sitios. Estas rutas incluyen VPN's con lo cual las etiquetas de este protocolo se envían en las actualizaciones hacia el vSmart, para indicar a los controladores qué VPN's son atendidas en un sitio remoto.

⁵ IPS: Intrusion prevention System. El sistema de prevención de intrusiones detecta y bloquea ataques de red conocidos.

Figura 10

OMP entre vEdge y vSmart



Nota. Tomado de Cisco SD-WAN, Cloud Scale Architecture

En la Figura 10 se muestra que la conexión entre el vSmart y vEdge se realiza mediante el protocolo OMP el cual mediante actualizaciones comunica los planos de datos y control definiendo que dispositivos pueden comunicarse estableciendo túneles entre estos. De la misma manera se observa que los túneles se forman mediante el establecimiento de VPN's entre los diferentes nodos, con lo cual la comunicación entre estos se realiza de manera segura. La Figura 10 también muestra que al generar los túneles no es necesario realizar una comunicación orquestada por el plano de control ya que esto retardaría la comunicación entre los nodos, con lo cual establecer una comunicación directa y segura es menos complejo para la red SD-WAN.

2.7.4 BFD (Bi-directional forwarding Detection)

La detección de reenvío bidireccional es el mecanismo utilizado por los vEdge para sondear y medir el rendimiento de los enlaces de transporte, estas sondas proporcionan información como; latencia, jitter, y pérdida de enlaces con la red de transporte, con estos datos, los vSmart son capaces de determinar la mejor ruta y comunicar las mismas con los routers vEdge para garantizar la comunicación de los diferentes nodos. (Juniper,2022) en el apartado de guías de alta disponibilidad r menciona que el protocolo BFD es un mecanismo de saludo que se usa para la detección de fallas

de una red, para ello emplea saludos entre el plano de control y datos, dichos saludos se efectúan en intervalos específicos, con lo cual se es capaz de tomar diferentes mediciones como las mencionadas anteriormente, BFD al funcionar en una gran variedad de red y topologías presenta una gran ventaja para una solución SD-WAN que no depende de la red de transporte.

Por otra parte, CISCO (2022), define que una vez que se ha establecido una sesión BFD y se ha definido los tiempos de saludo, se envían paquetes de control que actúan como los paquetes de saludo presentes en los protocolos de enrutamiento IGP (Interior Gateway Protocol) lo cual ayuda a detectar la actividad de los nodos requeridos, la principal diferencia entre un IGP y BDF es que este último se ejecuta con una mayor velocidad. En este sentido CISCO define varios parámetros a tomar en cuenta acerca de este protocolo los cuales se muestra a continuación:

1. El protocolo BFD es usado para la detección de fallas en una ruta de reenvío en la red de transporte. Con lo cual solamente es capaz de detectar la falla, el encargado de tomar acciones para no perder paquetes en el proceso de reenvío es el protocolo de enrutamiento.
2. BFD es capaz de trabajar en cualquier capa de los protocolos de enrutamiento, a pesar de ello debido a las versiones de IOS de los equipos se trabaja solamente en la capa 3 de estos.
3. En caso de tener más de un protocolo de enrutamiento por el mismo enlace, BFD no trabaja con todos estos, con lo cual establece una sola sesión para un solo protocolo y comparte la información con los demás.

2.8 Ingeniería de Tráfico

La ingeniería de tráfico es un proceso por el cual los flujos de tráfico pueden ser variados según especificaciones mismas del administrador de red, con lo cual las rutas pueden o no obedecer a los protocolos de enrutamiento usados por la misma red, el hecho de usar ingeniería de tráfico da lugar a que el uso de los recursos proporcionados por la red sea más eficiente, además de proteger la red ante fallos de los enlaces o nodos. De igual manera la IT, ofrece la posibilidad de garantizar servicios diferenciados y de igual manera capacidad de enlace garantizado.

Para garantizar que las aplicaciones críticas para la empresa funcionen de manera óptima, es necesario conocer las aplicaciones de la red y los controles adecuados que se establecerán para lograr los resultados deseados. Algunos de los problemas que afectan a la calidad de experiencia de la aplicación son: Pérdida de datos en circuitos de baja calidad, retraso y jitter excesivo en circuitos, lo que afecta a la voz y a otras aplicaciones, latencia debido a la retransmisión del tráfico desde la nube al centro de datos y viceversa, priorización inadecuada del tráfico, lo cual afecta a enlaces de menor ancho de banda.

De acuerdo con (CISCO,2019) en el apartado de conectividad SD-WAN, las políticas de control centralizado operan en la información de enrutamiento y localizador de transporte (TLOC) dentro de OMP y permiten la personalización de las decisiones de enrutamiento. Estas políticas se pueden usar para configurar la ingeniería de tráfico, la afinidad de rutas y la inserción de servicios. Nótese que las políticas al ser manejadas de manera centralizada en el plano de control es sencillo aplicar las mismas, con lo cual el administrador deberá simplemente crear las políticas dentro del vManage posteriormente se encargará de comunicar las mismas al vSmart y este las ejecuta y por ende decidirá las rutas preferidas y se las comunicará a los routers vEdge.

2.8.1 Priorización del tráfico

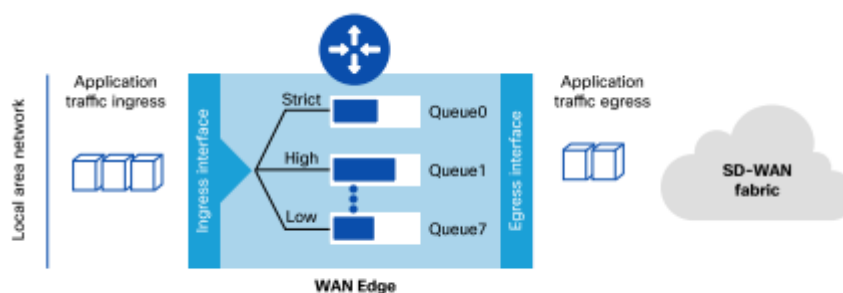
Las aplicaciones son diversas, y todas son diferentes entre sí, con lo cual algunas necesitan utilizar un gran porcentaje de la capacidad de un enlace de comunicación, por lo contrario, otras solamente se preocupan por la latencia, estos dos factores pueden hacer que el rendimiento de las mismas varíe dando mejores tasas de transferencia efectiva, de esta manera cuando el tráfico de las aplicaciones pasa por el vEdge tienen una gran capacidad de transferencia ya que están dentro de la red de área local, en donde la contención de recursos no es común, una red WAN tiene menor ancho de banda, donde cada bit cuenta y no se pueden estar realizando retransmisiones de paquetes perdidos ya que ocuparía capacidad del enlace saturando la red. El uso de circuitos de alta capacidad como parte de la solución de Cisco SD-WAN ha mejorado la contención de recursos de la red WAN, aunque siguen siendo un problema.

Cuando la red se ve congestionada, los routers vEdge emplean QoS, que ayudan a priorizar el tráfico. Para ello se utilizan las colas, la programación de “turnos”, ayuda a que todas las aplicaciones obtengan el recurso de ancho de banda. Con estas colas se puede minimizar el jitter y la latencia de las aplicaciones en tiempo real.

Los routers WAN Edge también pueden emplear mecanismos como la conformación del tráfico y el control del tráfico para cumplir con la capacidad del circuito de los circuitos entregados por el operador. Cisco vManage proporciona una interfaz para configurar las políticas de QoS así como para supervisar su comportamiento. (Cisco, 2019).

Figura 11

Esquema de funcionamiento de QoS en SD-WAN



Nota. Tomado de Cisco SD-WAN, Cloud Scale Architecture

En la Figura 11 se muestra cómo se realiza la priorización del tráfico para brindar QoS, en la imagen se observa las colas que se generan en el vEdge para cursar el tráfico, y como se agenda los recursos de ancho de banda según su prioridad.

2.8.2 Mapeo de tráfico de aplicaciones

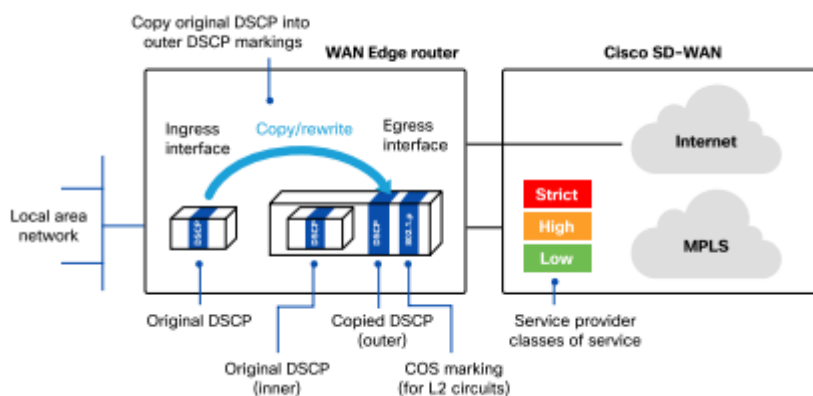
Cisco SD-WAN funciona de forma independiente al transporte, con lo cual aprovecha todos y cada uno de los circuitos que posee el vEdge. Estos circuitos son responsables de entregar el tráfico de la aplicación entre los nodos de la SD-WAN. Cuando se aprovechan los circuitos privados se puede aplicar clases de servicio específicas para priorizar el tráfico de aplicaciones cuando pasan por el núcleo de la red. La asignación de tráfico de aplicaciones se realiza mediante la coincidencia de las marcas DSCP (Differentiated Services Code Point), en el caso de las rutas calculadas con las direcciones de capa 3.

Para realizar el mapeo de aplicaciones, cisco SD-WAN aprovecha las tecnologías como IPsec para encapsular el tráfico y enviarlo por la red WAN de manera segura, este aspecto de seguridad es muy importante para la SD-WAN en base a que la red de

transporte puede ser de cualquier tipo y está fuera de nuestro dominio con lo cual la información transmitida está expuesta, este encapsulamiento coloca cabeceras IP adicionales al paquete original, lo cual impide que el proveedor de servicios aplique priorización del tráfico. Para lo cual copia las marcas DSCP del encabezado interno y lo encapsula con el DSCP en la cabecera IP, siendo el DSCP uno de los proporcionados por el operador de servicios.

Figura 12

Mapeo de aplicaciones



Nota. Tomado de Cisco SD-WAN, Cloud Scale Architecture

En la Figura 12 se muestra que las marcas DSCP dentro de la red SD-WAN se respetan dentro de su dominio hasta la frontera con el proveedor de servicios de internet, en donde debe encapsularse dentro de otro paquete IP y respetar las marcas ofrecidas por el proveedor, lo cual ayuda a garantizar una experiencia adecuada con las aplicaciones en redes de transporte privadas.

2.9 GNS3 como Herramienta de Simulación de Redes

GNS3 (Graphical Network Simulator) es una herramienta de simulación de redes, este software permite construir topologías de red muy sencillas y complejas, el alcance de las redes a emular depende directamente del hardware en el cual se esté ejecutando. El

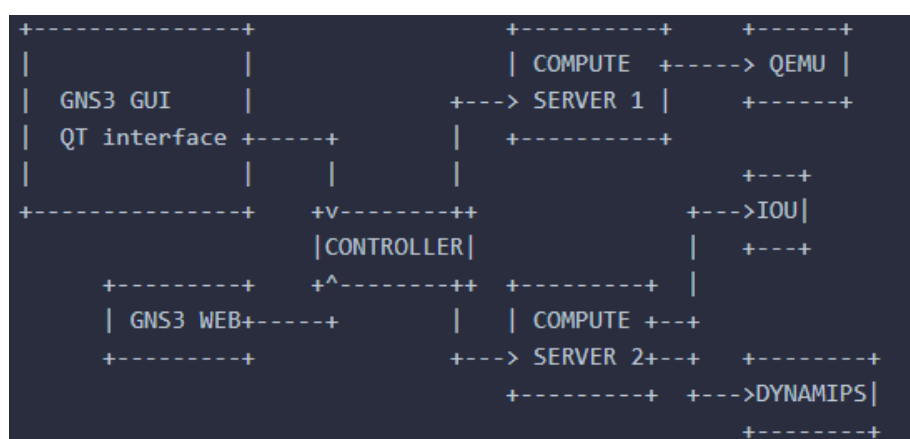
uso de este software provee beneficios en cuanto a que permite diseñar redes en un ambiente controlado, lo cual posibilita realizar pruebas sobre estas previo a su implementación física, de esta manera se evita poner en peligro los equipos de red adquiridos.

2.9.1 Arquitectura de GNS3

GNS3 básicamente consta de cuatro elementos de software, los cuales son; El software todo en uno conocido como GNS3 (GUI), controlador, cómputo y los emuladores. El controlador es el encargado de visualizar todos los proyectos, gestiona el estado de estos, solamente se puede ejecutar una vez, es decir con un solo controlador se puede monitorear varios proyectos, la GUI es la encargada de mostrar de manera gráfica la topología y realizar cambios sobre las misma, el cómputo controla los emuladores para ejecutar los procesos que estos solicitan, a continuación, dicho esquema de funcionamiento se muestra en la Figura 13.

Figura 13

Funcionamiento de GNS3



Nota: Imagen tomada de (GNS3, 2023a)

Dentro de la Figura 13 se observa que la interfaz de usuario puede ser brindada ya sea por el software directamente con su GUI o realizarlo mediante el acceso por la WEB,

por ello las dos opciones se muestran como el inicio del funcionamiento de un proyecto. Una vez se define el método de acceso al software, se tiene una sola controladora orquestando varios proyectos, con lo cual esta se encarga de comunicar las peticiones y cambios del nivel superior a los niveles más bajos. De la misma manera se observa diferentes cómputos que se encargan de controlar diferentes emuladores dependiendo de los dispositivos usados en el nivel superior, finalmente se tiene los emuladores, los cuales son los encargados de brindar las funciones de los equipos requeridos, nótese que el cómputo abre sesiones dependiendo del número de emuladores usados en el proyecto.

La comunicación en todos los niveles se realiza a través de HTTP (Hyper Text Transfer Protocol), utilizando datos en formato JSON. De la misma manera los errores son notificados mediante HTTP y mostrados dentro de la GUI o WEB. GNS3 también usa autenticación sobre HTTP para evitar solicitudes no autorizadas hacia el servidor.

2.9.2 *Requerimientos De Hardware Para el Despliegue de GNS3*

Para la implementación de GNS3 sobre un computador se tienen los siguientes requerimientos:

Tabla 1

Funcionamiento de GNS3

Requerimientos mínimos	
Sistema operativo	Windows 7, Mavericks 10.9, cualquier linux
Procesador	2 o más núcleos lógicos
Memoria RAM	4GB
Almacenamiento	1GB o más para la inclusión de imágenes

Fuente: Requerimientos tomados de (GNS3, 2023b)

Los requerimientos mínimos mostrados en la Tabla 1, son solamente de referencia de que el software podría ser instalado y usado de manera básica, es decir la

implementación de varios routers y switches; sin embargo, los requerimientos dependen directamente de la topología a emular, con lo cual dichos requerimientos no serían suficientes para realizar el tema propuesto. En este sentido en la Tabla 2, se muestran los requerimientos recomendados para un mejor desempeño del software.

Tabla 2

Requerimientos recomendados

Requerimientos recomendados	
Sistema operativo	Windows 7, Mavericks 10.9, linux en cualquier versión
Procesador	2 o más núcleos físicos, 4 o más núcleos lógicos, con virtualización
Memoria RAM	> a 16GB
Almacenamiento	SSD o HDD con más de 1TB

Fuente: Requerimientos tomados de (GNS3, 2023b)

Dentro de la Tabla 2 se muestra que para el objetivo del presente trabajo los requerimientos aumentan significativamente debido a las máquinas virtuales requeridas, además de los propios requerimientos de las controladoras y routers de acceso, con lo cual se debe realizar una correcta elección de sistema operativo para trabajar ya que el uso de los recursos de este puede ser crucial al momento de realizar las simulaciones.

3 CAPÍTULO III - Análisis e implementación de las arquitecturas de red para el uso de la tecnología SD-WAN

En este capítulo se presenta un análisis de las diferentes arquitecturas presentes para el despliegue de una red SD-WAN propuestas por el fabricante CISCO, de esta manera se analizará cada una de estas además de identificar las ventajas y desventajas de una posible implementación. Adicionalmente se analiza cómo ayuda una red SD-WAN híbrida a las prestaciones de la red juntamente con MPLS y de esta manera determinar la topología a implementar para el presente trabajo de titulación. Finalmente se realiza la elección del sistema operativo para la implementación del banco de pruebas de la red, además del despliegue de cada uno de los elementos que forman parte de esta para su funcionamiento.

3.1 Topología MESH y HUB and SPOKE

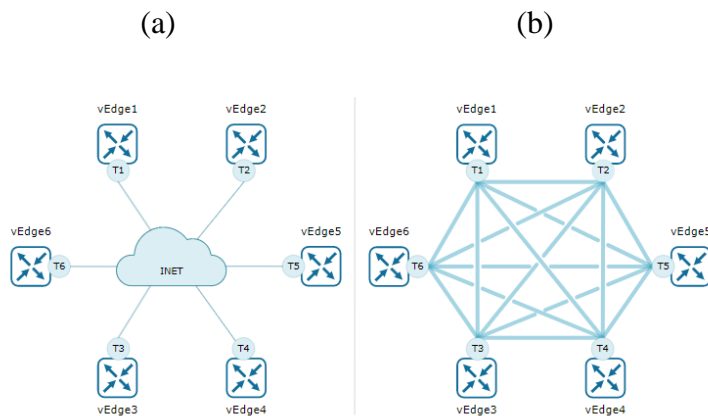
En una red Cisco SD-WAN los enrutadores vEdge generan una topología de malla completa con cada uno de sus pares, este es el comportamiento por defecto mencionado en el capítulo 2, de este modo todos los dispositivos dentro de un servicio VPN pueden comunicarse entre sí, sin embargo, este tipo de topología presenta problemas de escalabilidad debido a que no todos los puntos requieren conectarse, con lo cual dichos recursos pueden ser mejor utilizados.

Un claro ejemplo del problema de tener una topología de malla completa con SD-WAN, es que el número de túneles crece en proporción al tamaño de la red, lo cual no es saludable para la gestión de la red; dicho número se calcula haciendo uso de la Ec. 1; en donde n representa el número de enrutadores vEdge presentes en la red.

$$\#tuneles = n(n - 1)/2 \quad (\text{Ec. 1})$$

Figura 14

(a) Topología con 1 enlace físico de transporte (b) Topología lógica Full-Mesh



Nota. Imagen tomada de (NetworkAcademy, 2022)

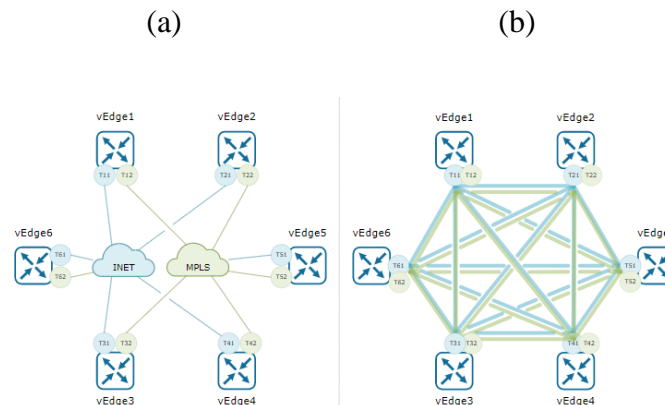
En la Figura 14a se muestra la topología a través de la red de transporte (INET) la cual puede ser privada o pública (internet), en este caso se tiene 6 vEdge, en donde cada vEdge se conecta con su respectivo enlace físico ; mientras que la Figura 14b, presenta los diferentes enlaces lógicos (túneles con IPsec) que tiene cada vEdge, en este caso un total de 15 túneles.

Por otra parte, si cada vEdge de la Figura 14a tiene uno o más enlaces físicos redundantes hacia la red de transporte, el número de túneles se calcula mediante la Ec. 2, en donde k es el número de enlaces redundantes, en este caso el número de túneles aumenta en un factor de k (ver Figura 15), afectando así aún más el problema de escalabilidad de la SD-WAN ya que se debe manejar más números de sesiones BFD en cada vEdge.

$$\#tuneles = k * n(n - 1)/2 \quad (\text{Ec. 2})$$

Figura 15

(a) Topología con 2 enlaces físicos de transporte (b) Topología lógica Full-Mesh



Nota. Imagen tomada de (NetworkAcademy, 2022)

La Figura 15a muestra la conexión de cada vEdge haciendo uso de dos enlaces físicos hacia diferentes redes de transporte, INET y MPLS respectivamente, en este sentido en la Figura 15b, se muestran los túneles lógicos que se crean en una topología de malla completa en una red SD-WAN, esto se debe a que la red de transporte es irrelevante mientras sea posible alcanzar los nodos vEdge, es decir los túneles se formaran extremo a extremo sin importar la infraestructura o tecnología que deban usar para realizar una conexión. Evidentemente no es saludable manejar tantos túneles debido a que no es posible tener control en el acceso entre sitios, lo cual deriva en problemas de seguridad ya que todos los nodos pueden accederse entre sí e incluso a través de diferentes redes de transporte.

Las repercusiones no solamente se reflejan en el excesivo número de túneles, ya que el establecer un túnel implica que; el vSmart está estableciendo comunicación con un nodo vEdge mediante su propio enlace físico de transporte, y una vez establecido el túnel se inicia una sesión BFD para definir el estado de la conexión, lo cual influye

directamente en el número de procesos que debe atender el vSmart, con lo cual su procesamiento y tráfico sobre la red superpuesta aumenta. En este sentido para evitar los problemas de malla completa se definen reglas dentro del plano de control para que los TLOC anunciados por cada vEdge sean filtrados por el vSmart y de esta manera definir que dispositivos pueden o no comunicarse entre sí. En este sentido, (NetworkAcademy, 2022) menciona que:

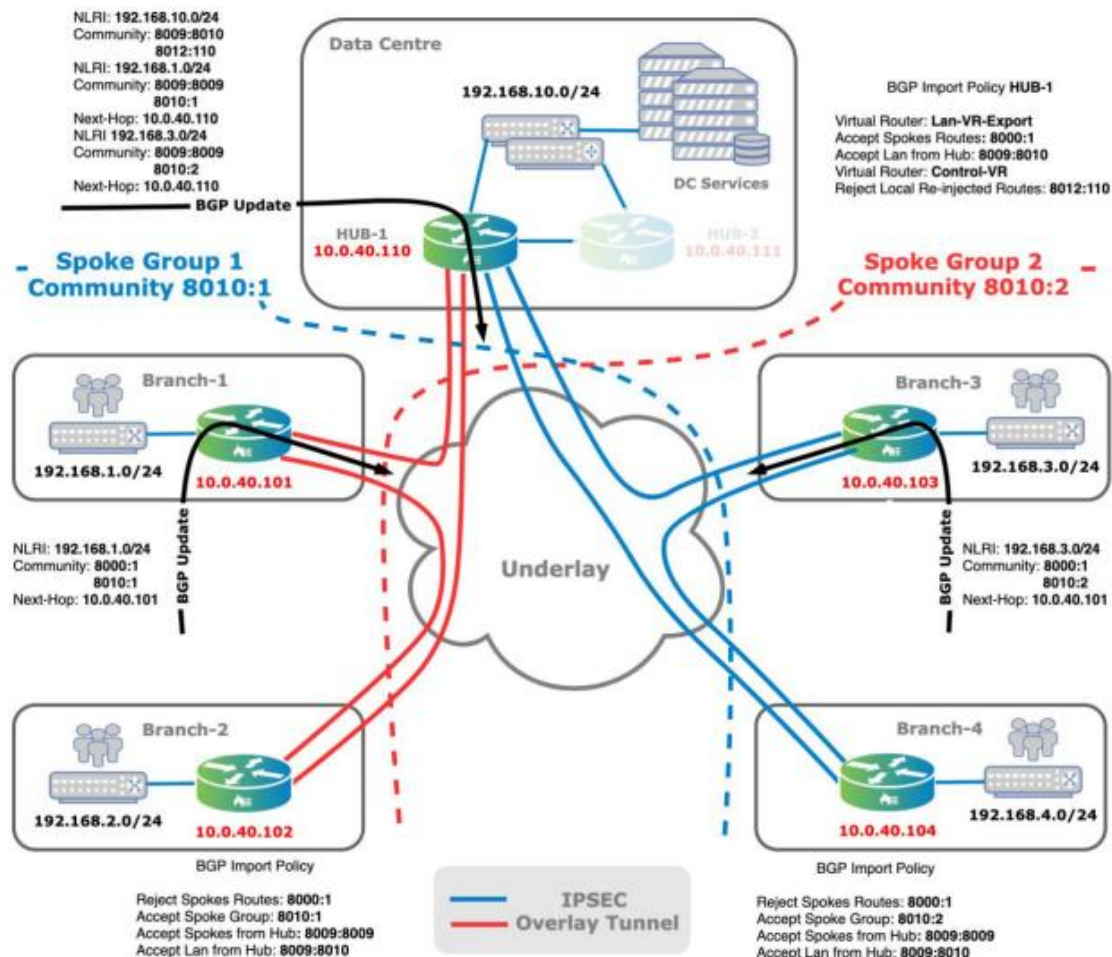
Esta podría ser la topología deseada, pero en la mayoría de las redes medianas y empresariales, hay poca necesidad de tener una comunicación directa de sucursal a sucursal. También hay una limitación de escalamiento porque los dispositivos de borde WAN en los sitios remotos normalmente no tienen el tamaño para manejar cientos de miles de túneles IPsec y sesiones de BFD. Un mejor enfoque de diseño más práctico es el uso de una topología Hub-and-Spoke.

3.2 Malla parcial

Una topología de malla parcial define que ciertos vEdge se puedan conectar directamente entre sí, mientras otros solamente se conectan a uno o dos vEdge de los permitidos, esta topología es útil cuando existen sitios dispersos sobre la misma región, y se desea conectar dichos nodos directamente, de esta manera esta topología es beneficiosa cuando hay un alto nivel de intercambio de tráfico entre sitios específicos, con lo cual, sería menos eficiente concentrar dicha información como en Hub and Spoke ya que en esta topología el tráfico se concentra en el Hub y este se encarga de enrutar los paquetes hacia los demás nodos.

Figura 16

Topología de Malla Parcial



Nota. Imagen tomada de (VersaNetworks, 2020)

En este sentido, la Figura 16 muestra cómo se realizarían las conexiones lógicas en una topología de malla parcial o Spoke to Spoke, de esta manera se observa que se definen grupos de nodos denominados Spokes, representados por las líneas azules y rojas respectivamente, grupos en los cuales se tiene una conexión de malla completa, en base a esto se define que; dentro de los grupos definidos se tendrá comunicación bidireccional entre todos los nodos pertenecientes a un grupo, y dispositivos que se encuentren fuera de este no se podrán conectar con dispositivos que forman parte de otro grupo de Spokes.

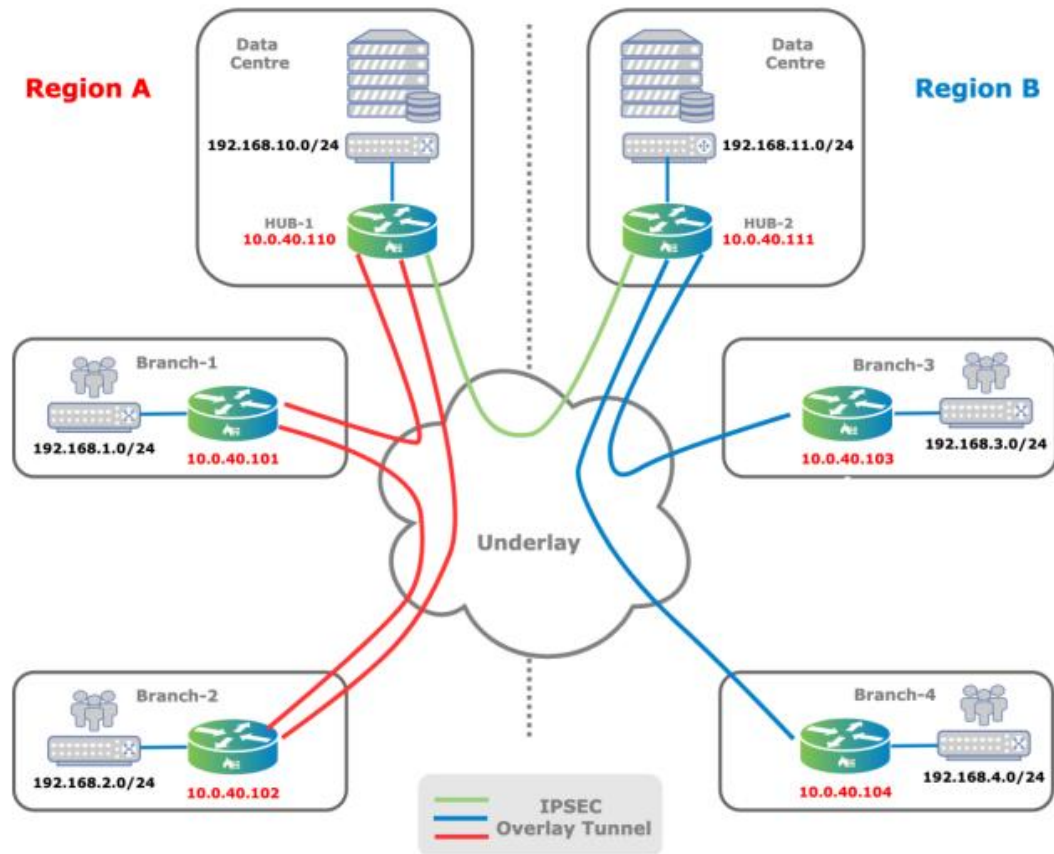
Al realizar la topología mostrada en la Figura 16, la capacidad de comunicación entre los grupos de Spokes será mayor debido a que no necesitan de un intermediario en dicha conexión, debido a esto existen menos procesos dentro del plano de orquestación y de la misma forma en los vEdge, ya que no deben manejar gran cantidad de TLOC's o sesiones BFD, ya que se reduce a su grupo.

3.3 Spoke-Hub-Hub-Spoke

En este tipo de topología (SHHS), también llamada topología de malla regional, se agrupan los dispositivos denominados HUB's y los grupos de Spokes para lograr comunicación extremo a extremo, de esta manera dentro de una región en particular, la topología puede ser cualquiera de las ya mencionadas y los vEdge internos se comunican mediante sus HUB's respectivos.

Figura 17

Topología Spoke-Hub-Hub-Spoke



Nota. Imagen tomada de (VersaNetworks, 2020)

En la Figura 17 se muestra cómo se realizan las conexiones lógicas en una topología SHHS, de esta manera se observa que se definen regiones dentro de las cuales existe cualquier tipo de topología para la comunicación entre sus nodos internos, con lo cual en la región A se observa una topología full-mesh y en la región B una topología Hub and Spoke, y la conexión entre regiones se realiza con SHHS. Cabe mencionar que, en la figura, se plasma los túneles ya operativos, es decir ya se han establecido en los diferentes vEdge y las redes físicas de transporte no influyen en la red superpuesta.

La comunicación en la Figura 17 dentro de la misma región será dirigida por la topología local, de este modo en la región A se tendrá comunicación entre todos los nodos

ya que es una topología Spoke to Spoke, y en la región B al ser Hub and Spoke se tendrá una comunicación dirigida por el Hub, ya que no existe comunicación directa entre todos los nodos. Finalmente, para la comunicación extremo a extremo entre las regiones se realizará mediante los Hub's locales de cada región.

3.4 Topología SD-WAN para regiones geográficamente aisladas

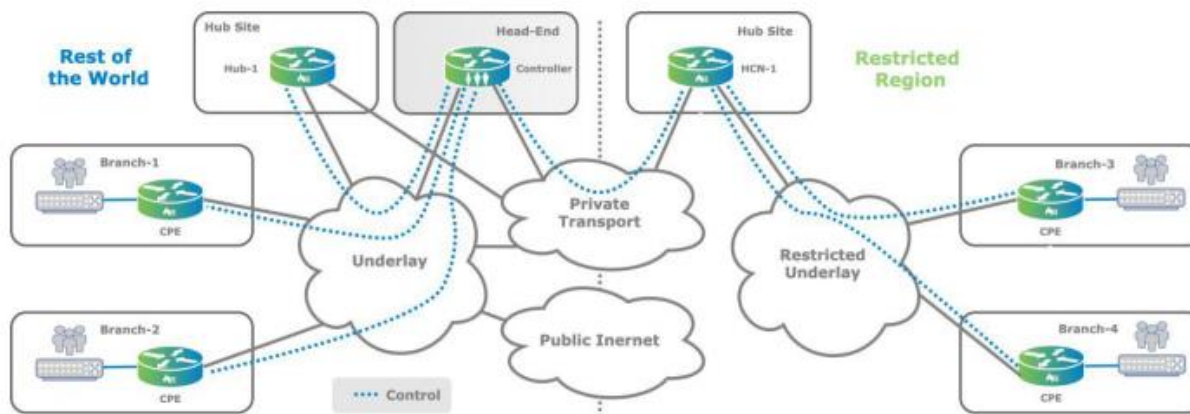
En algunas regiones del mundo el gobierno establece restricciones para el tráfico en túneles IPsec, con lo cual dentro de las redes de la misma región no existen problemas de tráfico, sin embargo, al tener que conectarse con otras regiones geográficas existe un problema, ya que el tráfico puede aislarse y de esta manera no se podrán conectar los dispositivos externos a dicha región con lo cual no se podrá establecer las políticas dentro de los nodos.

En este sentido la solución propuesta por CISCO es crear islas SD-WAN independientes en las que cada dominio tiene el control sobre sí mismo y no contiene ni envía información a otras regiones, para interconectar estos dominios independientes se utiliza IPsec o cualquier otra forma de conexión que debe ser administrada fuera del dominio SD-WAN, en este contexto resulta complicado realizar la conexión entre los nodos de frontera de la SD-WAN.

De acuerdo a las topologías analizadas, el uso de las SHHS resulta interesante debido a su escalabilidad y su forma de conexión en la que se aíslan regiones en las cuales se puede definir la topología de manera independiente tal como se muestra en la Figura 18.

Figura 18

Topología para regiones aisladas



Nota. Imagen tomada de (VersaNetworks, 2020)

En este sentido en la Figura 18, se muestra cómo se realizan las conexiones lógicas en una topología con regiones aisladas, de esta manera se observa que existen regiones en las cuales no existen restricciones, con lo cual, los nodos pueden establecer los túneles IPsec sin ninguna restricción, por lo contrario, en la zona restringida (Restricted Region) se observa que no es posible establecer túneles directamente desde el nodo deseado (Rest of the World), con lo cual se establece un nodo denominado Hub, el cual se encarga de brindar conectividad en las zonas restringidas sin necesidad de que estas zonas sean alcanzables desde los demás nodos.

El funcionamiento de este tipo de topologías no es complicado, ya que, al establecer un solo HUB (ver Fig. 18 Hub-1), el cual se encuentra entre la zona restringida y el resto del mundo, todo el tráfico generado deberá necesariamente ser enrutado mediante este, con lo cual será posible monitorear el estado de los túneles hacia la zona restringida sin necesidad de acceder a esta.

Nótese además que en la Figura 18, no se da importancia a la red física de transporte, ya que mientras los túneles se hayan establecido, existirá comunicación entre los diferentes vEdge, por consiguiente, los túneles se forman ya sea sobre la red privada, pública o restringida, la única diferencia con las demás topologías es los puntos finales de los túneles IPsec, ya que no podrán establecerse con libertad entre las zonas.

3.5 SD-WAN Híbrida

El funcionamiento de una SD-WAN híbrida es simple puesto que, este tipo de red ofrece conectividad extremo a extremo utilizando MPLS tradicional y también mediante otro tipo de redes como las redes públicas (Internet). De esta manera el tráfico puede enviarse de forma selectiva a través de cada una de las redes de transporte, con lo cual la capacidad de gestión del tráfico aumenta.

Con este tipo de red se mejora la eficiencia tanto de SD-WAN como MPLS, ya que el tráfico local no debe cursar por internet innecesariamente, con lo cual al tener una red MPLS resulta mucho más rápida la conexión al centro de datos de una empresa, y para procesos propios de acceso a recursos en la nube lo hace directamente y no debe pasar por el centro de datos, lo cual conlleva a que la red no se sature con tráfico ya sea interno o externo.

Esto permite que cada enlace (ya sea MPLS o ‘directo a Internet’) sea monitoreado de cerca en tiempo real para su uso actual, además de mostrar métricas como latencia, pérdida de paquetes y errores. Si una conexión falla o experimenta latencia o pérdida de paquetes excesivo, las conexiones restantes pueden hacerse cargo del tráfico.

3.6 Elección de la topología de red a simular

Para el diseño de red en el presente trabajo de grado, se tomará en cuenta factores de escalabilidad así como disponibilidad de la red. En este sentido, la topología de malla

completa (Full Mesh) se descarta debido al esquema de funcionamiento de esta, puesto que se necesitaría demasiados recursos físicos, debido al procesamiento de los equipos a simular, ya que, estos deben ser capaces de mantener muchas sesiones BFD y de la misma manera manejar gran cantidad de TLOC's tanto en el plano de orquestación como el plano de datos; además de los problemas de escalabilidad, ya que, al aumentar nodos el número de sesiones BFD aumenta excesivamente de acuerdo con la Ec.2 . Finalmente, esta topología no resulta beneficiosa debido a que podrían surgir problemas de seguridad debido a una conexión total entre nodos de la red.

Por otro lado, la topología HUB and SPOKE resulta interesante ya que permite definir un puente, el cual se encarga de dirigir las comunicaciones y de esta manera evitar establecer muchas sesiones BFD, así mismo como TLOC's manejados en el plano de orquestación. La desventaja de esta topología es que al definir un HUB, las comunicaciones deben necesariamente cursar por este dispositivo el cual se encarga de enrutar el tráfico, con lo cual los datos deben realizar saltos extras hasta ser entregados, lo cual se traduce como tráfico innecesario sobre la red superpuesta en caso de querer una comunicación directa entre nodos. Al igual que la topología FULL-MESH, HUB & SPOKE supone problemas de seguridad, ya que, toda la información cursará por un solo dispositivo (HUB). De la misma manera, esta topología supone problemas de disponibilidad de la red, puesto que, la comunicación entre nodos depende de un solo dispositivo y en caso de que este falle, la comunicación será interrumpida, con lo cual esta topología se descarta.

De la misma manera, la topología en malla parcial resulta interesante para el factor de escalabilidad debido a que en esta se define grupos de Spokes, los cuales se comunican entre sí, con lo cual se aísla la comunicación entre grupos garantizando la conectividad

entre los nodos internos y aislando el tráfico de otros, con lo cual, la seguridad de los datos aumenta, además de poder escalar la red aumentando más nodos los cuales no deben manejar excesivas cantidades de sesiones BFD o filtrar muchos localizadores de transporte, y no necesita un concentrador el cual se encargue de dirigir las comunicaciones. En base al funcionamiento de este tipo de topología, la red mejorará las prestaciones debido a que no se necesitaría un equipo robusto capaz de procesar y enrutar paquetes como lo sería un HUB. A pesar de las ventajas mencionadas, esta topología, queda descartada, debido a que no permite la comunicación entre diferentes regiones, con lo cual, supondría problemas de comunicación en caso de necesitar comunicar nodos de diferentes regiones.

De la misma manera, una de las soluciones más interesantes propuestas por SD-WAN para comunicar nodos aislados debido a políticas que no dependen de la administración de esta, es definir islas SD-WAN, en las cuales se define que para realizar una comunicación entre nodos que no son accesibles directamente, deben pasar por un puente, que no depende de la administración de la misma SD-WAN y de la misma manera anunciar rutas y acceder a la información de esta. En este sentido y para efectos del presente trabajo no sería beneficioso, ya que se debería tener un dispositivo como HUB independiente con requerimientos elevados de hardware para poder realizar la comunicación entre los dominios requeridos, con lo cual esta topología queda descartada.

Por lo contrario, una topología SHHS brinda una solución más compleja que las mencionadas hasta el momento, ya que en esta se definen regiones las cuales son independientes entre sí, a pesar de ello se comunican mediante la definición de un dispositivo como puente, lo cual aísla la comunicación entre regiones, sin embargo, esto no significa que no puedan acceder a la información entre sí, ya que mediante los HUB's

es posible alcanzar dichos destinos y al mismo tiempo bajar el número de sesiones BFD manejadas en cada nodo sin perder comunicación entre pares. Por otro lado, esta topología ayuda a mejorar la seguridad de la red, esto debido a que dentro de cada región se puede definir otro tipo de topologías para comunicar los nodos internos y de esta manera evitar un acceso total, incluso dentro de las mismas regiones.

Al igual que SHHS, una SD-WAN híbrida será de vital importancia, ya que, se encargará de aumentar las prestaciones de la red conjuntamente con MPLS para el manejo de información local de la red y de la misma manera evitar tráfico innecesario dentro de esta, y aún más importante garantizar la disponibilidad de los servicios.

En este sentido, en la Tabla 3, se presenta un resumen de las características de cada una de las topologías mencionadas para SD-WAN, en esta tabla se presentan criterios de disponibilidad de la red, uso de recursos físicos, seguridad entre nodos y el manejo de los TLOC's en cada uno de estos.

Tabla 3

Comparación Topologías SD-WAN

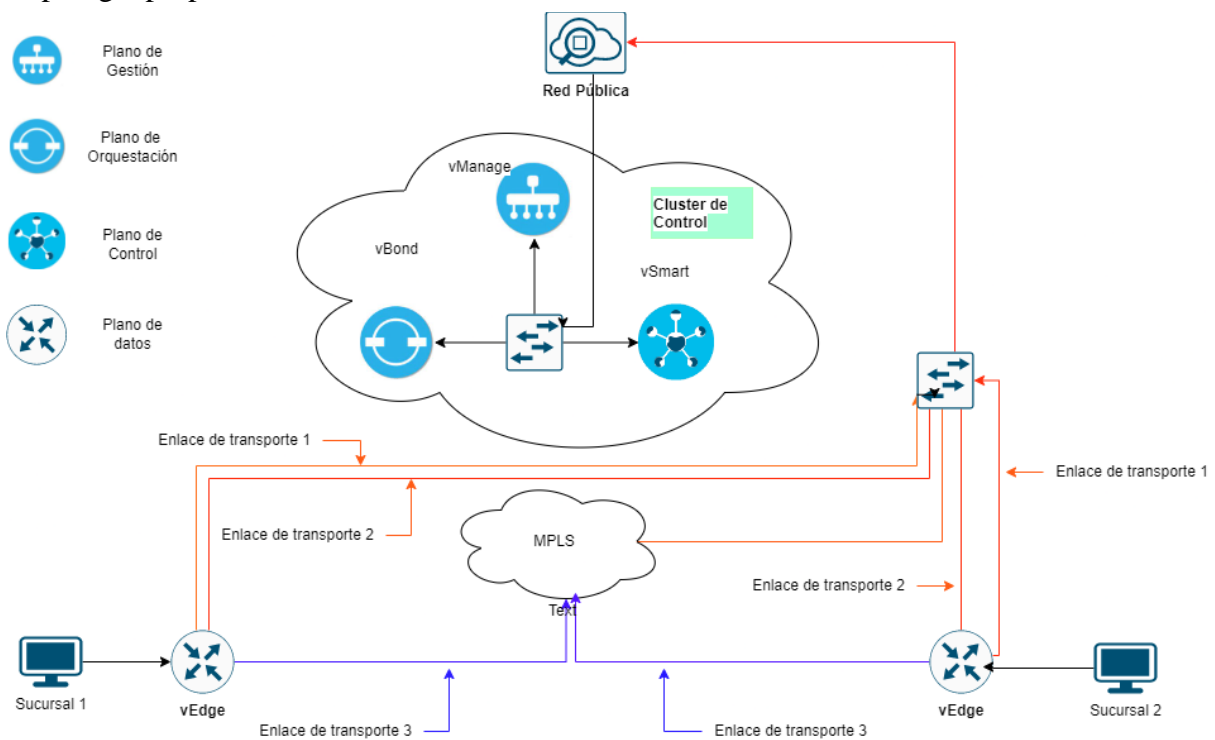
Topología	Número de sesiones BFD	Manejo de TLOC's	Seguridad en la red superpuesta	Disponibilidad de red	Consumo de recursos	
FULL-MESH	Depende de la Ec.1 y Ec.2	A mayor número de sesiones BFD.	TLOC's mayor número de sesiones BFD.	Acceso total de la red.	Elevado, ya que todos los nodos son accedidos independientemente de los demás nodos.	Elevado, debido a la gran cantidad de sesiones BFD.
HUB & SPOKE	Depende de la Ec.1 y Ec.2, donde $n = 2$.	Los TLOC's no son anunciados a toda la red.	Todo el tráfico se concentra sobre un solo dispositivo.	Medio, debido a que depende directamente del funcionamiento del HUB.	Bajo, puesto que, se inicia la sesiones solamente con el HUB.	
MALLA PARCIAL	Depende de la Ec.1 y Ec.2 pero se reduce a la región de Spokes ingresados.	Se anuncian solamente al grupo establecido.	Acceso total solo en grupos establecidos.	Elevado, ya que depende de cada región y su topología interna.	Medio, debido a que las sesiones que se establecen dependen directamente de los nodos que formen el grupo.	
Islas SD-WAN	Depende de la Ec.1 y Ec.2 donde $n = 2$, solo aplica a la zona restringida.	No se anuncian los TLOC's a la red, solamente al HUB dentro de la zona restringida.	Lo nodos no se acceden libremente, se acceden de acuerdo con la red de transporte.	Bajo, ya que no es accesible para nodos que no estén dentro de la zona restringida.	Bajo, puesto que, se inicia la sesiones solamente con el HUB.	

Spoke-Hub-Hub-Spoke	Depende de la Ec.1 y Ec.2, pero se reduce a la región de Spokes.	Se anuncian los TLOC's, de acuerdo con la región a la que pertenezcan.	El acceso se limita a la región establecida y nodos externos, lo realizan por los HUB's, con lo cual se tiene mayor control.	Medio, puesto que se reduce a cada región, y en caso de fallar el puente aún pueden accederse miembros de las mismas regiones.	Medio, debido a que las sesiones BFD que se establecen, depende directamente de los nodos que formen el grupo, y de la topología interna de la región.
----------------------------	--	--	--	--	--

En este sentido, y en base a la información proporcionada en la Tabla 3, para el desarrollo del presente trabajo se realizará la simulación de una red SD-WAN híbrida basada en parámetros de una topología SHHS, debido a las características y funcionalidades que la misma brindará para el filtrado de localizadores de transporte, además de reducir el número de sesiones BFD, lo cual conlleva a un menor procesamiento en los diferentes equipos. Estas características harán que la simulación no requiera demasiados recursos, además de demostrar los beneficios de una SD-WAN híbrida, con lo cual en la Figura 19 se muestra un esquema preliminar de cómo se plantea la red híbrida, evidenciando tanto el plano de control, orquestación y datos.

Figura 19

Topología propuesta



En la Figura 19 se muestra tanto la composición del plano de control, orquestación y datos de la red híbrida, de esta manera se identifica que el plano de control se lo manejará totalmente centralizado en un solo clúster, este diseño se lo realizó de acuerdo

con (Cisco,2018), ya que menciona que este tipo de configuración proporciona una máxima comodidad y menor trabajo de despliegue además de mejorar la seguridad dentro del plano de control, puesto que, en un ambiente físico, estos podrían ser gestionados desde un mismo lugar, además la comunicación entre estos será directa ya que pertenecen al mismo segmento de red, con lo cual las políticas creadas en el plano de gestión llegan directamente al plano de control.

De la misma manera en la Figura 19, se muestra que los enrutadores de borde vEdge se encuentran desplegados en dos sucursales, las cuales cuentan con tres enlaces de transporte (Enlace de transporte 1, Enlace de transporte 2, Enlace de transporte 3) para alcanzar los diferentes puntos de la red, de este modo un enlace de transporte para la red MPLS que comunica las dos sucursales directamente y dos enlaces de transporte por la red pública, con lo cual se tiene redundancia de enlaces y a su vez es posible realizar balanceos de carga de acuerdo con la necesidad de las sucursales. En este sentido si se quiere realizar una comunicación directa entre sucursales, se usará el transporte por MPLS, de lo contrario, si se requiere acceder a servicios en la nube se saldrá por la red pública, y finalmente para tener el control de los nodos se tiene una conexión directa hacia la controladora.

