

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE COACALCO

Título del proyecto

“Red empresarial con router cisco Nexus 7K
para la interconexión de centros de datos
regionales en sector financiero”

Opción de Titulación

“Estancias”

Que para obtener el título de
Ingeniero en Sistemas Computacionales
Con la Especialidad
Auditoria y seguridad informática

Presenta(n)

Carlos Hernández Meneses

Coacalco de Berriozábal, Septiembre/ 2023

AGRADECIMIENTOS.

En primer lugar, agradezco a dios por darme la vida y el don de la sabiduría y por qué a pesar de las adversidades que he vivido nunca dejo que las mismas me derroten.

Agradezco a mis padres que siempre me han brindado su apoyo incondicional para poder cumplir todos mis objetivos personales y académicos. Ellos son los que con su cariño me han impulsado siempre a perseguir mis metas y nunca abandonarlas frente a las adversidades, gracias padre por todo y a mi madre que ahora me cuida desde el cielo quiero decirle que finalmente lo logre, sé que estarás muy orgullosa de mí, te amo.

Agradezco al Tecnológico de Estudios Superiores de Coacalco por haberme abierto las puertas y permitirme estudiar mi carrera profesional, así como también a los diferentes docentes que brindaron sus conocimientos y su apoyo para seguir adelante día con día.

Agradezco también a mi asesor de proyecto al Ing. Roberto Carlos Muñoz Celaya por haberme brindado la oportunidad de recurrir a su capacidad y conocimiento, así como también haberme tenido toda la paciencia del mundo para guiarme durante todo el desarrollo del mismo.

También agradezco a todos los que fueron mis compañeros de clase durante los cuatro años y medio que curse la universidad ya que gracias al compañerismo, amistad y apoyo han aportado en un alto porcentaje a mis ganas de seguir adelante en mi carrera profesional.

A si mismo quiero expresar mi gratitud a mis colegas de trabajo quienes contribuyeron con el desarrollo del proyecto, Agradezco a todos los que me ayudaron a recopilar la información necesaria y aquellos que dedicaron su tiempo a revisar mi trabajo, Los comentarios de mejora, las sugerencias de bibliografía, las conversaciones para revisar conceptos, propuestas y análisis son la base de estas páginas.

RESUMEN.

El presente proyecto de estancias refleja todos mis conocimientos adquiridos en mi etapa académica y ahora ya como profesional dentro del área de sistemas, fue la compañía BBVA Axial Tech quien me dio la oportunidad de ejecutar mis conocimientos adquiridos durante mi formación profesional, BBVA es reconocida nacional e internacionalmente por ser una compañía líder en brindar servicios financieros a todos sus clientes, de la mano del fabricante Cisco implementa diferentes soluciones tecnológicas que ayudan a optimizar y solucionar diferentes conflictos en las redes corporativas de la institución.

Lo que pretendo demostrar en el presente trabajo, es la configuración, análisis y diseño necesario para lograr interconectar un centro de datos con otras regiones a través de tecnología cisco, Explico paso a paso como se fue dando la solución con diferentes configuraciones y protocolos de red hasta conseguir el mejor resultado en la compañía.

Sin duda alguna ha sido una etapa muy enriquecedora que me trajo mucha experiencia en el ámbito profesional, el mundo de las comunicaciones es muy extenso y en todas las compañías se requiere de personal calificado para implementar soluciones que involucran protocolos y estándares de comunicaciones, gracias a los conocimientos adquiridos durante mi formación académica me permitió aportar mis capacidades técnicas al resto del equipo de arquitectura con los que estuve trabajando de la mano en cada una de las etapas del proyecto.

La infraestructura de comunicaciones es importante dentro de una empresa ya que gracias a esta mantiene inter conectados a usuarios internos y externos que requieren acceder a información importante de la compañía del día a día.

INDICE DE CONTENIDO.

Pág.

CAPITULO I GENERALIDADES DEL PROYECTO

1.1 Introducción.	1
1.2 Descripción del centro, empresa u organismo.	2
1.3 Problemática.	3
1.4 Justificación.	4
1.5 Objetivos.	5
1.5.1 General.	5
1.5.2 Específicos.	5
1.6 Alcances y limitaciones.	5

CAPÍTULO II MARCO TEÓRICO

2.1 Introducción al capítulo.	7
2.2 Protocolos de ruteo dinámico.	7
2.2.1 Protocolo de apertura de la ruta más corta primero.	7
2.2.2 Protocolo de enlace de puerta fronteriza.	9
2.3 Cableado Estructurado.	10
2.4 Fibra óptica.	11
2.4.1 Tipos de Fibra óptica.	12
2.4.2 Distancia de fibra óptica Multimodo vs Monomodo	13
2.4.3 Ancho de banda de Fibra óptica Multimodo vs Monomodo.	13
2.5 Contexto virtual de dispositivos.	13
2.6 Protocolos de capa 2.	14
2.6.1 Detección de link unidireccional.	14
2.6.2 Detección de reenvío bidireccional.	15

2.7 Redes de área local.....	17
2.8 Redes de área amplia.....	18
2.9 Diferencia entre una red local y una red de área amplia.	19
2.9.1 Transmisión de datos.....	20
2.9.2 Seguridad.....	20
2.10 Centros de procesamiento de datos.	21
2.10.1 Auditoría Técnica.	21
2.10.2 Limpieza Técnica.	21
2.10.3 Mantenimiento.....	22
2.10.4 Instalaciones Anti vibraciones.	22
CAPÍTULO III DESARROLLO	
3.1 Introducción al capítulo.	23
3.2 Hardware para la implementación.	23
3.2.1 Cisco Nexus 7K.....	23
3.2.2 Módulos de fábrica.	25
3.2.3 Redundancia de fuentes de poder.	26
3.2.4 Transceptores Ópticos.	28
3.2.5 Versión de software.....	29
3.3 Configuración básica de equipo Router Cisco Nexus 7K.....	29
3.3.1 Configuración del nombre del equipo (hostname).....	29
3.3.2 Deshabilitar la traducción de nombres de dominio.....	30
3.3.3 Mensaje de aviso contra intrusos.	31
3.3.4 Usuario local y contraseña.	31
3.3.5 Protección del acceso a modo EXEC privilegiado	32
3.3.6 Protección del acceso a modo EXEC usuario.	33