De acuerdo con (cisco,2020) este tipo de topologías con enlaces redundantes benefician al rendimiento de la red, en base a que; se dispone una alta disponibilidad en aplicaciones críticas para los diferentes nodos conectados, de la misma manera es posible enrutar el tráfico de forma dinámica, es decir es posible realizar un reconocimiento de aplicaciones para así elegir el enlace por el cual debe dirigirse un determinado tipo de

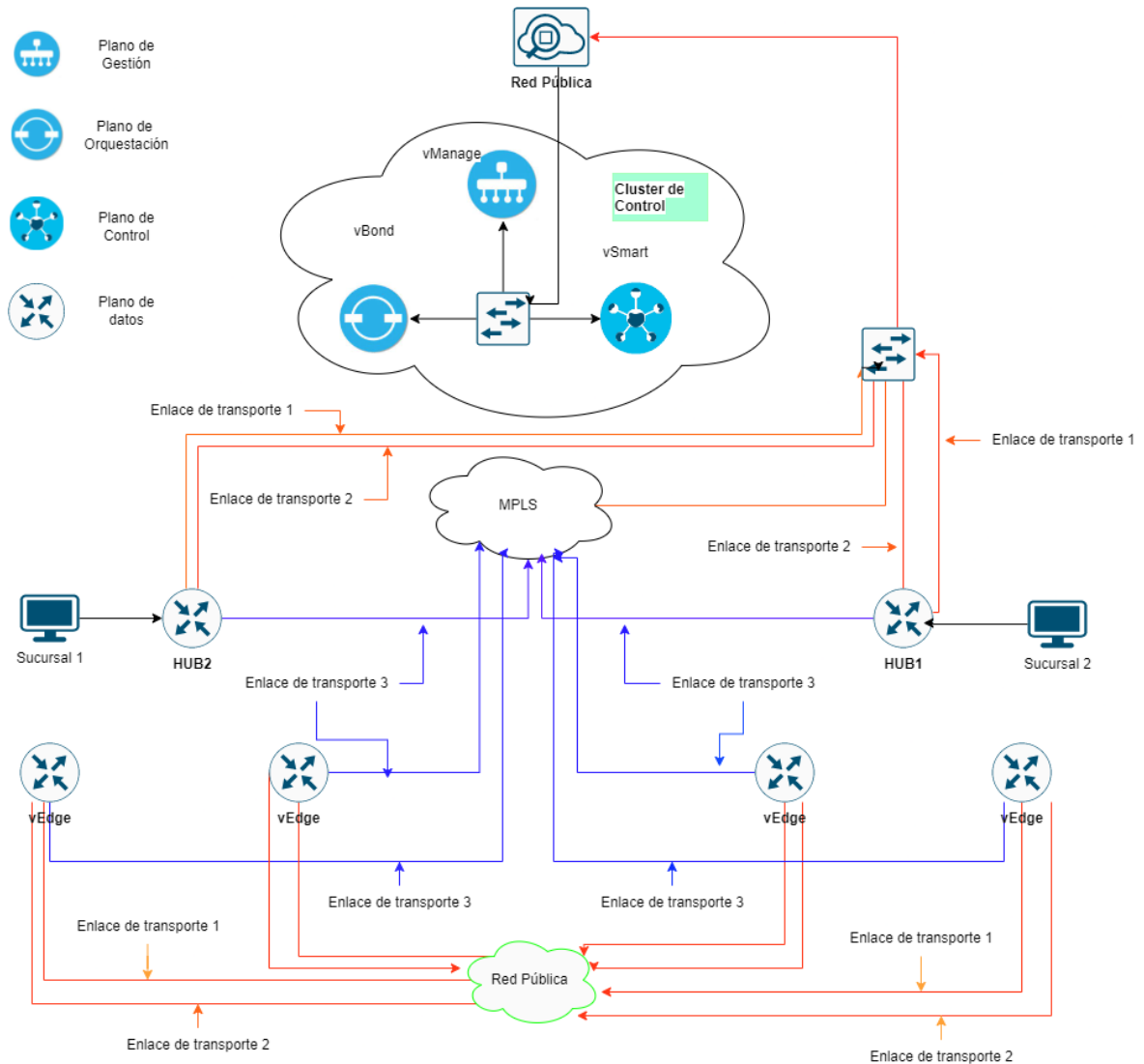
tráfico, lo cual se traduce en una mayor QoE (Quality Of Experience) ya que los paquetes se entregan de una manera más eficiente.

Para evidenciar como trabaja la topología SHHS, es necesario realizar varias modificaciones a la topología mostrada en la Figura 19, ya que el equipo vEdge que se observa en cada sucursal representaría el Hub de cada región, con lo cual a partir de este pueden desprenderse más nodos y las comunicaciones serán dirigidas por este, con lo cual a la topología presentada se aumentarán 2 nodos a cada sucursal.

Por lo tanto, la Figura 20 presenta las modificaciones realizadas a la topología, de esta manera se evidencia la inclusión de 4 nodos los cuales tienen 3 conexiones físicas de transporte, que se distribuyen 2 para la red pública y 1 para la red MPLS respectivamente. En este sentido, y usando la Ec.2 para el cálculo de túneles con redundancia en los enlaces de transporte, existirían 45 túneles entre los nodos en caso de ser una topología de malla completa, lo cual no sucederá debido a las configuraciones lógicas para el filtro de sesiones BFD y TLOC's para definir la topología propuesta.

Figura 20

Topología rediseñada



Además, en la Figura 20, se evidencia que dentro de cada nodo se tienen redes locales, es decir que dentro de estos pueden existir clientes o servicios con los cuales se realizarán las pruebas de rendimiento de la red. De la misma manera se observa los diferentes equipos que se desplegarán para el funcionamiento de la red, siendo estos de la marca CISCO, específicamente de la solución de VIPTELA, se considera esta solución en base a que, al proponer una red híbrida, VIPTELA es la solución que mejor diferencia

los enlaces de transporte, y lo realiza de manera automática y segura, además posibilita observar lo que sucede en la red en tiempo real.

Tabla 4

Comparación diferentes soluciones SD-WAN

Característica	Viptela SD-WAN	Meraki SD-WAN	FortiGate SD-WAN
Despliegue	Opciones en sitio y basadas en la nube.	Basado solo en la nube.	Opciones en sitio y basadas en la nube.
Escalabilidad	Alta para grandes empresas, y servicios de proveedores.	Escalabilidad limitada, usada para empresas medianas,	Escalable para empresas medianas y pequeñas
Seguridad	Ofrece funciones de seguridad elevadas (IPsec), para incluir redes de confianza y permite la segmentación.	Provee seguridad básica como un firewall y vpn.	Ofrece funciones de seguridad elevadas, incluyendo inspección SSL y control de aplicaciones.
Gestión	Centralizada, manejada desde el dashboard del vManage.	Centralizada, manejada desde el Meraki dashboard.	Centralizada, manejada desde el FortiManager dashboard.
Enrutamiento	Soporta protocolos de enrutamiento dinámico como OSPF y BGP.	Soporta protocolos de enrutamiento dinámico como OSPF y BGP.	Soporta protocolos de enrutamiento dinámico como OSPF y BGP.
Optimización de la WAN	Incluye optimización de la WAN como la optimización TCP y la compresión de datos.	No tiene optimización de la WAN.	Incluye optimización de la WAN como la optimización TCP y la compresión de datos.
WAN híbrida	Permite manejar SD-WAN y MPLS	-	-

En este sentido, en base a la información presentada en la Tabla 4, se selecciona VIPTELA SD-WAN debido a su capacidad superior de escalabilidad, ya que está diseñada específicamente para grandes empresas, además, las opciones de seguridad que presenta para el tráfico de datos son avanzadas, ya que, utiliza cifrado con IPsec. Además, es la única solución que permite una WAN híbrida, lo cual la convierte en una opción ideal para el desarrollo del presente trabajo de grado.

3.7 Elección del sistema operativo

Un sistema operativo es un programa que actúa como una interfaz entre el usuario y el hardware del computador, además se encarga del control de la ejecución de los programas que actúan sobre esta. Con lo cual, el sistema operativo es el encargado de tareas como gestionar archivos, manejar el uso de la memoria, procesos, además del manejo de dispositivos periféricos de entrada y salida.

En este sentido, existe gran variedad de sistemas operativos, con lo cual funcionan de diferentes maneras, lo que indirectamente afectará al rendimiento de ciertas aplicaciones, ya que los recursos son gestionados de acuerdo con este, de esta manera, los sistemas operativos más usados son: Linux, Windows y macOS.

Previo a la elección del sistema operativo, se debe tomar en cuenta que, el software de simulación para el presente trabajo de grado es GNS3, toda vez que es compatible con Windows, Mavericks y cualquier Linux, especialmente distribuciones basadas en Debian y Ubuntu, según (GNS3, s.f.) Para el desarrollo del presente trabajo de grado, el sistema operativo Windows, se descarta, debido al uso excesivo de recursos para el propio sistema operativo y además de la poca flexibilidad y personalización de este, ya que, en el desarrollo de las simulaciones, se realizarán puentes directos a las interfaces físicas para

poder salir a la red local directamente desde los nodos simulados, lo cual en Windows no será posible, ya que, no permite realizar este tipo de acciones directamente. Además, sería necesario desplegar una Máquina Virtual GNS3_VM para que sea posible emular tanto las controladoras como los nodos de acceso, lo cual a su vez consume más recursos para el desarrollo de las simulaciones necesarias.

Por lo tanto, (GNS3, 2023) recomienda las distribuciones de Ubuntu y Debian, por lo tanto, la elección del sistema operativo se reduce a estos dos. En primer lugar, cabe considerar que los dos, son sistemas operativos basados en Linux y están diseñados para optimizar recursos, sin embargo existe una gran diferencia entre estos, puesto que, Ubuntu se enfoca en brindar una mejor experiencia al usuario final, mientras que Debian está diseñado para ser utilizado en servidores que necesitan estar en funcionamiento constante, y por ende, está optimizado para consumir pocos recursos y bajar el impacto en el rendimiento del sistema. Además, para un rendimiento óptimo, GNS3 recomienda su GNS3_VM, la cual opera bajo una distribución basada en Debian. Por lo cual, el sistema operativo anfitrión para la implementación del presente trabajo de grado se escoge Debian.

Tabla 5

Resumen de requerimientos de Sistemas Operativos

Resumen de Requerimientos de Sistemas Operativos				
Sistema Operativo	RAM(Recomendado) [MBytes]	DISCO(Recomendado) [GBytes]	ARQUITECTURA	USO
DEBIAN	256	4	ARM, 64 y 32 bits	LIBRE
WINDOWS	2000	32	64 y 32 bits	PAGO
UBUNTU	384	5	ARM, 64 y 32 bits	LIBRE
FEDORA	4000	20	ARM, 64 y 32 bits	LIBRE
CENTOS	1000	20	ARM, 64 y 32 bits	LIBRE

Por otra parte, la Tabla 5, recoge de acuerdo con los sitios web oficiales respectivos los requerimientos para el uso de diferentes sistemas operativos, en este sentido, para el sistema operativo Debian, son bajos; adicionalmente hay que considerar que esta distribución, cuenta con varias ventajas en su implementación para servidores, entre las cuales destacan; es compatible con diferentes arquitecturas de hardware, de esta manera, podrá ser desplegado en una amplia gama de dispositivos, es estable y seguro, con lo cual no se presentarán errores dentro de su funcionamiento habitual además de actualizar su seguridad constantemente, finalmente tiene soporte a largo plazo, lo cual ayuda a que en caso de existir errores en su funcionamiento serán corregidos ya sea por la comunidad o por los propios desarrolladores de Debian; de esta manera, el sistema operativo elegido para el desarrollo del presente trabajo es Debian, en su versión 11.4 (versión actual al momento de realización del presente trabajo de grado).

3.8 Despliegue de vManage

Para el despliegue de la controladora vManage se debe tener en cuenta que, para el correcto funcionamiento de la red superpuesta⁶ se debe configurar al menos una interfaz de túnel VPN, la cual debe estar asociada a una red de transporte, de la misma manera, todos los dispositivos vEdge deben ser capaces de acceder a esta. Este túnel creado se encarga de transportar el tráfico del plano de control al plano de datos, para lo cual se ha definido el direccionamiento IPv4 que se muestra en la Tabla 6.

En resumen, la Figura 21, presenta el proceso de configuración de este dispositivo, en donde, se evidencia como realizar el ingreso del vManage al entorno de simulación y de

⁶ Red superpuesta: Es una idea, con la cual existe una red, que se superpone a las conexiones de red físicas, ya sean públicas o privadas, y de esta manera permitir un enrutamiento de tráfico basado en políticas.

esta manera lograr una comunicación hacia la red pública para posteriormente acceder al plano de control por el dashboard proporcionado por el mismo dispositivo.

Figura 21

Resumen de proceso de configuración de vManage

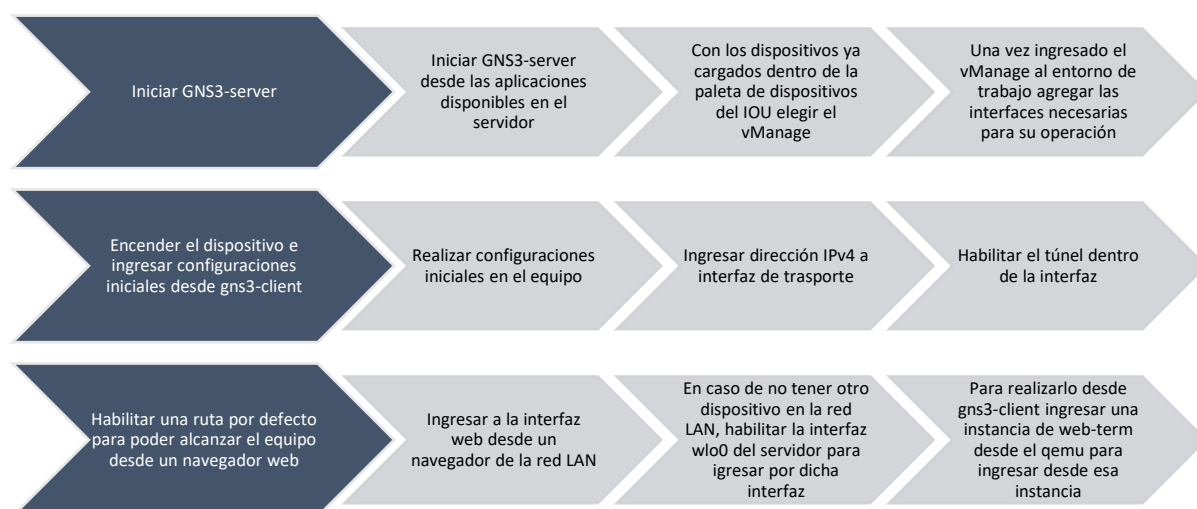


Tabla 6

Direccionamiento IPv4

Dispositivo	Interfaz	Dirección	Gateway	VPN
vBond	ge0/0	192.168.1.4/24	192.168.1.1	0
	Loopback	2.2.2.2/32	No aplica	
vManage	eth0	192.168.1.3/24	192.168.1.1	0
	Loopback	1.1.1.1/32	No aplica	
vSmart	eth0	192.168.1.5/24	192.168.1.1	0
	Loopback	3.3.3.3/32	No aplica	

SPOKE-1	ge0/0	192.168.1.54/2 4	192.168.1.1	0
	ge0/1	192.168.122.23 9/24	192.168.122. 1	0
	ge0/4	10.10.10.53/29	10.10.10.49	0
	ge0/2	10.10.10.50/29	10.10.10.49	1
	ge0/3	172.50.0.1/24	No aplica	1
	Loopback	6.6.6.6/32	No aplica	
SPOKE-2	ge0/0	192.168.100.18 0/24	192.168.100. 1	0
	ge0/2	192.168.1.55/2 4	192.168.1.1	0
	ge0/3	10.10.10.52/29	10.10.10.49	1
	ge0/1	10.10.10.51/29	10.10.10.49	1
	Loopback	7.7.7.7/32	No aplica	
SPOKE-3	ge0/0	192.168.1.52/2 4	192.168.1.1	0
	ge0/1	192.168.104.15 7/24	192.168.104. 1	0
	ge0/4	10.10.10.69/29	10.10.10.65	1
	ge0/2	10.10.10.66/29	10.10.10.65	1
	Loopback	9.9.9.9/32	No aplica	
SPOKE-4	ge0/1	192.168.101.17 7/24	192.168.101. 1	0
	ge0/2	192.168.1.57/2 4	192.168.1.1	0
	ge0/4	10.10.10.70/29	10.10.10.65	1
	ge0/0	10.10.10.67/29	10.10.10.65	1
	ge0/3	172.50.1.1/24	No aplica	1
	Loopback	10.10.10.10/32	No aplica	

HUB-1	ge0/0	192.168.103.21	192.168.103.	0
		7/24	217	
	ge0/2	10.10.10.68/29	10.10.10.65	1
	ge0/3	192.168.1.56/2	192.168.1.1	0
		4		
	ge0/1	10.10.10.34/30	10.10.10.33	1
	Loopback	4.4.4.4/32	No aplica	
HUB-2	ge0/0	192.168.1.53/2	192.168.1.1	0
		4		
	ge0/2	10.10.10.54/29	10.10.10.49	1
	ge0/3	192.168.102.2/	192.168.102.	0
		24	1	
	ge0/1	10.10.10.38/30	10.10.10.37	1
	Loopback	5.5.5.5/32	No aplica	
R1	f0/0	10.10.10.1/30	No aplica	
	f0/1	10.10.10.37/30	No aplica	
	f2/0	10.10.10.21/30	No aplica	
	Loopback	20.20.20.1/32	No aplica	
	0			
R2	f0/0	10.10.10.2/30	No aplica	
	f0/1	10.10.10.5/30	No aplica	
	f1/0	10.10.10.25/30	No aplica	
	Loopback	20.20.20.2/32	No aplica	
	0			
R3	f0/0	10.10.10.49/29	No aplica	
	f0/1	10.10.10.26/30	No aplica	
	f1/0	10.10.10.17/30	No aplica	
	f2/0	10.10.10.22/30	No aplica	
	Loopback	20.20.20.3/32	No aplica	
	0			
R4	f0/0	10.10.10.9/30	No aplica	

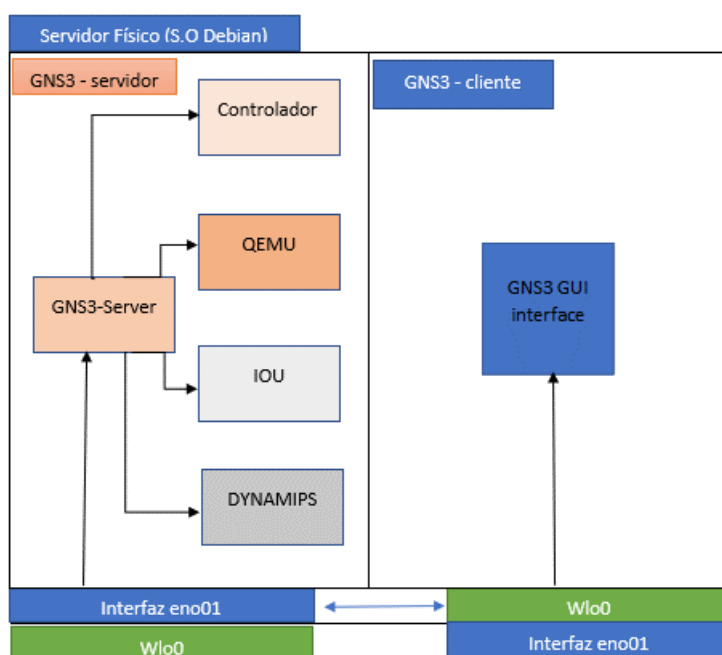
	f0/1	10.10.10.6/30	No aplica	
	f1/0	192.168.122.2/24	192.168.122.1	
	f2/0	10.10.10.29/30	No aplica	
	Loopback 0	20.20.20.4/32	No aplica	
R5	f0/0	10.10.10.65/29	No aplica	
	f0/1	10.10.10.13/30	No aplica	
	f1/0	10.10.10.18/30	No aplica	
	f2/0	10.10.10.30/30	No aplica	
	Loopback 0	20.20.20.5/32	No aplica	
R6	f0/0	10.10.10.10/30	No aplica	
	f0/1	10.10.10.14/30	No aplica	
	f1/0	10.10.10.33/30	No aplica	
	Loopback 0	20.20.20.6/32	No aplica	
R7	f0/0	192.168.122.1/24	192.168.122.2	
	f0/1	192.168.1.7/24	192.168.1.1	
	Loopback 0	20.20.20.7/24	No aplica	
WEB- TERM	e0	172.20.1.2/24	172.50.1.1	
VPC	e0	172.20.0.2/24	172.50.0.1	

Previo al arranque del vManage, es importante asegurarse que el gns3-server esté configurado como se muestra en la Figura 22, en donde, la interfaz **w1o0** se utiliza para acceder al servidor desde el gns3-cliente, mientras que, el vManage (que se ejecuta dentro de QEMU) estará conectado a la interfaz **eno01**,

Cabe señalar que, es esencial no asociar el GNS3-client (cuya función es dar acceso a la simulación) y el vManage a la misma interfaz de red física del servidor anfitrión, ya que esto puede provocar bucles de comunicación.

Figura 22

Esquema de funcionamiento del proyecto



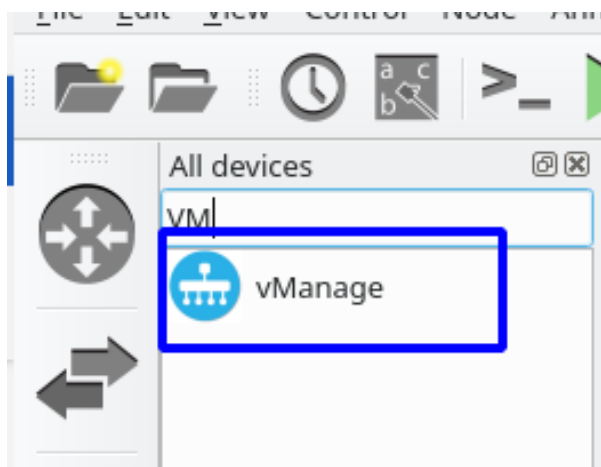
Después de verificar el esquema de funcionamiento de las interfaces de red del servidor, es necesario subir la imagen del equipo en el servidor de GNS3 para configurarlo en el cliente. Esto permite un mejor control de los recursos que se consumen durante la simulación y de la misma manera facilita el acceso a estos recursos desde cualquier host perteneciente a la red sin necesidad de consumir sus recursos locales.

Es importante tener en cuenta que cada equipo que utilice los recursos del servidor debe configurar su GNS3-cliente para realizar la conexión con el servidor remoto. En este

caso como el servidor y el cliente están en la misma máquina, no es necesario realizar el proceso de conexión.

Figura 23

Integración de equipos a GNS3



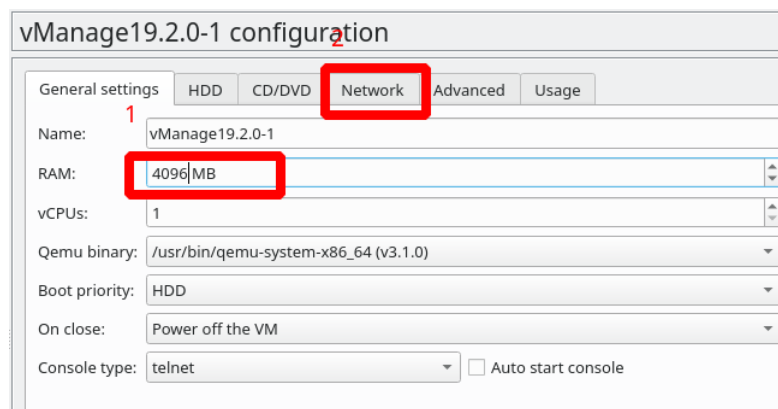
Una vez que se ha cargado el equipo dentro del servidor de GNS3, como se muestra en la Figura 23, es posible acceder al dispositivo vManage desde el cliente de GNS3. Esto indica que el dispositivo se ha cargado correctamente en el servidor.

De acuerdo con (cisco, s. f.), se recomienda una memoria RAM mínima de 32GB para desplegar la controladora en un entorno físico, aunque para despliegues en la nube este valor puede variar según los criterios de diseño propios. Según (Giovanni Augusto, 2019), en entornos de laboratorio se pueden asignar valores menores a los recomendados, siempre y cuando no se manejen grandes cantidades de tráfico ni se deba manejar una gran cantidad de nodos.

Dado que, para otros usuarios del software GNS3 una memoria RAM de 4GB ha funcionado correctamente para este dispositivo, se asignará este valor al dispositivo vManage para el desarrollo del presente trabajo de grado.

Figura 24

Configuraciones físicas vManage



Para asignar el valor de memoria RAM mencionado, se ingresa a las configuraciones del dispositivo realizando doble clic sobre el equipo, en donde se despliega un dashboard como se muestra en la Figura 24, y se ingresa el valor de 4GB transformado a MB en el campo (**RAM:**), los demás campos se definen por defecto.

A continuación, si las configuraciones físicas del equipo se han realizado de manera adecuada, se debe iniciar el mismo para la configuración lógica, de esta manera se debe esperar a que el sistema se marque como **system ready**, momento en el cual se realiza el ingreso de las credenciales por defecto, caso contrario a pesar de ingresar las credenciales adecuadas no se podrá realizar la autenticación.

Figura 25

Ingreso inicial vManage

```
Tue Apr  4 19:51:24 UTC 2023: System Ready

viptela 19.2.0
vmanage login: admin
Password:
Welcome to Viptela CLI
admin connected from 127.0.0.1 using console on vmanage
You must set an initial admin password.
Password:
Re-enter password: █
```

Después de la instalación inicial del sistema, es necesario crear una contraseña de administrador como se muestra en la Figura 25 para acceder a las funciones del sistema. Una vez completado este proceso, se mostrarán los dispositivos disponibles para el almacenamiento de datos del dispositivo. Es importante elegir el dispositivo con mayor capacidad de almacenamiento, ya que este dispositivo es el encargado de recopilar datos de cada uno de los nodos. Una vez que se ha elegido el dispositivo de almacenamiento, no se puede cambiar mientras el dispositivo está en funcionamiento. Es esencial elegir el tamaño de disco adecuado desde el principio, ya que si se elige uno inadecuado, esto puede provocar errores en el rendimiento del sistema, como la falla del servidor web del vManage y la desconexión del plano de control.

Figura 26

Proceso de carga de vManage

```
Available storage devices:
hdb 18GB ← 1
hdc 3GB
1) hdb
2) hdc
Select storage device to use: 1 ← 2
Would you like to format hdb? (y/n): y ← 3
mkfs2fs 1.43.8 (1-Jan-2018)
Creating filesystem with 4868500 4k blocks and 1218224 inodes
Filesystem UUID: 2905d1e1-a627-44dd-9e02-5b140452b7e9
Superblock backups stored on blocks:
32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
4096000

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
```

La Figura 26, muestra los tres pasos que se deben seguir obligatoriamente para levantar el sistema de manera adecuada. En el primer paso, se muestran los dispositivos de almacenamiento disponibles; en el segundo, se selecciona uno de ellos y, y finalmente, en el tercer paso se confirma la selección.

Es importante tener en cuenta que, si no se siguen estos pasos, el dispositivo no podrá iniciar el sistema para su configuración, ya que no cuenta con una unidad de almacenamiento en donde guardar la información. Asimismo, el servidor web no se iniciará debido a que, no hay espacio disponible para el almacenamiento de datos que serán mostrados posteriormente.

Figura 27

Nuevo ingreso a vManage

```
viptela 19.2.0
vmanage login: admin
Password:
Welcome to Viptela CLI
admin connected from 127.0.0.1 using console on vmanage
vmanage#
vmanage#
vmanage#
```

Después de completar la configuración del almacenamiento, se puede iniciar el sistema de la controladora, como se muestra en la Figura 27. En el recuadro rojo se indica que se deben utilizar las nuevas credenciales creadas para el usuario administrador (admin:admin) al realizar el primer inicio de sesión. Es importante tener en cuenta que, al realizar el primer inicio de sesión posterior a la configuración de almacenamiento, las credenciales por defecto ya no serán válidas y se deben utilizar las credenciales personalizadas creadas previamente en la consola. Además, es importante mencionar que las mismas credenciales mencionadas anteriormente también se deben utilizar para ingresar al portal web del vManage (<https://192.168.1.3>).

Asimismo, en el recuadro de color azul se indica que no se está ingresando por una IP asignada, ya que se realiza directamente al localhost, es decir, como si se estuviera conectado por consola.

Figura 28

Configuraciones iniciales vManage

```

vmanage# config ← 1
Entering configuration mode terminal
vmanage(config)# system ← 2
vmanage(config-system)# host-name vManage_CuaicalA ← 3
vmanage(config-system)# system-ip 1.1.1.1 ← 4
vmanage(config-system)# site-id 1 ← 5
vmanage(config-system)# organization-name cuaicalA_SD-WAN ← 6
vmanage(config-system)# clock timezone ← 7
Possible completions: (first 100):
Africa/Abidjan          Africa/Accra
Africa/Addis_Ababa     Africa/Algiers

```

En la Figura 28 se muestran las configuraciones iniciales del sistema, y es importante destacar que el parámetro "organization-name" es crucial para la integración del dispositivo a la red superpuesta. Si los nombres no coinciden, el equipo no podrá ingresar ni establecer comunicación con los demás nodos. Para realizar estas configuraciones, se debe seguir los siguientes pasos:

1. Acceder al modo de configuración del equipo.
2. Configurar un nombre
3. Configurar un ID
4. Configurar el nombre de organización
5. Configurar una "loopback" para identificar el nodo.
6. Establecer un número de sitio.
7. Indicar el nombre de la organización a la que pertenece el equipo.
8. Configurar la región en la que se desplegó el dispositivo para que los logs se registren con la hora adecuada.

Cabe destacar que estos pasos se pueden encontrar en la Figura 28. Por lo tanto, es importante revisar y verificar cuidadosamente que todas las configuraciones sean correctas antes de guardar los cambios. Si se configura incorrectamente algún parámetro, esto puede provocar problemas de conexión con los demás nodos de la red.

Después de las configuraciones del sistema, es necesario asignar una dirección IPv4 a una de las interfaces del equipo para poder ingresar al portal web a través de dicha dirección IP.

Figura 29

Configuración de interfaz ETH0 vManage

```
vmanage# conf t
Entering configuration mode terminal
vmanage(config)# vpn 0
vmanage(config-vpn-0)# interface eth0
vmanage(config-interface-eth0)# ip address 192.168.1.3/24
vmanage(config-interface-eth0)# no shutdown
vmanage(config-interface-eth0)# exit
vmanage(config-vpn-0)# commit
Commit complete.
```

Para ingresar una dirección IPv4 a la interfaz deseada, se debe seguir los siguientes pasos, los cuales se muestran en la Figura 29:

1. Acceder a las configuraciones globales del equipo.
2. Acceder a la vpn0, la cual permite conexiones con dispositivos externos sin utilizar un túnel cifrado.
3. Acceder a la interfaz específica que realizará la conexión con los demás dispositivos, en este caso, la eth0.

4. Asignarle una dirección IPv4 (192.168.1.3/24) ya sea estática u obtenida por DHCP.

5. Activar la interfaz administrativamente.

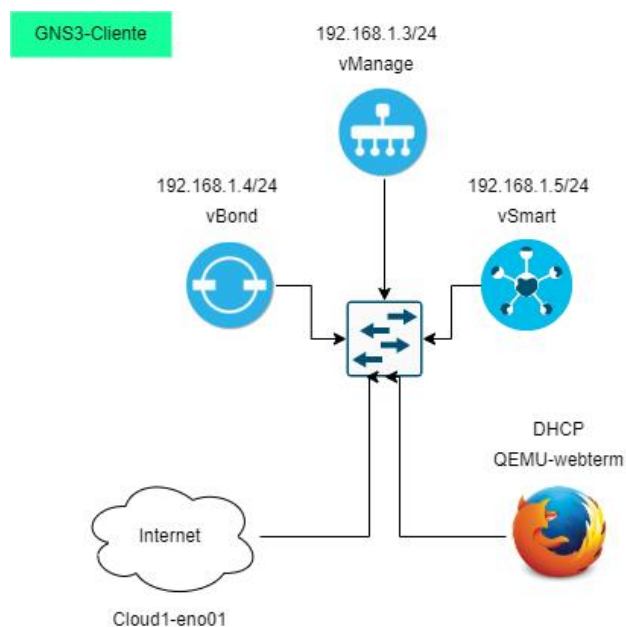
6. Confirmar las configuraciones utilizando el comando commit.

Es importante tener en cuenta que la dirección IPv4 asignada debe ser compatible con la red a la que se está conectando y que todas las configuraciones deben ser verificadas y confirmadas para que sean efectivas. Además, si se va a utilizar una dirección IP estática, se debe asegurar que no se esté utilizando esa misma dirección en otra parte de la red para evitar conflictos de dirección IP.

Una vez asignada la dirección IPv4 a la interfaz, se debe tomar en cuenta que, se debe ingresar una ruta por defecto para dicho enlace con el comando `ip route 0.0.0.0/0 192.168.1.1` y de esta manera el dispositivo sea capaz de salir tanto a la red pública como a los demás dispositivos de la red, en caso de elegir la configuración de la interfaz de red por DHCP no existe la necesidad de realizar este proceso.

Figura 30

Esquema de comunicación configuraciones iniciales

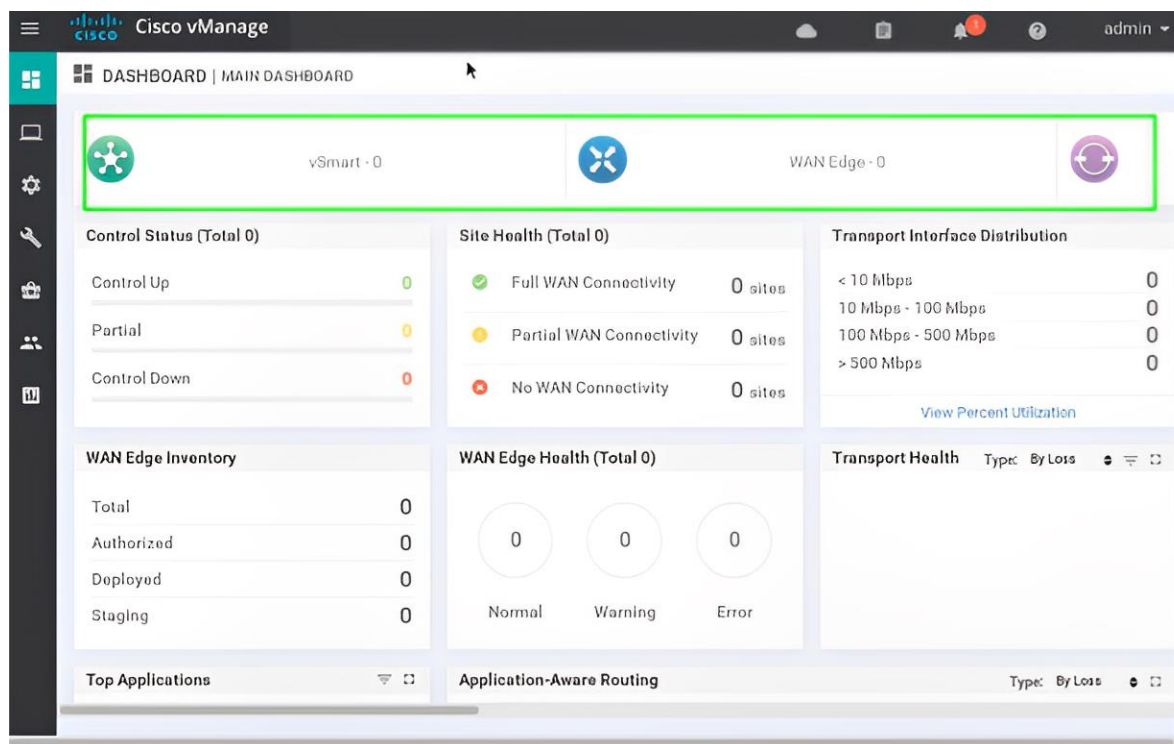


Para acceder al portal web del vManage por primera vez, se creó la topología que se muestra en la Figura 30. En esta figura, se observa que la salida a internet se realiza mediante la nube Cloud1, la cual está conectada a la interfaz física eno01. Para llevar a cabo esta conexión, se debe asignar una interfaz física del servidor a un elemento Cloud presente en GNS3. De esta manera, se puede salir a internet a través de la VPN0, la cual está enrutada para permitir dicha acción.

Una vez configurada la interfaz y su respectivo gateway, el administrador podrá acceder a las configuraciones mediante el navegador desde el QEMU, tal como se muestra en la Figura 31. Cabe destacar que, para realizar esta acción, se debe verificar que la interfaz esté habilitada administrativamente y que las configuraciones se hayan guardado mediante el comando "commit".

Figura 31

Vista de dispositivos interfaz web vista desde GNS3-cliente



Una vez que se ha preparado la topología para ingresar al portal de administración del vManage, desde la dirección IPv4 asignada (192.168.1.3), es posible acceder al panel de control a través de la interfaz web, tal como se muestra en la Figura 31, en donde se pueden visualizar los dispositivos presentes en el cluster de control, así como los enlaces de transporte activos de cada uno de los routers de acceso. Es importante destacar que aún no se ha desplegado el clúster completo del plano de control, por lo que en la Figura 31 se puede observar que los vEdges, vBond y vSmart están marcados en verde y el número de estos dispositivos ya desplegados es 0.

Figura 32

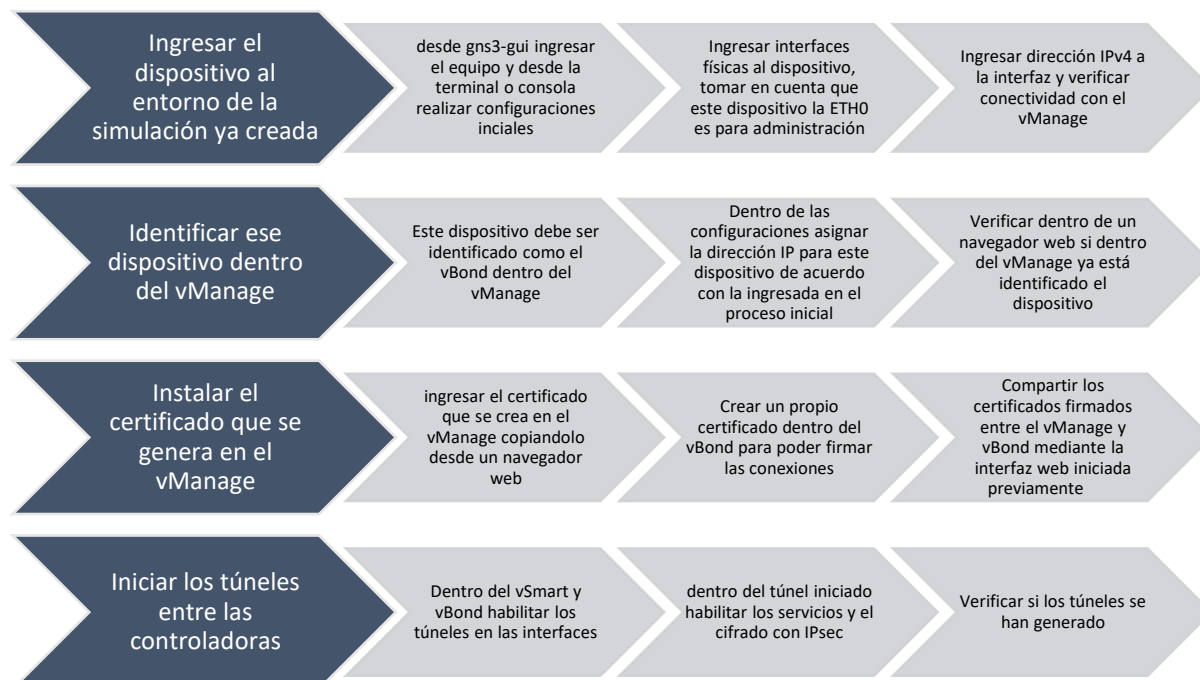
Vista del monitor de la red vista desde GNS3-cliente

Username	System IP	Device Model	Chassis Number/ID	State	Reachability	Site ID	BF
vManage_CuaicalA	1.1.1.1	vManage	94563e35-4f94-4130-856c-ad621e...	✓	reachable	1	--

En el apartado de monitor de red, presente en el mismo dashboard, se observa que actualmente no hay dispositivos conectados a la red superpuesta, a excepción del vManage que se muestra en la Figura 32, dicha información es mostrada en el apartado **Device Model1**. Además del modelo del equipo, se muestra información como, la dirección IPv4 del sistema (**System IP**), el número de chasis del equipo (**Chassis Number/ID**), el estado del equipo (**State**), dentro de las más importantes.

3.9 Despliegue de vBond

El despliegue de este dispositivo es de vital importancia debido a que, este es el encargado de añadir nodos a la red SD-WAN, en este sentido el vBond debe autenticarlos y brindarles recursos. Para la integración de este elemento a la red, es necesario tomar en cuenta que; se debe establecer un nombre de organización, el ID del sitio, la dirección IPv4 del sistema, así mismo como la información de los túneles VPN0 que se crearán en el vManage.

Figura 33**Proceso de despliegue de vBond**

El proceso para el despliegue del vBond se muestra en la Figura 33. Esta figura detalla cada uno de los procesos y subprocesos necesarios para la configuración del dispositivo, así como los dispositivos que interactúan para lograr la configuración deseada.

En primera instancia se debe configurar la información del sistema tal como en el vManage, para lo cual se debe ingresar mediante consola al equipo y asignar una dirección IPv4 a una interfaz de red perteneciente a la VPN0 y de esta manera pueda ser configurado y se comuniquen con el vManage.

Una vez configurada la dirección IPv4 del equipo se debe generar e instalar el certificado para el nodo y de esta manera sea capaz de realizar la conexión con el vManage

mediante los túneles IPsec, por lo cual, se debe ingresar este dispositivo dentro del vManage para que forme parte de la red superpuesta.

Para integrar el vBond al vManage, se deben seguir los siguientes pasos: Primero, agregar el vBond a la lista de dispositivos permitidos dentro del controlador vManage. Segundo, agregar el dispositivo a la VPN0 para que pueda ser alcanzado por el vManage. Cabe mencionar que el túnel necesario para esta conexión ya está creado por defecto en la controladora. Una vez que se haya completado el proceso, el vBond deberá aparecer dentro del vManage.

Figura 34

Configuraciones de iniciales vBond

```

contig
system
host-name vBond_CuaicalA
system-ip 2.2.2.2
site-id 1
organization-name cuaical-sdwan
clock timezone America/Bogota
vbond 192.168.1.4 local vbond-only
exit
vpn 0
int ge0/0
ip address 192.168.1.4/24
no shutdown
exit
commit and-quit

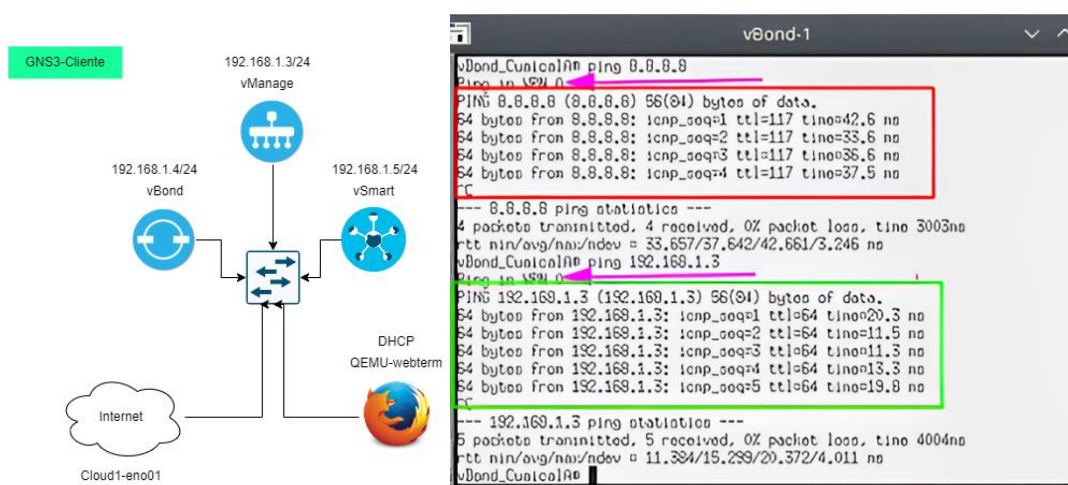
```

Las configuraciones básicas del vBond, a diferencia de las demás controladoras, este se autoidentifica como el vBond, al ser este dispositivo usado tanto para los vEdge como vBond debe identificarse su modo de operación, dicha configuración se la muestra dentro de la Figura 34 (`vbond 192.168.1.4 local vbond-only`), con la cual se identifica que solamente trabajará como vBond, además se autoidentifica como este.

Una vez se ingresa el vBond a la red, este ya debe alcanzar el vManage, a pesar de ello no forma parte de la red, esto se debe a que no se ha ingresado este dispositivo dentro del vManage, además de que aún no se han generado los certificados para la comunicación segura.

Figura 35

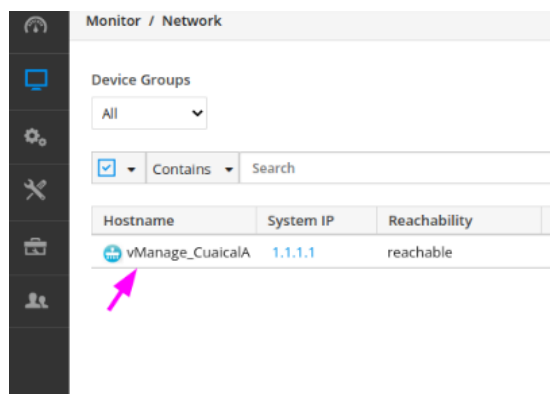
Verificación de comunicación



Una vez se han configurado los parámetros iniciales, se debe verificar la conectividad del dispositivo, tanto para la red interna como para la red pública, de esta manera, la Figura 35, en el cuadro de color rojo, se muestra que el vBond ya es capaz de salir por la red pública, con lo cual puede realizar un ping a la ip 8.8.8.8, de la misma manera en el recuadro de color verde se muestra que alcanza el vManage(192.168.1.3) ya que forman parte de la misma red, además, en el marcador de color rosa, se evidencia que realiza la comunicación por la VPN0.

Figura 36

Verificación del plano de control



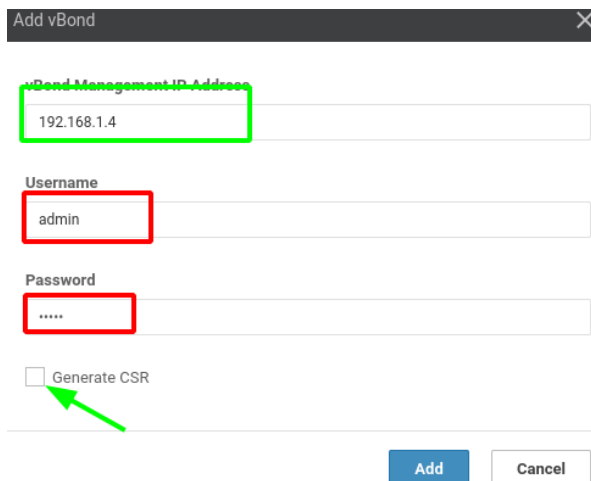
Como ya se mencionó, aunque los dispositivos son alcanzables, aún no es posible la comunicación e integración entre las controladoras debido a que es necesario generar certificados para establecer una comunicación segura mediante el uso de túneles IPsec. Por esta razón, en la Figura 36 se puede observar únicamente el dispositivo **vManage_CuaicalA** dentro del monitor de red.

Para agregar la controladora vBond al vManage, primero, se debe acceder a la sección de configuración del vManage, y luego seleccionar la opción de dispositivos. Dentro de esta sección, se debe elegir la opción de controladoras y, finalmente, agregar la controladora vBond de la siguiente manera:

1. Elegir vBond dentro de las controladoras, ingresar la IPv4 asignada al vBond dentro de la red (192.168.1.4), además de las credenciales de ingreso para el dispositivo seleccionado.

Figura 37

Ingreso de vBond en el vManage



En la Figura 37, se muestra cómo se debe ingresar el nuevo dispositivo, es importante no generar otra firma para este, ya que, los certificados serán creados posteriormente. De la misma manera, se debe tomar en cuenta que la dirección IPv4 ingresada, no podrá ser cambiada posterior a la creación del certificado, ya que las firmas, certificados y números de chasis serán asociados a dicha dirección IPv4 (192.168.1.4).

2. En caso de que exista un error al realizar el ingreso del vBond dentro del vManage, se debe verificar que, dentro de la interfaz de red usada para la comunicación, no se esté usando el cifrado para la comunicación, ya que, este aún no tiene las firmas para realizarlo. Y de la misma manera que dentro de la VPN0 se esté enrutando el tráfico de manera adecuada.

Figura 38

Configuración de interfaz vBond

```
vpn 0
interface ge0/0
ip address 192.168.1.4/24
ipvs dhcp-client
tunnel-interface
encapsulation ipsec
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
!
Aborted: by user
```

Los parámetros que se deben comprobar se muestran en la Figura 38, datos que se muestran usando el comando `show running-config | tab vpn 0`, con lo cual se evidencia como no debería estar configurada la interfaz(`tunnel-interface; encapsulation IPsec`) y de esta manera pueda ser agregado el dispositivo dentro del vManage. Para cambiar la configuración, se debe ingresar a la vpn 0, a la interfaz deseada, y desactivar el túnel de la interfaz con el comando `no tunnel interface`. Una vez se realice dicho proceso el vBond debería aparecer ya dentro de la interfaz gráfica de la controladora.

Figura 39

Vista del ingreso desde la web

Controller Type	Hostname	System IP	Site ID	Mode	Assigned Template	Device Status	Certificate Stat...
vManage	vManage_CuaicalA	1.1.1.1	1	CLI	--	In Sync	Installed
vBond	--	--	--	CLI	--		Not-Installed

En esta instancia ya debería observarse el ingreso del vBond como se muestra en la Figura 39, caso contrario se debe verificar el funcionamiento de la interfaz y las configuraciones iniciales realizadas, ya que, como se había mencionado previamente, el éxito de esta operación depende de la organización y la dirección IPv4 del propio vBond. Nótese que en el estado de los certificados (**Certificate State**), aún no se tiene uno instalado.

De esta manera, para que las conexiones sean seguras, se debe ingresar al apartado de certificados, en donde ya deben estar presentes los dispositivos instalados y generar su certificado, este proceso se muestra a detalle en el apartado de instalación de certificados, de esta manera, se debe copiar el certificado previamente generado en el vManage y realizar el siguiente proceso:

1. Crear un fichero denominado vbon.crt como se muestra en la Figura 40 con el comando `vim vbond.crt`.

Figura 42

Verificación de los dispositivos ingresados

	Controller Type	Hostname	System IP
▼	vBond	--	--
- [5-Sep-2022 12:51:44 COT] CSR Generated - [5-Sep-2022 13:03:12 COT] Installed			
▼	vSmart	--	--
- [5-Sep-2022 13:04:19 COT] CSR Generated - [5-Sep-2022 13:06:51 COT] Installed - [5-Sep-2022 13:06:53 COT] vBond Updated			

Dentro del dispositivo debe observarse que, se ha generado la solicitud de firma y está instalado correctamente.

5. Una vez estén listos los certificados para cada elemento, se debe enviar los mismos a cada dispositivo remoto, para de esta manera pueda generarse la conexión segura. Una vez el vBond acepte los dispositivos enviados en la lista, debe mostrar los mensajes presentados en la Figura 43.

Figura 43

Logs generados debido a la configuración

Status	Message	Device Type	Hostname	System IP	Site ID	vManage IP
Success	Done - Push vSmart List for ...	vBond		-	-	1.1.1.1
<pre>[5-Sep-2022 13:10:29 COT] Push vSmart List, on device f07f6aed-4244-40f7-a9f5-5a9be9a2cd7c, started by user "admin" from IP address "192.168.1.13" [5-Sep-2022 13:10:29 COT] Pushing serial list to vBond-f07f6aed-4244-40f7-a9f5-5a9be9a2cd7c [5-Sep-2022 13:10:30 COT] Started processing serial list file on vBond-f07f6aed-4244-40f7-a9f5-5a9be9a2cd7c [5-Sep-2022 13:10:31 COT] Completed processing serial list file on vBond-f07f6aed-4244-40f7-a9f5-5a9be9a2cd7c [5-Sep-2022 13:10:32 COT] Done - Push vSmart List for vBond-f07f6aed-4244-40f7-a9f5-5a9be9a2cd7c</pre>						
Success	Done - Push vSmart List for ...	vManage	vManage_CuaicalA	1.1.1.1	1	1.1.1.1
<pre>[5-Sep-2022 13:10:29 COT] Push vSmart List, on device 79acf7c7-f6ff-43ed-b611-632cbf6956b0, started by user "admin" from IP address "192.168.1.13" [5-Sep-2022 13:10:29 COT] Pushing serial list to vManage-79acf7c7-f6ff-43ed-b611-632cbf6956b0 (vManage_CuaicalA) [5-Sep-2022 13:10:30 COT] Started processing serial list file on vManage-79acf7c7-f6ff-43ed-b611-632cbf6956b0 (vManage_CuaicalA) [5-Sep-2022 13:10:31 COT] Completed processing serial list file on vManage-79acf7c7-f6ff-43ed-b611-632cbf6956b0 (vManage_CuaicalA) [5-Sep-2022 13:10:32 COT] Done - Push vSmart List for vManage-79acf7c7-f6ff-43ed-b611-632cbf6956b0 (vManage_CuaicalA)</pre>						

En donde se muestra los logs de las acciones realizadas, las cuales mencionan que se ha enviado la lista de los dispositivos y esta ha sido aceptada, además de que no existe ningún error en el proceso, por lo cual el estado debe ser **Success**

- Habilitar la comunicación segura en los dispositivos.

Figura 44

Habilitando la interfaz para la comunicación con IPsec

```
vManage_CuaicalA# config
Entering configuration mode terminal
vManage_CuaicalA(config)# vpn 0
vManage_CuaicalA(config-vpn-0)# interface eth0
vManage_CuaicalA(config-interface-eth0)# tunnel-interface
vManage_CuaicalA(config-tunnel-interface)# do commit
```

En el vBond debe habilitarse IPsec para que el plano de control pueda comunicarse de manera segura entre sí como se muestra en la Figura 44, caso contrario arrojará un error en el `commit` y no se realizarán las configuraciones deseadas.

Figura 45**Conexiones del cluster de control**

	Controller Type	Hostname	System IP	Expiration Date	uuid	Operation Status	Site ID	Certificate Serial	vEdge Lis...	Device IP	
>	vBond	vBond_CuaicalA	2.2.2.2	26 Feb 2028 1:02:01 PM -05	f07f6a...	Installed	1	8B73ECDCD0F13A4C	Sync	2.2.2.2	...
>	vSmart	vSmart_CuaicalA	3.3.3.3	26 Feb 2028 1:06:16 PM -05	cf69ba...	vBond Updated	1	8B73ECDCD0F13A4D	Sync	3.3.3.3	...
>	vManage	vManage_CuaicalA	1.1.1.1	26 Feb 2028 12:18:28 PM -05	79ac7...	vBond Updated	1	8B73ECDCD0F13A4B	-	1.1.1.1	...

En este punto, ya se pueden observar las conexiones dentro de la controladora, tal como se muestra en la Figura 45, en donde se evidencia que las direcciones IPV4 del sistema de las controladoras ya se han registrado, además que cada equipo se identifica de manera adecuada como se muestra en el campo **Controller Type**, en caso de no tener dicha información se debe verificar los certificados y que estos hayan sido instalados de manera adecuada.

3.10 Despliegue de vSmart

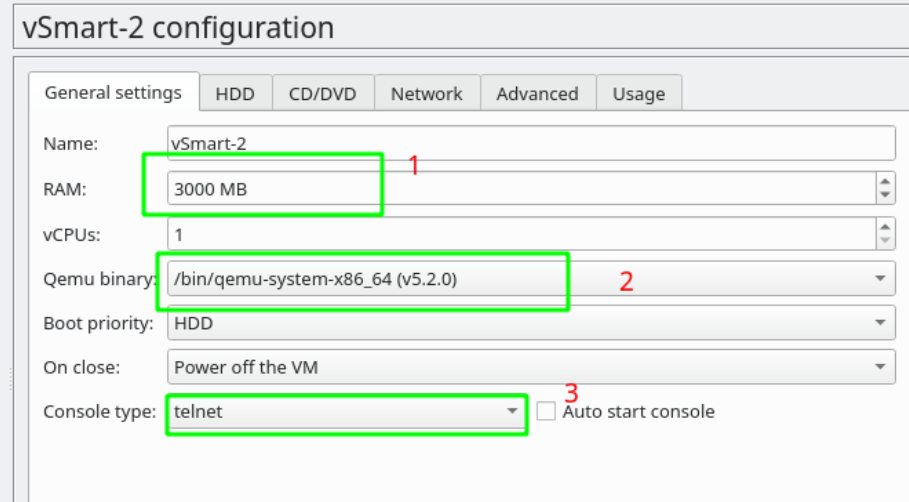
Para que el vSmart pueda ejecutar las políticas del vManage a través de la red superpuesta, es necesario que el protocolo OMP esté habilitado para el enrutamiento. Para ello, se deben realizar las siguientes configuraciones en el dispositivo: el vSmart solo utiliza el túnel 0, que se crea por defecto al activar el dispositivo, y al habilitar este túnel, se activa también el firewall por defecto ya que se supone que este dispositivo conectará redes no confiables.

Además, se debe considerar que el protocolo NetConf por defecto está bloqueado, con lo cual debe activarse para poder recibir y enviar actualizaciones del comportamiento de la red superpuesta, finalmente se debe instalar los certificados del vManage para que se identifiquen como puntos de confianza.

En el caso del vSmart al ser el encargado de ejecutar las reglas impuestas dentro del vManage no necesita de excesivos recursos físicos, con lo cual se le asignó 3GB de memoria RAM para su operación. De esta manera las configuraciones físicas del dispositivo se asignan tal como se muestra en la Figura 46.

Figura 46

Configuraciones físicas de vSmart



The image shows a configuration window titled "vSmart-2 configuration" with several tabs: "General settings", "HDD", "CD/DVD", "Network", "Advanced", and "Usage". The "General settings" tab is active. The configuration fields are as follows:

- Name: vSmart-2
- RAM: 3000 MB (highlighted with a green box and labeled with a red "1")
- vCPUs: 1
- Qemu binary: /bin/qemu-system-x86_64 (v5.2.0) (highlighted with a green box and labeled with a red "2")
- Boot priority: HDD
- On close: Power off the VM
- Console type: telnet (highlighted with a green box) and an unchecked checkbox for "Auto start console" (labeled with a red "3").

Para el correcto funcionamiento del equipo y realizar las configuraciones iniciales, es importante configurar los parámetros físicos del dispositivo, como se muestra en la Figura 46. En el punto 1 se puede observar la cantidad de memoria RAM asignada al equipo, mientras que en el punto 2 se muestra el directorio en el cual se emula dicho elemento. Dentro del apartado de redes, se ha configurado un solo adaptador para la conexión con el clúster propuesto para las controladoras. Estas configuraciones son de vital importancia para asegurar el correcto funcionamiento del equipo.

Figura 47

Configuraciones iniciales del sistema de vSmart

```
vsmart login: admin
Password:
Welcome to Viptela CLI
admin connected from 127.0.0.1 using console on vsmart
vsmart# config
Entering configuration mode terminal
vsmart(config)# system
vsmart(config-system)# host-name Smart_CuaicalA
vsmart(config-system)# system-ip 3.3.3.3
vsmart(config-system)# site-id 1
vsmart(config-system)# organization-name cuaical-sdwan
vsmart(config-system)# clock timezone America/Bogota
vsmart(config-system)# vbond 192.168.122.5
vsmart(config-system)# exit
vsmart(config)# vpn 0
vsmart(config-vpn-0)# int eth0
vsmart(config-interface-eth0)# ip address 192.168.122.5/24
vsmart(config-interface-eth0)# no shut
vsmart(config-interface-eth0)# exit
vsmart(config-vpn-0)# ip route 0.0.0.0/0 192.168.122.1
vsmart(config-vpn-0)# exit
vsmart(config)# commit and-quit
Commit complete.
cSmart_CuaicalA#
```

En la Figura 47 se muestran las configuraciones necesarias para asegurar un correcto funcionamiento del equipo dentro de la controladora. En el primer marcador, se asigna un nombre al equipo para que pueda ser fácilmente identificado en la red.

Además, se configura la dirección IPv4 del vBond, el cual tiene la función de autenticar y asignar recursos a los nodos. La correcta configuración de esta dirección es fundamental para que el equipo pueda conectarse y comunicarse adecuadamente con la controladora.

Por último, se establece el uso de la VPN0 para permitir la comunicación entre los elementos de la red OMP. También se configura la salida a internet y se enrutan los dispositivos para que puedan alcanzar el vManage, ya sea a través de la conexión dentro

del clúster o por la red pública. Todo esto garantiza que el equipo esté correctamente integrado en la red y pueda funcionar sin problemas.

De la misma manera que el vBond, se tiene que, los dispositivos son alcanzables por la red local del clúster, y además son capaces de realizar consultas en la red pública, a pesar de ello no son capaces aún de comunicarse de manera segura, ya que no se han generado los certificados e ingresados en cada uno de los dispositivos.

Para ingresar el vSmart dentro del vManage se debe realizar el mismo proceso que se mostró en el apartado de vBond hasta que el equipo se muestre tal como en la Figura 48.

Figura 48

Verificación de comunicación fallida

Controller Type	Hostname	System IP	Site ID	Mode	Assigned Template	Device Status	Certificate Stat...
vManage	vManage_CuaicalA	1.1.1.1	1	CLI	--	In Sync	Installed
vSmart	--	--	--	CLI	--		Not-Installed
vBond	--	--	--	CLI	--		Not-Installed

A pesar de que las controladoras ya se observan dentro de la interfaz gráfica del vManage, aún no se muestra información de estas, con lo cual el clúster para las controladoras no está totalmente configurado, para lo cual se debe instalar todos los certificados creados, en los dispositivos remotos.

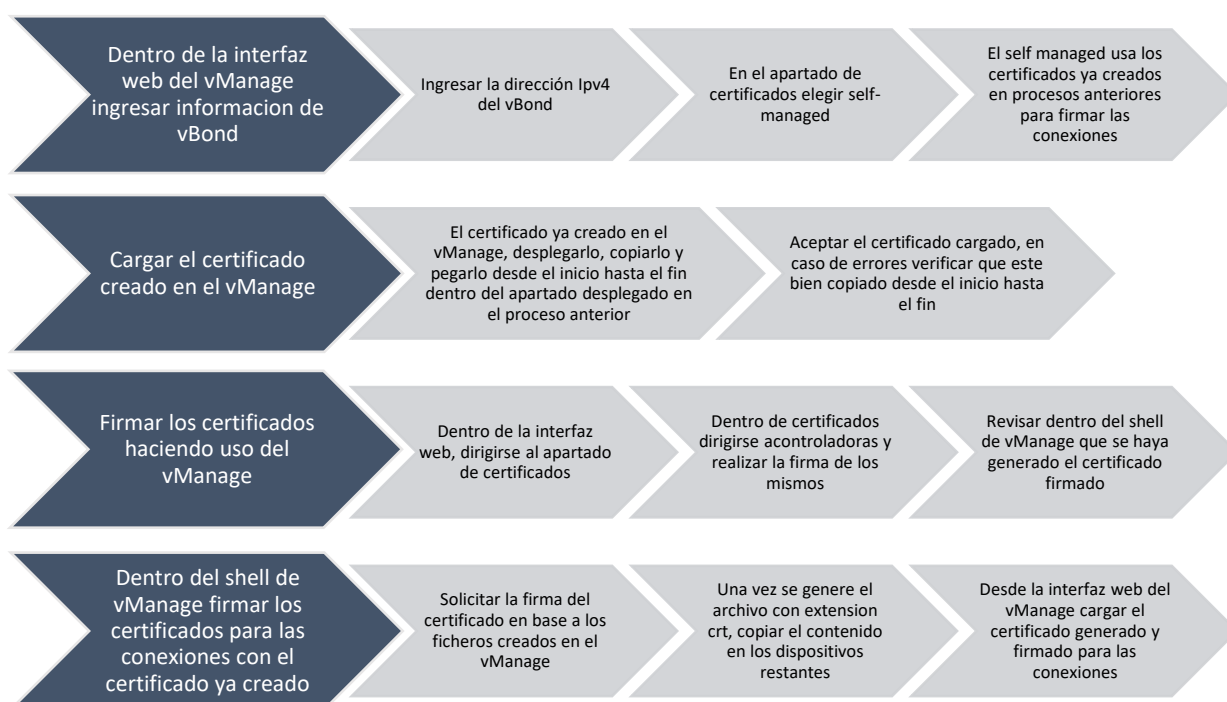
3.11 Instalación de certificados

La implementación de los certificados no es una tarea sencilla, ya que requiere la generación y firma de estos en el vManage. Este proceso se realiza utilizando tanto la interfaz web como el shell de los dispositivos del plano de control. Por lo tanto, es

necesario crear archivos de configuración mediante la consola y asegurarse de que coincidan con la información proporcionada en la interfaz web. En la Figura 49 se muestra de manera resumida el proceso de generación de certificados, así como los dispositivos en los que se ejecuta.

Figura 49

Instalación de certificados



Para que cada uno de los elementos del plano de control se vea reflejado dentro del vManage, se deben crear y asociar los certificados, tanto del vBond como vSmart para de esta manera tener una comunicación segura usando IPsec para el plano de control, dichos certificados deben ser creados y asociados de la siguiente manera:

1. Asignar la dirección IPv4 del vBond dentro de la interfaz gráfica del vManage.

Figura 50

Agregando vBond al plano de control

The screenshot shows the vManage Settings page. The 'vBond' section is currently 'Not Configured'. A modal dialog is open for configuring the vBond DNS/ IP Address : Port. The IP address is set to 192.168.1.4 and the port is 12346. There are 'Save' and 'Cancel' buttons. Other settings include Organization Name: cualcal-sdwan and Certificate Authorization: Manual.

La configuración que se debe realizar dentro del vManage es definir la dirección IPv4 del vBond (192.168.1.4), además del puerto por el cual se realizará la comunicación (12346) como se muestra en la Figura 50.

2. Definir cuál es la entidad que proporcionará las firmas y certificados para realizar las conexiones, de esta manera al no tener una entidad que proporcione dichos certificados, se genera un certificado local, y será firmado por el propio vManage.

Figura 51

Agregando vBond al plano de control

The screenshot shows the 'Controller Certificate Authorization' page. The 'Certificate Signing by' section has four radio buttons: 'Cisco Automated (Recommended)', 'Symantec Automated', 'Manual', and 'Enterprise Root Certificate'. The 'Enterprise Root Certificate' option is selected and highlighted with a pink box. Below this, the 'Validity Period' is set to '1 Year' and the 'Certificate Retrieve Interval' is set to '60 min'.

Definido el tipo de certificado como se muestra en la Figura 51, se debe conectar por consola al vManage, en el cual se generará una llave de 2048 bits, de la misma manera

se genera un certificado denominado **ROOTCA.key** que es una de las llaves, además del tiempo de vida de este. Finalmente se crea la organización que firma el certificado y se crea el archivo para poder observar dicha llave.

Figura 52

Líneas de comando para la creación de certificados

```
vshell
openssl genrsa -out ROOTCA.key 2048
openssl req -x509 -new -nodes -key ROOTCA.key -sha256 -days 2000 \
-subj "/C=SV/ST=SS/L=SS/O=cuaical-sdwan/CN=vmanage.lab" \
-out ROOTCA.pem
```

Los parámetros configurados para el certificado ya mencionados se muestran en la Figura 52, de esta manera y una vez ejecutada la creación de este en el shell del vManage, ya estará disponible el archivo que contiene la llave para habilitar la comunicación cifrada.

3. Una vez se ha generado el certificado, se ingresa al fichero **ROOTCA.pem** en el cual se encuentra el certificado, tal como se muestra en la Figura 53.

Figura 53

Verificación de creación de certificados.

```

vmanage_cuaical#
vManage_CuaicalA# vshell
bash-4.4$ ls
ROOTCA.key  ROOTCA.srl          vbond.crt  vmanage.crt  vsmart.crt
ROOTCA.pem  archive_id_rsa.pub vbond_csr  vmanage_csr  vsmart_csr
bash-4.4$ cat ROOTCA.key
-----BEGIN RSA PRIVATE KEY----- 1
MIIEowIBAAKCAQEAyOYJV8KvuMjzK1YziEcNaBsObucYcGfGscDdsV7H3hVQwK3b
okKnQVyf11nlwGCvphEkX1sUKkLvhnp22GYQMVP/9rSEn0gMiIitRVqW5hH4H1nuR
hsaPrjbejqRvU6obms05qqeuyRSHbuNLo2K429aPUKL03gf0I3p/GrILkKJqjL5h
BUA7m4LF62c/VuEcSeFSoE/09jKIEaeiuruE2IFIQtji0BbKcn+YfZ5c2rQt/1iB
iKQcQcWwMat68jZ/ckFx443pL09wjGkM1kqZ4YEW6NbkglY+v00BiJ19JVzFMzVl
uwIDDPU2Sh0vAeSYqZf10s5PjwK9iG3lw6UYJQIDAQABAoIBAAUDt+Z11g5ZfKvF
INbcollmJb//hKhu0ocxTU72p1pS5AHJdt5pJEW37Es4g1YzZ8MB8uqsv4RStHBNJ
6e5hw9KpBIyRUcPFJCEIqRZLut1DCKFivwtbDS2PNUq1NQkw1Qo00yxJEXZ6+o5T
PJAQz2sn/PckTZr+zQ9L/oSjuVBh2o74jZnt5gPnwWhnC4w3WY68J27vNVsU3xh
+S80ZTafjcf59JvI1t038dBSex4Tn0q+JY1Tb9D1tsvgdXb4H+E94ekqIZIvYG68
T/pfAYxJ6BAc2QJ0GwWbeDn5smCeaCrgFLJ+OHJi0f0PrqIb6r+WeCtmeVQpdsKj
BEAH08CgYEA7C7/v5zYcQKHxy0ubMBn0XSyK2dnQ111IeEhktmss0piFJ6zIkA
9w4F1TchbvtVbzd07FgitjYQX+6/Cx05tU8kjq2JxQDKA5o54RBwIDeu9vVKx
L170eRLLF8ck1mAkU3LLM4rRX2H1yT2r53gWw7oyw1HA1R6hgk0fycGyEA3FQp
VITYUnpHvD38S1J+GoE9HuY7P1xA6MdhVUGNw0DmMQcZvs+taukntwL/CWyc0NG
ojsbiQ+8cLxhABWhrBttVwDKPHUA400oDUtnjYqVnQ5NOHxyEY36JI/be5vJTjYt
xm5n6DX+zb3hR85tQAdX9IuIb5zPdRHAxuJMPdMCgYAix80Lt5oswX2jPckRBMiF
FM1EDQcs6W9dXNzn1jtxKztJgvPoe0h2eU8sleDLiGLrjv+r/f/2m6jwqsRelGRr
h/1bbJd6Q5Xv4UAQM7zMMuCCQxD19yta5jXU0otD5S+hDi1rTIVWAsRQaoc/0mC9
RnbmMrH/b0YfPGqKoIJ1kwkBgQDIBCNOu1Fydo2+5yqtmmlEXusErQ+1SgynBbFn
u04bhk+SvJZzsYcGIkmpEgjjH1VdEfsCddRGdiGk2m7Yq8qMQo31SNNPVQyMTNQK
VaTZSrEN1hjmI7SwmQo3vNOMdt2mAetGU55CoRoC3tiv3kcxtdj1y0IAKQPwJEBM
krQvfukBgC64mv7r5W50zMpctGYGVlbc1PUvIRhAYBrif3HPu3DiCkG1jUPTHa2v
mtuXY683pZ5yQhaHDIFDctJ646Q0ksh6RBy4VtqA91DGjqFF38EnHQEqSjplK47e
80mIvGYXwPmFjag+uIacpIJuKYTqd1UcD7bRG4jDhLPsgJ1Ewu40
-----END RSA PRIVATE KEY----- 2

```

Localizado el fichero **ROOTCA.pem**, se muestra su contenido con el comando “**cat**” de esta manera se debe copiar todo su contenido desde “**BEGIN CERTIFICATE**” (marcador 1 en la figura53) hasta “**END CERTIFICATE**” (marcador 2), caso contrario el certificado no será entendible para su instalación dentro del dispositivo, además se debe respetar su estructura de inicio y fin.

- Una vez copiado, se debe ingresar el contenido en el cuadro desplegado en el punto 2.

Figura 54

Carga de certificado

Certificate Signing by: Cisco Automated (Recommended) Symantec Automated Manual Enterprise Root Certificate

Certificate

```
VQQHDAJTUzEWMBQGA1UECgwNY3VhaWNhbC1zZDhbjEUMBIGA1UEAwWldm1hbmFn
ZS5sYWlwgEIMA0GCSqSib3DQEBAQUAA4BDWAwggEKAoIBAQDLRgXwq+4yPMr
Vj0IRw1oGw5u5xgKAUaxwN2y/sfeFVDArdulQqdBXJ/WWdYYJWmESReWxQqQu+Ge
nbYZhAxU//2t1SfSAyIk1FWpbmEgEWe5Gx0+uNt6OpG9Tghuayjmqp67JFidu
40ujYrjb1o9Qos7eB84jen8asguQomqMvmEFQDubgsXrZz9W4RxJ4VKgT872MqUR
p6K6u4TYgUhC20I4Fspyf5h9nlzatC3/WIGlpByooJZZq3ryNn9yR/HjjkvT2+M
aQzWSpnhgRbo1uSDXL687QGImX0IXMUxm8u7AgMM9TZKE68B5Jipl+U6zk+Nyr2l
beXdpRglAgMBAAGjUDBOMB0GA1UdDgQWBWRhK1QCKWc8XIV55oVIOJICcYZhnjAf
BgNVHSMEGDAWgBRhK1QCKWc8XIV55oVIOJICcYZhnjAMBgNVHRMBETADAQH/MA0G
CSqSib3DQEBCwUAA4IBAQCp4ydpLjk83iy6lUpceHw4sHgQFkWcgs49S3W0ESOs
7nuvWyAQND0AURGTJIMou2TYfifq9GyQO2fIZNlgvuy8boKss0l1x7dhB+GMtnwZt
sKUXyMVMmU2tDWI+H8lchyPVP17PKAttSljZYjdBz2pDEG/Kk5hecGJY8Y2QmGj
+TAXL47XPI26EQ9r/RPCj2EF1+6Vvgqy3W/PlhuQ6LAWuAHQ24AsWj4FqlkgD0DN
Ej7JvBBh893mQqq9LxROhwVc4KqalgJ2QXiz+B+EVm4yi/X7j0Ca4ZTSquACA6
wbcNbnrZD7mCKoFsw8nZ0x9rupdh9EENSip7sKUAxUE
-----END CERTIFICATE-----
```

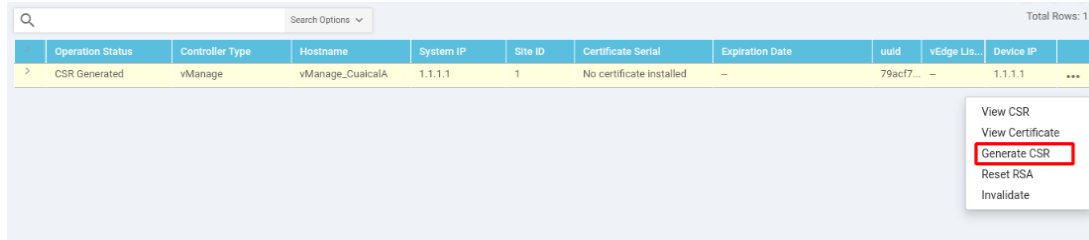
Set CSR Properties

En la Figura 54, se muestra cómo se debe ingresar el certificado dentro de las configuraciones del vManage, de esta manera ya está listo para ser usado en los túneles IPsec, ahora se debe firmar este como se muestra en el siguiente paso.

- Para firmar el certificado, se debe ingresar al apartado de configuraciones presentes en el dashboard del vManage y dentro del apartado de certificados, dirigirse a controladoras y generar la firma del certificado (**certificate signature**).

Figura 55

Generación de firma del certificado



Una vez generada la firma, tal como se evidencia en la Figura 55, se copia dicho certificado firmado, el cual se encuentra generado en los archivos raíz del vManage, al cual es posible ingresar desde el Shell de este.

Figura 56

Creación de fichero para firmar el certificado

```

/Manage_CuaicalA#
/Manage_CuaicalA# vshell
vash-4.4$ ls -l
total 36
-rw-r--r-- 1 admin admin 1675 Sep  5 2022 ROOTCA.key
-rw-r--r-- 1 admin admin 1269 Sep  5 2022 ROOTCA.pem
-rw-r--r-- 1 admin admin  17 Sep  5 2022 ROOTCA.srl
-rw-r--r-- 1 admin admin  0 May 17 08:31 archive_id_rsa.
-rw-r--r-- 1 admin admin 1314 Sep  5 2022 vbond.crt
-rw-r--r-- 1 admin admin 1220 Sep  5 2022 vbond_csr
-rw-r--r-- 1 admin admin 1314 Sep  5 2022 vmanage.crt
-rw-r--r-- 1 root root 1220 Sep  5 2022 vmanage_csr
-rw-r--r-- 1 admin admin 1314 Sep  5 2022 vsmart.crt
-rw-r--r-- 1 admin admin 1220 Sep  5 2022 vsmart_csr
vash-4.4$ █

```

La Figura 56, muestra el archivo generado visto desde el Shell del vManage, de esta manera se debe considerar que dicho archivo ha sido creado y firmado bajo las condiciones de una organización, con lo cual, equipos que no formen parte de la misma organización no podrán hacer uso de este, es por ello por lo que las configuraciones iniciales de los equipos previamente mostradas deben tener concordancia con las usadas para este apartado.

Figura 57

Parámetros de la firma del certificado

```
openssl x509 -req -in vmanage_csr \
-CA ROOTCA.pem -CAkey ROOTCA.key -CAcreateserial \
-out vmanage.crt -days 2000 -sha256
```

Para realizar la firma del certificado, es necesario ejecutar las líneas de comando que se muestran en la Figura 57. Estas líneas deben ser ejecutadas desde el Shell del vManage. Para acceder a este Shell, es necesario abrir una consola del vManage y luego ingresar las credenciales correspondientes, y posteriormente ingresar el comando "vshell".

Las líneas de comando mostradas en la Figura 57, utilizan el programa OpenSSL para generar un certificado firmado para el dispositivo vManage. A continuación, se explica el propósito de cada opción en las líneas de comando:

- openssl: Este es el nombre del programa que se utilizará para realizar la operación de generación del certificado.
- x509: Esta opción indica que se realizará una operación relacionada con certificados X.509.
- req: Esta opción indica que se utilizará un archivo de solicitud de certificado (CSR) para generar un certificado firmado.
- in vmanage_csr: Esta opción indica el nombre del archivo CSR que se utilizará para generar el certificado.
- CA ROOTCA.pem: Esta opción indica el archivo de certificado de la Autoridad de Certificación (CA) que se utilizará para firmar el certificado.

- CAkey ROOTCA.key: Esta opción indica el archivo de clave privada de la CA que se utilizará para firmar el certificado.
- CAcreateserial: Esta opción indica que OpenSSL creará un archivo de número de serie único para el certificado firmado.
- out vmanage.crt: Esta opción indica el nombre del archivo de certificado firmado que se generará.
- days 2000: Esta opción indica que el certificado será válido por 2000 días.
- sha256: Esta opción indica que se utilizará el algoritmo de hash SHA-256 para firmar el certificado.

Figura 58

Certificado generado shell vManage

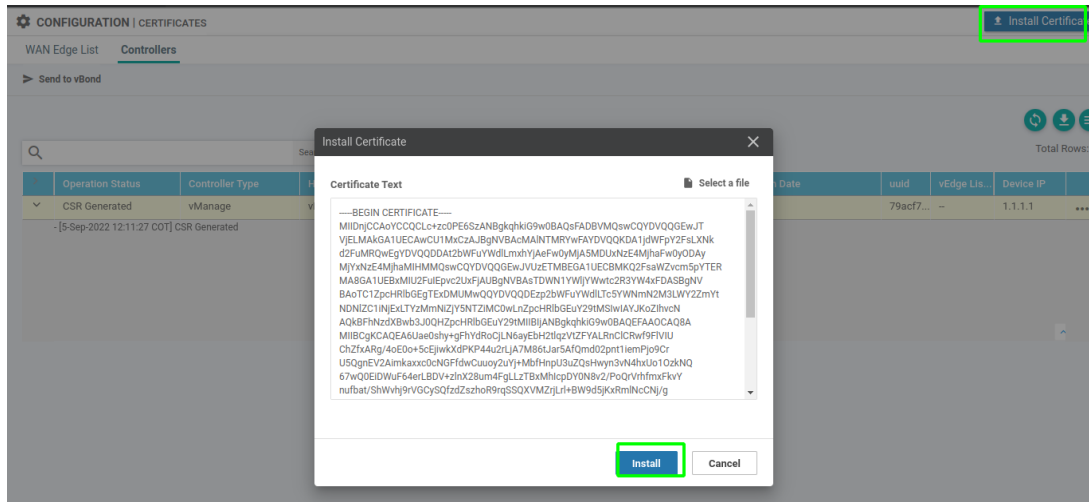
```
bash-4.4$ ls
ROOTCA.key  ROOTCA.srl  vmanage.crt
ROOTCA.pem  archive_id_rsa.pub  vmanage_csr
bash-4.4$
```

Una vez se haya generado el archivo `vmanage_csr` que contiene la firma del certificado, tal como se muestra en la Figura 56 y al ejecutar las líneas de la Figura 57, se genera un archivo con el nombre `vmanage.crt`, como se muestra en la Figura 58, el cual contiene el certificado firmado, de esta manera ya solamente queda subir dicho certificado firmado tanto en los equipos que conforman el cluster de controladoras cómo los vEdges y de esta manera puedan establecer los túneles IPsec.

6. Para cargar el certificado en los dispositivos restantes, con el comando `cat` se visualiza el contenido del fichero mostrado en el paso 5, y se copia el mismo para posteriormente subirlo dentro de los dispositivos restantes.

Figura 59

Carga del certificado firmado



Para cargar el certificado, se debe seguir los siguientes pasos: en el dashboard del vManage, ubicar el apartado de controladoras y seleccionar "Instalar Certificado", tal como se muestra en la Figura 59, ubicado en la parte superior derecha de la pantalla. Al seleccionar esta opción, se abrirá una ventana donde se puede pegar el contenido del certificado o cargar un archivo que contenga el mismo. En este caso, se pegó el contenido previamente copiado del certificado. Luego, se debe presionar el botón "install" para completar el proceso de instalación del certificado.

Cuando se haya realizado todo el proceso de ingreso de dispositivos con sus certificados, ya será posible verificar las conexiones que tienen con sus pares. En este sentido para los dispositivos vSmart y vEdge el comando a usar es `show control connections` y en el vBond el comando es `show orchestrator connections`.

Figura 60

Resumen de conexiones vSmart

```
vSmart_CuaicalA# show control connections
```

INDEX	PEER TYPE	PEER PROT	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIV PORT	PEER PUBLIC IP	PEER PUB PORT	REMOTE COLOR	STATE	UPTIME
0	vbond	dtls	0.0.0.0	0	0	192.168.1.4	12346	192.168.1.4	12346	default	up	0:00:04:49
0	vmanage	dtls	1.1.1.1	1	0	192.168.1.3	12346	192.168.1.3	12346	default	up	0:00:04:46

La Figura 60, muestra el resumen de las conexiones desde la consola del vSmart. Se puede observar el dispositivo conectado (**vbond**, **vmanage**), el tipo de conexión segura establecida, en este caso dtls⁷, la dirección IPv4 del dispositivo, el puerto de comunicación y la hora en la cual se estableció la conexión.

En el vBond el comando es **show orchestrator connections**, con el cual se despliega una tabla más completa de las conexiones, ya que se muestra el color o tipo de enlace de transporte, además del estado de la conexión.

La comunicación entre las controladoras es encriptada, de esta manera al realizar una captura de paquetes en el enlace de la controladora se observa que; en la capa transporte se usa los puertos definidos dentro del vManage (12346), de la misma manera se evidencia que el protocolo para la comunicación segura es DTLS como se muestra en la Figura 61.

⁷ DTLS: (Datagram Transport Layer Security) es un protocolo de seguridad que se utiliza para proteger las comunicaciones en tiempo real basadas en datagramas, es una variación de TLS (Transport Layer Security) usada para TCP.

Figura 61

Verificación de la comunicación con DTLS

No.	Time	Source	Destination	Protocol	Length	Info
3	0.376960	192.168.1.3	192.168.1.5	DTLSv1.2	224	Application Data
4	0.377442	192.168.1.5	192.168.1.3	DTLSv1.2	188	Application Data
7	1.380832	192.168.1.3	192.168.1.5	DTLSv1.2	224	Application Data
8	1.382462	192.168.1.5	192.168.1.3	DTLSv1.2	188	Application Data
10	2.384260	192.168.1.3	192.168.1.5	DTLSv1.2	224	Application Data
11	2.384826	192.168.1.5	192.168.1.3	DTLSv1.2	188	Application Data
12	3.387930	192.168.1.3	192.168.1.5	DTLSv1.2	224	Application Data
13	3.389688	192.168.1.5	192.168.1.3	DTLSv1.2	188	Application Data
17	4.391205	192.168.1.3	192.168.1.5	DTLSv1.2	224	Application Data
18	4.392062	192.168.1.5	192.168.1.3	DTLSv1.2	188	Application Data

Ethernet II, Src: 0c:03:53:e2:d4:00 (0c:03:53:e2:d4:00), Dst: 0c:03:53:d5:25:00 (0c:03:53:d5:25:00)
 Internet Protocol Version 4, Src: 192.168.1.3, Dst: 192.168.1.5
 User Datagram Protocol, Src Port: 12346, Dst Port: 12346
 Datagram Transport Layer Security
 DTLSv1.2 Record Layer: Application Data Protocol: Application Data
 Content Type: Application Data (23)
 Version: DTLS 1.2 (0xfe9d)
 Epoch: 1
 Sequence Number: 695
 Length: 169
 Encrypted Application Data: 5068f2370d9248357e08a527ab3d42b62dfcb563bbf45d26422ceb4fce3818955c0fb6ec...

```

0000  0c 03 53 d5 25 00 0c 03 53 e2 d4 00 00 45 c0  ..S%...S.....E
0010  00 d2 3d d5 40 00 40 11 78 2d c0 a8 01 03 c0 a8  ..=@@.x.....
0020  01 05 30 3a 30 3a 00 be 5d 79 17 fe fd 00 01 00  ..0:0:..jy.....
0030  00 00 00 02 b7 00 a9 50 68 f2 37 0d 92 48 35 7e  ....P h-7..H5-
0040  08 a5 27 ab 3d 42 b6 2d fc b5 63 bb f4 5d 26 42  ...=B-...c..j&B
  
```

3.12 Verificaciones plano de control

Una vez se ha levantado el plano de control, es importante conocer cómo solucionar errores en caso de que surjan. Para ello, existen diferentes líneas de comando que permiten verificar las conexiones realizadas por los dispositivos, así como acceder a los registros de eventos para analizar lo que sucede dentro de los nodos. A continuación, se presentan los comandos necesarios para llevar a cabo esta tarea:

1. Show control local-properties

Este comando puede ser usado en cualquiera de los dispositivos, ya que, este se encarga de mostrar todas las propiedades esenciales dentro del mismo como; el nombre de la organización, que papel desempeña el equipo, los certificados, así mismo como su

tiempo de vigencia, la dirección IPv4 del vBond y los puertos usados además de las interfaces en uso del dispositivo.

Figura 62

Verificación de propiedades locales.

```
vManage CuaicalA# show control local-properties
personality                               vmanage
sp-organization-name                      cuaical-sdwan
organization-name                         cuaical-sdwan
root-ca-chain-status                      Installed

certificate-status                        Installed
certificate-validity                       Valid
certificate-not-valid-before              Sep 05 17:18:28 2022 GMT
certificate-not-valid-after               Feb 26 17:18:28 2028 GMT

dns-name                                  192.168.1.4
site-id                                   1
domain-id                                 0
protocol                                  dtls
tls-port                                  23456
system-ip                                 1.1.1.1
chassis-num/unique-id                     79actf7c7-fb1f-43ed-b611-b32cbf696b0
serial-num                                 8B73ECD0F13A4B
cloud-hosted                               no
token                                      -NA-
retry-interval                             0:00:00:17
no-activity-exp-interval                   0:00:00:20
dns-cache-ttl                              0:00:02:00
port-hopped                               FALSE
time-since-last-port-hop                   0:00:00:00
number-vbond-peers                         0
number-active-wan-interfaces               1

-----
INSTANCE      INTERFACE  PUBLIC PRIVATE PRIVATE
PRIVATE      IPv4      PORT  IPv4   LAST
PORT         VS/VM    COLOR IPv4   IPv6
STATE        CONNECTION
-----
0             eth0       192.168.1,3 12346 192.168.1,3 2800:370:12f:25e0::1
              12346     1/0  default up          0:00:00:14
```

Este comando de verificación es crucial, como se puede observar en la Figura 62, ya que muestra las configuraciones mínimas necesarias para desplegar cualquier dispositivo. En el recuadro rojo, se puede visualizar el nombre de la organización, el cual debe ser idéntico en todo el plano de control, ya que se utiliza para firmar las conexiones, si este no coincide, el certificado no se instalará y los valores en el cuadro rojo aparecerán como nulos. En el recuadro verde, se muestra la duración del certificado, en este caso tienen una duración hasta el 26 de febrero de 2028. Además, en el recuadro morado, se muestra información detallada del vBond, que es el dispositivo en el que todos los

elementos deben autenticarse, así como también se presentan las conexiones físicas activas para evitar confusiones en el uso de las VPN y su asociación con las interfaces.

2. Show certificate installed

Este comando despliega información acerca del certificado instalado y generado para asegurar las conexiones. En este sentido, en la Figura 63, se muestra el resultado de la ejecución de este, en donde se incluyen parámetros con los cuales fue creado el certificado⁸, además del tiempo de duración de este. En este punto, el parámetro con mayor importancia a verificar es el nombre de la organización(O=cuaical-sdwan) ya que todos los equipos estarán asociados a dicha organización.

Figura 63

Verificación de certificados instalados

```
vManage_CuaicalA# show certificate installed
Server certificate
-----
Certificate:
  Data:
    Version: 1 (0x0)
    Serial Number:
      8b:73:ec:dc:d0:f1:3a:4b
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=SV, ST=SS, L=SS, O=cuaical-sdwan, CN=vmanage.lab
    Not Before: Sep  5 17:18:28 2022 GMT
    Not After: Feb 26 17:10:00 2030 GMT
    Subject: C=US, ST=California, L=San Jose, OU=cuaical-sdwan, O=Viptela LL
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
```

3. Show interface description

⁸ Campos del certificado: C en el certificado, significa country, SV el código para el salvador, ST significa el estado en el cual se encuentra el dispositivo, SS que no es un valor válido, L la entidad emisora del certificado, O el nombre de la organización y CN el nombre del dominio al que pertenece.

Este comando es usado para identificar las interfaces en uso del equipo, la importancia de este comando es verificar el estado de las interfaces, además de mostrar el nombre de estas. La información que despliega el comando es de relevancia puesto que al realizar las configuraciones iniciales, las interfaces que se muestran en la simulación no coinciden con las que autoidentifica el equipo, con lo cual se debe conocer como las reconoce el sistema.

Figura 64

Verificación de interfaces de los equipos

```
vManage_CuaicalA# show interface description
```

VPN	INTERFACE	AF TYPE	IP ADDRESS	IF ADMIN STATUS	IF OPER STATUS	IF TRACKER STATUS	DESC
0	eth0	ipv4	192.168.1.3/24	Up	Up	-	-
0	system	ipv4	1.1.1.1/32	Up	Up	-	-

La Figura 64 muestra (remarcado en rojo) la información proporcionada por el comando, en este caso el nombre de la interfaz (**INTERFACE**), así como las direcciones IPv4 (**IP ADDRESS**), el estado de las interfaces (**IF ADMIN STATUS**), además de la VPN a la cual pertenece dicha interfaz (**VPN**) y de esta manera identificar los datos que se mostraran dentro del dashboard del vManage.

Además, el comando `show interface | tab`, tiene un uso similar, sin embargo, proporciona información más detallada acerca de las interfaces, con lo cual en la Figura 65 se muestra la ejecución de este comando, en donde se despliega información como: la VPN a la que pertenece (**VPN**), el nombre de la interfaz (**INTERFACE**), el tipo de direccionamiento de capa III (**AF TYPE**), la propia dirección IPv4 de la interfaz (**IP**

ADDRESS), el estado de la interfaz, es decir si se encuentra encendida o apagada en el sistema (IF ADMIN STATUS), el tipo de encapsulamiento (ENCAP TYPE), la dirección MAC de la interfaz(HWADDR), la velocidad de operación de la interfaz (SPEED MBPS), el tipo de conexión (DUPLEX) y el número de paquetes transmitidos (TX PACKETS).

Figura 65

Verificación extendida de interfaces

VPN	INTERFACE	AF TYPE	IP ADDRESS	IF ADMIN STATUS	IF OPER STATUS	IF TRACKER STATUS	ENCAP TYPE	PORT TYPE	MTU	HWADDR	SPEED MBPS	DUPLEX	TCP MSS ADJUST	UPTIME	RX PACKETS	TX PACKETS
0	eth0	ipv4	192.168.1.3/24	Up	Up	-	null	transport	1500	0c:05:53:e2:d4:00	1000	full	-	0:00:36:04	10069	11190
0	system	ipv4	1.1.1.1/32	Up	Up	-	null	loopback	-	-	-	-	-	0:00:37:49	0	0

4. Show control connections

Este comando muestra información general acerca de las conexiones, como son; el dispositivo al que se conecta, la dirección de **loopback** con la cual se identifica, la dirección IPv4 pública con la cual puede ser alcanzado el nodo, el nombre de la organización a la que pertenece y el color del enlace.

Figura 66

Verificación de conexiones vManage

```
vManage_CuaicalA# show control connections
```

INDEX	TYPE	PEER REMOTE	PEER COLOR	PEER SYSTEM IP STATE	PEER CONFIGURED SYSTEM IP UPTIME	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER		PEER PUB PORT	PEER ORGANIZATION
									PORT	PUBLIC IP		
0	vsmart	dtls 3.3.3.3		up 3.3.3.3 0:00:09:15		1	1	192.168.1.5	12346	192.168.1.5	12346	cuaical-sdwan
0	vbond	dtls 2.2.2.2		up 2.2.2.2 0:00:09:16		0	0	192.168.1.4	12346	192.168.1.4	12346	cuaical-sdwan
1	vbond	dtls 0.0.0.0		up - 0:00:09:16		0	0	192.168.1.4	12346	192.168.1.4	12346	cuaical-sdwan

La salida de este comando se muestra en la Figura 66, en donde remarcado de color verde, se evidencia el dispositivo con el que ya se ha establecido conexión, además

del protocolo de comunicación segura usado para establecer esta (**PEER TYPE**, **PEER PROT**, **PEER SYSTEM IP**), de color rojo se muestra la dirección IPv4 con la cual fue configurado el sistema del dispositivo remoto, de morado se remarca la dirección IPv4 con la cual se alcanza el equipo, de la misma manera se identifica el puerto de capa transporte (**PEER PRIV PORT**, **PEER PUBLIC IP**) por el cual se realiza la conexión; finalmente, de color amarillo se encuentra la organización a la que pertenece el mismo (**ORGANIZATION**).