3.3.7 Contraseñas VTY.....	33
3.3.8 Contraseñas encriptadas.	34
3.3.9 Configuración manual de reloj en el dispositivo.	34
3.3.10 Configuración de Autenticación por Tacacs+.	35
3.4 Diseño Topología Red de área Local.....	36
3.4.1 Capa Core.....	37
3.4.2 Capa Agregación.....	37
3.4.3 Capa Acceso.....	38
3.5 Diseño de topología Red de área amplia.....	38
3.5.1 Topología física.....	39
3.5.2 Distribución geográfica.....	41
3.5.3 Topología lógica.....	42
3.5.4 Características de la implementación.....	43
3.6 Direccionamiento IP.....	44
3.7 Contexto virtual del dispositivo.	45
3.7.1 Recursos para cada contexto virtual del dispositivo.....	46
3.7.2 Asignación de interfaces en contextos virtuales.....	49
3.8 Diseño de capa 2.....	50
3.8.1 Detección de link unidireccional.	50
3.8.2 Detección de reenvío bidireccional.....	52
3.9 Capa Routing.....	53
3.9.1 Costos protocolo de apertura de la ruta más corta primero.	54
3.9.2 Configuración protocolo de apertura ruta más corta primero.	56
3.9.3 Puntos importantes protocolo de enlace de puerta fronteriza.	60
3.9.4 Configuración de protocolo de enlace fronteriza.....	61

3.9.5 Conexión con nubes publicas	64
---	----

CAPÍTULO IV RESULTADOS

4.1 Introducción al capítulo.	67
4.2 Topología final.	67
4.3 Equipos Data Center Cloud Edge (DCE).	68
4.3.3 Rutas aprendidas	72
4.3.3.1 Routing desde los equipos DCE2PROD1 y DCE2PROD2.....	72
4.3.3.2 Validar rutas desde los equipos DCVE	74
4.3.4 Rutas propagadas	78
4.4 Equipos DC2S en centro de datos DC2.....	78
4.4.1 Interfaces UP.	80
4.4.2 Adyacencias UP	81
4.4.3 Adyacencias con LANC y LANP:.....	82
4.4.4 Rutas aprendidas por ruteo dinámico.....	84
4.4.5 Validar rutas propagadas.	89
4.4.6 Planeación de actividades.....	89

Conclusiones.

Competencias desarrolladas.

Fuentes de Información.

Anexos.

INDICE DE FIGURAS.

	Pág.
Figura. 1 Cableado estructurado	11
Figura. 2 Tipos de fibraoptica.....	12
Figura. 3 Contexto virtual de dispositivos.....	14
Figura. 4 Red LAN.....	17
Figura. 5 Red WAN	19
Figura. 6 Centros de datos.....	22
Figura. 7 Nexus 7k configuracion.....	23
Figura. 8 N77-SUP2E.....	24
Figura. 9 N77- F324FQ-25	25
Figura. 10 N77-AC-3KW.....	25
Figura. 11 N77-C7706-FAB-2.....	26
Figura. 12 Comando para configurar fuentes de poder.....	27
<i>Figura. 13 Comando “show enviroment power”.....</i>	28
Figura. 14 QSFP-40G-SR-BD.	28
Figura. 15 Configuracion hostname.	30
Figura. 16 Deshabilitar traduccion de nombres.....	31
Figura. 17 Mensaje de aviso contra intrusos.....	31
Figura. 18 Configuración usuario local y contraseñas.....	32
Figura. 19 Proteccion del acceso a modo exec privilegiado.....	32
Figura. 20 Proteccion del acceso a modo exec usuario.	33
Figura. 21 Configuracion contraseña VTY.	33
Figura. 22 Configuracion contraseñas encriptadas.	34
Figura. 23 Configuracion manual de reloj en router.	34
Figura. 24 Configuracion de autenticacion por tacacs+.....	35
Figura. 25 Topologia LAN	36
Figura. 26 Capa Core.....	37
Figura. 27 Capa distribucion.....	37
Figura. 28 Capa Acceso	38

Figura. 29 Topologia WAN	38
Figura. 30 Topologia Fisica	39
Figura. 31 Equipos montados en Rack.	40
Figura. 32 Distribucion geografica de data centers	41
Figura. 33 Topologia logica.	42
Figura. 34 Comando “Show routing memory”.	46
Figura. 35 Configuracion recursos VDC.	47
Figura. 36 Comando “show vdc resource detail”.	48
Figura. 37 Configuracion de CPU en VDC.	49
Figura. 38 UDLD enlaces activos.	51
<i>Figura. 39 Configuración UDLD.</i>	<i>51</i>
<i>Figura. 40 Configuración para deshabilitar protocolo UDLD.</i>	<i>52</i>
Figura. 41 Enlaces BFD.	52
Figura. 42 Configuracion de BFD.	52
Figura. 43 Ruteo dinamico vista general.	53
Figura. 44 Ruteo interfaces punto a punto.	54
Figura. 45 Comportamiento del flujo de trafico.	55
Figura. 46 Costo de enlaces de OSPF.	56
<i>Figura. 47 Configuración de OSPF router 1.</i>	<i>56</i>
Figura. 48 Configuración de OSPF router 2.	57
<i>Figura. 49 Configuración de interfaces con ospf.</i>	<i>58</i>
<i>Figura. 50 Configuración de route-map en router 1.</i>	<i>59</i>
Figura. 51 Configuración de route map en router 2.	60
<i>Figura. 52 Configuración de BGP en router 1</i>	<i>61</i>
Figura. 53 Configuración de interfaces BGP en router 1 y 2	62
Figura. 54 Configuración de route-maps.	63
Figura. 55 Configuración OSPF hacia nubes router 1	64
Figura. 56 Configuracion OSPF hacia nubes router 2	65
<i>Figura. 57 Topología Final.</i>	<i>67</i>
Figura. 58 Salida comando “show ip interface brief” DCE2PROD1	69
Figura. 59 Salida comando “show ip interface brief” DCEDEV1	69