5. Show orchestrator summary

Este comando solo puede ser usado dentro del vBond, puesto que, es el “orquestador” de las conexiones, de esta manera el comando muestra la información de todos los túneles establecidos en el cluster de controladoras y hacia el plano de datos.

Figura 67

Verificación de conexiones en vBond

```
vBond_CuaicalA# show orchestrator connections
```

INSTANCE	PEER TYPE	PEER PROTOCOL	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIVATE PORT	PEER PUBLIC IP	PEER PUBLIC PORT	REMOTE COLOR	STATE	ORGANIZATION NAME	UPTIME
0	vsmart	dtls	3.3.3.3	1	1	192.168.1.5	12346	192.168.1.5	12346	default	up	cuaical-sdwan	0:01:05:49
0	vmanage	dtls	1.1.1.1	1	0	192.168.1.3	12346	192.168.1.3	12346	default	up	cuaical-sdwan	0:00:51:43

El resultado de la ejecución del comando se muestra en la Figura 67, en donde se evidencia información similar al comando mostrado en el ítem 4, la diferencia principal es la forma en la que esta es presentada, ya que, se muestra ordenada de mejor manera, tal que, cada equipo puede ser identificado claramente, así mismo como las conexiones, puertos y nombre de organización, cabe mencionar que aparece nueva información como el ID de sitio, y el ID del dominio (**SITE ID**, **DOMAIN ID**). Además, el tiempo de actividad

de dicha conexión, este parámetro puede ser de vital importancia cuando existen desconexiones del plano de control.

6. Monitor start /var/log/vsyslog

Este comando permite visualizar de manera activa los eventos (logs) que ocurren en la operatividad de la red, específicamente para las conexiones, con lo cual, en caso de existir fallas en el plano de control, serán registradas en este apartado.

Figura 68

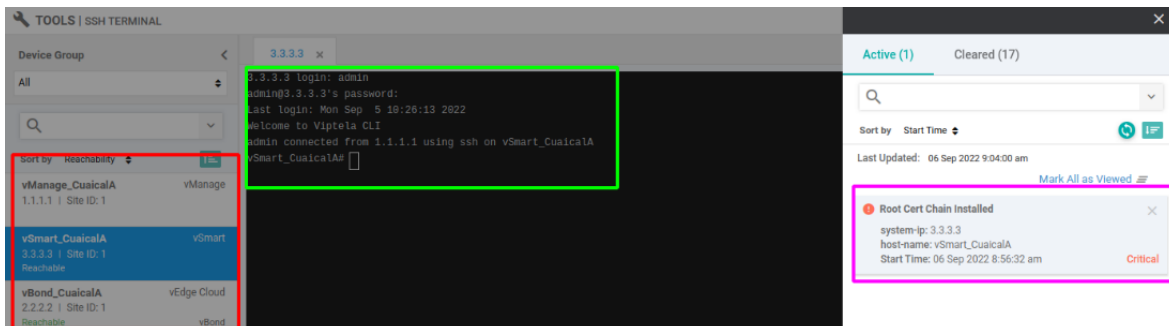
Verificación de LOGS desde el vBond

```
vBond_CuaicalA# show orchestrator-connections log:local7.info: Sep  6 08:56:14 vBond_CuaicalA VBOND[2484]: %Viptela-vBond_CuaicalA-vbond_0-6-INFO-1400002: Notification: 9/6/2022 13:56:14 control-connection-state-change severity-level:major host-name:"vBond_CuaicalA" system-ip:2.2.2.2 personality:vbond peer-type:unknown peer-system-ip::: peer-vmanage-system-ip::: public-ip:192.168.1.5 public-port:12346 src-color:default remote-color:default uptime: 0:00:00:00 new-state:up
log:local7.info: Sep  6 08:56:19 vBond_CuaicalA VBOND[2484]: %Viptela-vBond_CuaicalA-vbond_0-6-INFO-1400002: Notification: 9/6/2022 13:56:19 control-connection-state-change severity-level:major host-name:"vBond_CuaicalA" system-ip:2.2.2.2 personality:vbond peer-type:vsmart peer-system-ip:3.3.3.3 peer-vmanage-system-ip:0.0.0.0 public-ip:192.168.1.5 public-port:12346 src-color:default remote-color:default uptime: 0:00:00:04 new-state:down
log:local7.info: Sep  6 08:56:19 vBond_CuaicalA VBOND[2484]: %Viptela-vBond_CuaicalA-vbond_0-6-INFO-1400002: Notification: 9/6/2022 13:56:19 control-no-active-vsmart severity-level:critical host-name:"vBond_CuaicalA" system-ip:2.2.2.2 personality:vbond
log:local7.info: Sep  6 08:56:19 vBond_CuaicalA VBOND[2484]: %Viptela-vBond_CuaicalA-vbond_0-6-INFO-1400002: Notification: 9/6/2022 13:56:19 control-connection-state-change severity-level:major host-name:"vBond_CuaicalA" system-ip:2.2.2.2 personality:vbond peer-type:unknown peer-system-ip::: peer-vmanage-system-ip::: public-ip:192.168.1.5 public-port:12346 src-color:default remote-color:default uptime: 0:00:00:00 new-state:up
```

La Figura 68 muestra la respuesta del comando `monitor start /var/log/vsyslog`, con estos logs dentro del vBond o cualquier equipo se pueden tomar acciones tempranas, ya que muestra información como el dispositivo de origen (`host-name "vBond_CuaicalA" system-ip:2.2.2.2 personality:vbond peer-type:unknown peer-system-ip::: peer-vmanage-ip::: public-ip:192.168.1.5 public-port:12346`), la dirección IPv4 de este y el estado que cambió, es decir si la conexión cambia de up a down o viceversa (`Notification: 9/6/2022 control-connection-state-change severity-level: major`), esta misma información es presentada gráficamente dentro del dashboard del vManage tal como se muestra remarcado en morado en la Figura 69, en este caso se ha registrado un evento en el equipo con IP de sistema 3.3.3.3.

Figura 69

Verificación de control centralizado



Además, dentro de la interfaz web del vManage, en el dashboard principal (ver Figura 69), se encuentra el apartado de herramientas (Tools). Desde allí, se puede acceder a todos los dispositivos de la red SDWAN; esto brinda un control centralizado. Resaltado en rojo, se muestra en la Figura 69, la opción de iniciar sesión de forma segura mediante SSH en cada uno de los equipos del clúster de control. Por otro lado, en el recuadro verde, se destaca la capacidad de acceder a dichos equipos y enviar comandos para su configuración. Es importante destacar que esta interfaz web del vManage garantiza la seguridad de la comunicación mediante el uso del protocolo DTLS. En este sentido, para evidenciar el intercambio de mensajes del protocolo DTLS entre las controladoras vManage (192.168.1.3) y vSmart (192.168.1.5) por el puerto UDP 12346, la Figura 70 muestra una captura de paquetes utilizando la herramienta Wireshark en un enlace entre las controladoras.

Figura 70

Captura de paquetes en plano de control entre vManage y vSmart

No.	Time	Source	Destination	Protocol	Length	Info
272	47.013242	192.168.1.5	192.168.1.3	DTLSv1.2	188	Application Data
279	48.017306	192.168.1.3	192.168.1.5	DTLSv1.2	224	Application Data
280	48.017882	192.168.1.5	192.168.1.3	DTLSv1.2	188	Application Data
281	48.733711	192.168.1.5	192.168.1.3	DTLSv1.2	311	Application Data
282	48.737161	192.168.1.3	192.168.1.5	DTLSv1.2	143	Application Data
283	48.739160	192.168.1.3	192.168.1.5	DTLSv1.2	247	Application Data
284	48.782023	192.168.1.5	192.168.1.3	DTLSv1.2	143	Application Data
285	49.025913	192.168.1.3	192.168.1.5	DTLSv1.2	224	Application Data
286	49.026554	192.168.1.5	192.168.1.3	DTLSv1.2	188	Application Data

```

> Frame 279: 224 bytes on wire (1792 bits), 224 bytes captured (1792 bits) on interface -, id 0
> Ethernet II, Src: 0c:03:53:e2:d4:00 (0c:03:53:e2:d4:00), Dst: 0c:03:53:d5:25:00 (0c:03:53:d5:25:00)
> Internet Protocol Version 4, Src: 192.168.1.3, Dst: 192.168.1.5
> User Datagram Protocol, Src Port: 12346, Dst Port: 12346
  Datagram Transport Layer Security
  
```

3.13 Despliegue de vEdge

La configuración de los equipos de acceso “vEdge” presenta desafíos adicionales debido a su compleja topología, que incluye múltiples enlaces de transporte en contraste con el plano de control, que solo tiene un enlace de transporte. Por lo tanto, se requiere una configuración minuciosa para garantizar un acceso adecuado a la red superpuesta. Aunque la implementación inicial del vManage, vSmart y vBond generalmente no presenta problemas de configuración, el vEdge requiere un enfoque más cuidadoso para garantizar una conexión correcta y su integración efectiva.

El proceso de configuración del vEdge se resume en los siguientes pasos: En primer lugar, se deben realizar las configuraciones iniciales del sistema, como ingresar nombres, identificaciones y sitios en el equipo, así como la dirección IPv4. Luego, es necesario activar la comunicación a través del túnel 0. La diferencia principal con las configuraciones anteriores (vManage, vBond y vSmart) radica en la necesidad de agregar un color al enlace de transporte para el uso del protocolo TLOC.

Para realizar la configuración inicial dentro del equipo vEdge, se debe ingresar por consola al mismo, debido a que no tiene ninguna dirección IPv4 en las interfaces, con lo cual las configuraciones iniciales se encargarán de brindar conectividad dentro de la red.

Figura 71

Líneas de comando para configuración de vEdge desde consola

```
config
system
host-name vEdge-Cuaical-Prueba
system-ip 4.4.4.4
site-id 1
admin-tech-on-failure
organization-name cuaical-sdwan
clock timezone America/Bogota
vbond 192.168.1.4
exit
vpn 0
interface ge0/0
ip address 192.168.1.6/24
no shutdown
```

En la Figura 71 se muestran las configuraciones necesarias que se deben realizar en cada uno de los nodos vEdge. Estas configuraciones deben ejecutarse desde la consola de cada equipo. A continuación, se detallan los pasos a seguir:

1. Cambiar el nombre del nodo por el nombre deseado(**host-name**): Se debe modificar el nombre del nodo para que identifique su función, por ejemplo, Spoke, HUB entre otros.
2. Ingresar la dirección del sistema para identificar el nodo(**system-ip**): Consultar la Tabla 6 y proporcionar la dirección correspondiente para identificar el nodo.
3. Ingresar el identificativo para el sitio(**site-id**): El identificativo del sitio debe ingresarse de acuerdo con criterios propios.

4. Ingresar el nombre de la organización (**organization-name**): Se debe tener precaución con este campo, puesto que si no se ingresa el mismo **organization-name** que, en el plano de control, no se podrá agregar el nodo a la red.
5. Asignar la interfaz y la dirección IPv4: Se debe asignar la interfaz y la dirección IPv4 específica para cada equipo para que sea posible la comunicación entre los equipos.

Figura 72

Verificación de certificados

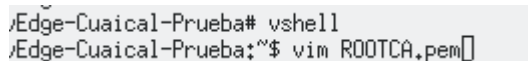
```
vEdge-Cuaical-Prueba# show certificate serial
Certificate not yet installed ... giving up.
Chassis number: cabrae0c-bb11-4da3-a3fb-23e74f4f361c serial number:
vEdge-Cuaical-Prueba#
```

Posterior a las configuraciones básicas, se debe verificar los certificados instalados como se muestra en la Figura 72, en donde se evidencia que el equipo va a ser ingresado a la red por primera vez, ya que, no tiene ningún certificado previamente instalado (**Certificate not yet installed**), con lo cual se deben instalar uno para que pueda pertenecer a un dominio SD-WAN.

Para ingresar el certificado al nuevo equipo vEdge, se debe ingresar por consola al vManage y copiar el contenido del fichero **ROOTCA.pem**, el cual contiene la llave pública para realizar la comunicación segura con DTLS, una vez copiado dicho contenido se debe crear el mismo fichero dentro del nuevo dispositivo (**ROOTCA.pem**) como se muestra en la Figura 73.

Figura 73

Creación de archivo contenedor de la llave pública



```

/Edge-Cuaical-Prueba# vshell
/Edge-Cuaical-Prueba:~$ vim ROOTCA.pem
  
```

Para realizar el proceso mencionado, es necesario seguir los siguientes pasos:

1. Acceder al Shell del dispositivo desde el modo privilegiado del equipo utilizando el comando "vshell".
2. Crear un archivo llamado "ROOTCA.pem" utilizando el comando "vim". Este archivo servirá para almacenar la llave correspondiente.
3. Una vez creado el archivo, copiar el contenido de la llave pública desde el vManage.
4. Insertar el contenido de la llave pública en el archivo "ROOTCA.pem" previamente creado.

Una vez copiado el certificado, se debe realizar la instalación de este con el comando `request root-cert-chain install /home/admin/ROOTCA.pem9`, con lo cual debe instalarse satisfactoriamente para la VPN0. El resultado de la ejecución del comando se muestra en la Figura 74, en donde se evidencia la instalación satisfactoria del certificado, en caso de fallar dicha instalación, se debe tomar acciones de acuerdo con la salida de los logs mostrados por la misma terminal.

⁹ Este comando específico indica al dispositivo que instale la cadena de certificados de raíz que se encuentra en el archivo "/home/admin/ROOTCA.pem". La cadena de certificados de raíz se utiliza para validar la autenticidad de los certificados emitidos por la autoridad de certificación raíz. Al instalar esta cadena de certificados de raíz, el dispositivo podrá verificar y confiar en los certificados emitidos por dicha autoridad de certificación al establecer conexiones seguras.

Figura 74

Instalación del certificado

```
vEdge-Cuaical-Prueba# request root-cert-chain install /home/admin/ROOTCA.pem
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/ROOTCA.pem via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
vEdge-Cuaical-Prueba#
```

Para activar el equipo desde el vManage, es necesario solicitar una SmartAccount que proporcione acceso a las licencias demostrativas de los equipos necesarios. Con la SmartAccount, se podrá buscar y obtener la plantilla específica del equipo requerido para que sea cargada en el vManage, lo que permitirá ingresar y activar equipos en la red.

Para llevar a cabo la solicitud SmartAccount al fabricante Cisco, es necesario crear una SmartAccount, y posteriormente crear un perfil para los equipos deseados. A continuación, se debe configurar una cuenta virtual, en este caso se la ha nombrado **SD-WAN**, tal como se muestra en la Figura 75. Esta cuenta virtual debe ser cargada en el vManage con las licencias de los equipos vEdge a desplegarse, ya que contiene los números de serie y chasis, necesarios para el despliegue del plano de datos de la red. Si no se realiza este proceso, no será posible obtener los números de serie y chasis, lo que impediría el despliegue adecuado de la red.

Figura 75

Cuenta usada para el desarrollo del trabajo

Virtual Accounts

Create Virtual Account Delete Selected... Export Selected...

Is there a question we can help you with?
 Type your question here Ask
 Not Now

Virtual Account	Description	Tags	Users			
<input type="checkbox"/> DEFAULT	This is the default virtu...	-	1	-	PUBLIC	Actions
<input type="checkbox"/> SD-WAN	SD-WAN Cuaical Adonis	-	1	-	PRIVATE	Actions

Filter by Virtual Account Name Filter by description

Figura 76

Detalles adicionales del perfil de vBond

Add Controller Profile

STEP 1 ✓ Profile Type

STEP 2 Profile Settings

STEP 3 Review

STEP 4 Confirmation

Profile Settings:

* Profile Name: VBOND_CUAICALA

Description: Description of this profile (optional)

En este sentido, el único equipo que debe ser ingresado a la SmartAccount es el vBond, tal como se muestra en la Figura 76. Para ello, se deben proporcionar la organización, el nombre del equipo y la dirección IPv4 que se configuró previamente en el equipo vBond, tal como se visualiza en la Figura 77.

Figura 77**Configuración del perfil de vBond**

Add Controller Profile

STEP 1 ✓ Profile Type | STEP 2 Profile Settings | STEP 3 Review | STEP 4 Confirmation

Profile Settings:

- Profile Name: VBOND_CUAICALA
- Description: *Description of this profile (optional)*
- Default Profile: Yes
- Deployment Type: Customer Hosted
- Multi-Tenancy: No
- Organization Name: cuaical-sdwan
- Primary Controller:
 - IPv4: DTLS:// 192.168.1.4 12346
 - Server Root CA: *Max file size up to 1 MB or max characters not to exceed 1048576* [Browse](#)

En caso de no colocar los mismos valores establecidos en el sistema propio del vBond, el establecimiento de las conexiones no será posibles, ya que no se podrá encontrar el equipo configurado en la Figura 77, ya que los nombres de organización e ID's no coincidirán.

Figura 78

Perfiles virtuales de equipos

Devices | Controller Profiles | Network | Certificates | Manage External Virtual Account | Event Log | Transactions

+ Add Devices... + Add Software Devices... Edit Selected... Delete Selected... Enable External Management... Transfer selected...

Serial Number	Base PID	Product Group	Controller	Last Modified	Status	Actions
5C758E54-638D-F242-1...	VEDGE-CLOUD-DNA	Router	VBOND_CUAICALA	2022-Sep-12, 13:01:17	Pending for publish	Show Log...
FDD5EB9A-9267-DB06-5...	VEDGE-CLOUD-DNA	Router	VBOND_CUAICALA	2022-Sep-12, 13:01:17	Pending for publish	Show Log...
9FC7865D-EEA5-34DC-...	VEDGE-CLOUD-DNA	Router	VBOND_CUAICALA	2022-Sep-12, 13:01:17	Pending for publish	Show Log...
1C542191-C161-72AD-A...	VEDGE-CLOUD-DNA	Router	VBOND_CUAICALA	2022-Sep-12, 13:01:17	Pending for publish	Show Log...
4B49A038-BC81-C419-9...	VEDGE-CLOUD-DNA	Router	VBOND_CUAICALA	2022-Sep-12, 13:01:17	Pending for publish	Show Log...
E7C04E05-A450-D0B9-B...	VEDGE-CLOUD-DNA	Router	VBOND_CUAICALA	2022-Sep-12, 13:01:17	Pending for publish	Show Log...

Por otra parte, los perfiles virtuales de los equipos vEdge mostrados en la Figura 78 son los que se usarán dentro de la topología propuesta, de esta manera, se evidencia la creación de un número de chasis y serie para los equipos virtuales. Nótese que los equipos aún no pueden ser usados debido a que la solicitud de aprovisionamiento está pendiente, con lo cual se debe esperar alrededor de 5 minutos para su aprovisionamiento.

Figura 79

Verificación de perfiles activos

<input type="checkbox"/>	5C758E54-638D-F242-1...	VEDGE-CLOUD-DNA	Router	VBOND_CUAICALA	2022-Sep-12, 13:02:04	Provisioned	Show Log... ▼
<input type="checkbox"/>	FDD5EB9A-9267-DB06-5...	VEDGE-CLOUD-DNA	Router	VBOND_CUAICALA	2022-Sep-12, 13:02:04	Provisioned	Show Log... ▼
<input type="checkbox"/>	9FC7865D-EEA5-34DC-...	VEDGE-CLOUD-DNA	Router	VBOND_CUAICALA	2022-Sep-12, 13:02:04	Provisioned	Show Log... ▼
<input type="checkbox"/>	1C542191-C161-72AD-A...	VEDGE-CLOUD-DNA	Router	VBOND_CUAICALA	2022-Sep-12, 13:02:04	Provisioned	Show Log... ▼
<input type="checkbox"/>	4B49A038-BC81-C419-9...	VEDGE-CLOUD-DNA	Router	VBOND_CUAICALA	2022-Sep-12, 13:02:04	Provisioned	Show Log... ▼
<input type="checkbox"/>	E7C04E05-A450-D0B9-B...	VEDGE-CLOUD-DNA	Router	VBOND_CUAICALA	2022-Sep-12, 13:02:04	Provisioned	Show Log... ▼
<input type="checkbox"/>	11358BC8-F22E-8212-8E...	VEDGE-CLOUD-DNA	Router	VBOND_CUAICALA	2022-Sep-12, 13:02:04	Provisioned	Show Log... ▼
<input type="checkbox"/>	86E226EB-C047-1F70-2...	VEDGE-CLOUD-DNA	Router	VBOND_CUAICALA	2022-Sep-12, 13:02:04	Provisioned	Show Log... ▼
<input type="checkbox"/>	80A83EC9-027E-96F5-C...	VEDGE-CLOUD-DNA	Router	VBOND_CUAICALA	2022-Sep-12, 13:02:04	Provisioned	Show Log... ▼
<input type="checkbox"/>	35B29E36-F9C4-900B-C...	VEDGE-CLOUD-DNA	Router	VBOND_CUAICALA	2022-Sep-12, 13:02:04	Provisioned	Show Log... ▼

En este punto, tal como se muestra en la Figura 79, los equipos han sido provisionados, lo que significa que ahora es posible utilizar el número de chasis y la serie del equipo virtual. Una vez que se haya completado esta configuración, se debe acceder al perfil de la controladora previamente creado y descargar el archivo de aprovisionamiento con extensión `viptela`. A continuación, se debe cargar el archivo en la controladora; para ello, en la sección de dispositivos, seleccionar la opción "Upload WAN Edge List" (Subir una lista de WAN Edge) y cargar el archivo `.viptela` descargado anteriormente. Y luego, confirmar la carga del documento. Siguiendo estos pasos, los dispositivos deberían estar disponibles en el vManage, tal como se muestra en la Figura 80, donde se muestra los números de serie y chasis solicitados, de esta manera se remarca de color verde los campos que se usarán para poder agregar un vEdge a la red superpuesta..

Figura 80

Dispositivos disponibles en el vManage

Device Model	Chassis Number	Serial No./Token
vEdge Cloud	9fc7865d-eea5-34dc-dfe2-639b5c5c0a2f	Token - 0f75188e16abc4662abf1357c6c9981e
vEdge Cloud	1c542191-c161-72ad-a9fe-9d06caf225...	Token - 8562fface3a6bfb52659e09d4757384e
vEdge Cloud	4b49a038-bc81-c419-9f22-912bc5607...	Token - 1aee05c1a5d4a83148c51f3b8bc1ec99
vEdge Cloud	e7c04e05-a450-d0b9-b6e2-7424b3626...	Token - 056bdc89fc22fce7f518bb1cb7e47c49
vEdge Cloud	11358bc8-f22e-8212-8ed2-fc3fc7cc883c	Token - 786d05900836ea5858d2d5f7242ae970
vEdge Cloud	86e226eb-c047-1f70-2b47-84096c9c5d...	Token - 06d85e4aaee5b1b9248f6ac2e5b8bbeb
vEdge Cloud	80a83ec9-027e-96f5-cb85-e3eb5691bd...	Token - cca3589632b8f3a2438aaa8a139943de
vEdge Cloud	35b29e36-f9c4-900b-c917-f2af2c1c1e60	Token - dee222fd5f25ca2e4398095834c24c07
vEdge Cloud	5c758e54-638d-f242-1c0c-52b333427a...	Token - 5dc03a33586bb935ecca7beb0dbee0ea
vEdge Cloud	ffd5eb9a-9267-db06-5bfb-1b8869c4a2...	Token - 0dde77af64a77de5b8280032a58bfa7

Figura 81

Campos de equipos provisionados

```
#cloud-config
vinitparam:
- uuid : 9fc7865d-eea5-34dc-dfe2-639b5c5c0a2f
- vbond : 192.168.1.4
- otp : 0f75188e16abc4662abf1357c6c9981e
- org : cuaical-sdwan
```

En este sentido, se elige uno de los equipos disponibles, desplegándose la información que se muestra en la Figura 81, en donde los campos uuid y otp, son el token y el número de chasis respectivamente, dichos campos se usarán para agregar el equipo a la red superpuesta, de esta manera se debe ingresar dichos datos en el vEdge de acuerdo con los siguientes pasos:

1. Activar la comunicación mediante IPsec a la interfaz conectada mediante la VPN0 y agregar un color al enlace usado.

Figura 82

Activando la comunicación cifrada en el equipo

```
vEdge-Cuaical-Prueba(config)# vpn 0
vEdge-Cuaical-Prueba(config-vpn-0)# interface ge0/0
vEdge-Cuaical-Prueba(config-interface-ge0/0)# tunnel-interface
vEdge-Cuaical-Prueba(config-tunnel-interface)# encapsulation ipsec
vEdge-Cuaical-Prueba(config-tunnel-interface)# color biz-internet
vEdge-Cuaical-Prueba(config-tunnel-interface)#
```

El encapsulamiento se activa directamente en la interfaz utilizada, como se muestra en la Figura 82. Para lograrlo, primero se accede a la configuración del sistema con el comando "config". Una vez dentro, se ingresa a la VPN 0 y luego se accede a la interfaz a la cual se desea activar los túneles (en este caso, la "ge0/0"). Finalmente, dentro de la interfaz, se activa el túnel utilizando el comando "tunnel-interface". Además, es necesario especificar el tipo de encapsulamiento que tendrán los túneles, en este caso se utiliza el encapsulamiento `ipsec`. Por último, se asigna un color al transporte, en este caso se utiliza "biz-internet", dicha opción tiene la característica que permite realizar NAT a las conexiones.

2. Solicitar autorización mediante el chassis y token dentro del vEdge para que se autorice el ingreso del equipo a la red.

Figura 83

Activación del equipo

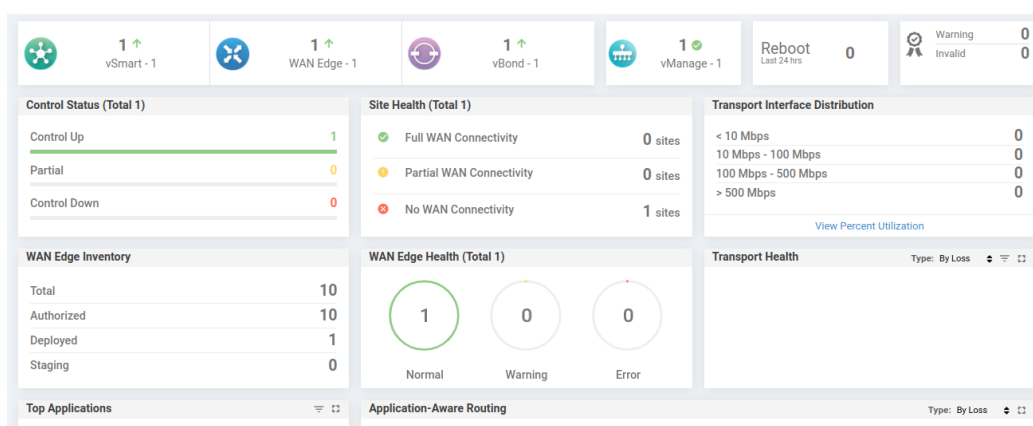
```
vEdge-Cuaical-Prueba# request vedge-cloud activate chassis-number 9fc7865d-eea5-34dc-dfe2-639b5c5c0a2f token 0
f75188e16abc4662abf1357c6c9981e
```

La solicitud de ingreso a la red se realiza ejecutando el comando mostrado en la Figura 83(`request vedge-cloud activate chassis-number # token #`). En esta

etapa, se solicita al vBond la petición de activación para el vEdge, utilizando el número de chasis y el token correspondientes. Es importante destacar que, si los valores ingresados en estos campos no coinciden con los previamente cargados en la lista de WAN Edge, la solicitud no será aceptada por la red OMP.

Figura 84

Vista desde el plano de control



En este sentido, al ingresar por la interfaz web mediante la URL: <https://192.168.1.3:8443>, la Figura 84, muestra que el plano de control ya detectó el nuevo equipo ingresado (WAN Edge ahora registra el valor 1), lo cual significa que ya puede ser monitoreado y controlado de manera segura mediante el protocolo DTLS. En caso de seguir ingresando más equipos, el valor de WAN Edge incrementará.

Figura 85**Conexiones de vEdge**

```
vEdge-Cuaical-Prueba# show control connections
```

CONTROLLER				PEER				PEER					
PEER	PEER	PEER	SITE	DOMAIN	PEER	PEER	PUB	PEER	PEER	PEER	PEER		
GROUP	GROUP	GROUP			PRIV	PEER		LOCAL	COLOR	PROXY	STATE	UPTIME	
TYPE	PROT	SYSTEM	ID	ID	PRIVATE	IP	PORT	PORT					
ID		IP			IP								
vsmart	dtls	3.3.3.3	1	1	192.168.1.5		12346	192.168.1.5	12346	biz-internet	No	up	0:00:0
6:23	0												
vbond	dtls	0.0.0.0	0	0	192.168.1.4		12346	192.168.1.4	12346	biz-internet	-	up	0:00:0
6:24	0												
vmanage	dtls	1.1.1.1	1	0	192.168.1.3		12346	192.168.1.3	12346	biz-internet	No	up	0:00:0
6:23	0												

```
vEdge-Cuaical-Prueba#
```

Por otro lado, la Figura 85 muestra el resultado del comando **show control connections**; es decir, las conexiones establecidas al desplegar un vEdge, en este sentido, se observa que el número de túneles generados por cada nodo puede llegar a ser excesivo, ya que en este caso, con un solo equipo y un único enlace físico de transporte se generan 3 conexiones; en general el número de túneles obedece a la Ec.2.

Además, es importante tener en cuenta que al agregar una cantidad considerable de vEdges, junto con las conexiones a vManage, vSmart y vBond, se requerirá manejar las conexiones entre los pares de vEdges. Esto implica asignar más recursos lo cual tendrá un impacto directo en los costos asociados para el despliegue de una red de este tipo.

Es necesario considerar cuidadosamente los recursos y costos adicionales que conlleva el aumento de vEdges en la red, ya que esto puede tener implicaciones significativas en la planificación y gestión de la infraestructura.

3.14 Despliegue de red MPLS

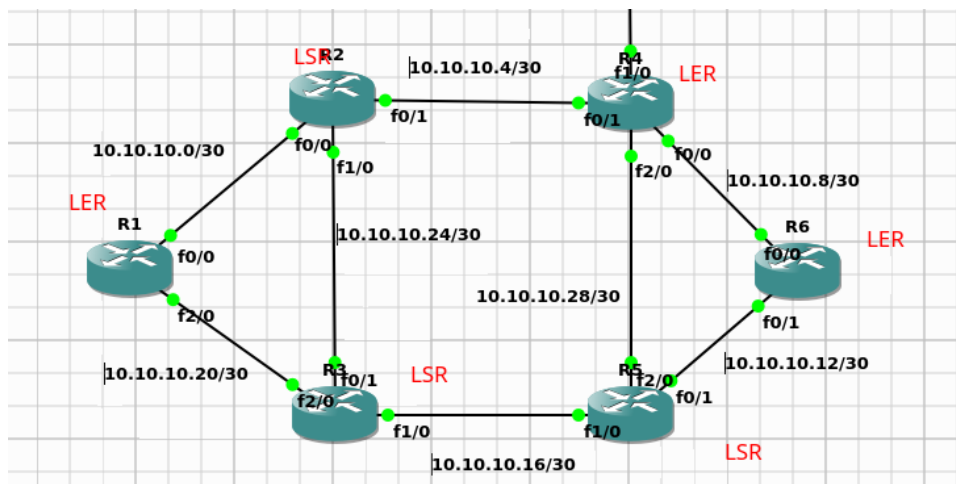
Para el despliegue de la red híbrida, se necesita una infraestructura de red MPLS que permita la correcta dirección del tráfico de interés, en este caso el proveniente de servicios en tiempo real, como, por ejemplo, tráfico con RTMP (Real Time Messaging

Protocol). En este caso, se considerarán 6 equipos de la marca Cisco, modelo c3725, los cuales soportan la tecnología MPLS.

La topología definida para la configuración MPLS se muestra en la Figura 86, donde cada equipo se nombra de acuerdo con su función. De este modo, LER se asigna a los routers R1, R6 y R4 ya que se encargarán de las acciones de push y pop de las etiquetas. Por otro lado, los routers restantes se encargarán de conmutar las etiquetas y de eliminarlas de acuerdo con el método PHP (Penultimate Hop Popping). Además, en la Figura 86, se presentan las subredes utilizadas para la configuración de las interfaces; el prefijo elegido para los enlaces entre los equipos es /30, ya que solo permite dos hosts en la subred, y de esta manera hacer un uso eficiente del pool de direcciones IPv4 elegido.

Figura 86

Topología de red para MPLS

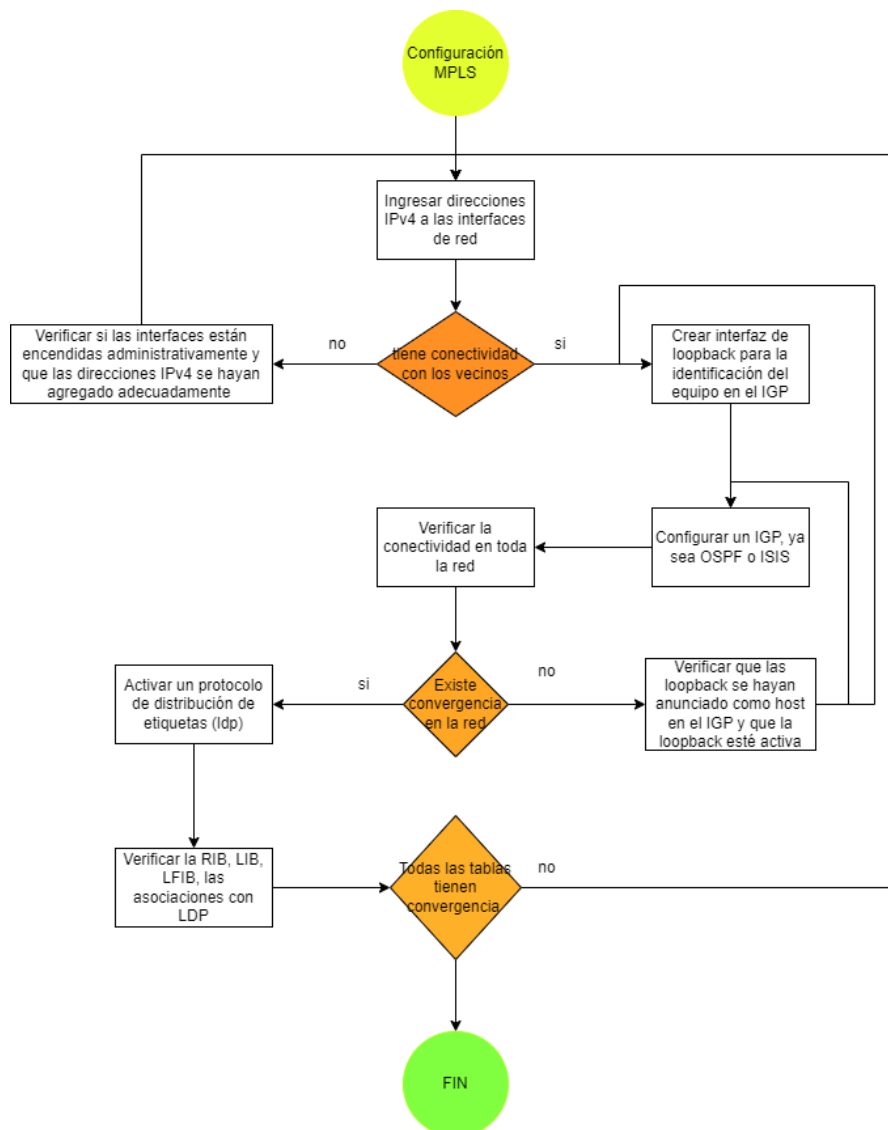


En la Tabla 6 se encuentra el detalle del direccionamiento IPv4 asignado a cada equipo e interfaz. Para este propósito, se ha asignado el pool de direcciones 10.10.10.0/24, el cual es suficiente para alojar 8 subredes punto a punto y 2 subredes con capacidad para 6 hosts cada una. Es importante destacar que se ha optado por utilizar

direccionamiento privado para evitar el uso de direcciones IPv4 ruteables en internet. En consonancia el direccionamiento elegido cumple con las recomendaciones establecidas en el RFC 1918.

Figura 87

Proceso de configuración MPLS



El proceso mostrado en la Figura 87, está definido para la configuración adecuada de MPLS de acuerdo con (cisco, 2005) en este sentido como ejemplo, a continuación, se detalla dicho proceso para el equipo R1:

1. Ingreso de direcciones IPv4 a las interfaces definidas en los equipos.

Para el ingreso de una dirección IPv4 en la interfaz deseada, es necesario acceder al equipo vía consola; una vez dentro, digitar el comando **enable** y posteriormente ingresar a la configuración global, de este modo se ingresa a la interfaz deseada y se asigna la dirección junto con su máscara de red; finalmente se activa administrativamente dicha interfaz, en la Figura 88 se muestra un ejemplo visual de este proceso.

Figura 88

Ingreso de dirección IPv4 a interfaz

```
R1#  
R1#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#interface Fa0/0  
R1(config-if)#ip address 10.10.10.1 255.255.255.252  
R1(config-if)#no shut  
R1(config-if)#
```

2. Crear una interfaz de loopback en cada equipo.

Una interfaz de loopback brinda estabilidad y continuidad en la identificación del equipo dentro de la operación de una red MPLS, cosa que no ocurre con una interfaz física. La creación de dicha interfaz se muestra detalladamente en la Figura 89.

Figura 89

Creación de Loopback

```
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#  
R1(config)#interface loopba  
R1(config)#interface loopback 0  
R1(config-if)#ip address 20.20.20.1 255.255.255.255  
R1(config-if)#no shut  
R1(config-if)#
```

3. Activar un protocolo de distribución de etiquetas LDP.

Este paso es de suma importancia para la configuración de MPLS, ya que este protocolo es el encargado de compartir las etiquetas en cada uno de los equipos y de esta manera generar un LSP (Label Switched Paths). Sin este paso, las etiquetas no se distribuirán a los nodos vecinos. En este sentido, para llevar a cabo esta configuración, es necesario dentro de la configuración global ingresar el comando `mpls label protocol ldp`.

4. Configurar un protocolo de enrutamiento interior (IGP).

Se ha elegido el protocolo OSPF como el IGP (Interior Gateway Protocol) debido a que proporciona una visión completa de toda la red y permite calcular los LSP. Además, dado que la red propuesta no es muy extensa, no presenta problemas para este protocolo de enrutamiento interior.

No obstante, en caso de tratarse de una red de gran envergadura, (Huawei, 2019), recomienda considerar el uso del protocolo ISIS. Este protocolo es especialmente adecuado para redes más grandes, ya que ofrece ventajas y capacidades específicas en términos de escalabilidad y eficiencia en el enrutamiento.

En este sentido, para la configuración de OSPF, desde la configuración global del equipo, se accede a cada una de las interfaces que se desea agregar al protocolo de enrutamiento dinámico. En cada una de estas interfaces, se ingresan los comandos "`ip ospf network point-to-point`" y "`ip ospf 101 area 0`". De esta manera, se logra una configuración eficiente de este protocolo, ya que se define explícitamente qué interfaces y subredes formarán parte del protocolo. Esto evita que el equipo realice un procesamiento adicional para descubrir las redes directamente conectadas, como ocurriría al anunciar una red sumariada sobre la instancia OSPF deseada.

La configuración correspondiente se muestra en la Figura 90. En esta configuración, se especifica un rango de interfaces al cual se le asigna un enlace punto a punto para OSPF. Se realiza esta configuración debido a que no hay un acceso múltiple en ninguno de los equipos de la red MPLS, lo cual requeriría el comando "`ip ospf network broadcast`". Por otro lado, el segundo comando presentado define la instancia de OSPF a la que pertenece la interfaz y el área a la cual está asignada.

Figura 90

Configuración de OSPF

```
R1(config)#interface range f0/0 , f0/1 , f2/0
R1(config-if-range)#ip ospf network point-to-point
R1(config-if-range)#ip ospf 101 area 0
R1(config-if-range)#
```

5. Activar la configuración LDP automática con OSPF

Existen dos formas de configurar y activar MPLS en las interfaces de cada equipo. La primera opción es ingresar manualmente el comando "`mpls ip`" en cada una de las interfaces del equipo. Sin embargo, esta opción requiere que el administrador acceda a

cada interfaz y realice esta configuración, lo cual implica un mayor número de tareas en el equipo. Por esta razón, esta opción no fue considerada para la configuración de la red propuesta.

La segunda opción es realizar la configuración de manera automática utilizando la instancia OSPF creada. Para esto, dentro de la instancia, se debe ingresar el comando "`mpls ldp autoconfig`", como se muestra en la Figura 91. Con este comando, se activarán todas las interfaces pertenecientes a la instancia OSPF seleccionada y formarán parte de la configuración para MPLS. Esto les permitirá distribuir las etiquetas a través de LDP.

De esta manera, el administrador solo necesita realizar una única configuración en el nodo para habilitar este protocolo, lo cual simplifica considerablemente el proceso.

Figura 91

Configuración de OSPF

```
R1(config-router)#mpls ldp au  
R1(config-router)#mpls ldp autoconfig  
R1#conf
```

6. Cambiar rangos de etiquetas

Para esta configuración, se consideraron los rangos de etiquetas mostrados en la Tabla 7. Dichas etiquetas se asignaron teniendo en cuenta que el primer dígito de cada etiqueta corresponde al número del equipo. Por ejemplo, si el equipo es el número 2, se utilizarán etiquetas desde 200 hasta 299. Esto permite identificar fácilmente en qué equipo se encuentra el paquete al realizar trazas y también indica de qué equipo a qué equipo se realiza la conmutación.

Tabla 7

Rangos de etiquetas

Dispositivos	Rango de etiquetas
R1	100-199
R2	200-299
R3	300-399
R4	400-499
R5	500-599
R6	600-699

Por otra parte, es importante además, tener en cuenta el tamaño de la red MPLS y la cantidad de equipos involucrados para determinar el rango adecuado de etiquetas a utilizar. Esto permitirá mantener una nomenclatura coherente y fácil de gestionar sin desperdiciar recursos. . Al configurar MPLS de manera predeterminada, todos los equipos tienen el mismo rango de etiquetas, lo que dificulta la identificación clara de qué equipo está aplicando cada etiqueta. Para solucionar este problema, es necesario modificar este parámetro, para ello, dentro de la configuración global se debe ingresar el comando `mpls label range` seguido del intervalo de las etiquetas deseado, tal como se muestra en la Figura 92. Una vez realizado el cambio de los rangos, se puede verificar los mismos con el comando `show mpls label range` como se muestra en la Figura 93, en donde, se evidencia que para el equipo R1 el rango es [100-199], mientras que el equipo R2 tiene el rango [200-299].

Figura 92

Configuración de OSPF

```

R1(config)#mpls label range ?
<16-1048575> Minimum label value
R1(config)#mpls label range

```

Figura 93

Verificación de rangos de etiquetas

```

R1#
R1#sh mpls label range
Downstream generic label region: Min/Max label: 100/199
R1#
R2#
R2#sh mpls label range
Downstream Generic label region: Min/Max label: 200/299
R2#

```

3.14.1. Verificación de la RIB

Para visualizar este parámetro, se debe desplegar la tabla de enrutamiento en el equipo deseado. En dicha tabla se muestran todos los destinos alcanzables desde el nodo, junto con la métrica, el costo y la interfaz utilizada para llegar a esos destinos. La información se obtiene ejecutando el comando "`show ip route`". Es importante tener en cuenta que, para que esta tabla exista, el dispositivo debe tener interfaces activas con direcciones IPv4 configuradas y debe estar configurado con un Protocolo de Enrutamiento Interior (IGP).

Como se mencionó previamente, la RIB (Routing Information Base) es fundamental para la configuración de MPLS, ya que sirve como punto de partida para definir los LSP (Label Switched Paths) en cada uno de los equipos. En la Figura 94 se presenta la RIB del equipo R1; tomando como ejemplo la primera entrada de esta tabla, se puede observar que desde R1 es posible alcanzar la red 20.20.20.4/32, que pertenece al equipo R4. Este prefijo ha sido aprendido a través del protocolo OSPF, como indica la

letra "O" al inicio de la entrada. Además, se muestra la métrica y el costo para esta entrada, que en este caso es [110/4]. El valor 110 corresponde al costo OSPF y el valor 4 representa el costo acumulado para alcanzar ese enlace.

Figura 94

Routing Information Base (RIB) en equipo R1

```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.10.10.22 to network 0.0.0.0

 20.0.0.0/32 is subnetted, 6 subnets
O    20.20.20.4 [110/4] via 10.10.10.22, 00:01:36, FastEthernet2/0
O    20.20.20.5 [110/3] via 10.10.10.22, 00:01:36, FastEthernet2/0
O    20.20.20.6 [110/13] via 10.10.10.22, 00:01:36, FastEthernet2/0
C    20.20.20.1 is directly connected, Loopback0
O    20.20.20.2 [110/11] via 10.10.10.2, 00:01:36, FastEthernet0/0
O    20.20.20.3 [110/2] via 10.10.10.22, 00:01:36, FastEthernet2/0
 172.20.0.0/24 is subnetted, 6 subnets
S    172.20.0.0 [1/0] via 10.10.10.38
O E2 172.20.1.0 [110/1] via 10.10.10.22, 00:01:38, FastEthernet2/0
S    172.20.2.0 [1/0] via 10.10.10.38
O E2 172.20.3.0 [110/1] via 10.10.10.22, 00:01:38, FastEthernet2/0
S    172.20.4.0 [1/0] via 10.10.10.38
O E2 172.20.5.0 [110/1] via 10.10.10.22, 00:01:39, FastEthernet2/0
 10.0.0.0/8 is variably subnetted, 12 subnets, 2 masks
O    10.10.10.8/30 [110/13] via 10.10.10.22, 00:01:39, FastEthernet2/0
O    10.10.10.12/30 [110/12] via 10.10.10.22, 00:01:40, FastEthernet2/0
C    10.10.10.0/30 is directly connected, FastEthernet0/0
O    10.10.10.4/30 [110/13] via 10.10.10.22, 00:01:40, FastEthernet2/0
O    10.10.10.24/30 [110/11] via 10.10.10.22, 00:01:40, FastEthernet2/0
O    10.10.10.28/30 [110/11] via 10.10.10.2, 00:01:40, FastEthernet0/0
O    10.10.10.28/30 [110/3] via 10.10.10.22, 00:01:40, FastEthernet2/0
O    10.10.10.16/30 [110/2] via 10.10.10.22, 00:01:40, FastEthernet2/0
O    10.10.10.20/30 is directly connected, FastEthernet2/0
C    10.10.10.32/30 [110/13] via 10.10.10.22, 00:01:40, FastEthernet2/0
C    10.10.10.36/30 is directly connected, FastEthernet0/1
O    10.10.10.48/29 [110/11] via 10.10.10.22, 00:01:40, FastEthernet2/0
O    10.10.10.64/29 [110/12] via 10.10.10.22, 00:01:40, FastEthernet2/0
O*E2 0.0.0.0/0 [110/1] via 10.10.10.22, 00:01:40, FastEthernet2/0
b**
```

Es importante destacar que, el costo de cada enlace es de 1, debido a que se están utilizando interfaces FastEthernet. Por lo tanto, el valor de 4 que se muestra en el costo de la primera entrada de la RIB representa la suma de los costos a lo largo del camino para alcanzar la red 20.20.20.4/32.

Además, en la primera entrada de la RIB mostrada en la Figura 94, la dirección IPv4 del siguiente salto utilizado para alcanzar el prefijo destino, es la dirección 10.10.10.22, que corresponde al equipo R3. Adicionalmente, se proporciona información

sobre el tiempo transcurrido desde que se aprendió esta entrada. Al final de la primera entrada, se indica la interfaz local a través de la cual se alcanza el prefijo mencionado.