Figura. 60 Ejemplo log caída de interfaz	70
Figura. 61 Salida de comando “show ip ospf neighbors” DCPROD1	70
Figura. 62 Salida de comando “show ip ospf neighbors” DCEDEV1	70
Figura. 63 Salida de comando “show ip bgp summary” DCE2PROD1	71
Figura. 64 Salida de comando “show ip bgp summary” DCEDEV1	71
Figura. 65 Salida de comando “show ip loggin last 50” DCEPROD1	72
Figura. 66 Salida de comando “show ip route ospf-1 sum” DCE2PROD1	73
Figura. 67 Salida de comando “show ip route ospf-1” DCE2PROD1	73
Figura. 68 Salida de comando “show ip bgp” DCE2PROD1	74
Figura. 69 Salida de comando “show ip route bgp” DCEPROD1	75
Figura. 70 Salida de comando “show bgp event-history” DCEPROD1	76
Figura. 71 Comando “show routing event-history delete-route” DCEPROD1	76
Figura. 72 Comando “show routing event-history add-route” DCEPROD1	77
Figura. 73 Salida de comando “show accounting log” DCEPROD1	77
Figura. 74 Salida de comando “show ip bgp” DCEPROD1	78
Figura. 75 Salida de comando “show ip interface brief” DCS1	80
Figura. 76 Salida de comando “show ip ospf neighbors” DCS1	81
Figura. 77 Salida de comando “show ip ospf neighbors” DCS2	81
Figura. 78 Salida de comando “show ip bgp summary” DC2S1	82
Figura. 79 Salida de comando “show ip bgp summary” DC2S2	83
Figura. 80 Salida de comando “show ip route ospf summary” DC2S1	84
Figura. 81 Salida de comando “show ip route ospf” DC2S1	85
Figura. 82 Salida de comando “show ip bgp i 6XXX0” DC2S1	86
Figura. 83 Salida de comando “show ip bgp i 6XXX1” DC2S1	87
Figura. 84 Salida de comando “show ip route bgp” DC2S1	88
Figura. 85 Comando “show ip bgp nei 3.XX.XX.6 advertised-routes” DC2S1	89
Figura. 86 Diagrama Gantt “Cronograma de actividades”	90

INDICE DE TABLAS.

	Pág.
Tabla 1 Detalles de las fuentes de poder.	26
Tabla 2 Requerimientos de voltaje por router.....	27
Tabla 3 Características de QSFP-40G-SR-BD.....	29
Tabla 4 Version de software para equipos Nexus 7K.....	29
Tabla 5. Matriz de cableado	40
Tabla 6 Direccionamiento Ip Loopback	44
Tabla 7 Direccionamiento IP fuera de banda	44
Tabla 8 Redes punto a punto entre enlaces WAN	45
Tabla 9 Limite de recursos por cada VDC.....	46
Tabla 10 Asignación de interfaces en switch router DC1	49
Tabla 11 Asignacion de interfaces en switch router DC2	49
Tabla 12 Asignacion de interfaces en switch DCR.....	49
Tabla 13 Costos de enlaces de OSPF.	55
Tabla 14 Infraestructura DCE.....	68
Tabla 15 Conexiones fisicas contexto vistual DCEPROD.	68
Tabla 16 Conexiones fisicas contexto vistual DCEDEV.	69
Tabla 17 Conexiones fisicas equipo DC2S1.	79
Tabla 18 Conexiones fisicas equipo DC2S2.	79
Tabla 19 Router ID de adyacencias OSPF DC2S1.....	82
Tabla 20 Router ID de adyacencias OSPF DC2S2.....	82
Tabla 21 Router ID adyacencias de BGP DC2S1.	83
Tabla 22 Router ID adyacencias de BGP DC2S2.	84
Tabla 23 Plan de actividades.	89

CAPITULO I GENERALIDADES DEL PROYECTO

1.1 INTRODUCCION.

A continuación, a manera de resumen se detalla el contenido de cada uno de los capítulos que contiene el presente trabajo de investigación con la finalidad de que el lector tenga un conocimiento general de este proyecto.

En el capítulo 1 “Generalidades del proyecto” se mencionan la descripción de la empresa u organismo donde se realizaron las estancias profesionales, la justificación del trabajo, los objetivos generales y específicos, así como los alcances y limitaciones.

En el capítulo 2 “Marco Teórico” se redacta la explicación detallada de los conceptos técnicos que el lector necesita saber, para una mejor comprensión del proyecto.

En el capítulo 3 “Desarrollo” se describe todo el procedimiento realizado para cumplir el objetivo del proyecto partiendo de la descripción del hardware que se utilizó para la implementación, la configuración básica de los dispositivos de red, el diseño de la topología de red LAN, el diseño de la topología de red WAN, los contextos virtuales de los dispositivos, el diseño de capa 2 y por último la capa de ruteo.

En el capítulo 4 “Resultados” se analizan los resultados obtenidos en este proyecto, topología final, validación de los equipos Data center cloud Edge y las validaciones de los equipos DC2S del centro de datos 2.

Al final se incluyen apartados de conclusiones, competencias a desarrollar, Anexos y fuentes de información.

1.2 DESCRIPCION DEL CENTRO, EMPRESA U ORGANISMO.

BBVA Axial Tech es una compañía compuesta por expertos tecnológicos globales que forman una empresa clave en el desarrollo de las estrategias del área global de ingeniería para impulsar la transformación tecnológica de BBVA.

Su ADN es la suma de la fortaleza de un banco con la capacidad de revolucionar de una empresa tecnológica

Uno de sus principios es potenciar el talento, Dar autonomía y oportunidades de desarrollo y crecimiento, potenciar el bienestar de los empleados.

Sus principales líneas de negocio son:

1. Infraestructura y operaciones: Unidad encargada del procesamiento y de operar soluciones de calidad, de manera segura, confiable y sostenible.
2. Arquitectura: Unidad que impulsa la adopción de la plataforma bancaria, la evolución de la nube, el robustecimiento de datos y la visión transversal de la arquitectura.
3. Desarrollo de software: Unidad enfocada en el desarrollo de software y sistemas para los programas top de tecnología en BBVA de forma global.

Nuestra visión es vivir en una transformación continua donde exploramos y aprendemos con la tecnología para mejorar la experiencia de nuestros clientes.

Nuestra Misión es no solo ser una compañía de tecnología, ser también una filosofía de trabajo donde puedes desarrollar tu talento mientras descubres y resuelves retos, apostamos por desarrollos que nos permitan aprender, generar y compartir más conocimiento.

La compañía está ubicada en la dirección Calz. Gral. Mariano Escobedo 303, Granada, Miguel Hidalgo, 11520 Ciudad de México, CDMX, corporativo BBVA parques Polanco.

1.3 PROBLEMÁTICA.

La compañía financiera decidió renovar la tecnología que provee la administración y comunicación principal en sus servicios e instalaciones de sus centros de datos mediante la compra de equipos cisco Nexus especializados para Data Center esto para proveer de mejores herramientas de trabajo a sus colaboradores de tal manera que era necesario equipamiento de networking de reciente tecnología, esto como parte de una estrategia para una mejor y mayor captación de oportunidades de negocio donde su personal cuente con los recursos tecnológicos necesarios que les permita desempeñar mejor su función.

La necesidad surge después de detectar problemas en la infraestructura de comunicaciones antigua, la cual no soportaba las cargas de trabajo de cada una de las regiones provocando latencia en las comunicaciones, perdidas de paquetes y afectación con impacto en servicios internos y externos de la institución financiera como lo es su aplicación móvil.

Con el surgimiento de proveedores de nube publica como lo son Amazon AWS, Google GCP y Microsoft Azure, surge la necesidad de conectar los centros de datos de la compañía con la nube de AWS donde es necesario comenzar a subir algunos de los servicios más críticos del banco, como actualmente lo están haciendo grandes compañías como Netflix, Spotify etc. Con el objetivo de ahorrar costos de operación que conlleva mantener un centro de datos, es por eso que se necesita interconectar los centros de datos privados de la institución financiera con AWS para formar una nube hibrida donde se puedan consumir recurso compartidos de un sitio a otro.

1.4 JUSTIFICACION.

Las Tecnologías de la información en las empresas actualmente juegan un papel muy importante ya que estas manejan grandes cantidades de información y necesitan de recursos tecnológicos para poder administrar todos estos datos y enviarlos o compartirlos con otros sitios, Se requiere que esta información siempre pueda estar disponible en cualquier parte del planeta y en todo momento, es aquí donde las telecomunicaciones Juegan un papel fundamental y muchas de las veces necesario.

Las comunicaciones en la actualidad continúan cambiando y adaptándose a las nuevas tecnologías que van saliendo en el mercado grandes proveedores como Cisco están constantemente innovando y experimentando en nuevos modelos de comunicación.

Los centros de datos son instalaciones físicas que las organizaciones utilizan para alojar sus aplicaciones y datos confidenciales, Entre los componentes clave del diseño de un centro de datos, se incluyen routers, switches, firewalls, sistemas de almacenamiento, servidores, balanceadores de carga y controladores de entrega de aplicaciones. La infraestructura ha pasado de servidores físicos tradicionales a redes virtuales que admiten aplicaciones y cargas de trabajo en un entorno multinube.

En esta época, los datos existen y están conectados en varios centros de datos, nubes públicas y privadas. El centro de datos debe poder comunicarse en todos estos sitios múltiples, tanto en las instalaciones privadas como en las nubes públicas. Incluso la nube publica es un conjunto de centros de datos, Al almacenar aplicaciones en la nube se utilizan recursos de centros de datos del proveedor de la nube.

La infraestructura de red en un centro de datos conecta servidores físicos y virtuales, servicios del centro de datos, almacenamiento y provee conexión externa a otros sitios en diferentes regiones.

1.5 OBJETIVOS.

1.5.1 General.

Desarrollar la red empresarial con router cisco 7K para la interconexión de centros de datos regionales aplicando la configuración de protocolos de ruteo dinámico y protocolos de capa 2 del modelo OSI en el sector financiero.

1.5.2 Específicos.

- 1 Definir Hardware necesario para la implementación.
- 2 Configuración básica de equipo Router Cisco Nexus 7000
- 3 Diseño topología LAN a bajo nivel.
- 4 Diseñar topología WAN a bajo nivel.
- 5 Diseñar direccionamiento IP.
- 6 Configurar virtualización de equipo Router Cisco 7K
- 7 Configurar protocolos de capa 2.
- 8 Configurar Ruteo dinámico.

1.6 ALCANCES y LIMITACIONES.

El presente trabajo describe el detalle la arquitectura que se utilizó en la implementación para la interconexión de los centros de datos regionales.

El alcance implica la interconexión de los centros de datos regionales con los equipos frontera hacia las nubes públicas y La interconexión con las redes de área local en el centro de datos DC2 GDL, así como la conexiones con los otros 2 centros de datos.

Estas integraciones en Data Center 2 GDL será de 4 puertos de 40g hacia las redes LANC y LANP mediante el protocolo de ruteo dinámico BGP, 2 puertos de 40G hacia los equipos data cloud edge equipos encargados del ruteo hacia la nube publica, 1 puerto de 10g hacia Data Center 1 MEX y una conexión de 10g hacia Data Center R DGO para así integrar la interconexión de los 3 centros de datos mediante el protocolo de ruteo dinámico OSPF en Área 0.

El objetivo final de este alcance es la completa migración de las conexiones actuales a esta nueva interconexión compuesta por equipos cisco Nexus 7K de altas capacidades de procesamiento de datos en DC2, DC1 Y DCR.

La configuración de la red LAN, así como las configuraciones de los proveedores de servicios de internet para interconectar los centros de datos están fuera del alcance de este proyecto, la configuración de los equipos DCE para conectar con las nubes públicas están fuera del alcance de este proyecto, esta administración y configuración la realiza otro equipo de trabajo dentro de la institución financiera, La configuración de los equipos cisco Nexus 7k en las regiones de DC1 Y DCR es una réplica del diseño y configuración de la región DC2.

CAPÍTULO II MARCO TEÓRICO

2.1 INTRODUCCION AL CAPITULO.

A continuación, se describen los conceptos técnicos más importantes con el objetivo de que el lector pueda entender mejor el proyecto, se abarcaran temas como protocolos de ruteo dinámico, cableado estructurado, contexto virtual de dispositivo, protocolos de capa 2, redes de área local, redes de área amplia y la descripción de un centro de procesamiento de datos.