Cabe señalar que las rutas que no estén instaladas en esta tabla no serán tomadas en cuenta para la asociación de los prefijos con las etiquetas conocidas como bindings, con lo cual, para que un destino sea alcanzable mediante MPLS debe primero ser aprendida por un protocolo de enrutamiento interior.

3.14.2. Verificación de la LIB

Para visualizar esta tabla, es necesario asegurarse de que exista una asociación entre el equipo local y los equipos remotos. Esta asociación se puede verificar utilizando el comando "`show mpls ldp neighbors`", el cual desplegará información sobre las sesiones establecidas con los vecinos, incluyendo si son alcanzables o no.

Es importante tener en cuenta que, para la configuración de MPLS, se utilizaron interfaces de loopback. Estas interfaces son más confiables que las interfaces físicas a la hora de identificar el equipo. Por tanto, es necesario agregar las direcciones de estas interfaces como hosts dentro del protocolo de enrutamiento utilizado en la red. Esto garantizará una correcta comunicación y descubrimiento de los equipos en la red MPLS.

Figura 95

Verificación de Neighbors

```

R1#sh mpls ldp ne
R1#sh mpls ldp neighbor
Peer LDP Ident: 20.20.20.2:0; Local LDP Ident 20.20.20.1:0
TCP connection: 20.20.20.2,40178 - 20.20.20.1,646
State: Oper; Msgs sent/rcvd: 70/71; Downstream
Up time: 00:42:27
LDP discovery sources:
FastEthernet0/0, Src IP addr: 10.10.10.2
Addresses bound to peer LDP Ident:
10.10.10.2 10.10.10.5 10.10.10.25 20.20.20.2
Peer LDP Ident: 20.20.20.3:0; Local LDP Ident 20.20.20.1:0
TCP connection: 20.20.20.3,23320 - 20.20.20.1,646
State: Oper; Msgs sent/rcvd: 71/70; Downstream
Up time: 00:42:25
LDP discovery sources:
FastEthernet2/0, Src IP addr: 10.10.10.22
Addresses bound to peer LDP Ident:
10.10.10.49 10.10.10.26 10.10.10.17 10.10.10.22
20.20.20.3
R1#
R1#

```

En este sentido, el resultado de la ejecución del comando mencionado se muestra en la Figura 95, en color rojo, se identifica la información de los pares con los cuales ha establecido una sesión con LDP; por otra parte, en color verde se muestra la dirección IPv4 asociada a la interfaz por la cual se descubrió dicho vecino. En caso de no tener esta tabla o que los destinos no sean alcanzables se debe verificar que las loopback o direcciones de identificación de los equipos sean alcanzables.

Además, en la Figura 95, remarcado de color rojo se evidencia que tiene dos vecinos, los cuales se identifican con las direcciones IPv4 20.20.20.2 y 20.20.20.3, dichas direcciones pertenecen a los equipos R2 y R3 respectivamente, lo cual coincide con la información proporcionada en la Figura 86, en donde R1, R2 y R3 están conectados directamente, con lo cual son vecinos y deben iniciar una sesión para el intercambio de etiquetas, este parámetro se comprueba con los datos mostrados en la Figura 87, ya que muestra que la dirección 20.20.20.2 es alcanzable por la interfaz f0/0, y en la Figura 95 remarcado con color verde se muestra que efectivamente se realiza la conexión a ese

equipo por dicha interfaz asociada a una dirección IPv4. Finalmente, de color morado, se muestran las direcciones vinculadas a dicho vecino.

La LIB (Label Information Base) contiene todas las asociaciones de los prefijos con etiquetas, tanto remotas como locales. Dentro de un mismo equipo, puede haber múltiples asignaciones hacia un mismo destino. Sin embargo, para la instalación de estas en la LFIB (Label Forwarding Information Base), se deben utilizar las asignaciones con el menor costo de acuerdo con el IGP (Protocolo de Enrutamiento Interior).

Para visualizar el contenido de la tabla LIB, se ejecuta el comando "`show mpls ldp bindings`". Esto desplegará la información correspondiente, tal como se muestra en la Figura 96. La tabla LIB proporciona detalles sobre las asociaciones de etiquetas y prefijos, permitiendo visualizar cómo se realizan las asignaciones dentro del MPLS.

Figura 96

Verificación de LIB equipo R1

```
R1#sh mpls ldp bindings
tib entry: 0.0.0.0/0, rev 38
  local binding: tag: imp-null
  remote binding: tsr: 20.20.20.2;0, tag: imp-null
  remote binding: tsr: 20.20.20.3;0, tag: imp-null
tib entry: 10.10.10.0/30, rev 4
  local binding: tag: imp-null
  remote binding: tsr: 20.20.20.2;0, tag: imp-null
  remote binding: tsr: 20.20.20.3;0, tag: 301
tib entry: 10.10.10.4/30, rev 18
  local binding: tag: 104
  remote binding: tsr: 20.20.20.2;0, tag: imp-null
  remote binding: tsr: 20.20.20.3;0, tag: 302
tib entry: 10.10.10.8/30, rev 20
  local binding: tag: 105
  remote binding: tsr: 20.20.20.2;0, tag: 201
  remote binding: tsr: 20.20.20.3;0, tag: 304
tib entry: 10.10.10.12/30, rev 16
  local binding: tag: 103
  remote binding: tsr: 20.20.20.2;0, tag: 206
  remote binding: tsr: 20.20.20.3;0, tag: 305
tib entry: 10.10.10.16/30, rev 10
  local binding: tag: 100
  remote binding: tsr: 20.20.20.2;0, tag: 205
  remote binding: tsr: 20.20.20.3;0, tag: imp-null
tib entry: 10.10.10.20/30, rev 6
  local binding: tag: imp-null
  remote binding: tsr: 20.20.20.2;0, tag: 204
  remote binding: tsr: 20.20.20.3;0, tag: imp-null
```

En este sentido, se toma como ejemplo la LIB de R1, en donde se tiene la siguiente información: Las entradas principales de la tabla muestran los prefijos que se toman desde la RIB, para los cuales se establece entradas secundarias que muestran las etiquetas remotas y locales. Las etiquetas locales son las que el propio equipo asigna a un prefijo, y estas son compartidas por el protocolo LDP a otros equipos, en los cuales son vistas como remotas, con lo cual, para alcanzar ese prefijo por el equipo vecino se debe usar la etiqueta compartida.

Asimismo, en la Figura 96, se resalta en color morado la información referida a las entradas principales aprendidas por el equipo (**tib entry**), de esta manera se evidencia en la misma línea un parámetro **rev**, el cual sirve para control interno de LDP, este valor sirve para identificar si los anuncios LDP son nuevos o simplemente han experimentado retrasos en el camino. El parámetro **rev**, al ser de control, cada que llega una actualización para un determinado prefijo sube el número de revisión y de esta manera organiza cada uno de los mensajes de actualización del protocolo.

En este sentido, la Figura 96, presenta siete casos diferentes de entradas principales en donde:

1. En el primer caso (**tib entry: 0.0.0.0/0, rev 38**), a sus entradas secundarias (local binding o remote binding) no se les asigna ninguna etiqueta (**tag: imp-null**), debido a que la entrada principal es una ruta por defecto, la cual es aprendida vía redistribución de ruta por defecto desde LSR-R4 ([Ver Figura 86](#)).
2. En el segundo caso (**tib entry: 10.10.10.0/30, rev 4**), se observa que no se asigna una etiqueta local en la entrada secundaria “**local binding:**

tag: imp-null ” debido a que el prefijo 10.10.10.0/30 está directamente conectado (enlace entre R1-R2), ni tampoco se asigna etiqueta a la entrada secundaria “**remote binding: tsr: 20.20.20.2:0, tag: imp-null** ” ya que desde el punto de vista de la LIB del LSR-R1, LSR-R2 cumple la función PHP (Penultimate Hop Popping), por lo que, la etiqueta debe eliminarse en el salto anterior, sin embargo este prefijo para el LER-R3 se encuentra a más de un salto, por lo que, la entrada secundaria “**remote binding: tsr: 20.20.20.3:0, tag: 301** ” se evidencia la asignación de la etiqueta 301.

3. En el tercer caso (**tib entry: 10.10.10.4/30, rev 18**), se asigna una etiqueta local y remota al prefijo 10.10.10.8/30 en la primera y tercera entradas secundarias, **local binding: tag: 104 y remote binding: tsr: 20.20.20.3:0, tag: 302** respectivamente, esto se debe a que la red se encuentra a más de un salto de distancia respecto a LSR-R1, es decir, no está directamente conectada y no cumple con la función de PHP, a pesar de ello, en la segunda entrada secundaria, “**remote binding: tsr: 20.20.20.2:0, tag: imp-null** ”, no se asigna una etiqueta, puesto que sí cumple con la función PHP y la etiqueta debe ser eliminada.
4. En el cuarto caso, en la entrada **tib entry: 10.10.10.8/30, rev 20**, se asignan tanto etiquetas locales como remotas, en este sentido, en las entradas secundarias **local binding: tag: 105, remote binding: tsr: 20.20.20.2:0, tag: 201 y remote binding: tsr: 20.20.20.3:0, tag: 304**, se asignan las etiquetas 105 para LSR-R1, 201 para el enlace entre LSR-R1 con LSR-R2 y 304 para el enlace entre LSR-R1 con LSR-R3, en este caso se asignan tanto,

etiquetas locales como remotas, debido a que, el prefijo se encuentra a más de un salto para su entrega y no cumplen con la función PHP.

5. El caso 5 es similar al 4, ya que, para la entrada principal `tib entry: 10.10.10.12/30, rev 38`, se asignan etiquetas tanto locales como remotas en las entradas secundarias.
6. Los casos 6 y 7, son similares al caso 3.

Es importante destacar que, no todos los bindings de la LIB será instalados en la LFIB; ya que, sería complicado y confuso para el equipo manejar todas estas asociaciones. Por lo tanto, se utiliza el costo de los enlaces y el IGP para determinar cuál es el binding más conveniente a instalarse, de acuerdo con la topología de red.

3.14.1 Verificación de LFIB

La Label Forwarding Information Base (LFIB), es una tabla que contiene los registros de los bindings establecidos para el Label Switched Path (LSP). En esta tabla, se registran los prefijos alcanzables junto con las etiquetas remotas que deben ser colocadas o conmutadas para el proceso de etiquetado.

En este sentido, la tabla LFIB proporciona información crucial para el enrutamiento y reenvío de paquetes en una red MPLS. Ya que, cada entrada en la tabla representa una combinación de etiqueta y prefijo de destino, lo que permite a los dispositivos de la red identificar cómo deben reenviar los paquetes a través del LSP. Esta tabla está disponible en todos los equipos pertenecientes al dominio MPLS, y para su visualización, se debe ejecutar el comando `show mpls forwarding-table`.

Figura 97

Verificación de LFIB en R1

```
R1#sh mpls forwarding-table
```

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
100	Pop tag	10.10.10.16/30	0	Fa2/0	10.10.10.22
101	303	10.10.10.28/30	0	Fa2/0	10.10.10.22
102	Pop tag	10.10.10.24/30	0	Fa2/0	10.10.10.22
	Pop tag	10.10.10.24/30	0	Fa0/0	10.10.10.2
103	305	10.10.10.12/30	0	Fa2/0	10.10.10.22
104	302	10.10.10.4/30	0	Fa2/0	10.10.10.22
105	304	10.10.10.8/30	0	Fa2/0	10.10.10.22
106	306	10.10.10.32/30	0	Fa2/0	10.10.10.22
107	Pop tag	10.10.10.48/29	0	Fa2/0	10.10.10.22
108	308	10.10.10.64/29	0	Fa2/0	10.10.10.22
109	Pop tag	20.20.20.2/32	0	Fa0/0	10.10.10.2
110	Pop tag	20.20.20.3/32	0	Fa2/0	10.10.10.22
111	311	20.20.20.4/32	0	Fa2/0	10.10.10.22
112	312	20.20.20.5/32	0	Fa2/0	10.10.10.22
113	313	20.20.20.6/32	0	Fa2/0	10.10.10.22

De este modo, en la Figura 97, se muestra el resultado de la ejecución del comando mencionado, en donde, en la columna “Local” (remarcado en color morado) corresponde a las etiquetas locales (**Local tag**), parámetro que indica las etiquetas que deben ser utilizadas para enviar los paquetes a través de este equipo. En color amarillo (**Outgoing tag or vc**), se muestra qué tipo de acción se debe realizar con el prefijo a la salida del equipo. Estas acciones pueden ser, colocar una etiqueta (**Push**), quitar una etiqueta (**Pop tag**) o cambiar etiquetas(**Swap**).

Así mismo la Figura 97, muestra (resaltado en color verde) el prefijo asociado a las etiquetas (**Prefix or Tunnel Id**), esto permite identificar claramente la asociación entre un prefijo y la etiqueta utilizada en el proceso de conmutación MPLS. Por último, en color rojo se muestra la dirección del siguiente salto (**Next Hop**), que indica, por dónde deben ser enviados los paquetes con el destino asociado utilizando la etiqueta correspondiente en la LFIB.

Para el diseño planteado, las etiquetas locales en el equipo R1 son elegibles en el rango de [100-199], lo cual se comprueba en la Figura 97, en donde no existen etiquetas superiores o inferiores al rango mencionado. En este sentido, tomando como ejemplo la primera entrada de la tabla LFIB de R1, se tiene una etiqueta local de 100, a pesar de ello, no se asocia a ninguna etiqueta remota, esto implica que, en el siguiente salto ya se entregará el paquete, con lo cual, se identifica con un Pop Tag. El prefijo asociado a dichos parámetros es 10.10.10.16/30 y se lo alcanza a través de la interfaz F2/0, que de acuerdo con la Tabla 6, dicha red pertenece a la conexión entre LER-R3 y LER-R5, con lo cual, se entiende que no haya una etiqueta saliente asociada ya que, se encuentra a un solo salto para alcanzar dicha red y por PHP se conoce que ya no se debe colocar ninguna etiqueta.

En el caso de tener una asociación de etiquetas tanto locales como remotas, significa que, el paquete se encuentra a más de 1 salto para su entrega, de esta manera en la última entrada de la LFIB, se muestra una etiqueta local 113 y una remota 313 que pertenece al equipo LSR-R3 y el prefijo asociado a dicha etiqueta es 20.20.20.6/32 perteneciente al router LSR-R6, de esta manera, al ingresar al equipo LSR-R3 se observará que la etiqueta local para el mismo prefijo debe ser 313 como se muestra en la Figura 98.

Figura 98

Verificación etiqueta local en R3

```

remote binding: tsr: 20.20.20,1:0, tag: 112
tib entry: 20.20.20,6/32, rev 36
local binding: tag: 313
remote binding: tsr: 20.20.20,2:0, tag: 214
remote binding: tsr: 20.20.20,5:0, tag: 511
remote binding: tsr: 20.20.20,1:0, tag: 113
}3#

```

En caso de existir problemas en la conmutación de etiquetas se debe dirigir a la tabla LFIB para verificar que tenga un binding instalado, caso contrario se debe seguir el proceso de verificación en cada una de las tablas (LFIB – LIB – LDP – RIB) hasta encontrar el error para el prefijo deseado.

3.15 Conexión de vEdges remotos

En el presente trabajo de grado, para establecer la conexión de los equipos remotos (SPOKE-1, SPOKE-2, SPOKE-3, SPOKE-4, HUB-1, HUB-2), cada equipo dispone de dos conexiones a una red de acceso múltiple utilizando la red MPLS. Además, se establece una conexión a través de la red local a la interfaz `cloud-x eno1` (donde X representa el número de la Cloud) y otra mediante una interfaz virtual `cloud-x virbrY` (donde X representa el número de la Cloud y Y el número de red NAT), tal como se muestra en la Figura 99.

Esta configuración con enlaces redundantes permite asignar diferentes colores al protocolo TLOC y anunciar redes de diferentes VPN's por la VPN 0. Además, la redundancia de enlaces garantiza que siempre haya un camino disponible para la comunicación entre los nodos, mejorando la continuidad y minimizando las interrupciones en la conectividad.

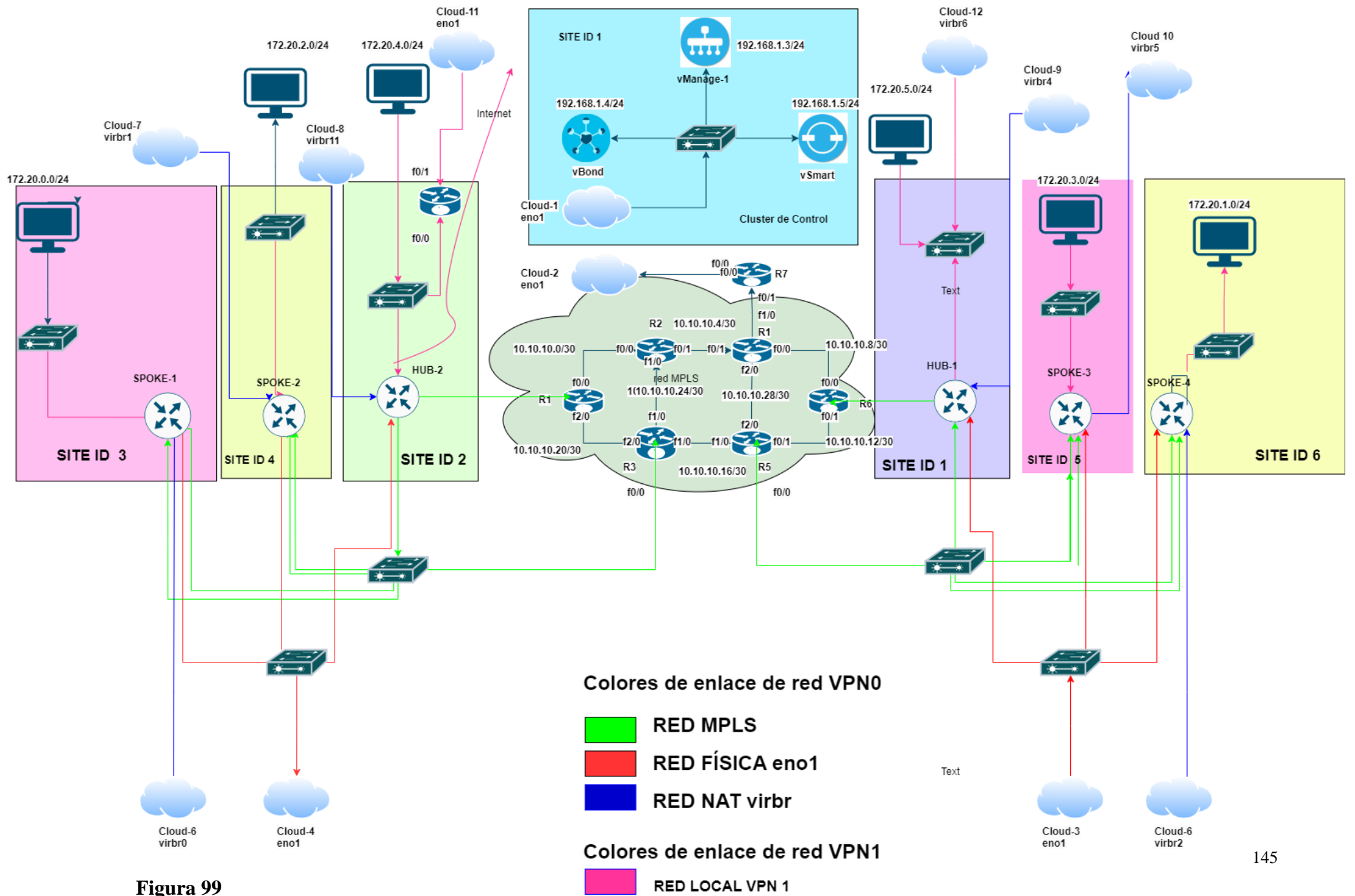


Figura 99

Red, integrando vEdges remotos

En este sentido, en el plano de control, no se realiza una distinción automática del tipo de red con la que se está comunicando el plano de datos. Con lo cual, es responsabilidad del administrador de red asignar un color a la interfaz física para establecer los túneles IPsec correspondientes. Esto garantiza una identificación y gestión adecuada de los enlaces en el plano de control, permitiendo un direccionamiento y enrutamiento adecuado de los paquetes de datos mediante el protocolo TLOC.

De esta manera, para realizar la conexión de un vEdge remoto, el vBond, debe ser capaz de salir por la red pública, es decir que, además de la comunicación por la red interna deben salir a internet mediante la VPN0, para lo cual, se debe ingresar una ruta por defecto en la VPN mencionada y de esta manera alcance los equipos requeridos.

Figura 100

Equipos activados y disponibles(Configuración->Dispositivos)

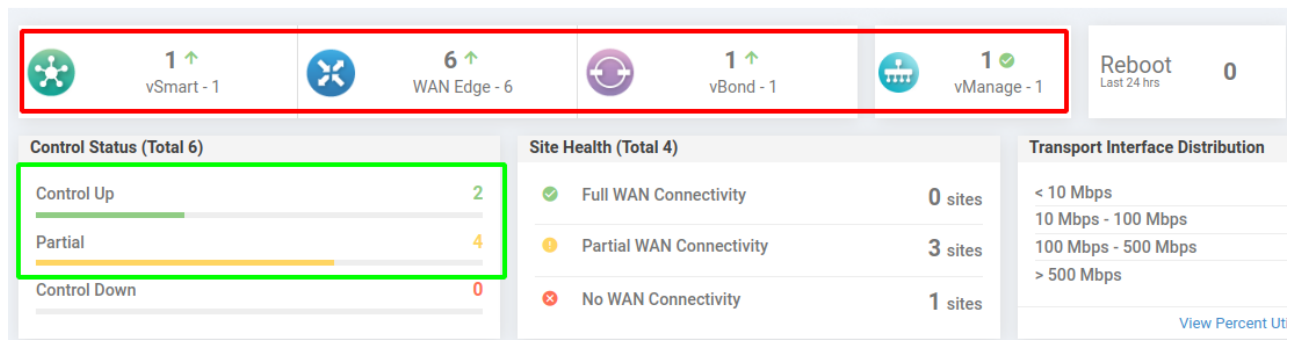
State	Device Model	Chassis Number	Serial No./Token	Enterprise Cert Serial No	Enterprise Cert Expiration Date	
Active	vEdge Cloud	9fc7865d-aaa5-34dc-dfe2-639b5c5c0a2f	A726AC8F	NA	NA	...
Active	vEdge Cloud	1c542191-c161-72ad-a9fe-9a06caf22517	97062A47	NA	NA	...
Active	vEdge Cloud	4b49a038-bc81-c419-9f22-912bc5607276	2285B20C	NA	NA	...
Active	vEdge Cloud	e7c04e05-a450-d8b9-b6e2-7424b3626c24	EBB39C3D	NA	NA	...
Active	vEdge Cloud	11358bc8-f22e-8212-8ed2-4c3fc7cc883c	9AEA899C	NA	NA	...
Active	vEdge Cloud	86e226eb-c047-1f70-2b47-94096c9c5670	67333611	NA	NA	...
Active	vEdge Cloud	80a83ec9-027e-96f5-cb85-e3eb5691bd3c	Token -cca3589632b8f3a2438aaa9a13...	NA	NA	...
Active	vEdge Cloud	35b29e36-f9c4-900b-c917-f2af2c1c1e60	Token -dee222fd5f25ca2e4398095834...	NA	NA	...
Active	vEdge Cloud	5c758e54-6386-f242-1c0c-52b333427a37	Token -5dc03a33586bb935ecca7beb0d...	NA	NA	...
Active	vEdge Cloud	5d5e99a-9267-4b06-0bfb-1b889c4a22c	Token -0dd677af64a77d65b8280032a5...	NA	NA	...

En este punto, los equipos han sido ingresados de la misma manera que se muestra en el apartado “Despliegue de vEdge”, añadiendo los enlaces correspondientes. Como resultado, cada equipo se registra en el plano de control como un equipo válido, tal como se muestra en la Figura 100. Por otro lado, en caso de que algún equipo no pueda

registrarse, se debe verificar si el túnel para IPsec está activo, así como verificar la conectividad a través de la WAN y que la interfaz física esté activa.

Figura 101

Equipos registrados en el plano de control (<https://10.24.8.65:8443>)



De la misma manera, dentro del dashboard del vManage, es posible observar todos los equipos ingresados como se muestra en la Figura 101. Esta vista proporciona un resumen general de la red superpuesta, mostrando los equipos sobre los cuales se tiene control, tanto en el plano de control como en el plano de datos. Es importante destacar que en el estado de control sobre los equipos (Control Status (Total6)), no se muestra ningún equipo con control deshabilitado o inalcanzable, lo que indica que todos los equipos están correctamente registrados y en funcionamiento.

Sin embargo, el campo Site Health muestra en este caso, que la conectividad no alcanza el 100% . Esto se debe a que los equipos aún están en el proceso de identificación de la red y no se han establecido los túneles sobre la misma red de transporte. Es decir, aunque los equipos están registrados y operativos, todavía no han completado la configuración de los túneles IPsec necesarios para establecer la conectividad completa entre ellos. Es importante tener en cuenta que, este estado transitorio es normal durante el proceso de implementación y configuración de la red SD-WAN.

Figura 102

Estado del protocolo BFD (Monitor -> Network)

Hostname	System IP	Device Model	Chassis Number/ID	State	Reachability	Site ID	BFD	Control	Version*
vBond_CuaicalA	2.2.2.2	vEdge Cloud (vBond)	f07f6aed-4244-40f7-a9f5-5a9be9a...	✓	reachable	1	--	--	18.4.4
vEdge-Cuaical-HUB1	4.4.4.4	vEdge Cloud	9fc7865d-eea5-34dc-dfe2-639b5c...	✓	reachable	1	4 (5)	2	18.4.4
vEdge-Cuaical-HUB2	5.5.5.5	vEdge Cloud	1c542191-c161-72ad-a9fe-9d06ca...	✓	reachable	2	0 (5)	2	18.4.4
vEdge-Cuaical-SPOKE1	6.6.6.6	vEdge Cloud	4b49a038-bc81-c419-9f22-912bc...	✓	reachable	3	4 (5)	2	18.4.4
vEdge-Cuaical-SPOKE2	7.7.7.7	vEdge Cloud	e7c04e05-a450-d0b9-b6e2-7424b...	✓	reachable	4	2 (3)	2	18.4.4
vEdge-Cuaical-SPOKE3	9.9.9.9	vEdge Cloud	11358bc8-f22e-8212-8ed2-fc3fc7...	✓	reachable	4	2 (3)	2	18.4.4
vEdge-Cuaical-SPOKE4	10.10.10.10	vEdge Cloud	86e226eb-c047-1f70-2b47-84096...	✓	reachable	4	2 (3)	2	18.4.4

Por otro lado, en la Figura 102 se muestra el número de sesiones BFD que cada equipo debe establecer, estas sesiones brindan la información necesaria para identificar los mejores enlaces de transporte, y de esta manera identificar si existe algún enlace que no presente métricas adecuadas o esté inestable. Además, en el recuadro verde se muestra el número de sesiones ya establecidas, lo cual resulta útil para identificar la cantidad de túneles disponibles y aquellos que aún no se han establecido, por ejemplo, para el HUB1 se tienen 4 sesiones establecidas de las 5 posibles.

Es importante destacar que estos valores tienen un impacto directo en las métricas de los túneles, puesto que, en los túneles activos, las métricas se basarán en las mediciones de jitter, pérdida de paquetes y latencia dentro del propio túnel, y en los túneles inactivos, las métricas mostrarán una pérdida del 100%, lo cual afectará los valores promedio calculados y mostrados en el panel de control.

Figura 103

Estado de los túneles (Monitor->Network->HUB1->Tunnels)

Tunnel Endpoints	Protocol	State	Jitter (ms)	Loss (%)	FEC Loss Recovery (%)	Latency (ms)
biz-internet	--	--			--	
<input checked="" type="checkbox"/> vEdge-Cuaical-HUB1.biz-internet-vEdge-Cuaical-HUB2.biz...	IPSEC	↑	0.00	99.94	N/A	0.00
<input checked="" type="checkbox"/> vEdge-Cuaical-HUB1.biz-internet-vEdge-Cuaical-SPOKE1.b...	IPSEC	↑	4.00	0.00	N/A	29.50
<input checked="" type="checkbox"/> vEdge-Cuaical-HUB1.biz-internet-vEdge-Cuaical-SPOKE2.b...	IPSEC	↑	8.00	0.00	N/A	34.00
<input checked="" type="checkbox"/> vEdge-Cuaical-HUB1.biz-internet-vEdge-Cuaical-SPOKE3.b...	IPSEC	↑	14.00	0.67	N/A	32.00
<input checked="" type="checkbox"/> vEdge-Cuaical-HUB1.biz-internet-vEdge-Cuaical-SPOKE4.b...	IPSEC	↑	4.00	0.00	N/A	30.00

Por otro lado, en la Figura 103 se muestra los túneles establecidos mediante un enlace de transporte desde el HUB1 (**biz-internet**). En este caso, el equipo cuenta con 5 túneles generados; con lo cual, se evidencia que a medida que la red crece, el número de túneles a gestionar también crece de acuerdo con la Ec.2, ya que cada enlace de transporte formará sus propios túneles.

En este contexto, el tener un solo enlace de transporte activo, no presenta dificultades al iniciar las sesiones BFD entre vEdge. Sin embargo, al aumentar el número de enlaces de transporte para cada vEdge, la situación cambia; ya que, en el vSmart (Plano de control) encargado de recibir todos los TLOC's y redistribuirlos en toda la red superpuesta, cada equipo aparece duplicado (ver Figura 104), lo que conlleva un aumento significativo en el número de conexiones que deben ser gestionadas y controladas desde el plano de control.

Figura 104

Plano de orquestación con dos enlaces de transporte

```
vSmart_Cuical1A# show control connections
```

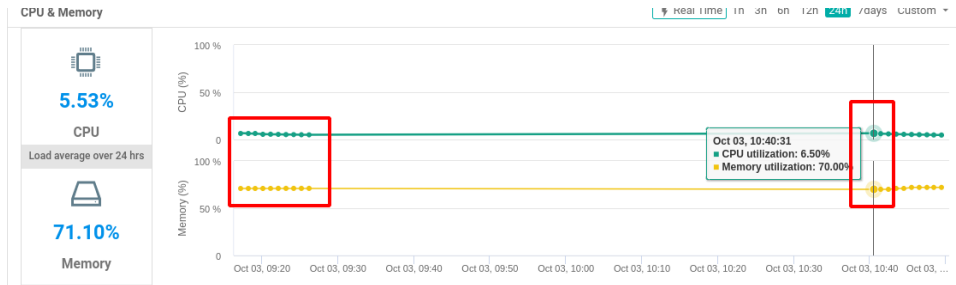
INDEX	TYPE	PEER PROT	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIV PORT	PEER PUBLIC IP	PEER PUB PORT	REMOTE COLOR	STATE	UPTIME
0	vedge	dtls	4.4.4.4	1	1	192.168.103.217	12346	192.168.1.58	29290	public-internet	up	0:00:13:11
0	vedge	dtls	4.4.4.4	1	1	192.168.1.66	12346	192.168.1.66	12346	biz-internet	up	0:00:22:27
0	vedge	dtls	5.5.5.5	2	1	192.168.1.57	12346	192.168.1.57	12346	biz-internet	up	0:00:43:37
0	vedge	dtls	5.5.5.5	2	1	192.168.102.163	12346	192.168.1.58	61820	public-internet	up	0:00:14:38
0	vedge	dtls	6.6.6.6	3	1	192.168.122.239	12346	192.168.1.58	17050	biz-internet	up	0:00:16:17
0	vedge	dtls	6.6.6.6	3	1	192.168.1.92	12346	192.168.1.92	12346	public-internet	up	0:00:29:06
0	vedge	dtls	9.9.9.9	4	1	192.168.1.54	12366	192.168.1.54	12366	biz-internet	up	0:00:09:01
0	vedge	dtls	7.7.7.7	4	1	192.168.1.55	12346	192.168.1.55	12346	public-internet	up	0:00:15:09
0	vedge	dtls	10.10.10.10	4	1	192.168.101.177	12346	192.168.1.58	12346	public-internet	up	0:00:38:31
0	vedge	dtls	9.9.9.9	4	1	192.168.104.157	12346	192.168.1.58	19095	public-internet	up	0:00:12:24
0	vedge	dtls	7.7.7.7	4	1	192.168.100.180	12346	192.168.1.58	54573	biz-internet	up	0:00:15:33
0	vedge	dtls	10.10.10.10	4	1	192.168.1.94	12366	192.168.1.94	12366	biz-internet	up	0:00:33:27
0	obonu	dtls	0.0.0.0	0	0	192.168.1.4	12346	192.168.1.4	12346	default	up	0:00:43:59
0	vmanage	dtls	1.1.1.1	1	0	192.168.1.3	12346	192.168.1.3	12346	default	up	0:00:42:47

Puesto que cada equipo se registra dos veces en el plano de orquestación como se muestra en la Figura 104, no es posible identificar que enlace de transporte está presente en cada entrada, con lo cual, para diferenciar claramente que son dos enlaces de transporte, se cambia el color a uno de estos, es por ello que, en la columna **REMOTE COLOR** se observa “biz-internet” y “public-internet” para un mismo equipo, ya que son los dos enlaces de transporte diferentes por los cuales se alcanza el plano de control.

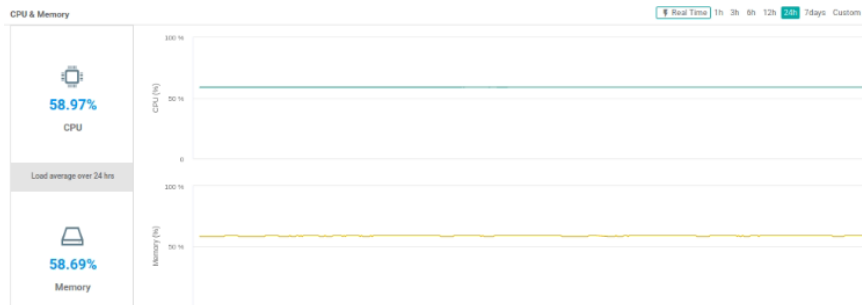
En este sentido, cuando la red está configurada en un estado por defecto, el número de sesiones BFD son excesivas para su manejo en los vEdge, lo cual tiene repercusiones en el procesamiento y uso de memoria de estos, tal como se muestra en la Figura 105. El consumo de recursos puede ser visualizado desde el vManage de manera centralizada, con lo cual al ingresar a un equipo se evidencia que cuando la red tenía un solo enlace de transporte, el uso de la CPU era del 5.53% (ver Figura 105 (a)), por el contrario, al activar el segundo enlace de transporte, este se ve modificado aumentando hasta un 58.97% del uso del procesador como se muestra en la Figura 105 (b).

Figura 105

(a) Consumo de recursos con un solo enlace de transporte (Monitor-> Network ->HUB2 ->Device)



(b) Consumo de recursos con dos enlaces de transporte



En contraste con la situación anterior, en donde solo se tenía un enlace de red, ahora se establecen túneles independientes por cada red de transporte como se muestra en la Figura 106. Este escenario implica un incremento en el número de sesiones BFD que cada equipo debe gestionar en comparación con la Figura 102, en donde, se establecían 5 sesiones, pero ahora ese número ha aumentado a 45.

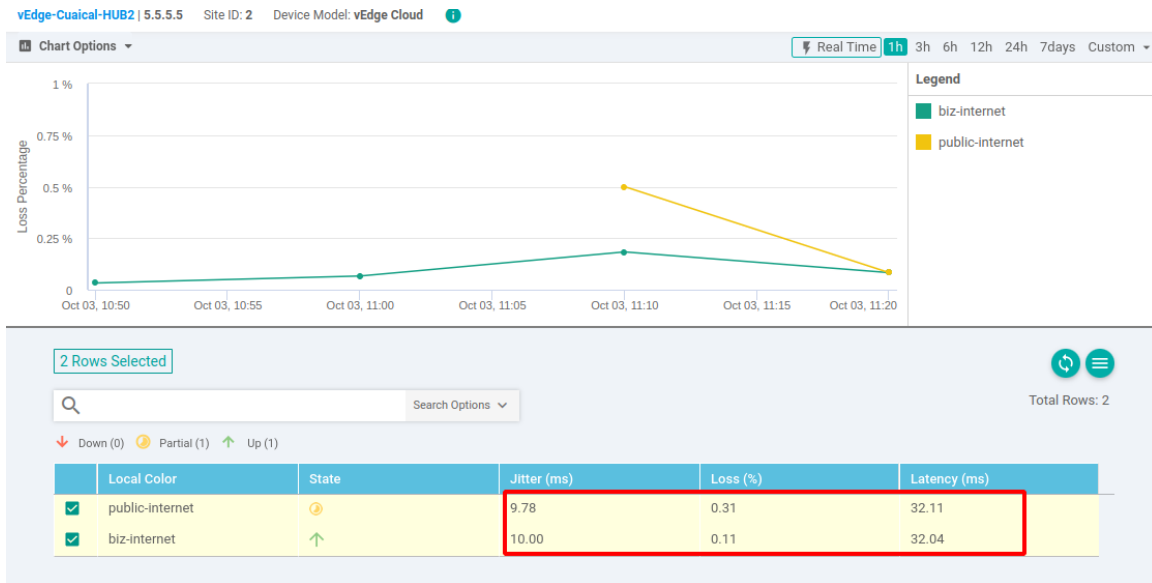
Figura 106

Plano de orquestación

SYSTEM IP	SITE ID	STATE	SOURCE COLOR	TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP	DST PUBLIC IP	DST PUBLIC PORT	ENCAP	DETECT MULTIPLIER	Tx INTERVAL(msec)	UPTIME	TRANSITIONS
5.5.5.5	2	up	mpls	mpls	mpls	10.10.10.68	10.10.10.54	12346	ipsecc	7	1000	0:00:49:20	0
5.5.5.5	2	up	mpls	mpls	biz-internet	10.10.10.68	192.168.1.53	12346	ipsecc	7	1000	0:00:04:27	30
5.5.5.5	2	down	mpls	mpls	public-internet	10.10.10.68	192.168.1.53	53114	ipsecc	7	1000	NA	76
5.5.5.5	2	up	biz-internet	mpls	public-internet	192.168.1.96	192.168.1.7	12346	ipsecc	7	1000	0:00:51:31	3
5.5.5.5	2	up	biz-internet	mpls	biz-internet	192.168.1.96	192.168.1.53	12346	ipsecc	7	1000	0:00:03:16	50
5.5.5.5	2	up	biz-internet	mpls	public-internet	192.168.1.96	192.168.1.53	53114	ipsecc	7	1000	0:00:00:00	93
5.5.5.5	2	down	public-internet	mpls	public-internet	192.168.103.217	192.168.1.7	12346	ipsecc	7	1000	NA	0
5.5.5.5	2	down	public-internet	mpls	biz-internet	192.168.103.217	192.168.1.53	12346	ipsecc	7	1000	NA	0
5.5.5.5	2	down	public-internet	mpls	public-internet	192.168.103.217	192.168.1.53	53114	ipsecc	7	1000	NA	0
7.7.7.7	4	up	mpls	mpls	mpls	10.10.10.68	10.10.10.52	12346	ipsecc	7	1000	0:00:49:24	0
7.7.7.7	4	down	mpls	mpls	biz-internet	10.10.10.68	192.168.1.53	31054	ipsecc	7	1000	NA	38
7.7.7.7	4	up	mpls	mpls	public-internet	10.10.10.68	192.168.1.55	12346	ipsecc	7	1000	0:00:49:24	0
7.7.7.7	4	up	biz-internet	mpls	public-internet	192.168.1.96	192.168.1.7	1031	ipsecc	7	1000	0:00:51:34	3
7.7.7.7	4	up	biz-internet	mpls	biz-internet	192.168.1.96	192.168.1.53	31054	ipsecc	7	1000	0:00:00:06	33
7.7.7.7	4	up	biz-internet	mpls	public-internet	192.168.1.96	192.168.1.55	12346	ipsecc	7	1000	0:00:51:35	3
7.7.7.7	4	down	public-internet	mpls	public-internet	192.168.103.217	192.168.1.7	1031	ipsecc	7	1000	NA	0
7.7.7.7	4	down	public-internet	mpls	biz-internet	192.168.103.217	192.168.1.53	31054	ipsecc	7	1000	NA	0
7.7.7.7	4	down	public-internet	mpls	public-internet	192.168.103.217	192.168.1.55	12346	ipsecc	7	1000	NA	141
8.9.9.9	5	up	mpls	mpls	mpls	10.10.10.68	10.10.10.69	12346	ipsecc	7	1000	0:00:49:25	0
8.9.9.9	5	up	mpls	mpls	biz-internet	10.10.10.68	192.168.1.52	12346	ipsecc	7	1000	0:00:11:34	1
8.9.9.9	5	down	mpls	mpls	public-internet	10.10.10.68	192.168.1.53	12406	ipsecc	7	1000	NA	76
8.9.9.9	5	up	biz-internet	mpls	public-internet	192.168.1.96	192.168.1.7	1026	ipsecc	7	1000	0:00:51:35	3
8.9.9.9	5	up	biz-internet	mpls	biz-internet	192.168.1.96	192.168.1.52	12346	ipsecc	7	1000	0:00:11:35	4
8.9.9.9	5	up	biz-internet	mpls	public-internet	192.168.1.96	192.168.1.53	12406	ipsecc	7	1000	0:00:00:06	87
8.9.9.9	5	down	public-internet	mpls	public-internet	192.168.103.217	192.168.1.7	1026	ipsecc	7	1000	NA	0
8.9.9.9	5	down	public-internet	mpls	biz-internet	192.168.103.217	192.168.1.52	12346	ipsecc	7	1000	NA	144
8.9.9.9	5	down	public-internet	mpls	public-internet	192.168.103.217	192.168.1.53	12406	ipsecc	7	1000	NA	0

Figura 107

Estadísticas de los túneles (Monitor->Network->HUB2)



Del mismo modo, en el plano de control es posible monitorear cada uno de los túneles, con lo cual, dentro de cada equipo se desplegará la información mostrada en la Figura 107, en donde se observa un resumen de cada uno de los enlaces de transporte usados y las estadísticas del mismo, de esta manera en el recuadro de color rojo se muestra

tanto la latencia, jitter y pérdida de paquetes en los enlaces de transporte **biz-internet** y **pubic-internet**.

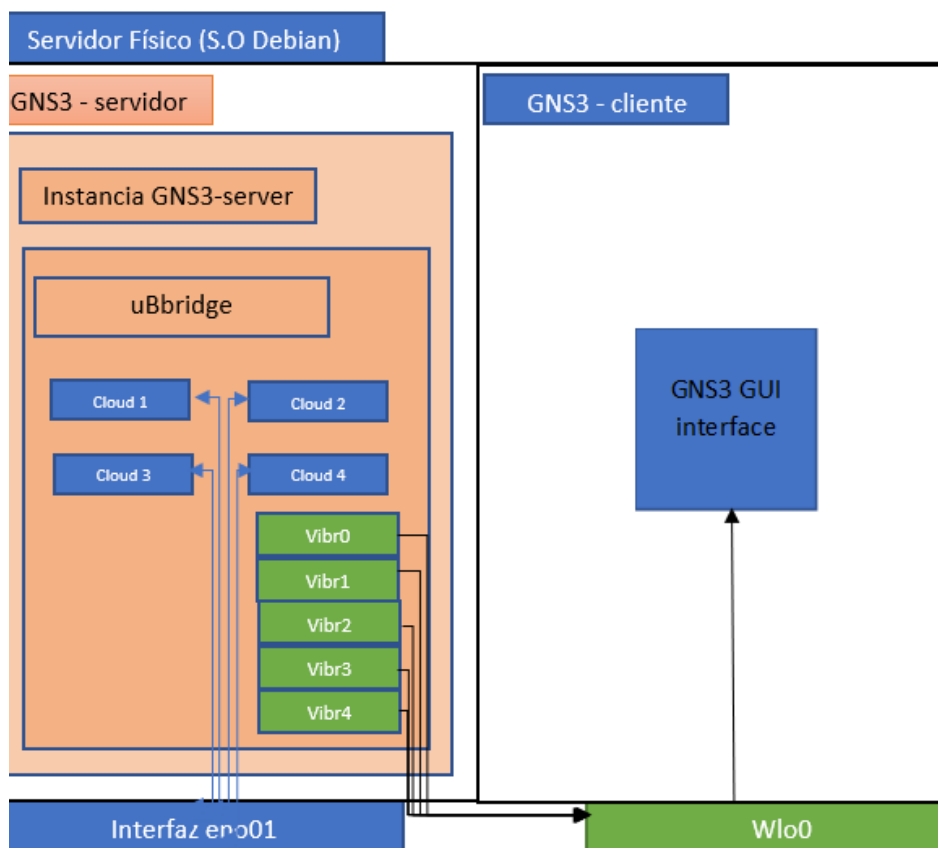
De esta manera, en el enlace **públic-internet**, la pérdida de paquetes es de 0.31% debido a que, al activar los dos enlaces de transporte en simultáneo, el procesamiento se ocupa en dichas tareas y no solamente en enrutar los paquetes. En cuanto al jitter, presenta un buen comportamiento debido a que se encuentra por debajo de los 20ms; y de igual forma, la latencia es de 32.11ms, lo cual se encuentra dentro de buena-baja ya que se sitúa por debajo de la mínima aceptable de 100ms de acuerdo con (UIT, 2013).

Por otro lado, una vez que se han identificado todas las interfaces de red que forman parte de la red SD-WAN, es crucial definir el esquema de funcionamiento de la simulación entre el servidor gns3-server y los clientes. En la Figura 21 se mostró únicamente las interfaces que interactúan entre el servidor físico y el gns3-server; sin embargo, es fundamental tener precaución al utilizar las interfaces del servidor físico, ya que una mala configuración provocaría un bucle en las comunicaciones, imposibilitando el correcto funcionamiento de la red SD-WAN.

Es por ello por lo que, en la Figura 108 se presenta la arquitectura final del testbed con las interfaces virtuales mencionadas anteriormente. Esto se realiza debido a que algunos nodos requieren ser accesibles desde cualquier ubicación de la red, como lo son, el vManage para los accesos a través de la web, y el vBond para permitir el ingreso de equipos independientemente de si pertenecen a la red local o no. Por otro lado, las interfaces virtuales no necesitan ser accesibles desde la red local (red física), ya que se utilizan para demostrar el funcionamiento de un transporte con el uso de NAT.

Figura 108

Uso de las interfaces para la simulación



Dentro del servidor físico, se están ejecutando diferentes instancias para el funcionamiento de GNS3. Una de ellas es el uBridge, encargado de administrar las interfaces dentro de la simulación. En este sentido, en la Figura 108, se muestra cómo se establece la asociación entre las interfaces virtuales (**cloud-x**) y físicas (**eno1** y **wlo0**).

Las interfaces virtuales conectadas a la interfaz eno01 del servidor, actúan como un puente directo hacia la red local. Esta configuración es fundamental para el funcionamiento y visualización de la red superpuesta, ya que permite que el vBond sea accesible desde toda la red física del servidor.

Por otro lado, la Figura 108, muestra también las interfaces virtuales (**virbr-y**), las cuales tienen un funcionamiento diferente a las interfaces cloud, ya que estas interfaces no tienen acceso directo a la red local (red física) del servidor, puesto que, para poder hacerlo, se ayudan de un NAT ligado a la interfaz wlo0.

4 CAPÍTULO IV Aplicación de ingeniería de tráfico y pruebas de funcionamiento de una red SD-WAN

En este capítulo, se llevará a cabo la aplicación de ingeniería de tráfico a la topología propuesta y desplegada en el capítulo anterior. Dado que se cuenta con una topología de malla completa, se aprovecharán las capacidades del plano de control y gestión para establecer redes independientes entre algunos equipos pertenecientes a la red SD-WAN, por ejemplo, una topología SHHS (Regional).

En este sentido, el objetivo principal de la aplicación de ingeniería de tráfico es utilizar la topología de red híbrida presentada en el capítulo III para manipular el flujo de tráfico y aplicar políticas que permitan el uso simultáneo de la red MPLS y la red pública. Para lograr esto, se llevará a cabo un mapeo de las aplicaciones utilizadas en la red, lo que permitirá tener un mayor control y direccionamiento del tráfico en toda la infraestructura.

4.1 Creación de política para topología HUB and SPOKE

Para crear la topología HUB and SPOKE, es fundamental identificar cada uno de los nodos con sus respectivos IDs de sitio. Esto se puede realizar siguiendo un proceso de identificación adecuado, como se muestra en la Tabla 8; en donde se listan el nombre del dispositivo, el ID de sitio y la función que cumplirá dentro de la red. Es importante destacar que este proceso de identificación es esencial, ya que, desde el plano de control, la única forma de reconocer y diferenciar los nodos es mediante el ID de sitio asignado a cada uno de ellos.

Tabla 8

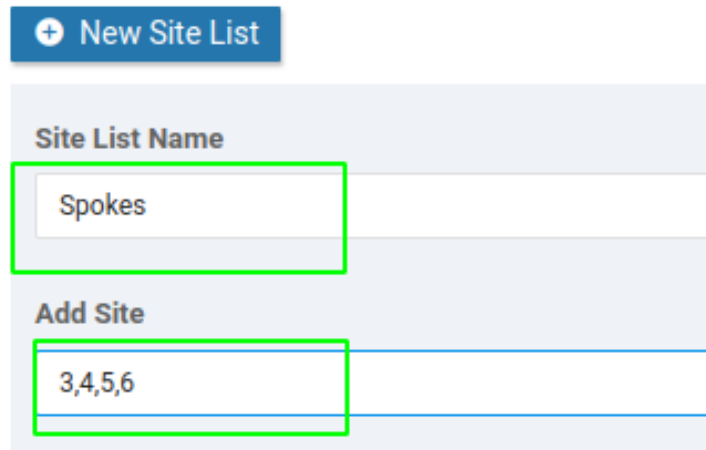
Resumen de ID's de equipos

Dispositivo	ID-Sitio	Función
SPOKE-1	3	spoke
SPOKE-2	4	spoke
SPOKE-3	5	spoke
SPOKE-4	6	spoke
HUB-1	1	hub
HUB-2	2	hub

Cuando se hayan definido los parámetros de identificación de los equipos, se debe acceder al apartado de políticas centralizadas en la interfaz web del vManage. En este apartado, se definen los grupos de SPOKES y HUBS para la configuración de la topología mencionada, tal como se muestra en la Figura 109.

Figura 109

Sites ID de SPOKES (Monitor->Configuration->Policies->Centraliced)



The image shows a web interface for creating a new site list. At the top, there is a blue button with a white plus sign and the text "New Site List". Below this, there is a light blue form area. The first section is labeled "Site List Name" and contains a text input field with the value "Spokes". The second section is labeled "Add Site" and contains a text input field with the value "3,4,5,6". Both input fields are highlighted with a green border.

Una vez dentro de la política centralizada, se debe añadir una nueva lista de sitios como se muestra en la Figura 109. En esta sección, se asigna un nombre a la lista de sitio (**Site List Name**) y se añaden los IDs de sitio en el campo añadir sitio (**Add Site**).

Es importante tener en cuenta que, los nombres asignados a los sitios deben identificar la función de los equipos ingresados tal como se muestra en la Figura 110. Esto se debe a que no será la única lista existente al momento de crear la política, y se deben evitar confusiones al momento de crear una topología específica.

De esta manera, al asignar nombres descriptivos a los sitios, se facilita la gestión y configuración de la red. Además, al crear múltiples listas de sitios, se puede lograr una mayor flexibilidad en la asignación de políticas y configuraciones específicas, adaptando la topología a las necesidades particulares de la red.







Al desplegar los grupos creados en la sección de políticas centralizadas, como se muestra en la Figura 110, se despliega información relevante sobre su creación. Esta información incluye el nombre de la lista (**Name**), que identifica de manera clara el grupo

creado. Además, se muestran las entradas (**Entries**) que contienen los IDs de los nodos que forman parte del grupo específico.

Es relevante tener en cuenta que el parámetro "**Reference Count 0**" indica que los grupos han sido creados, pero aún no han sido utilizados en ninguna política centralizada. Este valor cambiará cuando se active una política y se aplique a los nodos correspondientes. Los demás parámetros son de control y se utilizan para identificar quién creó el grupo (**Updated By**) y mantener un registro de las actualizaciones realizadas en ella.

Figura 110

Listas creadas de HUBS y SPOKES (Monitor->Configuration->Policies->Site Lists)

Name	Entries	Reference Count	Updated By	Last Updated	Action
Spokes	3, 4, 5, 6	0	admin	24 Oct 2022 10:18:57 AM ...	  
Hubs	1, 2	0	admin	24 Oct 2022 10:19:21 AM ...	  

Una vez creados los grupos o listas de sitio, es necesario definir la VPN por la cual trabajará la política creada. Para lo cual, se crea un grupo de VPNs a las cuales se aplicará la política centralizada, y se ingresa el número específico de la VPN que se desea agregar, en este caso específico, solo se desea aplicar la política por la VPN 0, tal como se muestra en la Figura 111 en el parámetro (**Entries**).

Figura 111

Asociación de política a una VPN (Monitor->Configuration->Policies->VPN service)

Name	Entries	Reference Count	Updated By	Last Updated	Action
Servicio_VPN_0	0	0	admin	24 Oct 2022 10:24:51 AM -05	 

Una vez configurado los parámetros anteriores, será posible realizar la configuración de la política, ya que, se tiene la referencia de los dispositivos a los cuales se deben aplicar las reglas y de la misma manera por cuál VPN se realizarán las mismas.

En este sentido, en la Figura 112 se muestra la creación de la política centralizada, donde se realizan las siguientes asignaciones:

1. Se asigna el nombre "**TOPOLOGIA_HUB_N_SPOKE**" a la política centralizada, proporcionando una identificación clara y descriptiva para su posterior referencia.
2. Se selecciona la VPN por la cual operará la política, en este caso, "**Servicio_VPN_0**". Este paso es importante para asegurar que la política se aplique a la VPN específica definida previamente, como se muestra en la Figura 111.
3. En el campo "**Add Hub Sites**", se ingresan los nombres de la lista creada para los Hubs. Esto permite asociar los sitios designados como Hubs a la política centralizada, asegurando que se apliquen las configuraciones y directivas correspondientes a estos nodos.
4. En el campo "**Add Spokes Sites**", se ingresan los nombres de la lista creada para los Spokes. Esto permite asociar los sitios designados como Spokes a la política

centralizada, asegurando la aplicación adecuada de las configuraciones y reglas específicas para estos nodos.

Figura 112

Creación de política (Monitor->Configuration->Policies->Centraliced->Topology->Hub-and-Spoke)

The screenshot displays a configuration form for a policy. The fields are as follows:

Name	Topologia_HUB_N_SPOKE
Description	Topologia_HUB_N_SPOKE
VPN List	Servicio_VPN_0

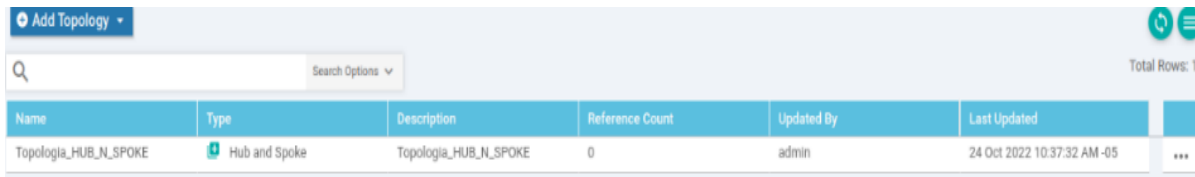
Below the form, there are two sections for adding sites:

- Add Hub Sites:** A table with columns 'Site Lists' and 'Action'. The 'Site Lists' column contains 'Hubs'.
- Add Spoke Sites:** A table with columns 'Site Lists' and 'Action'. The 'Site Lists' column contains 'Spokes'.

En este punto, se ha finalizado el proceso de configuración del comportamiento de la política, lo cual involucra la identificación de los dispositivos y la especificación de los modos de operación correspondientes. Como resultado, la política ha sido creada y se muestra en la Figura 113.

Figura 113

Topología creada dentro de la política (Monitor->Configuration->Policies->Centraliced->Topology->Hub-and-Spoke)



Name	Type	Description	Reference Count	Updated By	Last Updated
Topologia_HUB_N_SPOKE	Hub and Spoke	Topologia_HUB_N_SPOKE	0	admin	24 Oct 2022 10:37:32 AM-05

Sin embargo, la política aún no está en ejecución. Esto se evidencia en la Figura 114, donde en la sección "**Activated**" se muestra el estado de "**false**", lo que indica que la política no ha sido activada. Para activarla, se requiere realizar un proceso adicional de manera manual, tal como se muestra en la Figura 115. En esta figura, al hacer clic en los tres puntos asociados a la política, se despliega un menú que presenta la opción de activación. Una vez ejecutada esta opción, se espera que la política cambie su estado a "**activo**" o "**true**", lo cual en este caso no sucede (ver Figura 116), ya se encuentra en modo de operación CLI.

Por lo tanto, el vSmart debe cambiar el modo de operación de CLI a vManaged¹⁰; de lo contrario, no se podrán ejecutar las políticas y el plano de gestión mostrará un mensaje de error al intentar activarlas (**vSmarts 3.3.3.3 are not in vManaged mode**), tal como se muestra en la Figura 116.

¹⁰ El equipo puede estar en dos estados, los cuales son; vManaged o CLI.

Figura 114

Estado de la política

Name	Description	Type	Activated	Updated By	Policy Version	Last Updated	
Politica_Hub_N_Spoke	Politica_Hub_N_Spoke	UI Policy Builder	false	admin	10242022T104145275	24 Oct 2022 10:41:45 AM -05	...

Figura 115

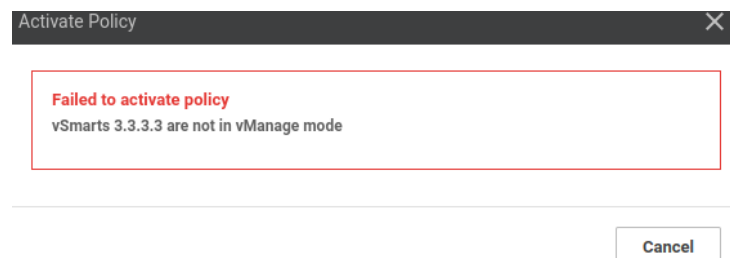
Activación de la política

Name	Description	Type	Activated	Updated By	Policy Version	Last Updated	
Politica_Hub_N_Spoke	Politica_Hub_N_Spoke	UI Policy Builder	false	admin	10242022T104145275	24 Oct 2022 10:41:45 AM -05	...

- View
- Preview
- Copy
- Edit
- Delete
- Activate

Figura 116

Mensaje de estado erróneo del vSmart



En este sentido con el comando "**show system**" (ver Figura 117) se verifica que efectivamente el dispositivo se encuentra en modo CLI ya que el campo vManaged tiene el valor "**false**". Además que con ello se verifica que las interfaces o los túneles entre vSmart y vManage no presentan errores.

Figura 117

Verificación del modo de vSmart

```
Personality:          vsmart
Model name:          vsmart
Services:            None
vManaged:           false
Commit pending:     false
Configuration template: None
Policy template:     None
Policy template version: None
Chassis serial number: None
```

Por lo tanto, para cambiar el modo de operación de CLI a vManaged, se debe llevar a cabo el siguiente proceso:

1. Ingresar a templates dentro del vManage y crear un nuevo template en caso de no existir (**Configuration->Templates**).
2. Elegir el modo “**From Featured Template**”.
3. Dentro del template creado, dirigirse a OMP y modificar este como se muestra en la Figura 118.

Figura 118

Creación del template para OMP del vSmart

The screenshot displays the configuration page for a vSmart template. At the top, the 'Template Name' and 'Description' fields are both set to 'vSmart_OMP_Template'. Below this, the 'Basic Configuration' tab is selected, showing several settings:

- Graceful Restart for OMP:** Set to 'On' (radio button selected).
- Graceful Restart Timer (seconds):** Set to 43200.
- Number of Paths Advertised per Prefix:** Set to 4.
- Send Backup Paths:** Set to 'Off' (radio button selected).
- Shutdown:** Set to 'No' (radio button selected).
- Discard Rejected Routes:** Set to 'Off' (radio button selected).

En este sentido, en la Figura 118 se muestra que se asigna un nombre al template (`vSmart_OMP_Template`) y se activa el campo "Graceful Restart for OMP"¹¹. Además, se establece que el protocolo no debe estar desactivado (`no Shutdown`).

4. Dentro del template creado en el paso 2, dirigirse a VPN en donde se creará un template nuevo para la VPN 0, tal como se muestra en la Figura 119.

¹¹ El estado Gracefull Restart For OMP asegura que los dispositivos de la red mantengan la conectividad y minimiza las interrupciones durante los reinicios o actualizaciones de software en Cisco SD-WAN.

Figura 119

Configuración de la VPN 0 para vSmart

The screenshot shows the configuration page for a VPN feature template. The 'BASIC CONFIGURATION' section has a 'VPN' dropdown menu set to 'VPN 0' with a globe icon, and a 'Name' field. The 'DNS' section has a 'Primary DNS Address' field and an empty table with columns 'Optional', 'Hostname', and 'List of IP Addresses (Maximum: 8)'. The 'IPV4 ROUTE' section has a table with columns 'Optional', 'Prefix', 'Gateway', and 'Selected Gateway Configuration'. The table contains one entry with a checkbox, a globe icon, the prefix '[vpn0_ipv4_ip_prefix]', the gateway 'Next Hop', and the configuration '1'. Red boxes highlight the 'VPN 0' selection and the route entry.

De esta manera, dentro del template, se debe definir el modo de operación de la VPN 0, tal como se muestra en la Figura 119, (**VPN**; **VPN0**), este parámetro debe definirse como global, es por ello por lo que delante de VPN0 se muestra un símbolo de globo. De la misma manera, se debe definir que el gateway será por esta VPN, tal como se muestra en el apartado de **IPV4 ROUTE**, en donde se define que debe ser mediante un prefijo IPv4 `[vpn0_ipv4_ip_prefix]`.

5. Una vez se hayan definido todos los templates, tanto para la VPN0 y OMP, se observarán tal como se muestra en la Figura 120, en donde cada elemento configurado genera un template individual.

Figura 120

Creación de templates para OMP y VPN (Monitor->Configuration->Policies->Featured Templates)

Name	Description
vSmart_OMP_Template	vSmart_OMP_Template
vSmart_VPN0_Template	vSmart_VPN0_Template
vSmart-VPN0_interface-template	vSmart_VPN0_Template

En este punto, se debe considerar qué, el protocolo NetConf debe estar habilitado dentro de los túneles, para ello, desde las configuraciones globales del vSmart, se debe ingresar a la VPN0, posteriormente a la interfaz ge0/0, y finalmente dentro del túnel de la interfaz (**tunnel-interface**) permitir el servicio para NetConf con el comando **allow-service netconf** ó **allow-service all** para permitir todos los protocolos.

6. Realizar el lanzamiento de la configuración. Para ello se debe identificar los equipos disponibles con el **attach devices**, y posteriormente realizar el envío de los templates a los dispositivos.
7. Una vez realizado el paso anterior, el plano de gestión debe sincronizar las configuraciones lanzadas hacia el plano de control, una vez se validen estas, el vSmart se registra tal como se muestra en la Figura 121, en donde el modo de operación (**mode**) será vManaged.

Figura 121

Verificación del modo de operación de vSmart visto desde el vManage (Monitor->Devices->Controllers)

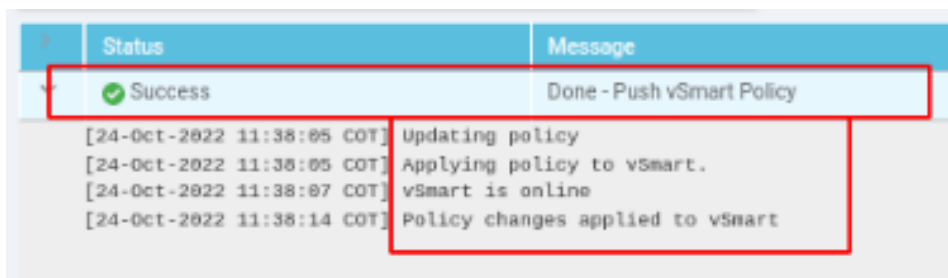
Controller Type	Hostname	System IP	Site ID	Mode	Device Status	Certificate Status	UUID
vSmart	vSmart_CuaicalA	3.3.3.3	1	vManage	In Sync	Installed	cf69baef-c771-4555-b175-1.
vManage	vManage_CuaicalA	1.1.1.1	1	CLI	In Sync	Installed	79acf7c7-f6ff-43ed-b611-6..
vBond	vBond_CuaicalA	2.2.2.2	1	CLI	In Sync	Installed	f07f6aed-4244-40f7-a9f5-5..

En la Figura 121, se presenta información relevante sobre el estado de los dispositivos vSmart, vBond y vManage en el plano de control. En la primera entrada, se muestra un dispositivo de tipo **vSmart (Controller Type)** llamado **vSmart_CuaicalA (Hostname)**. Además, se registra la dirección IPv4 del sistema, que identifica al dispositivo como **3.3.3.3 (System IP)**. Al igual que los vEdge, estos equipos tienen un ID de sitio (Site ID) que los identifica en el plano de control. Además, se proporciona el estado actual del dispositivo y el modo de operación. En el ejemplo tomado, el estado es **"In Sync" (Sincronizado)** y el modo de operación es **"vManaged"**, lo cual indica que el dispositivo está sincronizado y puede ser controlado desde el plano de gestión.

En esta instancia, ya es posible realizar la configuración de las políticas, ya que el dispositivo deseado está en el modo de configuración administrado por el vManage, por lo cual al aplicar las políticas ya no mostrará el mensaje de error en el modo de operación, en su lugar enviará una acción satisfactoria de las políticas, tal como se muestra en la Figura 122.

Figura 122

Estado satisfactorio de la configuración remota del dispositivo



Status	Message
Success	Done - Push vSmart Policy
[24-Oct-2022 11:38:05 COT]	Updating policy
[24-Oct-2022 11:38:05 COT]	Applying policy to vSmart.
[24-Oct-2022 11:38:07 COT]	vSmart is online
[24-Oct-2022 11:38:14 COT]	Policy changes applied to vSmart

Una vez el estado de activación de las políticas centralizadas sea satisfactorio (**Success**) tal como se muestra en la Figura 122, ya será posible observar las políticas en ejecución desde el plano de control. Para obtener dicha información, desde la terminal del vSmart se ejecuta el comando `show running-config policy`, el cual desplegará la política creada para Hub and Spoke como se muestra en la Figura 123.

Figura 123

Visualización de políticas creadas desde el plano de gestión desde el plano de control

```

policy
lists
vpn-list Servicio_VPN_0
  vpn 0
  !
site-list Hubs
  site-id 1
  site-id 2
  !
site-list Spokes
  site-id 3
  site-id 4
  site-id 5
  site-id 6
  !
!
control-policy control_-2127028953
sequence 10
  match route
  site-list Hubs
  vpn-list Servicio_VPN_0
  !
  action accept
  !
sequence 20
  match route
  site-list Hubs
  vpn-list Servicio_VPN_0
  !
  action accept
  !
sequence 30
  match tloc
  site-list Hubs
  !
  action accept
  !
  default-action reject
  !
!
apply-policy
site-list Spokes
control-policy control_-2127028953 out
!
!

```

En este sentido, la política empieza con el encabezado denominado política (**policy**), a continuación se presentan las listas creadas, la primera de ellas corresponde a las VPNs, que está compuesta exclusivamente por la VPN 0. La siguiente lista hace referencia a los sitios que actúan como HUBS, en este caso los sitios 1 y 2. De la misma manera, se presenta la lista que conforman los SPOKES en la cual se encuentran los sitios 3, 4, 5, 6.

Posterior a la creación de las listas, se define el comportamiento de las mismas dentro de la política. De esta manera, el parámetro **control-policy** especifica el número que identifica el control, por ejemplo, **control_-2127028953** valor que hace referencia a la entrada para la topología HUB and SPOKE. Dentro de este control, se encuentra el parámetro "**sequence**", que indica la secuencia en la que se ejecutan las políticas y se

realizan los emparejamientos. Cada secuencia culmina con una acción, en este caso "accept", ya que se trabaja con una denegación implícita (`default-action reject`).

Finalmente, en el campo "`apply-policy`" se definen las listas de HUBs y SPOKES, y se especifica el sentido en el que actuará la política "`control_-2127028953`". En este caso, para los SPOKES, la política se aplicará en la salida (`control-policy control_-2127028953 out`), lo que implica que no podrán anunciar sus TLOC's de manera libre a toda la red SD-WAN.

Cabe mencionar que al cambiar el modo de operación del vSmart, no será posible crear ni modificar políticas directamente desde el dispositivo. Esto se debe a que el modo de operación vManaged solo permite la creación y modificación de políticas a través de los templates lanzados desde el vManage mediante el protocolo NETCONF. Por lo tanto, es importante asegurarse que exista una comunicación segura establecida y que el servicio esté habilitado antes de realizar cualquier configuración de políticas.

En este contexto, una vez que las políticas han sido aceptadas, se establecerán las sesiones BFD entre los equipos de la siguiente manera: (SPOKE1 y SPOKE2 con HUB2) y (SPOKE3 y SPOKE4 con HUB1). Dentro de cada SPOKE, se observará que se establecen sesiones BFD con su respectivo HUB a través de los dos enlaces de transporte. Esto significa que en el HUB se tendrán múltiples sesiones BFD, ya que es el responsable de dirigir las comunicaciones y debe conocer las rutas del dominio del HUB secundario.

Es así como la Figura 124 muestra las sesiones BFD que el SPOKE1 establece únicamente con el HUB2, ya que el SITE ID es 2 ([ver tabla 7](#)). Este enfoque evita tener las 20 sesiones mostradas en la Figura 106 al manejar múltiples enlaces de transporte.

Figura 124

Sesiones BFD filtradas SPOKE 1

```
vEdge-Cuaical-SPOKE1# show bfd sessions
```

SYSTEM IP	SITE ID	STATE	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP
5.5.5.5	2	up	public-internet	biz-internet	192.168.1.57
5.5.5.5	2	up	public-internet	public-internet	192.168.1.57
5.5.5.5	2	up	biz-internet	biz-internet	192.168.122.239
5.5.5.5	2	down	biz-internet	public-internet	192.168.122.239

Por otro lado, el HUB será capaz de alcanzar a más equipos que los pertenecientes a su propio dominio, ya que es el encargado de enrutar los paquetes hacia otro dominio o grupo de HUBS. Sin embargo, a pesar de que un HUB es capaz de comunicarse con miembros de otras regiones (SPOKES), no podrá establecer una sesión BFD directamente con dichos SPOKES, ya que el miembro interno de la región deseada no podrá establecer comunicación con un miembro externo al dominio delimitado por su HUB respectivo.

Figura 125

Sesiones BFD de HUB's

```
vEdge-Cuaical-HUB1# show bfd sessions
```

SYSTEM IP	SITE ID	STATE	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP	DST PUBLIC IP
5.5.5.5	2	up	mpls	mpls	10.10.10.68	10.10.10.54
5.5.5.5	2	up	biz-internet	biz-internet	192.168.1.56	192.168.1.53
5.5.5.5	2	down	public-internet	public-internet	192.168.103.217	192.168.1.55
9.9.9.9	5	up	mpls	mpls	10.10.10.68	10.10.10.69
9.9.9.9	5	up	biz-internet	biz-internet	192.168.1.56	192.168.1.52
9.9.9.9	5	down	public-internet	public-internet	192.168.103.217	192.168.1.55
10.10.10.10	6	up	mpls	mpls	10.10.10.68	10.10.10.70
10.10.10.10	6	up	biz-internet	biz-internet	192.168.1.56	192.168.1.57
10.10.10.10	6	down	public-internet	public-internet	192.168.103.217	192.168.1.55

De esta manera, en la Figura 125, se muestra el establecimiento de sesiones BFD entre el HUB1 y HUB2, ya que la dirección IPV4 del par OMP para el HUB1 es 5.5.5.5 (**SYSTEM IP**). Además, se muestra el establecimiento de sesiones BFD entre el HUB1 y los respectivos miembros del dominio (10.10.10.10, 9.9.9.9).

4.2 Creación de VPN para el tráfico de datos de clientes

En este punto, cabe mencionar que, para la gestión de la red SD-WAN, se hace uso de la VPN0, ya que esta VPN es capaz de ser enrutada tanto hacia internet como por la red MPLS, en este sentido para el tráfico generado dentro de las redes locales de cada nodo de acceso a la red del cliente, se debe crear una VPN distinta a la 0.

La creación de esta VPN tiene como finalidad alojar las redes locales para cada uno de los nodos vEdge y permitir el anuncio de estas a través de los túneles establecidos entre los miembros de la red SD-WAN por la VPN0. Por lo tanto, para el presente trabajo de grado se creará la VPN1.

Es importante destacar que en los vEdge se genera una tabla de enrutamiento específica para cada una de las VPNs. Esto significa que la VPN0 y VPN1 calculan sus propias tablas de enrutamiento, las cuales son independientes entre sí. Además, es necesario tener en cuenta que el tráfico generado dentro de cada VPN no puede ser conmutado hacia otras VPN's.

Para la creación de la VPN1 dentro de los equipos, se deben seguir los siguientes pasos:

1. Acceder a la configuración global del equipo.
2. Crear la VPN1
3. Ingresar a la VPN1.
4. Dentro de la VPN1, se ingresa a la interfaz correspondiente.
5. Asignar una dirección IPv4 a la interfaz correspondiente.
6. Habilitar administrativamente la interfaz.

Se debe asegurar que la configuración de la interfaz debe estar acorde con la Figura 126, en donde al asignar una dirección IPv4 estática (10.10.10.50/29) a la interfaz, se previenen problemas al agregar dicha interfaz al protocolo de enrutamiento dinámico. Esto se debe a que estos equipos no admiten interfaces con direcciones asignadas de forma dinámica.

Figura 126

Interfaces asociadas a la vpn1

```
vEdge-Cuaical-SPOKE1# sh interface vpn 1
interface vpn 1 interface ge0/2 af-type ipv4
ip-address 10.10.10.50/29
if-admin-status Up
if-oper-status Up
if-tracker-status NA
encap-type null
port-type service
mtu 1500
hwaddr 0c:03:53:65:23:03
speed-mbps 1000
duplex full
tcp-mss-adjust 1416
uptime 0:00:24:08
rx-packets 707
tx-packets 187
```

Otro valor importante a verificar es el valor de MTU, ya que para el protocolo IPv4 el valor configurado por defecto es 1500 de acuerdo con (Juniper Networks, 2023), por último, es necesario asegurarse que la interfaz en cuestión (ge0/2) esté configurada en modo **full duplex**, tal como se muestra en la Figura 126. Esta configuración garantizará un correcto funcionamiento de la interfaz y evitará problemas de rendimiento en la comunicación.

Después de haber asociado una interfaz a la VPN1 establecida, es necesario configurar el protocolo de enrutamiento dinámico OSPF dentro de dicha VPN. Para ello, se crea una instancia de OSPF, se define el área en la que se va a trabajar, se habilitan las

interfaces correspondientes y, finalmente, se redistribuyen las rutas aprendidas por el protocolo OMP y las interfaces conectadas.

Figura 127

Configuración de OSPF

```

vEdge-Cuaical-SPOKE1(config-vpn-1)# router ospf
vEdge-Cuaical-SPOKE1(config-ospf)# area 0
vEdge-Cuaical-SPOKE1(config-area-0)# interface ge0/2
vEdge-Cuaical-SPOKE1(ospf-if-ge0/2)# exit
vEdge-Cuaical-SPOKE1(config-area-0)# exit
vEdge-Cuaical-SPOKE1(config-ospf)# redistribute omp
vEdge-Cuaical-SPOKE1(config-ospf)# redistribute connected
vEdge-Cuaical-SPOKE1(config-ospf)# exit
vEdge-Cuaical-SPOKE1(config-router)# commit
Commit complete.

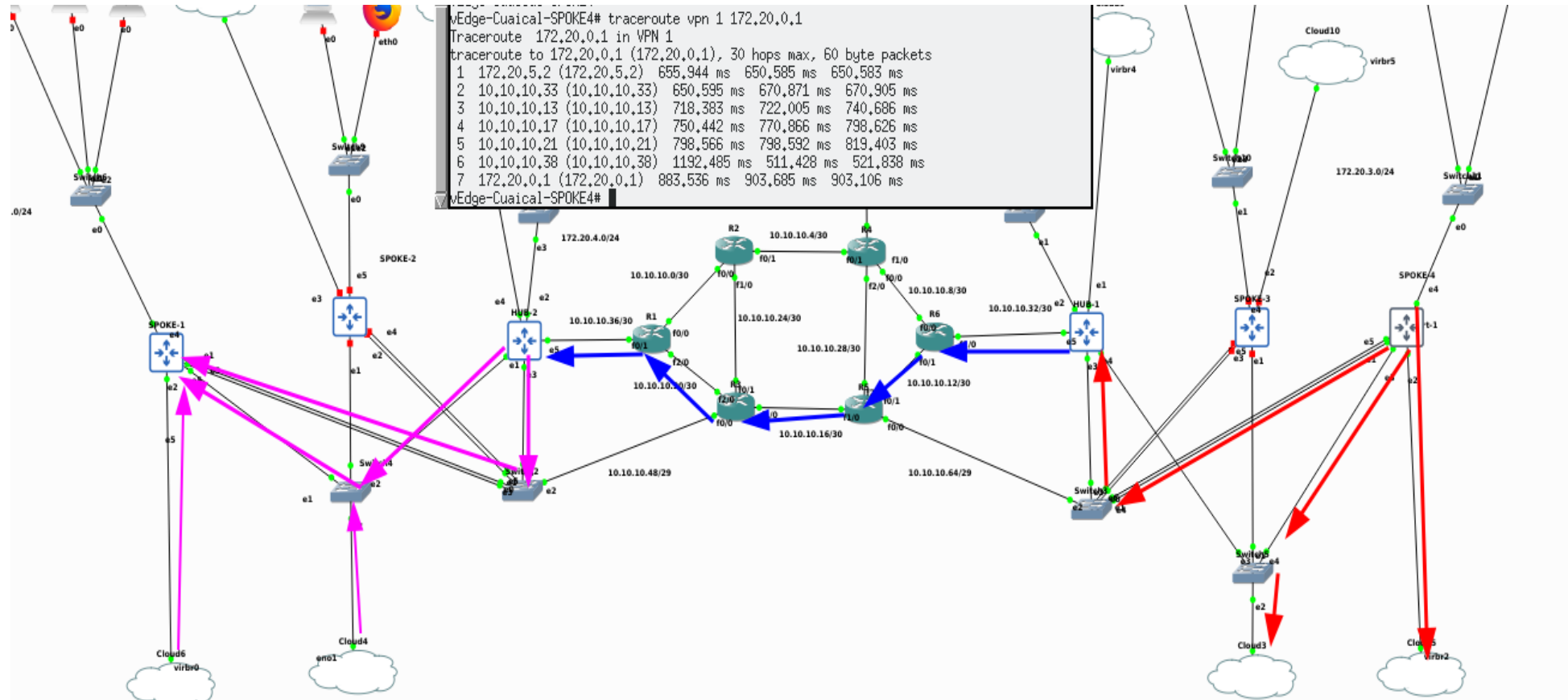
```

Cabe destacar la necesidad de definir una instancia OSPF específica para la VPN deseada; ya que esto asegurará que dicha instancia solo funcione para la VPN en cuestión. Asimismo, es importante que el área en la que opera el dispositivo coincida con el área utilizada en el LER de la red MPLS. Esto permitirá que el equipo participe en el algoritmo OSPF y calcule las mejores rutas para la VPN. La Figura 127 ilustra el proceso de configuración del protocolo OSPF y la redistribución de las rutas necesarias para la VPN, asegurando así que el equipo sea alcanzable dentro de la red.

Las configuraciones mencionadas anteriormente fueron aplicadas a los equipos SPOKE1, SPOKE2, SPOKE3, SPOKE4, HUB1 y HUB2, lo que garantiza que todos los equipos de la red SD-WAN sean alcanzables a través de la red MPLS. Para verificar la comunicación a través de esta red, se realiza una traza desde el SPOKE4 hasta el SPOKE1. Esto proporcionará información sobre la ruta tomada por los paquetes durante su viaje entre los dos nodos.

Figura 128

(a) Demostración de uso de la red MPLS



(b) Verificación de etiquetado de LSR-R5 a LSR-R3

No.	Time	Source	Destination	Protocol	Length	Info
4820	186.566520	192.168.1.55	10.10.10.54	ICMP	199	Destination unreachable (Port unreachable)
4823	190.104013	192.168.1.52	10.10.10.54	ICMP	199	Destination unreachable (Port unreachable)
4826	190.104111	172.20.1.1	172.20.0.1	ICMP	102	Echo (ping) request id=0x4b90, seq=34/8704, ttl=62 (reply in 4853)
4830	190.104180	172.20.1.1	172.20.0.1	ICMP	102	Echo (ping) request id=0x4b90, seq=35/8960, ttl=62 (reply in 4856)
4833	190.104243	172.20.1.1	172.20.0.1	ICMP	102	Echo (ping) request id=0x4b90, seq=36/9216, ttl=62 (reply in 4857)
4836	190.449915	172.20.1.1	172.20.0.1	ICMP	102	Echo (ping) request id=0x4b90, seq=37/9472, ttl=62 (reply in 4858)
4839	191.449335	172.20.1.1	172.20.0.1	ICMP	102	Echo (ping) request id=0x4b90, seq=38/9728, ttl=62 (reply in 4859)
4853	192.509590	172.20.0.1	172.20.1.1	ICMP	102	Echo (ping) reply id=0x4b90, seq=34/8704, ttl=62 (request in 4826)
4856	192.519718	172.20.0.1	172.20.1.1	ICMP	102	Echo (ping) reply id=0x4b90, seq=35/8960, ttl=62 (request in 4830)
4857	192.519737	172.20.0.1	172.20.1.1	ICMP	102	Echo (ping) reply id=0x4b90, seq=36/9216, ttl=62 (request in 4833)
4858	192.519755	172.20.0.1	172.20.1.1	ICMP	102	Echo (ping) reply id=0x4b90, seq=37/9472, ttl=62 (request in 4836)
4859	192.519769	172.20.0.1	172.20.1.1	ICMP	102	Echo (ping) reply id=0x4b90, seq=38/9728, ttl=62 (request in 4839)
4871	192.569719	192.168.1.55	10.10.10.54	ICMP	199	Destination unreachable (Port unreachable)
4873	192.640173	192.168.1.52	10.10.10.54	ICMP	199	Destination unreachable (Port unreachable)
4898	193.559248	192.168.1.55	10.10.10.54	ICMP	199	Destination unreachable (Port unreachable)

```

> Frame 4826: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface -, id 0
> Ethernet II, Src: c2:05:0d:9f:00:10 (c2:05:0d:9f:00:10), Dst: c2:03:0d:7d:00:10 (c2:03:0d:7d:00:10)
MultiProtocol Label Switching Header, Label: 316, Exp: 0, S: 1, TTL: 61
  0000 0000 0001 0011 1100 ..... = MPLS Label: 316
  ..... 0000 ..... = MPLS Experimental Bits: 0
  ..... 1 ..... = MPLS Bottom Of Label Stack: 1
  ..... 0011 1101 = MPLS TTL: 61
> Internet Protocol Version 4, Src: 172.20.1.1, Dst: 172.20.0.1
> Internet Control Message Protocol

```

(c) Verificación de etiquetado de LSR-R3 a LSR-R5

No.	Time	Source	Destination	Protocol	Length	Info
4820	186.566520	192.168.1.55	10.10.10.54	ICMP	199	Destination unreachable (Port unreachable)
4823	190.104013	192.168.1.52	10.10.10.54	ICMP	199	Destination unreachable (Port unreachable)
4826	190.104111	172.20.1.1	172.20.0.1	ICMP	102	Echo (ping) request id=0x4b90, seq=34/8704, ttl=62 (reply in 4853)
4830	190.104180	172.20.1.1	172.20.0.1	ICMP	102	Echo (ping) request id=0x4b90, seq=35/8960, ttl=62 (reply in 4856)
4833	190.104243	172.20.1.1	172.20.0.1	ICMP	102	Echo (ping) request id=0x4b90, seq=36/9216, ttl=62 (reply in 4857)
4836	190.449915	172.20.1.1	172.20.0.1	ICMP	102	Echo (ping) request id=0x4b90, seq=37/9472, ttl=62 (reply in 4858)
4839	191.449335	172.20.1.1	172.20.0.1	ICMP	102	Echo (ping) request id=0x4b90, seq=38/9728, ttl=62 (reply in 4859)
4853	192.509590	172.20.0.1	172.20.1.1	ICMP	102	Echo (ping) reply id=0x4b90, seq=34/8704, ttl=62 (request in 4826)
4856	192.519718	172.20.0.1	172.20.1.1	ICMP	102	Echo (ping) reply id=0x4b90, seq=35/8960, ttl=62 (request in 4830)
4857	192.519737	172.20.0.1	172.20.1.1	ICMP	102	Echo (ping) reply id=0x4b90, seq=36/9216, ttl=62 (request in 4833)
4858	192.519755	172.20.0.1	172.20.1.1	ICMP	102	Echo (ping) reply id=0x4b90, seq=37/9472, ttl=62 (request in 4836)
4859	192.519769	172.20.0.1	172.20.1.1	ICMP	102	Echo (ping) reply id=0x4b90, seq=38/9728, ttl=62 (request in 4839)
4871	192.569719	192.168.1.55	10.10.10.54	ICMP	199	Destination unreachable (Port unreachable)
4873	192.640173	192.168.1.52	10.10.10.54	ICMP	199	Destination unreachable (Port unreachable)
4898	193.559248	192.168.1.55	10.10.10.54	ICMP	199	Destination unreachable (Port unreachable)

```

> Frame 4853: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface -, id 0
> Ethernet II, Src: c2:03:0d:7d:00:10 (c2:03:0d:7d:00:10), Dst: c2:05:0d:9f:00:10 (c2:05:0d:9f:00:10)
MultiProtocol Label Switching Header, Label: 505, Exp: 0, S: 1, TTL: 61
  0000 0000 0001 1111 1001 ..... = MPLS Label: 505
  ..... 0000 ..... = MPLS Experimental Bits: 0
  ..... 1 ..... = MPLS Bottom Of Label Stack: 1
  ..... 0011 1101 = MPLS TTL: 61
> Internet Protocol Version 4, Src: 172.20.0.1, Dst: 172.20.1.1
> Internet Control Message Protocol

```

Una vez que la topología haya alcanzado la convergencia, en la Figura 128(a), se realiza una traza desde la red local de la VPN1 del SPOKE4 hacia la VPN1 del SPOKE1. En esta traza se observa que, para salir de la VPN1 del SPOKE4, se utiliza el HUB1 como punto de salida. El primer salto se realiza hacia la dirección 172.20.5.2, que corresponde

a la VPN1 del HUB1. Después de este salto, el paquete se envía a través de la red MPLS para finalmente ingresar al HUB2 y ser entregado a la dirección 172.20.0.1/24.

De la misma manera, en la Figura 128(a), se resaltan en color rojo los posibles caminos para salir de la VPN1 local del SPOKE4, mientras que en color morado se indican los posibles enlaces que el HUB2 puede utilizar para entregar el paquete.

Por otro lado, en la Figura 128(b) se muestra el etiquetado de los paquetes para un (**echo-request**) desde el SPOKE4 al SPOKE1. En este caso, el LSR-R5 asigna la etiqueta 316 al prefijo 172.20.0.0/24, mientras que para la respuesta (**echo-reply**), tal como se muestra en la Figura 128(c), el LSR-R3 utiliza la etiqueta 505. Estas asignaciones de etiquetas demuestran el correcto funcionamiento de las configuraciones realizadas para la red MPLS, tal como se detalla en el Capítulo III.

Una vez se hayan configurado las redes locales para cada uno de los equipos vEdge, en la tabla de enrutamiento para la VPN1, se observará que ya se anuncian redes por los diferentes enlaces de transporte mediante OMP. Para visualizar esta información, desde la consola de cualquier equipo vEdge se ejecuta el comando **show ip routes vpn #** en donde # representa el número de la VPN deseada. El resultado de la ejecución de este comando se muestra en la Figura 129; en donde, en la columna **VPN**, se evidencia que se encuentra en la RIB de la VPN1, de la misma manera, en la columna **PREFIX**, se evidencia todos los prefijos alcanzables desde esta VPN. Por otro lado, en la columna **TLOC IP**, se muestra la dirección IPv4 del sistema que anuncia el prefijo y en la columna **COLOR**, se muestra el color de transporte remoto que anuncia dicha red.

Figura 129

Rutas aprendidas en vpn 1 por OMP

VPN	PREFIX	PROTOCOL	PROTOCOL SUB TYPE	NEXTHOP IF NAME	NEXTHOP ADDR	NEXTHOP VPN	TLOC IP	COLOR	ENCAP	STATUS
1	10.10.10.48/29	omp		-	-	-	7.7.7.7	biz-internet	ipsec	F,S
1	10.10.10.48/29	omp		-	-	-	7.7.7.7	public-internet	ipsec	F,S
1	10.10.10.64/29	omp		-	-	-	9.9.9.9	biz-internet	ipsec	F,S
1	10.10.10.64/29	omp		-	-	-	9.9.9.9	public-internet	ipsec	F,S
1	172.20.0.0/24	omp		-	-	-	6.6.6.6	biz-internet	ipsec	F,S
1	172.20.0.0/24	omp		-	-	-	6.6.6.6	public-internet	ipsec	F,S
1	172.20.1.0/24	ospf	A	ge0/3	-	-	-	-	-	-
1	172.20.1.0/24	connected		ge0/3	-	-	-	-	-	F,S
1	172.20.2.0/24	omp		-	-	-	7.7.7.7	biz-internet	ipsec	F,S
1	172.20.2.0/24	omp		-	-	-	7.7.7.7	public-internet	ipsec	F,S
1	172.20.3.0/24	omp		-	-	-	9.9.9.9	biz-internet	ipsec	F,S
1	172.20.3.0/24	omp		-	-	-	9.9.9.9	public-internet	ipsec	F,S
1	192.168.1.0/24	omp		-	-	-	7.7.7.7	biz-internet	ipsec	F,S
1	192.168.1.0/24	omp		-	-	-	7.7.7.7	public-internet	ipsec	F,S
1	192.168.1.0/24	omp		-	-	-	9.9.9.9	biz-internet	ipsec	F,S
1	192.168.1.0/24	omp		-	-	-	9.9.9.9	public-internet	ipsec	F,S
1	192.168.100.0/24	omp		-	-	-	9.9.9.9	biz-internet	ipsec	F,S
1	192.168.100.0/24	omp		-	-	-	9.9.9.9	public-internet	ipsec	F,S
1	192.168.101.176/30	natpool-outside		natpool1	-	-	-	-	-	F,S
1	192.168.104.0/24	omp		-	-	-	7.7.7.7	biz-internet	ipsec	F,S
1	192.168.104.0/24	omp		-	-	-	7.7.7.7	public-internet	ipsec	F,S
1	192.168.122.0/24	omp		-	-	-	7.7.7.7	biz-internet	ipsec	F,S
1	192.168.122.0/24	omp		-	-	-	7.7.7.7	public-internet	ipsec	F,S

A pesar de que no es posible alcanzar el plano de control a través de la red MPLS, los vEdge utilizan los enlaces que sí permiten esta comunicación para anunciar la presencia de un enlace de transporte con color MPLS. Esto permite que el plano de control pueda propagar esta información a todos los equipos de la red SD-WAN, lo que les permite establecer túneles de forma transparente sobre la red MPLS.

En este sentido, en la Figura 130 se muestra un ejemplo de un equipo que anuncia un enlace de transporte MPLS (`tloc entries for 4.4.4.4`) y utiliza el encapsulamiento IPSEC para los túneles. Esto indica que el equipo tiene conectividad a través de la red MPLS y puede utilizarla para formar túneles con otros nodos de la red SD-WAN.

Cabe mencionar, que esta información solo puede ser desplegada en el vSmart (plano de control), haciendo uso del comando `show omp tlocs`, esto se debe a que este es el equipo encargado de recibir y redistribuir los TLOC's sobre toda la red SD-WAN.

Figura 130

TLOC con color MPLS recibido en el vSmart

```
vSmart_CuaicalA# show omp tlocs
-----
tloc entries for 4.4.4.4
      mpls
      ipsec
-----
```

Es importante mencionar también que los túneles se forman en función del color asignado al protocolo TLOC. Esto significa que, para los colores "public-internet" y "biz-internet", es posible establecer túneles de manera cruzada, es decir, entre nodos que utilizan diferentes colores (por ejemplo, un túnel entre un transporte con color "public-internet" y otro con color "biz-internet", y viceversa), tal como se muestra en la Figura 131.

Sin embargo, es importante tener en cuenta que esto no es factible con el color MPLS, ya que no es accesible directamente desde internet y no se puede utilizar el protocolo de traducción de direcciones de red (NAT). A pesar de ello, debido al funcionamiento de la red OMP, el equipo trata de establecer sesiones de este tipo, tal como se muestra en la Figura 131 (`down mpls public-internet`), lo cual consume recursos de procesamiento innecesariamente. Para evitar este problema, dentro del enlace con color MPLS se debe ejecutar el comando `color mpls restrict`, comando con el cual se define que no se intente realizar conexiones que no sean `mpls-mpls`.

Figura 131

Túneles establecidos en SPOKE 2

```
Edge-Cuaical-SPOKE2# show bfd sessions
```

SYSTEM IP	DST PUBLIC		STATE	DETECT		SOURCE TLOC		REMOTE TLOC		DST PUBLIC IP
	SITE ID	PORT		ENCAP	MULTIPLIER	COLOR	TX INTERVAL(msec)	COLOR	UPTIME	
.5.5.5	2	12346	up	ipsec	7	mpls	1000	mpls	0:00:26:06	10.10.10.52
.5.5.5	2	12366	up	ipsec	7	mpls	1000	biz-internet	0:00:00:05	10.10.10.52
.5.5.5	2	31448	down	ipsec	7	mpls	1000	public-internet	0:00:00:05	10.10.10.52
.5.5.5	2	31448	down	ipsec	7	ipsec	1000	NA	0	192.168.1.53
.5.5.5	2	1073	up	ipsec	7	public-internet	1000	mpls	0:00:26:00	192.168.1.55
.5.5.5	2	12366	up	ipsec	7	public-internet	1000	biz-internet	0:00:00:04	192.168.1.55
.5.5.5	2	31448	up	ipsec	7	public-internet	1000	public-internet	0:00:00:17	192.168.1.55
.5.5.5	2	1073	down	ipsec	7	biz-internet	1000	mpls	0:00:00:17	192.168.100.180
.5.5.5	2	1073	down	ipsec	7	ipsec	1000	NA	0	192.168.1.7
.5.5.5	2	12366	down	ipsec	7	biz-internet	1000	biz-internet	0:00:00:04	192.168.100.180
.5.5.5	2	12366	down	ipsec	7	ipsec	1000	NA	0	192.168.1.53
.5.5.5	2	31448	down	ipsec	7	biz-internet	1000	public-internet	0:00:00:17	192.168.100.180

4.3 Uso de ingeniería de tráfico desde las políticas del vManage

La ingeniería de tráfico en SD-WAN brinda la capacidad de gestionar y dirigir flujos de tráfico específicos a través de enlaces deseados, teniendo en consideración la importancia y los requisitos de las aplicaciones. En este sentido, en el presente trabajo de grado, se lleva a cabo un control de tráfico mediante el mapeo de aplicaciones para determinar el enlace de salida más apropiado.