2.2 PROTOCOLOS DE RUTEO DINAMICO.

En una red corporativa con gran cantidad de redes y subredes, la configuración y el mantenimiento de rutas estáticas entre dichas redes implica gran cantidad de trabajo operativo, Se puede volver una tarea tediosa y complicada si se realizan cambios en la red. La mejor opción es implementar protocolos de ruteo dinámico esto puede disminuir las tareas de configuración y de mantenimiento, además de proporcionar escalabilidad a la red. (Walton A. , CCNA desde Cero, 2018)

El enrutamiento es el proceso de selección de rutas en cualquier red. Una red de computación está formada por muchas máquinas, llamadas *nodos*, y rutas o enlaces que conectan dichos nodos. La comunicación entre dos nodos en una red interconectada se puede producir a través de muchas rutas diferentes. El enrutamiento es el proceso de seleccionar la mejor ruta mediante algunas reglas predeterminadas. (AWS, s.f.)

En el enrutamiento dinámico, la tabla de enrutamiento se actualiza automáticamente a medida que los cambios en la red se producen. Los protocolos de enrutamiento dinámico, como el protocolo de apertura de la ruta más corta primero (OSPF) y el protocolo de enrutamiento de puerta de enlace interior mejorado (EIGRP), utilizan información sobre la topología de la red para calcular la mejor ruta a utilizar. (Sepulveda, 2023)

2.2.1 Protocolo de apertura de la ruta más corta primero.

Como lo menciona cisco en su guía de diseño el protocolo de apertura de la ruta más corta primero (OSPF) es un protocolo de Gateway interior que se usa para

distribuir la información de ruteo dentro de un solo sistema autónomo, El protocolo OSPF se desarrolló debido a la necesidad dentro de la comunidad de Internet de introducir un Internal Gateway Protocol (IGP) no patentado de gran funcionalidad para la familia de protocolos TCP/IP, El protocolo OSPF está basado en tecnología de estado de link, la cual es una desviación del algoritmo basado en el vector Bellman-Ford usado en los protocolos de ruteo de Internet tradicionales, como el RIP. (Cisco, 2023)

2.2.1.1 Ventajas principales.

En comparación con los protocolos de direccionamiento de distancia vector como el protocolo RIP, OSPF es más adecuado para servir entre redes de gran tamaño, puede calcular las rutas en muy poco tiempo cuando cambia la topología de red. Puede dividir un sistema autónomo en áreas y mantenerlas separadas para disminuir el tráfico de direccionamiento de OSPF y el tamaño de la base de datos en enlace estado de cada área. (IBM, S.)

2.2.1.2 Como funciona.

Como menciona Marcelo en el artículo “Introducción a OSPF” Los protocolos de estado de enlace crean rutas IP con un par de pasos importantes:

1. Primero, todos los routers juntos construyen la información sobre la red: routers, enlaces, direcciones ip, información de estado.
2. Luego los routers inundan la red de información, así que todos los routers conocen la misma información. En este punto cada router puede calcular las rutas a todas las subredes, pero desde la perspectiva de cada router. (Marcelo, 2020)

OSPF puede construir una base de datos que incluya todos los enlaces en la red y luego utilizar el algoritmo primero el camino más corto (SPF, Shortest Path First) para determinar cuáles son los caminos más cortos a todos los destinos. Como cada enrutador contiene el mismo mapa de topología, OSPF no requiere que las actua

lizaciones se envíen a intervalos regulares. A no ser que se produzca un cambio en OSPF. (HUAWEI, 2020)

2.2.2 Protocolo de enlace de puerta fronteriza.

BGP es un conjunto de reglas que determinan las mejores rutas de red para la transmisión de datos en internet, Internet se compone de muchas redes privadas, publicas, corporativas y gubernamentales vinculadas entre si mediante protocolos, dispositivos y tecnologías de comunicación estandarizados. Cuando navega por internet los datos viajan a través de varias redes antes de llegar a su destino, la responsabilidad de BGP es analizar todas las rutas disponibles por las que podrían viajar los datos y seleccionar la mejor ruta, por ejemplo, cuando un usuario de los Estados Unidos carga una aplicación con servidores de origen Europa, el protocolo BGP hace que la comunicación sea rápida y eficiente. (AWS, s.f.)

2.2.2.1 Como funciona.

Cada AS en Internet está conectado directamente a un conjunto de terminales que probablemente se encuentren dentro de un determinado rango de direcciones IP. En BGP, cada sistema autónomo es responsable de recopilar y comunicar información de enrutamiento con sus pares (los ASN con los que está directamente conectado) como anuncios de prefijo de red. Por ejemplo, un AS anunciará que está conectado directamente a ciertas direcciones IP, que está a un salto de otras, y así sucesivamente. Dado que cada AS comunicará la información de enrutamiento que ha recibido a sus pares, esta información eventualmente se filtrará a través de toda la red. Como resultado, un ASN aprenderá los prefijos de red incluso para los ASN a los que no está conectado directamente. (Netalit, 2023)

Todos los demás protocolos de routing se ocupan únicamente de encontrar la ruta optima hacia todos los destinos conocidos. BGP no puede adoptar ese enfoque simplista por que los acuerdos de pares entre ISP casi siempre resultan en políticas de routing complejas. Para ayudar a los operadores de red a implementar estas

políticas, BGP lleva una gran cantidad de atributos con cada prefijo IP, incluidos los siguientes: (Walton A. , CCNA desde cero, 2020)

1. La ruta del sistema autónomo (AS).
2. La preferencia local.
3. El discriminados de múltiples salidas.
4. Comunidades.

2.3 CABLEADO ESTRUCTURADO.

Como menciona Albarrán en la página de internet Redes & Telecom el cableado estructurado es una infraestructura común de telecomunicaciones construida para conectar distintos dispositivos-transportar señales desde dispositivos emisores a otros receptores- en redes locales. Es el conjunto de cables, conectores, canalizaciones y dispositivos que componen la infraestructura de telecomunicaciones interior de un edificio o data center. Consiste en cables de par trenzado protegidos STP o UTP en el interior de un edificio con el propósito de implantar una red local. (Albarran, 2022)