El enfoque de mapeo de aplicaciones implica identificar y clasificar las aplicaciones según sus características y necesidades de rendimiento. Mediante la configuración de políticas y reglas de enrutamiento, se asigna a cada aplicación un enlace de salida preferido. Esto permite que el tráfico de cada aplicación sea dirigido a través del enlace que mejor se adapte a sus requisitos, considerando aspectos como el ancho de banda, la latencia, la pérdida de paquetes y otros parámetros relevantes.

Para configurar ingeniería de tráfico desde el plano de gestión, se debe seguir los siguientes pasos:

1. Acceder a la sección de "Configuración" en la interfaz web del vManage.
2. Dentro de la sección de "Configuración", buscar y seleccionar "Políticas" (**Policies**).
3. Una vez en la sección de "Políticas", elegir la opción de editar la política existente para HUB & SPOKE. Esto te permitirá modificar la configuración de la política ya creada.
4. Dentro de la configuración de la política, buscar la opción de "Reglas de tráfico" (**Traffic Rules**). Esta sección permitirá definir las reglas específicas para la ingeniería de tráfico en la red superpuesta.
5. Añadir una nueva secuencia de reglas haciendo clic en ingeniería de tráfico (**Traffic Engineering**) tal como se muestra en la Figura 132.

Figura 132

Aplicación de Ingeniería de Tráfico a la red SD-WAN (Monitor->Configuration->Policies->Topologia_HUB-N_SPOKE->Traffic Rules->add)



6. En este punto, cabe considerar que la familia de aplicaciones debe ser creada tal como se muestra en la Figura 133, en donde se crea la lista de aplicaciones

Trafico_RTMP_Streaming_De_Video y el protocolo sobre el cual trabajará es RTMP (Real Time Messaging Protocol). En este sentido, dentro de la nueva secuencia creada, se ingresa el emparejamiento (**Match**) el cual para este caso es (**Application/Application Family List**) tal como se muestra en la Figura 134, una vez elegido el emparejamiento, se debe ingresar las acciones (**Actions**), en donde se debe definir un TLOC mpls en (**Local TLOC List**) y un encapsulamiento IPsec en (**Encapsulation**), tal como se muestra en la Figura 135.

Figura 133

Creación de Famili Llist (Configuration->Policies->applications)

The screenshot shows a configuration window titled 'New Application List'. It has a text input field for 'Application List Name' containing 'Trafico_RTMP_Streaming_De_Video'. Below this, there are two radio buttons: 'Application' (which is selected) and 'Application Family'. A dropdown menu below the radio buttons shows 'Real Time Messaging Protocol'. At the bottom right, there are 'Add' and 'Cancel' buttons.

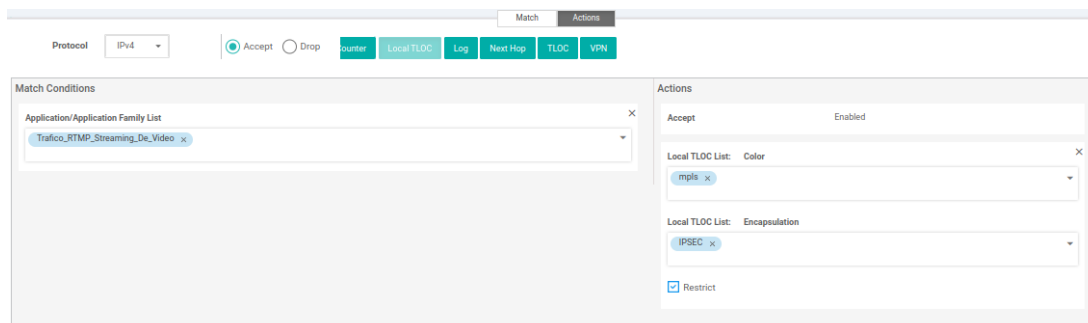
Figura 134

Emparejamiento con la familia de aplicaciones

The screenshot shows the 'Traffic Engineering' configuration page. The 'Sequence Rule' section is active, and the 'Match' tab is selected. The 'Match Conditions' section shows 'Application/Application Family List' selected in the dropdown menu, with 'Trafico_RTMP_Streaming_De_Video' listed below it. The 'Actions' section shows 'Accept' and 'Enabled'.

Figura 135

Definir acciones para el emparejamiento





En resumen, la acción para este apartado es identificar las aplicaciones seleccionadas y definir un TLOC local para su salida, de esta manera se puede diferenciar cada aplicación y definir un enlace para la comunicación. En este caso, se usa el enlace **MPLS restrict** para el tráfico de streaming de video con el protocolo RTMP.

Es importante tener en cuenta que la nueva política ingresada no surtirá efecto hasta que se le asignen los sitios correspondientes y se configure una VPN a través de la cual operará. Para ello, es necesario asignar todos los sitios creados previamente y configurar el servicio de la VPN0 tal como se muestra en la Figura 136.

Figura 136

Ingreso de sitios y vpn a la política

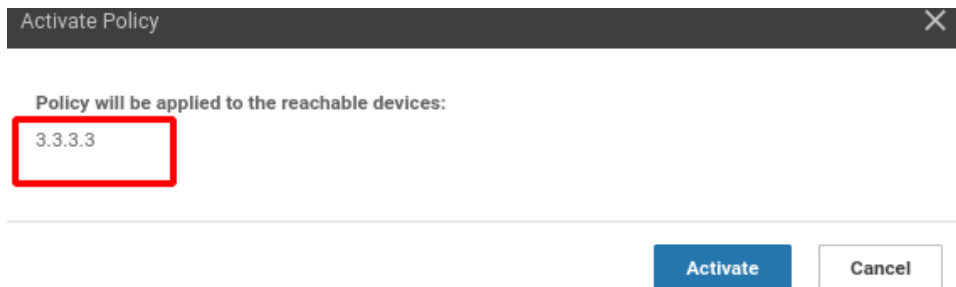
Site List	VPN List	Direction	Action
Hub_sitio_2, Spokes_sitio1, Hub_sitio_1, Spokes_sitio2	Servicio_VPN_0	service	 

Una vez que se haya creado la política y asignado los sitios, se debe activar o actualizar la política en operación en caso de ya estar activa, de esta manera al activar la

política se mostrará los dispositivos alcanzables para el plano de gestión, en este caso solamente se encuentra uno, como se muestra en la Figura 137.

Figura 137

Envío de políticas a vSmart



Es importante destacar que, al activar la política centralizada, el resultado esperado debe ser similar al que se muestra en la Figura 138. En esta figura, se observa un estado satisfactorio (**success**) para la actualización de la política. Sin embargo, si se visualiza un estado fallido (**fail**) en lugar de uno satisfactorio, es necesario revisar los registros (**logs**) que se presentan en la misma figura. Estos registros proporcionarán información sobre los errores ocurridos durante el envío de la política.

Algunas posibles causas de un estado fallido podrían ser que los túneles en el vSmart no estén activos, que el vSmart no esté funcionando correctamente o que se hayan ingresado TLOCs o IDs de sitio incorrectos en la configuración. Es importante revisar cuidadosamente estos aspectos y corregir cualquier error para asegurar que la actualización de la política sea exitosa.

De este modo, dentro del vSmart se evidenciará que las políticas están activas, tal como se muestra en la Figura 139; en este sentido, se aprecia la política (`data-policy _Service_VPN1_Ingenier_695689183`), la cual se aplica a la lista de vpn's denominada `Service_VPN1`; esta regla específica tiene asignada la secuencia 1.

En esta regla, se realiza un emparejamiento para cualquier dirección IPv4 y para las aplicaciones que pertenecen a la familia `Trafico_RTMP_Streaming_De_Video`. Esto significa que se aceptará el tráfico de cualquier dirección IP dentro de la familia Ipv4 y de las aplicaciones relacionadas con el streaming de video en tiempo real. En este sentido, si el tráfico proveniente de la VPN específica cumple con el match, será aceptado y la acción será reenviarlo por el enlace con color `mpls restrict` con un encapsulamiento `ipsec`.

Por último, la acción por defecto es eliminar, lo que significa que cualquier paquete que no cumpla con las condiciones establecidas en la regla será descartado.

4.4 Pruebas de funcionamiento

En este apartado, se realizan las pruebas de funcionamiento a la red propuesta, en este sentido se verifica tanto las políticas creadas para la topología SHHS, como las configuraciones para ingeniería de tráfico.

En relación a SHHS, permite filtrar los localizadores de transporte (tlocs) según el nodo de origen, lo que implica que se pueden establecer políticas en el vManage para determinar las comunicaciones permitidas entre equipos. Por ejemplo, si un nodo actúa como HUB, podrá comunicarse con otros nodos HUB y con los SPOKES pertenecientes a su dominio. Por otro lado, si un nodo es un SPOKE, solo podrá comunicarse con el HUB de su zona. Esto reduce la cantidad de sesiones BFD (Bidirectional Forwarding

Detection) que cada equipo debe manejar y de esta manera, optimiza el enrutamiento en la red SD-WAN.

La principal ventaja de esta configuración es que se reduce el número de conexiones que se deben manejar en el plano de datos. Esto implica que se utiliza menos recursos para el establecimiento de los túneles y se pueden aprovechar de mejor manera en el enrutamiento de paquetes. Al reducir la carga de trabajo en el plano de datos, se mejora la eficiencia y el rendimiento general de la red.

Por consiguiente, desde el plano de control, no se registran cambios, puesto que, los vEdge anuncian sus tres enlaces de transporte mediante el protocolo TLOC, tal como se muestra en la Figura 140. Esto implica que el vSmart no sufre cambios en el consumo de recursos, ya que aún debe gestionar los 3 enlaces de transporte de cada equipo.

Figura 140

Verificación Conexiones Plano de Control

```
vSmart_CuaicalA# show control connections
```

INDEX	TYPE	PEER	PEER			SITE	DOMAIN	PEER	PEER	
			PEER	PEER	PEER				PRIV	PEER
			PROT	SYSTEM	IP	ID	ID	PRIVATE	IP	
			PORT	REMOTE	COLOR	STATE	UPTIME			
0	vedge	dtls 4.4.4.4	12346	mpls	1	up	0:00:40:21	10.10.10.68		12346 192.168.1.7
0	vedge	dtls 4.4.4.4	52588	public-internet	1	up	0:00:08:05	192.168.103.217		12366 192.168.1.53
0	vedge	dtls 4.4.4.4	12346	biz-internet	1	up	0:00:40:56	192.168.1.56		12346 192.168.1.56
0	vedge	dtls 5.5.5.5	1076	mpls	2	up	0:00:25:47	10.10.10.54		12346 192.168.1.7
0	vedge	dtls 5.5.5.5	31448	public-internet	2	up	0:00:08:38	192.168.102.2		12346 192.168.1.53
0	vedge	dtls 7.7.7.7	1127	mpls	4	up	0:00:09:21	10.10.10.52		12346 192.168.1.7
0	vedge	dtls 7.7.7.7	38503	biz-internet	4	up	0:00:01:48	192.168.100.180		12406 192.168.1.53
0	vedge	dtls 7.7.7.7	12346	public-internet	4	up	0:00:25:35	192.168.1.55		12346 192.168.1.55
0	vedge	dtls 0.0.0.0	1057	mpls	5	up	0:00:08:21	10.10.10.69		12346 192.168.1.7
0	vedge	dtls 0.0.0.0	12346	biz-internet	5	up	0:00:32:30	192.168.1.52		12346 192.168.1.52
0	vedge	dtls 0.0.0.0	48100	public-internet	5	up	0:00:08:05	192.168.104.157		12346 192.168.1.53
0	vbond	dtls 0.0.0.0	12346	default	0	up	0:01:03:33	192.168.1.4		12346 192.168.1.4
0	vmanage	dtls 1.1.1.1	12346	default	1	up	0:01:03:29	192.168.1.3		12346 192.168.1.3

4.4.1. Verificación de Sesiones BFD en HUB's y SPOKES

En el plano de datos, se producen cambios notables en comparación con el plano de control en un entorno SD-WAN. Ya que, al ingresar a un SPOKE, se reduce drásticamente el número de sesiones BFD establecidas, pasando de 45 a solo 3 sesiones BFD gracias a las restricciones configuradas en la política centralizada, tal como se muestra en la Figura 141. En este sentido, desde el SPOKE1, solo se establecen sesiones BFD con el equipo 5.5.5.5 (HUB2) por cada uno de los enlaces de transporte (`mpls-mpls; public-internet - public-internet; biz-internet - biz-internet`). Estas modificaciones optimizan el uso de recursos y mejoran la eficiencia de la red en el plano de datos.

Figura 141

Verificación sesiones BFD SPOKE1

```
vEdge-Cuaical-SPOKE1# show bfd sessions
```

SYSTEM IP	SITE ID	STATE	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP	DST PUBLIC IP
5.5.5.5	2	up	mpls	mpls	10.10.10.53	10.10.10.54
5.5.5.5	2	up	public-internet	public-internet	192.168.1.54	192.168.1.55
5.5.5.5	2	up	biz-internet	biz-internet	192.168.122.239	192.168.1.53

En contraste con las sesiones establecidas desde un SPOKE, en un HUB se establecen sesiones tanto con los SPOKES de su propio dominio como con los HUBS de otros dominios. Esto resulta en el aumento del número de sesiones BFD a 9 debido a las restricciones establecidas en las políticas. De este modo, en la Figura 142 se muestra las conexiones realizadas por el HUB1 con sus vecinos, incluyendo 3 conexiones hacia el SPOKE3, 3 hacia el SPOKE4 y 3 conexiones con el HUB2. Estas conexiones permiten un mayor flujo de datos entre los diferentes nodos de la red SD-WAN, lo que mejora significativamente la comunicación y el enrutamiento dentro del sistema.

Figura 142**Verificación sesiones BFD HUB1**

```
vEdge-Cuaical-HUB1(config-interface-ge0/0)# do show bfd sessions
```

SYSTEM IP	SITE ID	STATE	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP	DST PUBLIC IP
5.5.5.5	2	up	mpls	mpls	10.10.10.68	10.10.10.54
5.5.5.5	2	up	biz-internet	biz-internet	192.168.1.56	192.168.1.53
5.5.5.5	2	down	public-internet	public-internet	192.168.103.217	192.168.1.55
9.9.9.9	5	up	mpls	mpls	10.10.10.68	10.10.10.69
9.9.9.9	5	up	biz-internet	biz-internet	192.168.1.56	192.168.1.52
9.9.9.9	5	down	public-internet	public-internet	192.168.103.217	192.168.1.55
10.10.10.10	6	up	mpls	mpls	10.10.10.68	10.10.10.70
10.10.10.10	6	up	biz-internet	biz-internet	192.168.1.56	192.168.1.57
10.10.10.10	6	down	public-internet	public-internet	192.168.103.217	192.168.1.55

4.4.2. Verificación de rutas para la VPN 1

Como se mencionó anteriormente, se ha creado la VPN1 para el tráfico de datos de clientes (redes locales de cada nodo en el entorno SD-WAN); es importante tener en cuenta que cada nodo anuncia la presencia de estas redes a través de la VPN0. Como resultado, al examinar la tabla de enrutamiento (RIB) de la VPN1, se observarán rutas duplicadas. Esta duplicidad surge debido a que los prefijos de las redes locales se anuncian a través del protocolo OMP (Overlay Management Protocol) por todos los enlaces de transporte disponibles en la red SD-WAN.

Cabe señalar que la presencia de rutas duplicadas es una consecuencia inherente de la forma en que se difunden y anuncian los prefijos en la arquitectura SD-WAN. En este sentido, para visualizar y comprender esta tabla de enrutamiento, desde la consola del equipo deseado, se ejecuta el comando `show ip routes vpn #`, en donde # identifica el número de la VPN específica, tal como se muestra en la Figura 143.

Figura 143

RIB de HUB1 para la VPN1

```

MEdge-Cuaical-HUB1(config-interface-ge0/0)# do show ip routes vpn 1
Codes Proto-sub-type:
 IA -> ospf-intra-area, IE -> ospf-inter-area,
 E1 -> ospf-external1, E2 -> ospf-external2,
 N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
 e -> bgp-external, i -> bgp-internal
Codes Status flags:
 F -> fib, S -> selected, I -> inactive,
 B -> blackhole, R -> recursive

```

VPN	PREFIX	PROTOCOL	PROTOCOL SUB TYPE	NEXTHOP IF NAME	NEXTHOP ADDR	NEXTHOP VPN	TLOC IP	COLOR	ENCAP	STATUS
1	0.0.0.0/0	static	-	ge0/4	10.10.10.33	-	-	-	-	F,S
1	10.10.10.32/30	connected	-	ge0/4	-	-	-	-	-	F,S
1	10.10.10.36/30	omp	-	-	-	-	5.5.5.5	mpls	ipsec	F,S
1	10.10.10.36/30	omp	-	-	-	-	5.5.5.5	biz-internet	ipsec	F,S
1	172.20.0.0/24	static	-	ge0/4	10.10.10.33	-	-	-	-	F,S
1	172.20.1.0/24	omp	-	-	-	-	10.10.10.10	mpls	ipsec	F,S
1	172.20.1.0/24	omp	-	-	-	-	10.10.10.10	biz-internet	ipsec	F,S
1	172.20.2.0/24	static	-	ge0/4	10.10.10.33	-	-	-	-	F,S
1	172.20.3.0/24	omp	-	-	-	-	9.9.9.9	mpls	ipsec	F,S
1	172.20.3.0/24	omp	-	-	-	-	9.9.9.9	biz-internet	ipsec	F,S
1	172.20.4.0/24	static	-	ge0/4	10.10.10.33	-	-	-	-	F,S
1	172.20.5.0/24	connected	-	ge0/1	-	-	-	-	-	F,S

En la información proporcionada por la RIB para la VPN-1 en el HUB1 de la Figura 143, se presentan los siguientes campos, los cuales se detallan a continuación:

1. **VPN**: Este campo indica el número de la VPN para la cual se ha instalado la ruta.
2. **PREFIX**: En esta columna, se listan los prefijos alcanzables por la VPN-1 desde el HUB1.
3. **PROTOCOL**: En este campo, se muestra el protocolo a través del cual se aprendió la ruta instalada. Puede ser **static**, **connected**, **omp**, **ospf**, entre otros.
4. **NEXT HOP IF NAME**: Este campo tiene valor únicamente cuando se instala una ruta estática en el dispositivo o cuando se trata de una red directamente conectada para la VPN específica. De este modo, muestra la interfaz física a través de la cual se puede acceder a la ruta.
5. **NEXT HOP ADDRESS**: A diferencia del campo **NEXT HOP**, este campo muestra la dirección IPv4 del siguiente salto en lugar de la interfaz de salida.

6. **TLOC IP**: En este campo se registran las direcciones IPv4 del sistema del par OMP que anuncia la ruta. En el caso del HUB1, se muestran tres direcciones diferentes: `5.5.5.5`, `9.9.9.9` y `10.10.10.10`.
7. **COLOR**: Este campo registra el color a través del cual se aprendió la ruta. En este caso, se registran los colores `"mpls"` y `"biz-internet"`.
8. **STATUS**: En esta columna, se muestra si las rutas están instaladas en la FIB. Además, indica si la ruta ha sido seleccionada para el reenvío de paquetes y si está activa o no(**F, S**).

En la red propuesta, cada vEdge establece su propia RIB en donde se registran las rutas aprendidas mediante OMP. En este sentido, es esencial que desde los HUBs se anuncie una ruta por defecto hacia los SPOKES de su dominio. En el caso del HUB2, ya se realiza este anuncio de ruta por defecto, permitiendo que los SPOKES tengan salida a Internet ([ver Figura 99](#)). Sin embargo, en el HUB1 no se ha configurado esta opción. Para solucionarlo, dentro de la VPN1, se anuncia una ruta por defecto utilizando el comando `ip route 0.0.0.0/0 null0`. Esto permite al HUB1 anunciar dicha ruta hacia los SPOKES, logrando así un enrutamiento adecuado de los paquetes en la red.

4.4.3. Verificación de política enviada desde el vSmart en vEdge

A diferencia de la política SHHS, que opera de forma transparente¹², en este caso, al requerir coincidencias en el tráfico proveniente de la VPN1, dicha política debe ser instalada en los equipos vEdge. Para visualizarla, desde la terminal, se debe ejecutar el comando `"show policy from-vsmart"`, tal como se muestra en la Figura 144. La

¹² El vSmart se encarga de filtrar y anunciar los TLOC's a los vEdge, sin necesidad de la intervención de estos.

ejecución de este comando desplegará la política de tráfico previamente creada y mostrada desde el vSmart. Esta acción permite verificar y examinar los detalles de la política de enrutamiento y los criterios de coincidencia utilizados en la red SD-WAN.

Figura 144

Política de Ingeniería de tráfico vista en SPOKE4

```

vEdge-Cuaical-SPOKE4# show policy from-vsmart
from-vsmart data-policy _Service_VPN1_Ingeni_-1160468007
direction from-service
vpn-list Service_VPN1
sequence 1
match
source-ip 0.0.0.0/0
app-list Trafico_RTMP_Streaming_De_Video
action accept
set
local-tloc-list
color mpls
encap ipsec
restrict
default-action accept
from-vsmart lists vpn-list Service_VPN1
vpn 1
from-vsmart lists app-list Trafico_RTMP_Streaming_De_Video
app rtmp

```

En la sección 4.3 se proporcionó una explicación detallada sobre el funcionamiento de esta política. Al poder visualizar la política en el plano de datos, se confirma que las configuraciones realizadas en el plano de control han sido implementadas correctamente. Esta visualización verifica que las políticas de enrutamiento y los criterios de coincidencia establecidos en el plano de control se están aplicando de manera efectiva en la red SD-WAN.

4.4.1.1 Verificación de match en la política de datos

Para verificar las coincidencias (match) en la política, es necesario desplegar los flujos correspondientes a la VPN1; para ello, se ejecuta el comando "**show app dpi flows vpn 1**" desde la consola del equipo deseado, tal como se muestra en la Figura 145.

En la figura se puede apreciar que la aplicación rtmp (`application rtmp`) está activa y ha realizado match en 87151 paquetes. Este despliegue de flujos permite observar el tráfico correspondiente a la VPN1 y verificar si las políticas de enrutamiento y los criterios de coincidencia están funcionando correctamente.

Figura 145

Flujos para la VPN1 desde SPOKE4

```

/Edge-Cuaical-SPOKE4# show app dpi flows vpn 1
app dpi flows vpn 1 172.20.1.253 172.20.5.1 37158 1935 tcp
application rtmp
family "Network Service"
active-since 2023-07-02T19:37:13+00:00
packets 87151
octets 96117943
app dpi flows vpn 1 172.20.5.1 172.20.1.253 36368 1716 tcp
application unknown
family Standard
active-since 2023-07-02T19:00:39+00:00
packets 1185
octets 69117
/Edge-Cuaical-SPOKE4# █

```

De este modo, la Figura 145 muestra que, la política está activa en todos los equipos disponibles en el plano de datos. Esto significa que cada uno de ellos tiene la capacidad de realizar match con el tráfico relacionado con RTMP y determinar su salida a través del enlace `mpls-mpls restrict` definido en la política de ingeniería de tráfico. Esta configuración garantiza que el tráfico específico de RTMP sea enrutado de manera adecuada según las reglas establecidas en la política, lo que contribuye a un mejor control y gestión del flujo de datos en la red SD-WAN.

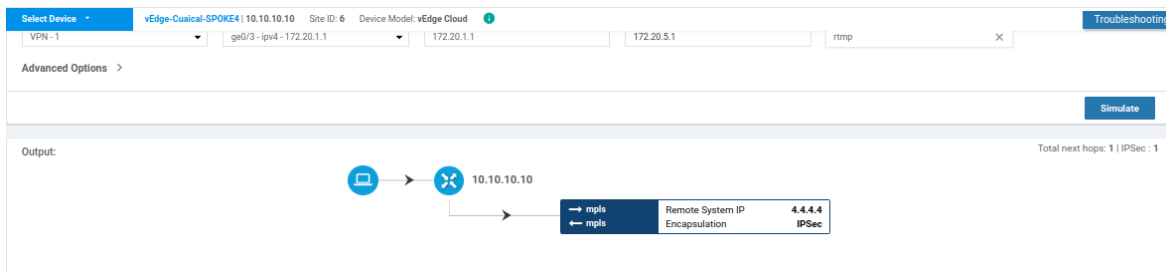
4.4.4. Simulación de flujos RTMP (*Real Time Messaging Protocol*)

Además de la verificación a través de las coincidencias (matches) en el plano de datos, desde el plano de control es posible simular flujos específicos para comprobar el

correcto funcionamiento de las políticas creadas. Esta capacidad de simulación se logra utilizando la opción de **Troubleshooting**, la cual permite establecer una VPN sobre la cual se desea simular el flujo. Asimismo, se puede seleccionar la interfaz por la cual se desea simular este, definir una dirección IPv4 de origen y destino, y especificar el protocolo a utilizar para el flujo, tal como se muestra en la Figura 146.

Figura 146

Simulación de Flujo RTMP (Monitor->Network->SPOKE4->Troubleshooting->Simulate Flows)



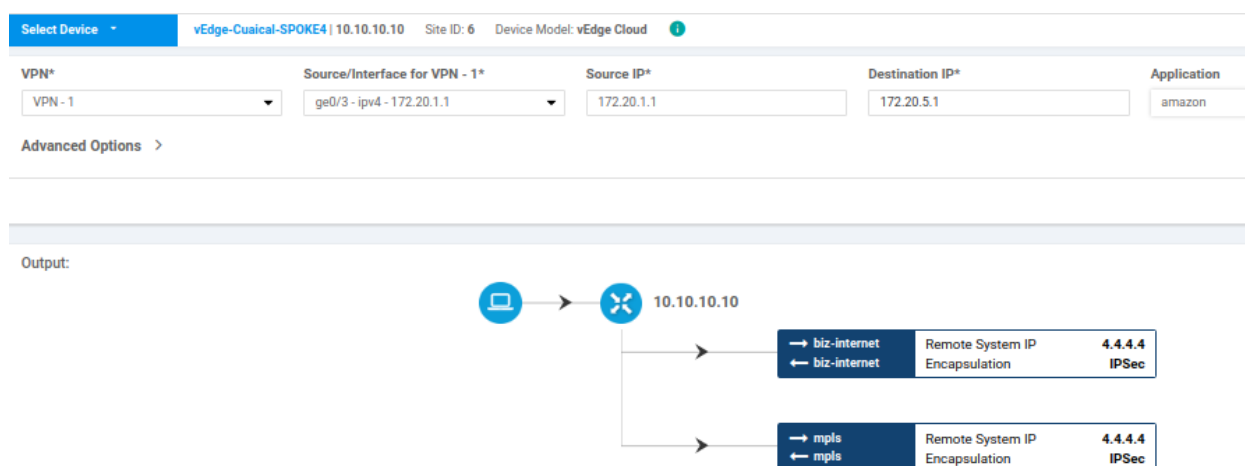
Gracias a esta funcionalidad de simulación, es posible verificar de forma controlada y precisa cómo se comportarán los flujos de tráfico según las políticas configuradas. Esto permite probar diferentes escenarios y asegurar que las políticas están correctamente aplicadas, contribuyendo a un mejor control y ajuste de la red SD-WAN.

Al ejecutar la simulación del flujo RTMP mostrada en la Figura 146, se evidencia que, desde el SPOKE4, para las aplicaciones que utilizan el protocolo RTMP, el túnel que debe utilizarse es el mpls-mpls. Esta verificación confirma que las configuraciones realizadas para la ingeniería de tráfico están funcionando correctamente. De esta manera, se asegura que el tráfico de las aplicaciones RTMP se dirija a través del túnel designado, optimizando así el enrutamiento y garantizando un rendimiento óptimo para estas aplicaciones.

Por otro lado, al ejecutar la simulación con las mismas condiciones mostradas en la Figura 146, pero cambiando el protocolo de capa aplicación, tal como se muestra en la Figura 147, se observa que el flujo no coincide con la política creada. Esto significa que no se puede utilizar únicamente el túnel `mpls-mpls` para enrutar este tipo de tráfico, ya que no se cumplen los criterios de coincidencia establecidos en la política. Esta observación demuestra que las configuraciones de las políticas están diseñadas de manera precisa y selectiva, permitiendo un enrutamiento diferenciado y adecuado para cada tipo de tráfico en la red SD-WAN.

Figura 147

Simulación de flujo no RTMP



4.4.5. Generación de tráfico RTMP (Streaming de video) y HTTP (web)

El servicio web se aloja en el HUB1 y para acceder a él desde los nodos de la red OMP, se utiliza la dirección IPv4 172.20.5.1. En este sentido, para visualizar la página web, es necesario ingresar la URL: <http://172.20.5.1>. Al hacerlo, se mostrará la página web correspondiente, tal como se ilustra en la Figura 148.

Figura 148

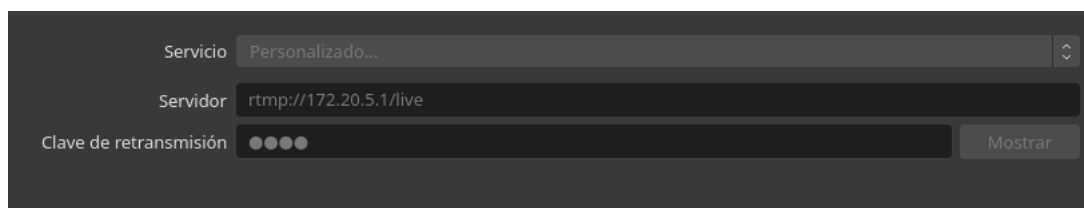
Ingreso al servicio web, desde SPOKE4



Por otro lado, para iniciar el streaming de video, se activa la transmisión desde OBS, tal como se muestra en la Figura 149. Al igual que con el servicio web, el enrutamiento del tráfico se realiza mediante SHHS, lo que evita el acceso directo entre los nodos. En este escenario, los HUBS desempeñan un papel crucial al orquestar la comunicación para permitir una transmisión extremo a extremo.

Figura 149

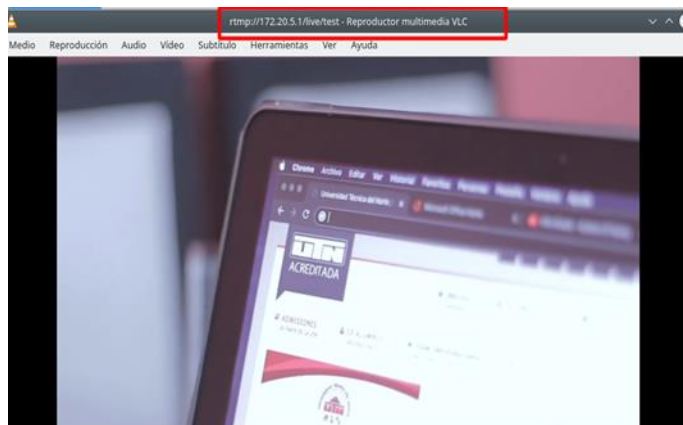
Inicio de transmisión con OBS



Una vez iniciada la transmisión desde la red LAN del HUB1, ya es posible acceder al Streaming de video, tal como se muestra en la Figura 147. En este sentido, de manera subjetiva, se concluye que el Streaming de Video se realiza de manera adecuada, ya que no sufre cortes y es posible acceder desde cualquier nodo perteneciente a la red SD-WAN, garantizando una experiencia de transmisión fluida y sin interrupciones.

Figura 150

Ingreso de Streaming de video desde SPOKE-4



4.4.6. Verificación de métricas sobre la red SD-WAN

Las métricas presentadas en la Figura 107 se calculaban en base a datos recolectados por el protocolo BFD sin tráfico real en la red. Sin embargo, al transmitir video a través de RTMP, se generará un tráfico real que permitirá obtener métricas más precisas. En este caso, al utilizar una política de enrutamiento específica para el túnel **mpls-mpls**, se prestará especial atención a estos túneles.

En este sentido, en la Figura 151 se destaca en rojo el túnel **mpls-mpls** para el SPOKE4 y HUB1, en el cual se tiene la siguiente información: **Jitter(ms) : 6.17**, **Loss (%) : 0.03**, **Latency (ms) : 28.83**, **QoE Score : 10**. Por otro lado, en la Figura 107, las métricas para otro túnel (configurado sin las mejoras de SDWAN) presenta valores más altos: **jitter: 9.78ms**, **Loss (%) : 0.31%**, **y Latency (ms) : 32.11ms**. Estas mejoras en las métricas demuestran una mayor calidad y rendimiento en la transmisión de datos a través del túnel **mpls-mpls** en comparación con los valores de la red en un estado por defecto.

Figura 151**Métricas túnel mpls-mpls SPOKE-4**

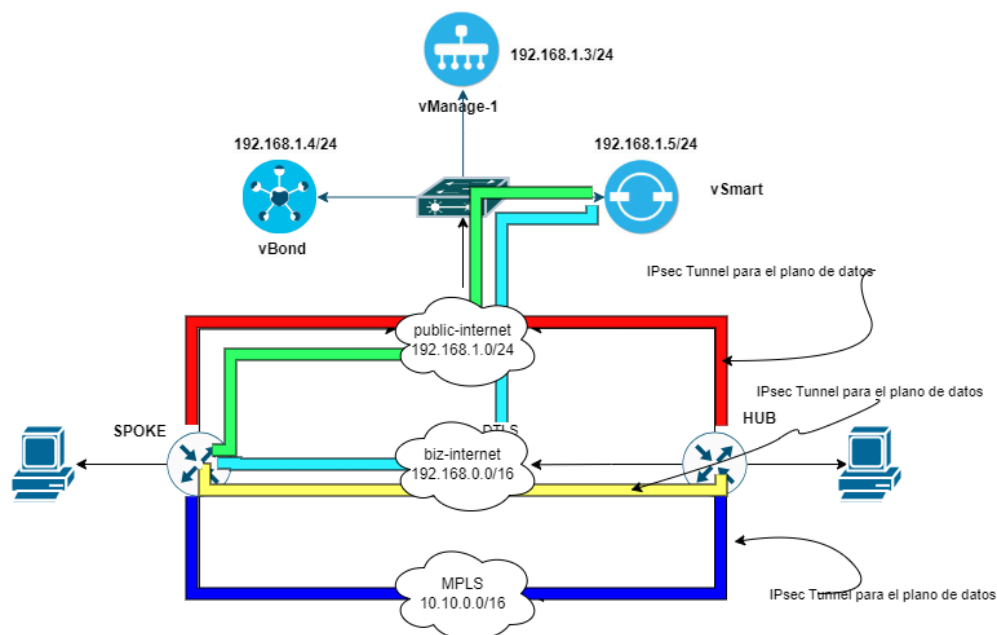
Tunnel Endpoints	Protocol	State	Jitter (ms)	Loss (%)	FEC Loss Recovery (%)	Latency (ms)	QoS Score
▼ biz-internet	--	--	--	--	--	--	--
<input checked="" type="checkbox"/> vEdge-Cuaical-SPOKE4.biz-internet-vEdge-Cuaical-HUB1.biz-internet	IPSEC	↑	6.00	0.17	N/A	23.14	7.00
<input checked="" type="checkbox"/> vEdge-Cuaical-SPOKE4.biz-internet-vEdge-Cuaical-SPOKE3.biz-internet	IPSEC	—	9.00	0.17	N/A	22.00	7.00
<input checked="" type="checkbox"/> vEdge-Cuaical-SPOKE4.biz-internet-vEdge-Cuaical-SPOKE3.public-internet	IPSEC	—	18.00	0.50	N/A	31.00	5.00
▼ mpls	--	--	--	--	--	--	--
<input checked="" type="checkbox"/> vEdge-Cuaical-SPOKE4.mpls-vEdge-Cuaical-HUB1.mpls	IPSEC	↑	6.17	0.03	N/A	28.83	10.00
<input checked="" type="checkbox"/> vEdge-Cuaical-SPOKE4.mpls-vEdge-Cuaical-SPOKE3.mpls	IPSEC	—	7.00	0.17	N/A	35.00	7.00
▼ public-internet	--	--	--	--	--	--	--
<input checked="" type="checkbox"/> vEdge-Cuaical-SPOKE4.public-internet-vEdge-Cuaical-HUB1.public-internet	IPSEC	↓	0.00	100.00	N/A	0.00	5.00
<input type="checkbox"/> vEdge-Cuaical-SPOKE4.public-internet-vEdge-Cuaical-SPOKE3.public-internet	IPSEC	—	0.00	100.00	N/A	0.00	5.00
<input type="checkbox"/> vEdge-Cuaical-SPOKE4.public-internet-vEdge-Cuaical-SPOKE3.biz-internet	IPSEC	—	17.00	0.67	N/A	31.00	5.00

De esta manera, las políticas creadas y enviadas desde el plano de gestión han demostrado ser efectivas en el plano de datos. Esto se refleja en la reducción de túneles y en el enrutamiento basado en la ingeniería de tráfico. Las verificaciones realizadas en esta sección confirman que las políticas están funcionando correctamente y logrando los resultados esperados en términos de optimización de la red, lo cual demuestra el éxito en la implementación de las políticas y la contribución de SDWAN en la mejora del rendimiento y la eficiencia de la red.

Para concluir este capítulo, es importante destacar el esquema de establecimiento de túneles en los planos de control y datos. Ya que, en este caso, se establecen tres túneles entre los dispositivos SPOKE y HUB, lo cual permite la comunicación eficiente y segura entre ellos. Además, se establecen otros dos túneles hacia el plano de control de la red OMP, garantizando así la correcta gestión y control de la red tal como se muestra en la Figura 152. Estos túneles desempeñan un papel fundamental en el funcionamiento y despliegue de la infraestructura SD-WAN.

Figura 152

Esquema de establecimiento de túneles



En este sentido, en la Figura 152, se muestra que, desde un SPOKE hacia un HUB se forman los túneles de color rojo, azul y amarillo, los cuales son restrictos¹³. Por otro lado, se tiene que se establecen dos túneles hacia el plano de control, los cuales se representan de color verde y celeste.

¹³ Estos túneles permiten el establecimiento de túneles entre los mismos colores de red. Dichas configuraciones fueron realizadas en este capítulo mediante las políticas creadas en el plano de gestión.

5 CAPÍTULO V – PRÁCTICAS DE LABORATORIO

En este capítulo, se describen las prácticas de laboratorios propuestas para aprender la tecnología SD-WAN, las cuales abarcan desde la instalación y configuración del entorno para simular una red SD-WAN con equipos CISCO, hasta la gestión de la red SD-WAN mediante políticas y la optimización de la red mediante el uso de MPLS-VPN para mejorar el enrutamiento en la convergencia de la red SD-WAN y MPLS.

5.1 Práctica de laboratorio 1: Despliegue del Plano de Control en un Clúster Centralizado para la Implementación del TESTBED SD-WAN.

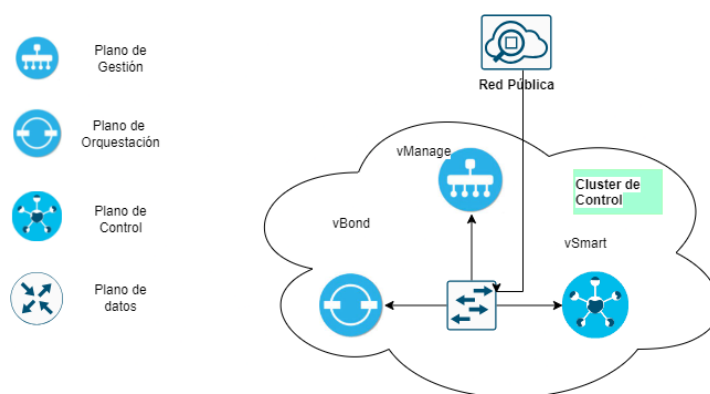
En esta práctica de laboratorio, el objetivo es desplegar los planos de gestión, orquestación y control en un clúster centralizado para establecer una infraestructura de red eficiente y segura. Para lograrlo, se requiere asignar los recursos físicos y lógicos

adecuados. Durante el laboratorio, se llevará a cabo el despliegue de dispositivos como vManage, vBond y vSmart, así como la configuración de certificados necesarios para establecer una comunicación segura entre ellos. Este despliegue permitirá la administración óptima y segura de la red SD-WAN, garantizando un funcionamiento eficiente y confiable de la infraestructura.

5.1.1 Topología de Red

Figura 153

Topología de red



La Figura 153, presenta la topología propuesta para el cluster de control, en este sentido, las direcciones IPv4, se asignan de acuerdo con la Tabla 6, en donde se identifica, el equipo, la interfaz de red y dirección IPv4 para el despliegue de cada uno de los dispositivos requeridos.

5.1.2 Objetivo General:

Realizar la implementación integral¹⁴ de los planos de gestión, orquestación y control en una red SD-WAN.

¹⁴ Se refiere a llevar a cabo todas las etapas necesarias para establecer con éxito los planos de gestión, orquestación y control en la red SD-WAN

5.1.3 *Objetivos Específicos:*

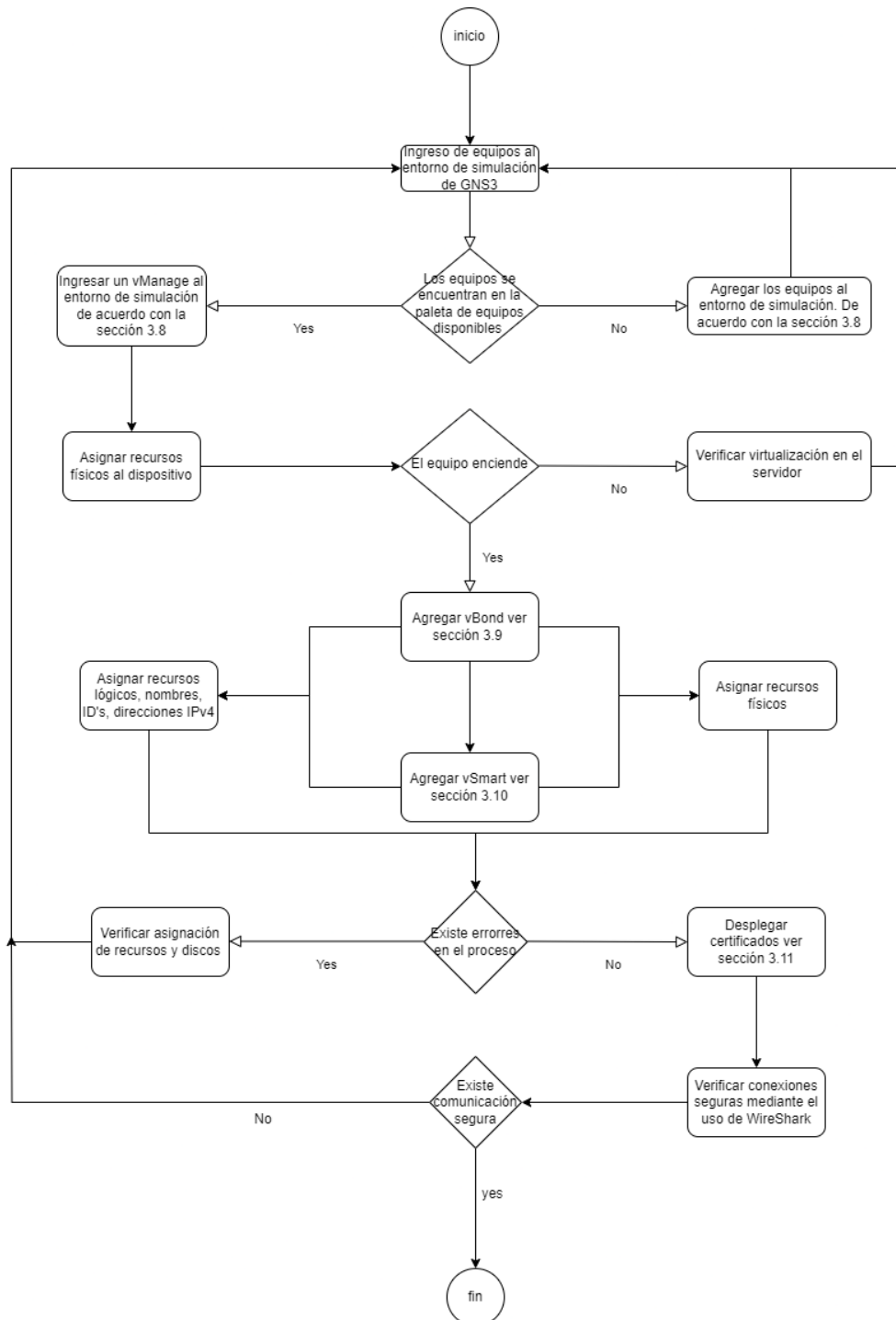
- Ingresar dispositivos del plano de control a GNS3 y conectarlos de acuerdo con la topología mostrada en la Figura 150.
- Asignar direccionamiento IPv4 a cada una de las interfaces de los dispositivos del plano de control.
- Generar certificados individuales para los componentes del clúster centralizado con el propósito de habilitar la comunicación segura entre las controladoras.
- Verificar la conectividad en el clúster centralizado al agregar el plano de orquestación y control en el panel de control del plano de gestión.
- Demostrar la comunicación segura mediante la captura y análisis de paquetes utilizando la herramienta Wireshark.

5.1.4 *Desarrollo*

Para lograr la implementación completa del clúster centralizado, se requiere desplegar los planos de gestión, orquestación y control. Esto se logra utilizando el dispositivo vManage para el plano de gestión, vBond para el plano de orquestación y vSmart para el plano de control. Para ello se debe seguir el proceso que se muestra en la Figura 154.

Figura 154

Diagrama de flujo del despliegue del cluster central



5. Para el despliegue de vManage ([Consultar sección 3.8](#)).
6. Para el despliegue de vBond ([Consultar sección 3.9](#)).
7. Para el despliegue del vSmart ([Consultar sección 3.10](#)).
8. Para el despliegue de certificados ([Consultar sección 3.11](#)).

En cada una de las secciones referenciadas, se muestra paso a paso el proceso para el despliegue del clúster de control.

5.1.5 Resultados

Tabla 9

Listado de actividades cumplidas laboratorio 1

Acción	Estado
Ingreso de dispositivos al entorno de simulación GNS3.	Se ingresó un vManage, un vSmart y un vBond.
Asignación de direcciones IPv4 a los dispositivos.	Se asignó el direccionamiento IPv4 a todos los equipos de acuerdo con la tabla 6.
Generar certificados individuales para cada dispositivo del plano de control.	Se generó el certificado para el vSmart, vBond y vManage.
Verificar conectividad en el plano de gestión.	Todos los equipos están disponibles en el plano de gestión.
Demostrar comunicación segura.	Mediante el uso de WireShark, se capturó los paquetes de comunicación entre las controladoras, los cuales están cifrados con DTLS.

Para la verificación de resultados, [consultar sección 3.12](#).

5.2 Práctica de laboratorio 2: Integración del plano de datos al TESTBED SD-WAN

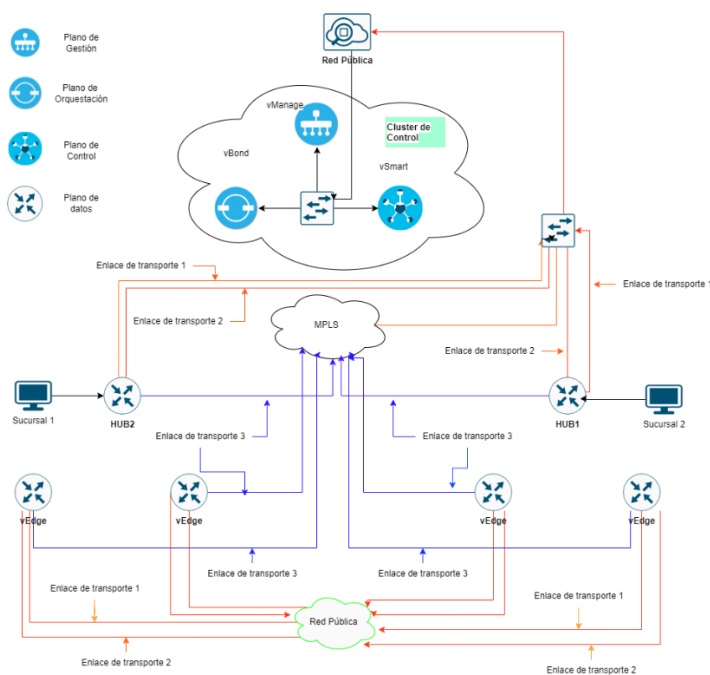
En esta práctica de laboratorio, se continúa con el despliegue del clúster de control, incorporando los equipos de acceso vEdge de acuerdo con la topología que se ilustra en la Figura 155. Para acceder a los detalles relacionados con la asignación de direcciones IPv4, se consulta la Tabla 6, la cual proporciona un desglose del plan de direccionamiento IPv4 diseñado específicamente para la red híbrida SD-WAN.