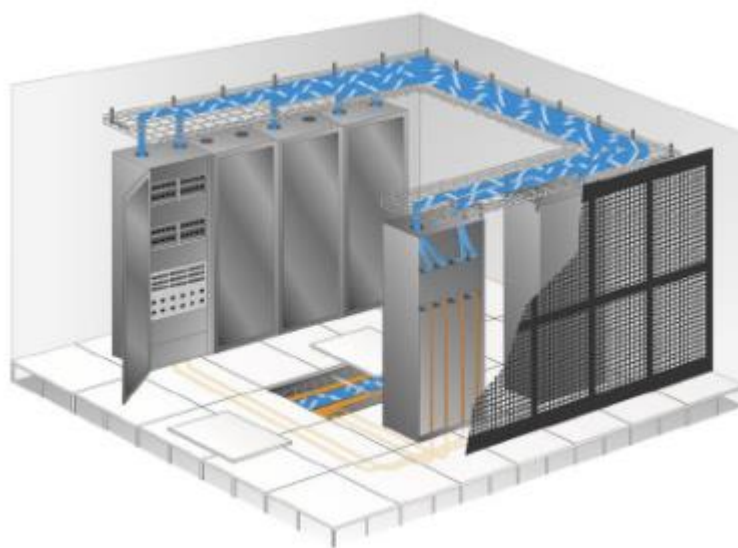
Estos sistemas han ido evolucionando para ofrecer mayores velocidades y arquitecturas de red que permitan una gestión eficiente para los edificios inteligentes, existen diferentes categorías:

1. Cat 1 Usando para comunicaciones telefónicas.
2. Cat 2 Frecuentemente utilizado para redes token ring.
3. Cat 3 Actualmente usado para redes ethernet 10 mb/s.
4. Cat 4 Utilizado en redes token ring, diseñado para transmisión a frecuencias de hasta 20 MHz.
5. Cat 5 Frecuentemente utilizado en redes ethernet, fast ethernet 100 mb/s.
6. Cat 5e Se encuentra en redes fast ethernet 100 mb/s y gigabit ethernet 1000 mb/s.
7. Cat 6 Usado en redes gigabit ethernet 1000 mb/s.
8. Cat 6a Usado en redes 10 gigabit ethernet diseñado para transmitir a frecuencias de hasta 500 MHz

9. Cat 7 Se usa en redes de 10 gigabit ethernet y comunicaciones de alta confiabilidad, diseñado para transmitir 600 Mhz.
10. Cat 7a Caracterización para cable de 1000 Mhz. Se emplea en redes 10 gigabit ethernet y futuras comunicaciones de mayor velocidad de transmisión de datos.
11. Cat 8 Ofrece un ancho de banda de hasta 2 ghz y velocidad de hasta 25 gb y 40gb uso casi exclusivo de entornos CPD.

(Albarran, 2022)

Figura. 1 Cableado estructurado



FUENTE: <https://www.c3comunicaciones.es/data-center-el-estandar-tia-942/>

2.4 FIBRA OPTICA.

La fibra óptica se compone de filamentos de vidrio, aunque algunas veces se pueden encontrar de plástico. La forma de enviar información a través de la fibra óptica es a través de haces de luz, los cuales viajan dentro de ella. En telecomunicaciones, es el medio de transmisión más utilizado gracias a la gran capacidad que tiene de enviar información, ya que a través de un hilo de fibra óptica se pueden enviar millones de bits por segundo (bps) y acceder a servicios de manera simultánea con gran velocidad y calidad. (ABC de la Fibra Óptica - MINTIC - Vive Digital. (n.d.). , s.f.)

2.4.1 Tipos de Fibra óptica.

2.4.1.1 Fibra Monomodo:

Solo dispone de un modo de propagación, una sola longitud de onda de luz en el núcleo de fibra, esto significa que no hay interferencias ni solapamientos entre distintas longitudes de onda de luz que pudieran distorsionar sus datos a grandes distancias. (Protected, E, s.f.)

El cable monomodo tiene un núcleo de vidrio pequeño que es mucho más pequeño que el multimodo y solo una ruta para la luz o modo de propagación. (Protected, E, s.f.)

2.4.1.2 Fibra Multimodo:

Fibra utilizada habitualmente en aplicaciones informáticas. Clasificada en varios tipos (OM1, OM2, OM3 y OM4) en función de su ancho de banda, de su aplicación y de la distancia cubierta por el enlace. La de tipo OM2 permite soluciones económicas al utilizarla para la transmisión analógica de señal banda base (CCTV) en distancias hasta 2 o 3 Km. (Diferentes tipos de fibra óptica | Grupo COFITEC. (n.d.), s.f.)

Figura. 2 Tipos de fibraoptica



FUENTE: <https://www.aunadistribucion.com/blog/tipos-de-fibra-optica-openetics/>

2.4.2 Distancia de fibra óptica Multimodo vs Monomodo

La fibra multimodo ofrece una distancia máxima mucho más corta que la fibra monomodo, siendo la opción ideal para aplicaciones locales. La fibra monomodo puede llegar a cubrir distancias de 40 km o más sin dañar la señal, siendo ideal para aplicaciones de largo alcance. (Black Box Mexico, s.f.)

2.4.3 Ancho de banda de Fibra óptica Multimodo vs Monomodo.

La fibra monomodo tiene un ancho de banda significativamente mayor que la fibra multimodo. Puede utilizar un par de hilos de fibra monomodo full dúplex para obtener hasta dos veces el rendimiento de un cable de fibra multimodo. Las longitudes y velocidades que se obtienen con el cable monomodo se deben a que, al transmitir la luz en un solo modo, se anula el retardo de modo diferencial (DMD) que es el principal factor limitante del ancho de banda de la fibra multimodo. (Black Box Mexico, s.f.)