En este laboratorio, se enfocará en la verificación de las sesiones BFD que han sido establecidas por los equipos de acceso vEdge, así como en la evaluación de los recursos consumidos por estos dispositivos.

5.2.1 Topología de red

Figura 155

Topología de red para full mesh



5.2.2 *Objetivo General*

Realizar la integración del plano de datos con el plano de control en el TESTBED SD-WAN.

5.2.3 *Objetivos específicos*

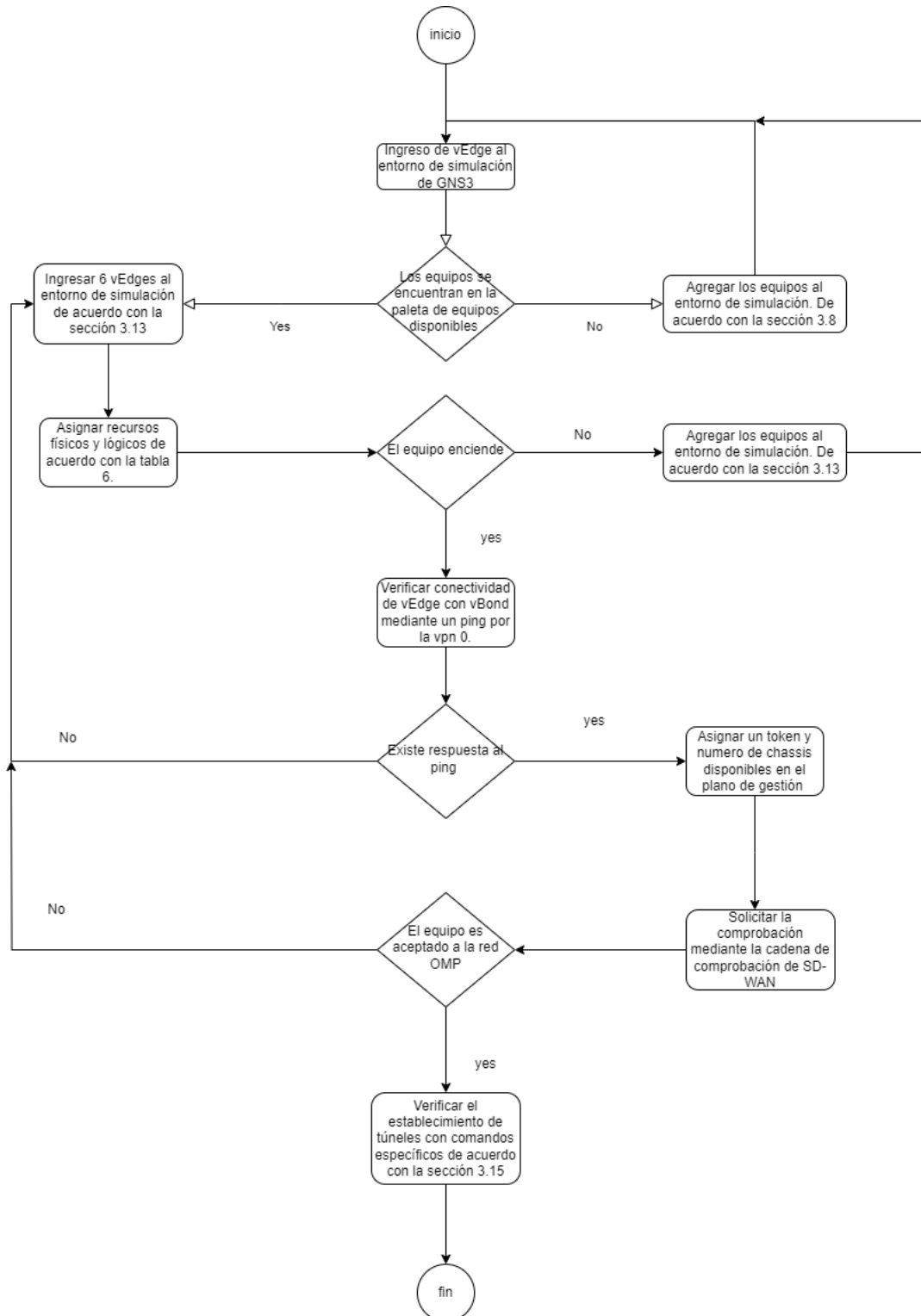
- Incorporar los equipos de acceso vEdge en la simulación, estableciendo las conexiones físicas con las redes de transporte según se indica en la Figura 155.
- Asignar recursos físicos a los dispositivos con el propósito de preparar una configuración lógica exitosa posterior.
- Incluir los equipos vEdge en la red OMP mediante la configuración de tokens y chassis virtuales proporcionados por el plano de gestión.
- Verificar las conexiones con el plano de control mediante el uso de comandos específicos para el plano de datos.
- Validar tanto las sesiones BFD establecidas como el consumo de recursos en el plano de datos.

5.2.4 *Desarrollo*

Para una correcta integración del plano de datos con el plano de control, se debe ingresar los equipos de acceso vEdge, además de realizar las configuraciones físicas y lógicas de estos para que sean capaces de interactuar en la simulación, en este sentido para el correcto despliegue de este plano se debe seguir el proceso que se muestra en la Figura 156.

Figura 156

Diagrama de flujo para integración de vEdges al testbed SD-WAN



- Para el ingreso de los vEdges a la simulación ([Consultar sección 3.13](#)).
- Para añadir los equipos a la red SD-WAN ([Consultar sección 3.15](#)).
- Para verificar las sesiones BFD ([Consultar sección 3.15](#)).

En cada una de las secciones de referencia, se muestra el proceso específico para el despliegue del plano de datos para una red en estado por defecto.

5.2.5 Resultados

Tabla 10

Listado de acciones cumplidas para el laboratorio 2

Acción	Estado
Ingreso de dispositivos al entorno de simulación GNS3.	Se ingresó 6 vEdges al entorno de simulación.
Asignación de direcciones IPv4 a los dispositivos.	Se asignó el direccionamiento IPv4 a todos los equipos de acuerdo con la tabla 6.
Ingreso de tokens y números de chasis para los dispositivos de acceso.	Se generó el archivo de configuración para 6 equipos CSR(Cloud Service Routers), para los cuales se extrajo el chasis y el token.
Verificar sesiones BFD en los equipos de acceso vEdge.	En los equipos se despliega las sesiones BFD establecidas con sus pares OMP, además desde el plano de gestión, se verifica los recursos físicos consumidos por los nodos específicos.

Los resultados, son presentados en la misma sección 3.15 en la página 148 posterior al ingreso de los equipos a la red.

5.3 Práctica de laboratorio 3: Manipulando el estado por defecto del TESTBED SD-WAN.

Posterior al desarrollo de la práctica 2, en donde la red se encuentra en su estado predeterminado, se llevará a cabo esta práctica de laboratorio para configurar la topología SHHS sobre la topología FULL-MESH. Es fundamental tener en cuenta que la comunicación entre el plano de control y el plano de datos ya se ha establecido y los túneles correspondientes han sido configurados en los dispositivos de red. Esto proporciona la base necesaria para la configuración exitosa de la topología SHHS y asegura un entorno preparado para realizar los pasos necesarios en esta práctica de laboratorio.

5.3.1 Topología de red

La topología de red para este laboratorio se presenta en la Figura 99, la misma que puede ser visualizada de mejor manera en el siguiente enlace:

[Topología Final SD-WAN.png](#)

En esta topología, se expone el diseño de la red híbrida SD-WAN implementada en el TESTBED. Hasta este punto, es necesario haber completado la configuración del clúster de control centralizado, así como la integración exitosa del plano de datos en la red SD-WAN

5.3.2 Objetivo General

Crear una política centralizada para la configuración de la topología SHHS en el TESTBED SD-WAN.

5.3.3 *Objetivos Específicos*

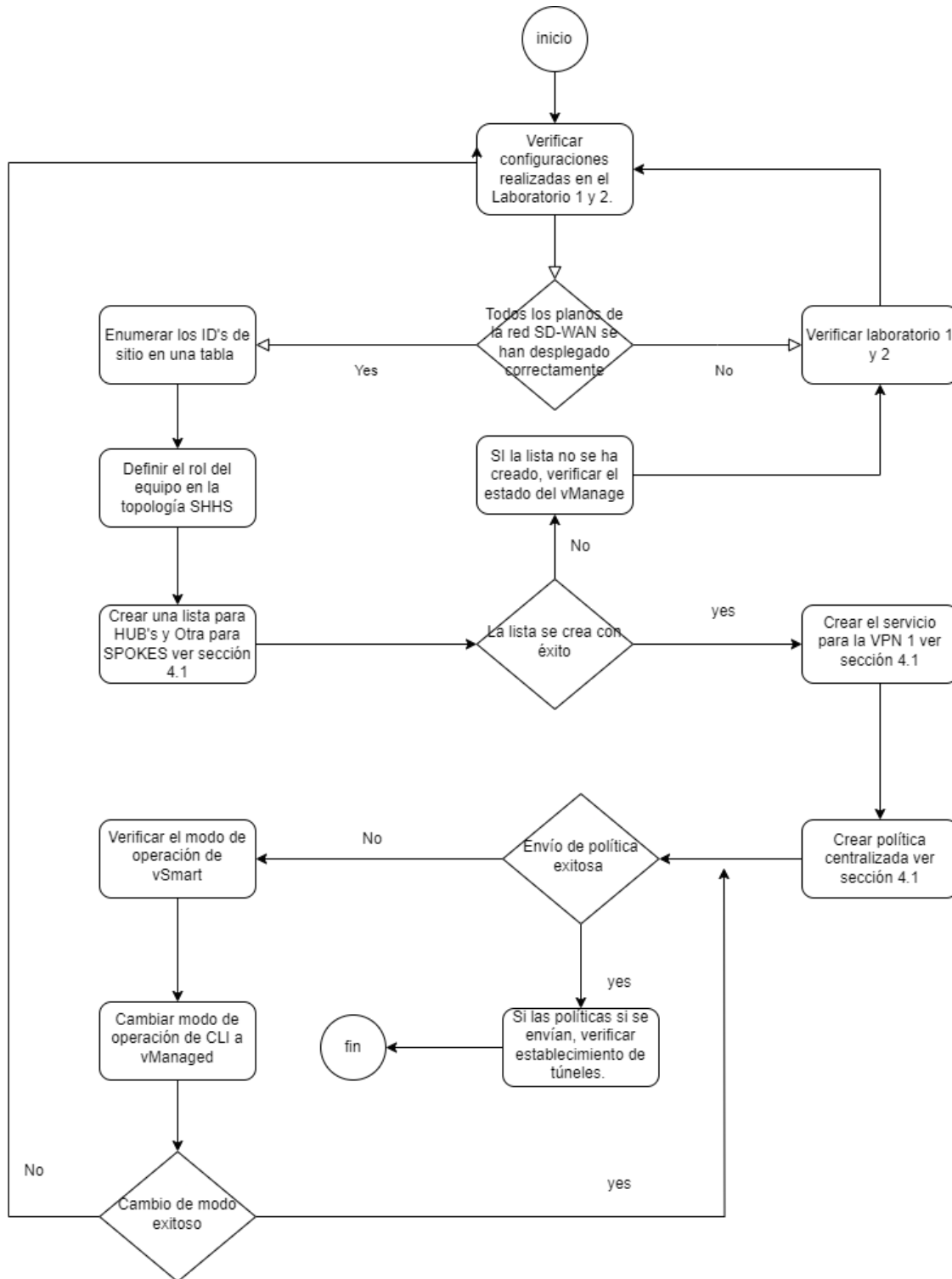
- Enumerar los ID de sitio de los nodos de acceso vEdge presentes en el TESTBED SD-WAN, con el propósito de facilitar su posterior identificación en la red OMP.
- Crear listas para HUBs y SPOKES, destinadas a su posterior uso en la configuración de la topología SHHS.
- Establecer una VPN para la transmisión de datos de los clientes a través de los nodos de acceso vEdge.
- Aplicar políticas centralizadas para el filtro TLOC's en la red OMP.
- Verificar la ejecución efectiva de las políticas en los equipos de acceso vEdge mediante el uso de comandos específicos.

5.3.4 *Desarrollo*

Previo a la ejecución de este laboratorio, se debe tener en cuenta que los planos de gestión, orquestación, control y datos ya están desplegados y su funcionamiento ha sido verificado, en este sentido para la configuración de una infraestructura de red reconfigurable, se creará una topología SHHS mediante el uso de políticas de datos centralizada. Para llevar a cabo este laboratorio, se cambiará el modo de operación del vSmart para que sea manejado desde el plano de gestión. En este sentido, para una correcta ejecución de este laboratorio, se debe seguir el proceso mostrado en la Figura 157.

Figura 157

Diagrama de flujo para la configuración de la topología SHHS en el TESTBED SD-WAN.



Para el desarrollo de toda la práctica ([Consultar sección 4.1](#)).

5.3.5 Resultados

Tabla 11

Actividades Cumplidas del laboratorio

Acción	Estado
Enumerar los ID's de sitio de los dispositivos de acceso.	Se realizó una tabla en la cual se resume el ID de sitio de cada nodo, además del papel desempeñado en la topología SHHS.
Crear listas para HUB's y SPOKES.	Se creó una lista para los SPOKES del sitio 1, una lista para los SPOKES del sitio 2, además de una lista para el HUB1, y otra para el HUB2.
Establecer una VPN para el servicio de tráfico de datos.	Se creó el servicio para la VPN1 de acuerdo con la topología presentada.
Aplicar la política centralizada a la red OMP.	Se cambió el estado de operación del vSmart, posteriormente se envió las políticas al plano de control, en donde se ejecutan con éxito.
Verificar el funcionamiento de las políticas centralizadas.	Se verificó el funcionamiento de las políticas, gracias a la reducción de sesiones BFD establecidas por cada nodo.

Los resultados para esta práctica de laboratorio se muestran en la sección 4.1 en la página 170.

5.4 Práctica de laboratorio 4: Aplicación de ingeniería de tráfico sobre el TESTBED SD-WAN.

En esta práctica de laboratorio, el objetivo principal es implementar una política de datos que permita realizar el mapeo de aplicaciones específicas, en este caso RTMP, y así definir el enlace de salida más adecuado para optimizar el rendimiento de la red SD-WAN. Para llevar a cabo esta práctica, es necesario asegurar la conectividad entre los nodos de acceso vEdge utilizando la red MPLS.

5.4.1 Topología de red

La topología de red para este laboratorio se presenta en la Figura 99, la misma que puede ser visualizada de mejor manera en el siguiente enlace:

[Topología Final SD-WAN.png](#)

Cabe mencionar que no es necesario tener activa toda la topología mostrada, ya que, para la verificación de las configuraciones para ingeniería de tráfico, se puede realizar entre un HUB y un SPOKE.

5.4.2 Objetivo General

Implementar una política de datos (ingeniería de tráfico) de manera centralizada para toda la red SD-WAN.

5.4.3 Objetivos Específicos

- Generar una lista de sitios que contenga todos los ID de los nodos de acceso de la red SD-WAN, con el propósito de facilitar su gestión y seguimiento.
- Elaborar una política centralizada para la ingeniería de tráfico mediante la herramienta Traffic Engineering de Viptela SD-WAN.

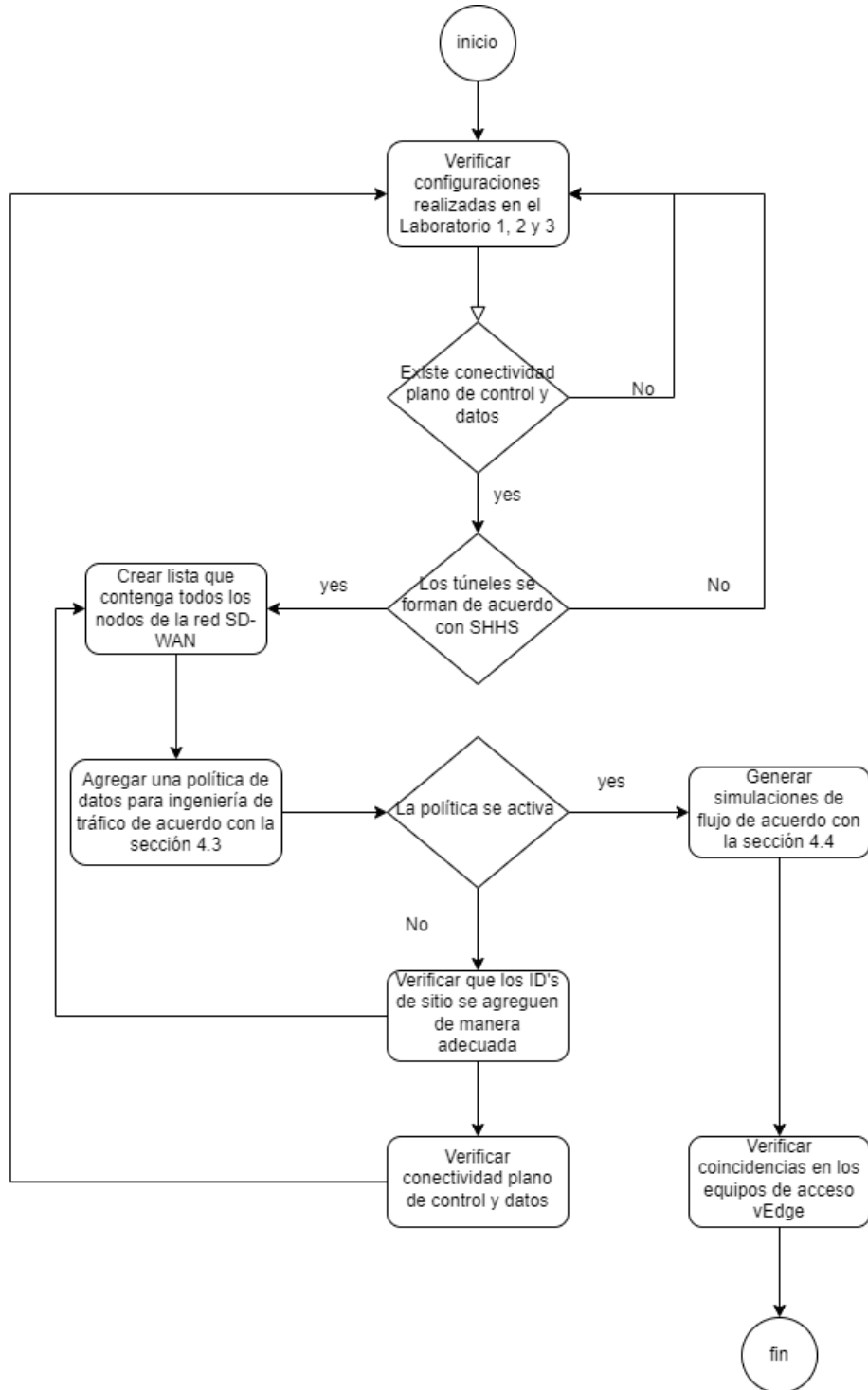
- Configurar el emparejamiento para familia de aplicaciones RTMP, con el objetivo de lograr enrutamiento selectivo.
- Verificar la efectividad de la política centralizada a través de simulaciones de flujo, utilizando la herramienta de resolución de problemas (troubleshooting).

5.4.4 Desarrollo

El desarrollo para esta práctica de laboratorio se encuentra en la [sección 4.3](#). En esta sección se presenta paso a paso la aplicación de una política centralizada para el mapeo de aplicaciones con el protocolo de capa aplicación RTMP y se define un enlace de salida para este tipo de tráfico. En este sentido, para un correcto desarrollo de este laboratorio, se debe seguir el proceso que se muestra en la Figura 158.

Figura 158

Diagrama de flujo, para configuración de ingeniería de tráfico



5.4.5 Resultados

Tabla 12

Acciones cumplidas laboratorio 4

Acción	Estado
Crear una lista que contenga todos los nodos de la red SD-WAN.	Se creó la lista que contiene todos los ID's de los nodos de acceso para la política de datos.
Elaborar una política centralizada para ingeniería de tráfico.	Sobre la política de datos existente para SHHS, se ingresa a editar la política de datos para agregar los nuevos requerimientos.
Crear una política de datos que permita realizar el emparejamiento para la familia RTMP.	Dentro de la política existente, se ingresa la nueva política de datos para el emparejamiento RTMP, y se añade una salida por el enlace MPLS restrict.
Verificar la ejecución de la política en la operación de la red SD-WAN	Se verifica los emparejamientos en el equipo mediante los flujos, además se verifica con la simulación gráfica de flujos en el plano de gestión.

Los resultados para esta práctica de laboratorio se encuentran en la [sección 4.4](#).

En esta sección se muestra la comprobación del envío de la política centralizada al plano de datos, y de la misma manera se verifica los match para RTMP en los equipos de acceso. De la misma manera se establece una simulación de flujos RTMP, para verificar el circuito que usa para la comunicación.

5.5 Practica de laboratorio 5: Mejorando la integración de la red MPLS y la red SD-WAN.

En esta sección, se presenta una guía detallada sobre cómo realizar la integración de la red SD-WAN y la red MPLS mediante MPLS-VPN. Esta configuración contribuye a mejorar la seguridad de la red al evitar que los dispositivos de la red MPLS tengan acceso a la información de las rutas anunciadas por la red OMP. Como resultado, la red será conocida únicamente por los pares OMP, lo que fortalece la protección de la red y preserva la confidencialidad de los datos transmitidos.

5.5.1 *Objetivo General:*

Realizar la integración de la red SD-WAN con la red MPLS, mediante MPLS-VPN.

5.5.2 *Objetivos Específicos:*

- Configurar 802.1Q en los switches de acceso y en las subinterfaces de los enlaces de transporte de los HUBS y SPOKES.
- Configurar iBGP entre los PE routers, para el transporte de rutas desde un sitio a otro mediante las vrfs.
- Configurar eBGP entre los PE y CE routers, para el anuncio de rutas desde los nodos de acceso vEdge.
- Anunciar rutas sobre la red MPLS por la VPN 0, para una correcta convergencia de la red híbrida SD-WAN.

5.5.3 *Introducción*

En la práctica anterior, se llevó a cabo la configuración de ingeniería de tráfico para optimizar el uso de la red en servicios en tiempo real, específicamente para el

streaming de video. También se ha verificado el funcionamiento de una red SD-WAN híbrida configurada por defecto. En esta nueva práctica, el enfoque se centrará en la convergencia entre la red MPLS y la red SD-WAN, buscando una integración fluida y eficiente de ambas tecnologías.

5.5.4 Desarrollo

A. Configuración del protocolo 802.1Q

En la topología desarrollada en la Figura 99, se deben identificar los switches 4 y 7 para llevar a cabo la configuración de las Vlans 10, 20, y 30, así como establecer un enlace troncal para el tráfico proveniente de estas Vlans mencionadas. De manera similar, en los Routers R3 y R5, se crearán las subinterfaces detalladas en la Tabla 13 para permitir una comunicación adecuada entre los routers CE y PE. Con stas acciones, se logrará una comunicación efectiva entre los distintos dispositivos de la red.

Tabla 13

Distribución de puertos y Vlans

Equipo	Interfaz	VLAN	Type
Switch 4	E1	20	access
	E2	10	access
	E3	30	access
	E0	-	Dot1q
Switch 7	E1	10	access
	E2	20	access
	E3	30	access
	E0	-	Dot1q
R3	F0/0.10	10	Dot1q

	F0/0.20	20	Dot1q
	F0/0.30	30	Dot1q
R5	F0/0.10	10	Dot1q
	F0/0.20	20	Dot1q
	F0/0.30	30	Dot1q

En este sentido, la configuración de los switches genéricos es sencilla, para lo cual se debe seguir los siguientes pasos:

1. Elección del puerto físico: Remarcado en color rojo en la Figura 159, se muestra cómo se debe seleccionar el puerto físico que se desea configurar. Esto se realiza mediante la especificación del número de puerto correspondiente en el switch.
2. Definición de la VLAN¹⁵: Remarcado en color azul en la misma figura, se muestra cómo se asigna una VLAN al puerto seleccionado.
3. Modo de operación: El modo de operación se especifica al puerto seleccionado, y se puede identificar por el color verde en la Figura 159. Este modo puede ser "Acceso" (**Access**), donde el puerto se conecta a un único dispositivo final, o "Troncal" (**Trunk**), donde el puerto se utiliza para transmitir múltiples VLAN's.

¹⁵ Una VLAN es una red virtual que permite segmentar el tráfico en la red física y proporciona mayor seguridad y gestión.

Figura 159

Configuración de Vlans Switch 4

The screenshot shows the configuration page for Switch4. The 'General' section has 'Name: Switch4' and 'Console type: none'. The 'Settings' section includes 'Port: 1', 'VLAN: 20', 'Type: access', and 'QinQ EtherType: 0x8100'. The 'Ports' table lists configurations for ports 0 through 6.

Port	VLAN	Type	EtherType
0	1	dot1q	
1	20	access	
2	10	access	
3	30	access	
4	1	access	
5	1	access	
6	1	access	

Por otro lado, en los routers R3 y R5, es necesario crear subinterfaces y configurar el encapsulamiento con 802.1Q utilizando la VLAN adecuada para establecer la comunicación entre los dispositivos de red. Para realizar esta configuración, se deben seguir los siguientes pasos:

1. Ingresar a la interfaz deseada desde la configuración global: Acceda al modo de configuración del router y seleccione la interfaz en la que desea crear la subinterfaz. Por ejemplo, si desea configurar la subinterfaz en la interfaz FastEthernet0/0, ejecute el comando `interface f0/0` desde la configuración global.
2. Crear la subinterfaz: Una vez dentro de la interfaz, al ejecutar el comando `interface f0/0.#` en donde # es el número de la subinterfaz, esta se creará

automáticamente. Por ejemplo, para crear la subinterfaz 10, use el comando `interface f0/0.10`.

3. Configurar el encapsulamiento dot1q: Después de crear la subinterfaz, ejecute el comando `encapsulation dot1q #vlan` dentro de la subinterfaz recién creada. Asegúrese de ingresar el número de etiqueta VLAN adecuado para la subinterfaz. Esta etiqueta VLAN debe coincidir con la configuración del switch en el enlace troncal. Por ejemplo, si la VLAN es 10, use el comando `encapsulation dot1q 10` en la subinterfaz.
4. Repita los pasos anteriores para todas las subinterfaces necesarias en los routers LER-R3 y LER-R5.

Al completar estos pasos, se habrá creado y configurado correctamente las subinterfaces en los routers R3 y R5 utilizando el encapsulamiento 802.1Q con la VLAN adecuada. Esto permitirá la comunicación entre los dispositivos de red a través de las subinterfaces y garantizará un enlace troncal efectivo entre los routers y los switches.

B. Creación de vrf, asignación de interfaces y direccion ipv4

Para las vrf, al igual que para todo el dominio MPLS, se hará uso de direccionamiento IPv4 privado, en este caso se hará uso el plan de direccionamiento IPv4 mostrado en la Tabla 11.

Tabla 14

Direccionamiento IPv4 MPLS-VPN para el laboratorio 5.

Dispositivos	Subred
HUB2	10.10.10.48/29

SPOKE2	10.10.20.0/29
SPOKE1	10.10.20.8/29
HUB1	10.10.10.64/29
SPOKE3	10.10.20.16/29
SPOKE4	10.10.20.24/29

Una vez listo el plan de direccionamiento IPv4, se crea la vrf “*redhibrida*”, para la cual se debe asignar un rd (route distinguisher), en este sentido para el equipo R3 es 65200:1, para R5 65200:2, y para R4: 65200:3, esto permitirá hacer uso de los mismos segmentos de direccionamiento IPv4 para los CE routers. Para la creación de la vrf, desde la configuración global, se ingresa el comando `ip vrf redhibrida`, posterior a la creación de esta, se asigna el rd para esta vrf con el comando `rd: 65200:1` para el equipo R3, de la misma manera se debe exportar el rd del propio equipo e importar el rd de los demás equipos tal como se muestra en la Figura 160.

Figura 160

Configuración de vrf en R3

```

R3(config)#ip vrf redhibrida
R3(config-vrf)#rd 65200:1
R3(config-vrf)#route
R3(config-vrf)#route-target export 65200:1
R3(config-vrf)#route-target import 65200:2
R3(config-vrf)#do sh run | sec vrf
ip vrf redhibrida
rd 65200:1
route-target export 65200:1
route-target import 65200:2
R3(config-vrf)#

```

En este sentido, para verificar la creación de las vrf, se ejecuta el comando `show running-config | sec vrf`, en donde se debe mostrar todos los parámetros previamente configurados.

Una vez creada la vrf, se debe asignar interfaces a la misma, para lo cual, se ingresa a la interfaz que se desea pertenezca a esta vrf y se ejecuta el comando `ip vrf forwarding redhibrida`, tal como se muestra en la Figura 161, una vez se ejecute el comando la interfaz perderá cualquier dirección IPv4 previamente asignada, con lo cual se debe asignar las direcciones IPv4 de acuerdo con la Tabla 13.

Figura 161

Asignación de interfaz a vrf redhibrida

```
R3(config-vrf)#interface f0/0
R3(config-if)#ip vrf forwarding redhibrida
% Interface FastEthernet0/0 IP address 10.10.10.49 removed due to enabling VRF redhibrida
R3(config-if)#
*Mar 1 00:23:29.099: %TDP-4-IDENT: cannot set VRF redhibrida TDP ident
R3(config-if)#
```

Una vez que se hayan ingresado todas las interfaces a la vrf y se hayan configurado las direcciones IPv4 correspondientes, será posible visualizar esta configuración utilizando el comando `show running-config` en la sección de interfaces. Esto permitirá verificar que cada una de las subinterfaces haya sido agregada correctamente a la vrf denominada `redhibrida` y que estén encendidas administrativamente tal como se muestra en la Figura 162.

Figura 162

Ingreso de interfaces a la vrf red hibrida

```
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip vrf forwarding redhibrida
 ip address 10.10.10.49 255.255.255.248
 !
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip vrf forwarding redhibrida
 ip address 10.10.20.1 255.255.255.248
 !
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip vrf forwarding redhibrida
 ip address 10.10.20.9 255.255.255.248
 !
```

C. Configuración de iBGP y activación de características extendidas

Para configurar MPLS-VPN, es necesario establecer una sesión iBGP (Interior Border Gateway Protocol) entre los routers CE a través de la red MPLS tal como se muestra en la Figura 163. A continuación, se detallan los pasos para realizar esta configuración:

1. Iniciar una instancia BGP: Desde la configuración global del router CE, inicie una instancia BGP utilizando el comando `router bgp <AS>` donde <AS> corresponde al número de Sistema Autónomo asignado para el dominio MPLS. Por ejemplo, si el AS asignado es 65100, ejecute `router bgp 65100` para iniciar la instancia BGP.
2. Asignar un ID de proceso: Dentro de la instancia BGP, asigne un ID de proceso utilizando el comando `bgp router-id <router_id>`. El ID de proceso debe ser el mismo que el de la interfaz Loopback 0 que se creó anteriormente. Esto garantiza que el proceso BGP se asocie correctamente con

la interfaz Loopback 0. Por ejemplo, si el ID de Loopback 0 es 20.20.20.3 use el comando `bgp router-id 20.20.20.3`.

3. Agregar el vecino y el sistema autónomo: Especifique el vecino BGP y el número de sistema autónomo al que pertenece utilizando el comando `neighbor <neighbor_ip> remote-as <AS>`. `<neighbor_ip>` corresponde a la dirección IP del vecino BGP y `<AS>` es el número de sistema autónomo al que pertenece el vecino. Por ejemplo, si el vecino tiene la dirección IP 20.20.20.5 y pertenece al AS 65100, utilice el comando `neighbor 20.20.20.5 remote-as 65100`.
4. Definir la interfaz Loopback 0 para el proceso BGP: Especifique que todo el proceso BGP se realice a través de la interfaz Loopback 0 utilizando el comando `neighbor <neighbor_ip> update-source loopback0`. Esto asegura que el tráfico BGP se enrute a través de la interfaz Loopback 0. Reemplace `<neighbor_ip>` con la dirección IP del vecino BGP.

Figura 163

iBGP entre R3 y R5

```

Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router bgp 65100
R3(config-router)#bgp router-id 20.20.20.3
R3(config-router)#nei
R3(config-router)#neighbor 20.20.20.5 remote-as 65100
R3(config-router)#neighbor 20.20.20.5 update-source lo 0
R3(config-router)#

Enter configuration commands, one per line. End with CNTL/Z.
R5(config)#router bgp 65100
R5(config-router)#bgp router-id 20.20.20.5
R5(config-router)#neighbor 20.20.20.3 remote-as 65100
R5(config-router)#neighbor 20.20.20.
R5(config-router)#neighbor 20.20.20.3 update sour
R5(config-router)#neighbor 20.20.20.3 update sour

```

Una vez establecida la sesión iBGP entre los routers PE, es necesario activar las características extendidas de BGP. Para ello, se accede a la instancia BGP previamente creada y se configura el `address-family vpnv4 unicast`. A continuación, se activa las características extendidas de BGP utilizando el comando `"neighbor <neighbor_ip>`

`activate`", reemplazando `<neighbor_ip>` por la dirección IP del router PE vecino, tal como se muestra en la Figura 164.

Figura 164

Activación de características extendidas de BGP

```

R3(config)#router bgp 65100
R3(config-router)#address
R3(config-router)#address-family vpnv4 unicast
R3(config-router-af)#neighbor 20.20.20.5 activate
R3(config-router-af)#

```

D. Establecimiento de eBGP entre CE y PE routers

Para establecer las sesiones eBGP entre los routers CE y PE, es necesario configurar el PE router dentro de la VRF "red hibrida". Para ello, primero, se ingresa a la configuración de la VRF utilizando el comando `address-family ipv4 unicast vrf redhibrida`. Luego, configura la entrada para el vecino en el otro sistema autónomo utilizando el comando `neighbor 10.10.10.54 remote-as 65200`. A continuación, activa el vecino con el comando `neighbor 10.10.10.54 activate`. Una vez ejecutados estos comandos, como se muestra en la Figura 165, ya se podrá iniciar la sesión BGP desde el router CE y establecer la comunicación requerida.

Figura 165

Establecimiento de eBGP (configure terminal -> vpn 0)

```

R3(config-router)#router bgp 65100
R3(config-router)#address-family ipv4 unicast vrf redhibrida
R3(config-router-af)#neighbor 10.10.10.54 remote-as 65200
R3(config-router-af)#neighbor 10.10.10.54 activate

```

Para establecer la sesión BGP desde los vEdges (CE routers), primero se debe crear una instancia BGP con su respectivo sistema autónomo sobre la VPN 0. Luego, se

configura una entrada para el vecino utilizando el comando "`neighbor 10.10.10.49 remote-as 65100`", donde 10.10.10.49 es la dirección IP del vecino BGP y 65100 es el número de sistema autónomo correspondiente. A continuación, se ingresa al modo de configuración del `address-family ipv4-unicast` y se anuncia la red deseada utilizando el comando "`network 10.10.10.53/32`", donde 10.10.10.53/32 representa la red que desea anunciar. De esta manera, ya se establece la sesión BGP y se anuncia la red especificada desde los vEdges (CE routers), tal como se muestra en la Figura 166.

Figura 166

Establecimiento de eBGP en vEdge

```
vEdge-Cuaical-SPOKE1(config-vpn-0)# router bgp 65205
vEdge-Cuaical-SPOKE1(config-bgp-65205)# no shut
vEdge-Cuaical-SPOKE1(config-bgp-65205)# neighbor 10.10.10.49 remote-as 65100
vEdge-Cuaical-SPOKE1(config-neighbor-10.10.10.49)# address-family ipv4-unicast
vEdge-Cuaical-SPOKE1(config-address-family-ipv4-unicast)# exit
vEdge-Cuaical-SPOKE1(config-neighbor-10.10.10.49)# exit
vEdge-Cuaical-SPOKE1(config-bgp-65205)# address-family ipv4-unicast
vEdge-Cuaical-SPOKE1(config-address-family-ipv4-unicast)# network 10.10.10.53/32

vEdge-Cuaical-SPOKE1(config-address-family-ipv4-unicast)# commit
Commit complete.
vEdge-Cuaical-SPOKE1(config-address-family-ipv4-unicast)# exit
vEdge-Cuaical-SPOKE1(config-bgp-65205)# exit
vEdge-Cuaical-SPOKE1(config-router)# exit
```

Cabe recalcar que, dentro de la interfaz física de red, se debe permitir el protocolo BGP, para lo cual se debe ingresar a la interfaz física, al túnel de la interfaz y finalmente ingresar el comando `allow-service all`, de esta manera, ya se tiene establecida la configuración de MPLS-VPN.

Las interfaces físicas de los vEdges (CE routers), ya pertenecen a la red SD-WAN por la VPN0, con lo cual ya solamente queda esperar a que se establezcan los túneles por la red MPLS.

E. Resultados

Una vez se haya logrado la convergencia de la red SD-WAN y MPLS mediante BGP, en la VPN0, se observará las rutas aprendidas mediante este protocolo, además se observará que los túneles IPsec se establecerán al igual que si se lo realizase con OSPF.

En este sentido, la principal diferencia al realizarlo mediante OSPF y BGP es que con este último las rutas no son anunciadas a todo el dominio MPLS, sino solo las conocen los PE routers mediante la vrf y los CE routers mediante BGP, de la misma manera, es posible discriminar las redes anunciadas desde OMP sobre BGP para mejorar la seguridad de la red.

Figura 167

Verificación eBGP

```
vEdge-Cuaical-HUB2# show ip routes vpn 0
Codes Proto-sub-type:
IA -> ospf-intra-area, IE -> ospf-inter-area,
E1 -> ospf-external1, E2 -> ospf-external2,
N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
e -> bgp-external, i -> bgp-internal
Codes Status flags:
F -> fib, S -> selected, I -> inactive,
B -> blackhole, R -> recursive
```

VPN	NEXTHOP	PREFIX	PROTOCOL	PROTOCOL	NEXTHOP	NEXTHOP	ADDR
VPN	VPN	TLOC IP	COLOR	SUB TYPE	IF NAME	STATUS	
0	-	0,0,0,0/0	bgp	-	ge0/2	-	10,10,10,49
0	-	0,0,0,0/0	static	-	ge0/0	-	10,0,0,1
0	-	0,0,0,0/0	static	-	ge0/3	F,S	192,168,102,1
0	-	5,5,5,5/32	connected	-	system	F,S	-
0	-	10,0,0,0/24	connected	-	ge0/0	-	-
0	-	10,10,10,48/29	connected	-	ge0/2	-	-
0	-	10,10,10,64/29	bgp	e	ge0/2	-	-
0	-	10,10,20,0/29	bgp	e	ge0/2	-	-
0	-	10,10,20,8/29	bgp	e	ge0/2	-	-
0	-	10,10,20,24/29	bgp	e	ge0/2	-	-
0	-	192,168,102,0/24	connected	-	ge0/3	-	-

Una vez se han establecido las sesiones BGP, las subredes de cada nodo de acceso son alcanzables desde todos los vEdge pertenecientes a la red SD-WAN, ya que como se muestra en la Figura 167, desde el equipo HUB2, es posible alcanzar las subredes

10.10.10.64/29, 10.10.20.0/29, 10.10.20.8/29, 10.10.20.24/29 con lo cual se establecerán los túneles IPsec sobre estas redes.

CONCLUSIONES

En base a las pruebas realizadas, se pudo comprobar el correcto funcionamiento tanto del entorno de pruebas (TESTBED) como de la red SD-WAN híbrida propuesta. Durante las pruebas, se logró manipular los enlaces físicos de red y crear redes virtuales para simular la interacción de la red SD-WAN en un entorno controlado. Con lo cual, el despliegue del TESTBED permitió una simulación efectiva de la red SD-WAN híbrida y llevar a cabo diversas pruebas de rendimiento y optimización. Los resultados obtenidos fueron satisfactorios, ya que se logró mejorar las métricas de rendimiento de la red, tales como la latencia, el jitter y la pérdida de paquetes.

El sistema operativo utilizado en el testbed desempeña un papel fundamental en el despliegue del software de simulación. Con lo cual, es esencial considerar factores como el uso de kvm, qemu y uBridge, así como la posibilidad de personalizar el entorno de simulación. En este sentido, si no se tienen en cuenta estos factores, es posible que se requiera utilizar máquinas virtuales adicionales para garantizar el correcto funcionamiento de GNS3. Sin embargo, esto puede ser poco práctico, ya que implica asignar recursos adicionales a las tareas de virtualización en lugar de utilizarlos para la emulación de redes en GNS3.

La disponibilidad limitada de documentación bibliográfica sobre redes SD-WAN debido a su naturaleza nueva y en constante evolución, resalta la importancia de establecer escenarios de pruebas y tener la oportunidad de interactuar directamente con esta tecnología. A través de la práctica y la experimentación, se puede obtener un conocimiento más profundo y práctico sobre las redes SD-WAN, lo que resulta crucial para comprender su funcionamiento, sus capacidades y desafíos.

Por otra parte, si no se realiza un dimensionamiento adecuado de los equipos, la red SD-WAN puede experimentar problemas en su rendimiento. Esto puede afectar la capacidad de procesamiento, el rendimiento de la controladora y, en última instancia, la calidad del servicio ofrecido por la red.

En el despliegue de una red SD-WAN híbrida, es de gran importancia tomar decisiones estratégicas sobre los tipos de enlaces que se utilizarán tanto para la comunicación en el plano de control como en el plano de datos. El objetivo principal es optimizar la utilización de recursos y minimizar el número de sesiones BFD (Bidirectional Forwarding Detection) en los equipos del plano de datos.

El uso de una red SD-WAN en comparación con una red MPLS implica importantes diferencias tanto en términos de infraestructura como en la gestión de la red. En este sentido, el despliegue de una red MPLS tiende a ser más compleja debido a la infraestructura de red específica que se requiere para su funcionamiento adecuado.

Desde la perspectiva de gestión, una red SD-WAN ofrece ventajas significativas en comparación con una red MPLS tradicional. Esto se debe a que la configuración lógica de una red SD-WAN se basa en la implementación de plantillas y políticas de datos, lo cual simplifica y agiliza el proceso de configuración y gestión de la red.

Las prácticas de laboratorio propuestas son una herramienta fundamental para facilitar la comprensión y configuración de la tecnología SD-WAN. A través de estas prácticas, los estudiantes y profesionales tienen la oportunidad de poner en práctica los conceptos teóricos aprendidos y adquirir experiencia práctica en la configuración de los protocolos específicos de SD-WAN, como OMP (Overlay Management Protocol), TLOC (Transport Locator) y BFD (Bidirectional Forwarding Detection).

RECOMENDACIONES

Es recomendable no realizar actualizaciones en el entorno de simulación utilizado en el TESTBED, ya que el uso de versiones diferentes puede ocasionar problemas en la virtualización y el uso del qemu. Mantener la versión establecida evita posibles dificultades técnicas y garantiza un funcionamiento adecuado de la simulación de la red SD-WAN.

Asimismo, es importante manejar más de una interfaz de red en el servidor físico, lo que permite una configuración diversa en las interfaces virtuales y su uso para las redes locales dentro de la simulación.

Previo a la manipulación de las redes SD-WAN, es aconsejable adquirir conocimientos en redes tradicionales como MPLS, así como en protocolos de enrutamiento dinámico como OSPF y BGP para enrutamiento interior y exterior respectivamente. Estos conocimientos previos resultan fundamentales para un mejor entendimiento y abordaje efectivo de la tecnología SD-WAN.

Durante la ejecución de este trabajo de grado, se ha logrado el estudio de la tecnología SD-WAN mediante la implementación de una red híbrida y la configuración de políticas centralizadas para una infraestructura de red altamente adaptable. A pesar de estos avances, se identifica la necesidad imperante de profundizar en el ámbito de la seguridad de la red OMP. VIPTELA SD-WAN, en particular, integra una solución de Firewall de Nueva Generación (NGFW), dotando a su tecnología con funciones de seguridad diversas, que incluyen filtrado de tráfico basado en IP y protocolo, análisis de paquetes a nivel de aplicación, prevención de intrusiones y detección de virus y malware, entre otras. Por lo tanto, se sugiere un enfoque investigativo más profundo en esta área de

seguridad con el propósito de maximizar la comprensión y optimización de la seguridad en la red.

Por otra parte, aunque el plano de gestión a través del vManage brinda una visión integral del rendimiento de la red SD-WAN, es crucial destacar que VIPTELA SD-WAN va más allá al introducir un plano adicional en paralelo al plano de gestión. Este plano adicional no solo permite un análisis en tiempo real del rendimiento de la red, sino también la identificación precisa de patrones de tráfico en toda la infraestructura. Sumado a la potencia del NGFW, este análisis puede ser aprovechado para investigar y mitigar incidentes de seguridad en la red de manera efectiva. La implementación de este plano adicional no solo empoderaría el control sobre la red propuesta, sino también habilitaría la generación automatizada de informes detallados sobre el rendimiento y la seguridad de la red, lo cual representa una mejora sustancial en la toma de decisiones informadas.

BIBLIOGRAFÍA

CCNA. (s. f.). *Infraestructuras WAN Privadas - CCNA desde Cero*. Recuperado 23 de septiembre de 2023, de Recommended Computing Resources for Cisco SD-WAN Controller Release 20.4.x (On-Prem Deployment)

cisco. (s. f.). *Recommended Computing Resources for Cisco SD-WAN Controller Release 20.4.x (On-Prem Deployment)*. Recuperado 7 de mayo de 2023, de <https://ccnadesdecero.es/infraestructuras-wan-privadas/>

cisco. (2005). *Configuraciones iniciales para el protocolo OSPF (Abrir la ruta más corta en primer lugar) sobre las subinterfaces del Frame Relay*. - Cisco. https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/13693-22.html

cisco. (2023). *What Is SD-WAN? - Software-Defined WAN (SDWAN)* - Cisco. <https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/what-is-sd-wan.html>

Cisco Press. (2017, mayo 17). *WAN Technologies Overview (1.1) > WAN Concepts* / Cisco Press. <https://www.ciscopress.com/articles/article.asp?p=2832405&seqNum=4>

Giovanni Augusto. (2019). *Community* / GNS3. <https://gns3.com/community/featured/viptela-lab-in-gns3-is-it-possib>

GNS3. (2023a). *Architecture* / GNS3 Documentation. <https://docs.gns3.com/docs/using-gns3/design/architecture/>

GNS3. (2023b). *Software* / GNS3. <https://www.gns3.com/software>

huawei. (2019). *ISIS vs OSPF - Huawei Enterprise Support Community*.

<https://forum.huawei.com/enterprise/en/isis-vs-ospf/thread/494381-861>

Juniper Networks. (2023). *MTU de medios y MTU de protocolo | Juniper Networks*.

<https://www.juniper.net/documentation/mx/es/software/junos/interfaces-fundamentals/topics/topic-map/media-mtu.html>

RF Wireless World. (2012). *Difference between SD-WAN and Traditional WAN*.

<https://www.rfwireless-world.com/Terminology/Difference-between-SD-WAN-and-Traditional-WAN.html>

UIT. (2013). *UIT-T Rec. H.810 (12/2013) Directrices de diseño para la interoperabilidad*

de sistemas de salud personal. <http://handle.itu.int/11.1002/1000/11830-en>.

Universidad Internacional de Valencia. (2016, mayo 6). *Ventajas y desventajas de la*

conmutación de circuitos | VIU España.

<https://www.universidadviu.com/es/actualidad/nuestros-expertos/ventajas-y-desventajas-de-la-conmutacion-de-circuitos>

vmware. (s. f.). *WAN tradicional frente a VMware SD-WAN | VMware | ES*. (2023).

Recuperado 5 de mayo de 2023, de <https://www.vmware.com/es/solutions/sd-wan-traditional-wan.html>