2.5 CONTEXTO VIRTUAL DE DISPOSITIVOS.

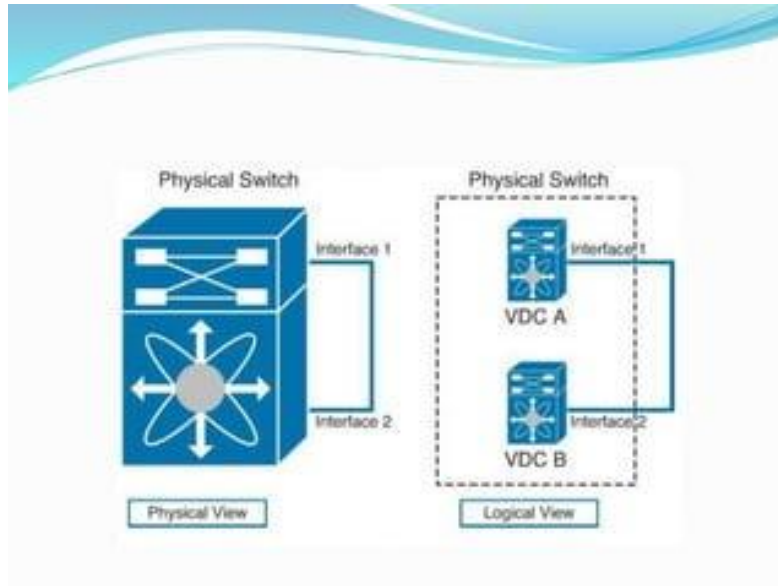
EL software de cisco NX-OS soporta VDC's, lo cual significa que puedes particionar un solo router cisco 7k en múltiples dispositivos lógicos que proporcionan aislamiento de fallas, aislamiento de administración, aislamiento de asignación de direcciones y administración adaptable de recursos. Puede administrar una instancia de VDC dentro de un dispositivo físico de forma independiente. Cada VDC aparece como un dispositivo único para los usuarios conectados. (CISCO, 2021)

VDC se ejecuta como una entidad lógica separada dentro del dispositivo físico, mantiene su propio conjunto único de procesos de software, tiene su propia configuración y es administrado independientemente. (CISCO, 2021)

Los VDC también virtualizan el plano de control que incluye todas aquellas funciones de software que procesa la CPU en el módulo supervisor activo. El plano de control soporta los procesos de software para los servicios en el dispositivo físico,

como la base de información de enrutamiento (RIB) y los protocolos de enrutamiento. (CISCO, 2021)

Figura. 3 Contexto virtual de dispositivos



FUENTE: <https://es.slideshare.net/networkershome/4vdc>

2.6 PROTOCOLOS DE CAPA 2.

En el modelo OSI cada capa agrupa algunas de las funciones requeridas para comunicar sistemas. Estas capas poseen estructura jerárquica. Cada capa se apoya en la anterior, realiza su función y ofrece un servicio a la capa superior. Este modelo posee la ventaja de poder cambiar una capa sin necesidad de modificar el resto. (Tolosa, 2014)

La capa 2 del modelo OSI capa de enlace de datos, su función principal es lograr una comunicación confiable entre equipos adyacentes, la unidad de información son las tramas (paquetes), en esta capa los protocolos realizan control de errores de secuencia y de flujo. (Tolosa, 2014)

2.6.1 Detección de link unidireccional.

Detección de enlace unidireccional (UDLD) permite el monitoreo de cables de fibra óptica, Opera transmitiendo paquetes UDLD a un dispositivo vecino que incluyen el

sistema ID y puerto ID de la interfaz que transmite el paquete UDLD. El dispositivo vecino repite esta misma información de regreso al dispositivo origen. Uldd es habilitado globalmente con el comando `ulld enable`, `ulld` puede ser deshabilitado de un puerto con el comando `ulld port disable`. (Brad Edgeworth, CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide, 2020)

Los mensajes UDLD se envían cada 15 segundos por default. UDLD puede detectar un enlace unidireccional después de aproximadamente tres veces el intervalo de tiempo en que envían los mensajes UDLD (45 segundos en total. Utilizando el valor predeterminado). (JM, s.f.)

UDLD tiene dos modos de operación:

1. Normal cuando se detecta una condición de enlace unidireccional, el puerto puede continuar su operación. UDLD simplemente marca el puerto como que tiene un estado indeterminado y genera un mensaje syslog
2. Aggressive cuando se detecta una condición de enlace unidireccional, el switch toma medidas para restablecer el enlace. Los mensajes UDLD se envían una vez por segundo durante 8 segundos. Si ninguno de esos mensajes se repite, el puerto se coloca en el estado errordisable para que no se pueda usar. (JM, s.f.)

2.6.2 Detección de reenvío bidireccional.

Como menciona cisco en su página Web el protocolo de reenvío bidireccional (BFD) es un protocolo de detección diseñado para proporcionar tiempos rápidos de detección de fallas en la ruta de reenvío para todos los tipos de medios, encapsulaciones, topologías y protocolos de enrutamiento. Además de la detección rápida de fallas en la ruta de reenvío, BFD proporciona un método consistente de detección de fallas para los administradores de red. Debido a que el administrador de la red puede usar BFD para detectar fallas en la ruta de reenvío a una velocidad uniforme, en lugar de velocidades variables para diferentes mecanismos de saludo del protocolo de enrutamiento, la creación de perfiles y la planificación de la red

serán más fáciles y el tiempo de reconvergencia será consistente y predecible. *(CISCO, 2015)*

BFD se ejecuta independientemente de cualquier otro protocolo (de enrutamiento). Una vez que esté en funcionamiento, puede configurar protocolos como OSPF, EIGRP, BGP, HSRP, MPLS LDP, etc. para utilizar BFD para la detección de fallas de enlaces en lugar de sus propios mecanismos. Cuando el enlace falla, BFD informará al protocolo. Hay dos modos de funcionamiento para BFD, modo asíncrono y modo de demanda. El modo asíncrono es similar a los temporizadores de saludo y espera, BFD seguirá enviando paquetes de saludo (llamados paquetes de control BFD) y cuando no recibe algunos de ellos, la sesión se cancela. *(Molenaar R. , 2020)*

El modo de demanda es diferente: una vez que BFD ha encontrado un vecino, no enviará paquetes de control continuamente, sino que solo utilizará un mecanismo de sondeo. Se debe utilizar otro método para verificar la accesibilidad; por ejemplo, podría verificar las estadísticas de recepción y transmisión de la interfaz. En este momento, Cisco (o cualquier otro proveedor que conozca) no admite el modo de demanda BFD. *(Molenaar R. , 2020)*

Ambos modos también admiten algo llamado modo eco. Cuando un dispositivo envía paquetes de eco BFD, el receptor los devolverá sin procesarlos. Cuando el remitente no recupera los paquetes de eco, sabe que algo anda mal y cancelará la sesión. *(Molenaar R. , 2020)*

Los protocolos de enrutamiento tienen un mecanismo de saludo de forma predeterminada para declarar fallas en los enlaces, pero este mecanismo se diferencia de un enrutador a otro. Con la detección de reenvío bidireccional, se creó un mecanismo de detección de fallas de enlace común, por lo tanto, este mecanismo proporciona una convergencia muy rápida después de una falla en el enlace en comparación con el mecanismo hello del protocolo de enrutamiento. *(IPCISCO, 2023)*

BFD es un protocolo unidireccional para utilizar este protocolo se debe aplicar la configuración en ambos extremos. Existen 2 planos en una red uno de ellos es el plano de control donde se realiza el procesamiento de rutas y el otro es el plano de reenvío en el que el envío de los datos se establece tras el establecimiento de la sesión, BFD opera en el plano de reenvío. (IPCISCO, 2023)

2.7 REDES DE AREA LOCAL.

Como menciona Walton en el sitio web CCNA desde cero una red de área local conecta a equipos informáticos ubicados en un área geográfica reducida, como un edificio o un centro de datos. (Walton A. , 2022)

Una LAN es una infraestructura de la red que abarca un área geográfica pequeña, Las LANs tienen características específicas: (Walton A. , 2022)

1. Las LANs interconectan terminales en un área limitada, como una casa, un lugar de estudios, un edificio de oficinas o un campus. (Walton A. , 2022)
2. Por lo general, la administración de las LANs está a cargo de una única organización o persona. El control administrativo se aplica a nivel de red y rige las políticas de seguridad y control de acceso. (Walton A. , 2022)
3. Las LANs proporcionan ancho de banda de alta velocidad a dispositivos finales internos y dispositivos intermedios, como se muestra en la figura. (Walton A. , 2022)

Una red que sirve una casa, un edificio pequeño o un campus se considera una LAN. (Walton A. , 2022)

Figura. 4 Red LAN



FUENTE: <https://www.globenetcorp.com/es/elblog/red-lan-cloud-computing/>

2.8 REDES DE AREA AMPLIA.

Las redes de área extensa permiten que las redes de áreas locales o metropolitanas, hagan uso de ciertos servicios que éstas necesitan, para realizar sus labores, ya que las redes WAN le dan la oportunidad de transmitir grandes volúmenes de información; de igual manera estas redes le han facilitado las tareas a la sociedad en general, especialmente a las empresas ya que estas están en un crecimiento continuo. (Cabarcas Martínez, A., & Marrugo Castro, A., 2008)

Las redes WAN, han permitido que las transferencias de información de grandes volúmenes sean cada vez más requeridas por las empresas y usuarios, de igual manera las conexiones a larga distancia les han permitido a las personas vinculadas a éstas, que no se trasladen hasta los lugares de trabajo, ya que pueden hacer las labores desde sus hogares. (Cabarcas Martínez, A., & Marrugo Castro, A., 2008)

Una WAN define la forma en que los datos se desplazan a través de una zona geográficamente extensa, Las redes WAN interconectan diferentes redes LAN utilizando los servicios de un proveedor, las tecnologías de señalización y transporte que utilizan estos proveedores de servicios suelen ser transparentes para los usuarios finales. (Pavón, 2012)

Dentro de la nube WAN se dan tres tipos de conexiones:

1. Líneas alquiladas: también se llaman líneas punto a punto o líneas dedicadas ofrecen una comunicación por un medio exclusivo para el cliente. Estas líneas eliminan los problemas de conexión /desconexión de llamada y aportan mayor privacidad y seguridad. Suelen emplearse en conexiones serie síncronas manteniendo constantes la utilización del ancho de banda, son las líneas más costosas económicamente hablando. (Pavón, 2012)
2. Circuitos conmutados: sólo se establece comunicación entre el emisor y el receptor durante el tiempo que dura la transmisión y las sucesivas conexiones pueden o no utilizar la misma ruta u otra diferente. Este tipo de conexiones suele emplearse para entornos que tengan un uso esporádico, enlaces de respaldo o enlaces bajo demanda. También es posible

aprovecharse de los servicios de telefonía básicos mediante una conexión asíncrona conectada a un módem, como por ejemplo una línea RDSI. (Pavón, 2012)

3. Paquetes conmutados: es un método de conmutación donde los dispositivos comparten un único enlace punto-a-punto o punto-multipunto para transportar paquetes desde un origen hacia un destino a través de una red portadora. Este tipo de redes utilizan circuitos virtuales para ofrecer conectividad de forma permanente o conmutada (PVC o SVC). (Pavón, 2012)

Figura. 5 Red WAN



FUENTE: <http://informaciondeapoyoredes.wikidot.com/red-wan>

2.9 DIFERENCIA ENTRE UNA RED LOCAL Y UNA RED DE AREA AMPLIA.

Una red de área local (LAN) conecta dispositivos que están físicamente cerca unos de otros mediante conectores como enrutadores y conmutadores. Permite que los dispositivos intercambien datos y se comuniquen de forma segura a pequeña escala. Una red de área extendida (WAN) se extiende más allá de un edificio o de un gran recinto para incluir múltiples ubicaciones repartidas a lo largo de una zona geográfica concreta, o incluso del mundo. Las organizaciones utilizan las WAN para facilitar las interacciones digitales y el intercambio de datos entre empleados y clientes en diferentes regiones o países. (AWS., s.f.)

Las LAN y las WAN son redes de computación compuestas de nodos y enlaces. Necesitan dos o más nodos para crear una red de computación. (AWS., s.f.)

Un nodo de red puede ser un equipo de comunicación de datos (DCE) o un equipo terminal de datos (DTE). El DCE incluye elementos como módems, concentradores o conmutadores, mientras que el DTE puede incluir dos o más computadoras e impresoras. (AWS., s.f.)

Un enlace es el medio de transmisión que conecta dos nodos. Las conexiones cableadas utilizan cables Ethernet fabricados con tecnología coaxial, de fibra óptica o de par trenzado. Por otro lado, las conexiones inalámbricas utilizan ondas de radio, como la tecnología 3G, 4G o 5G, para conectar nodos. (AWS., s.f.)

2.9.1 Transmisión de datos

Tanto las LAN como las WAN utilizan dispositivos de red DCE. Estos dispositivos ayudan a las redes a dirigir el tráfico y entregan los datos a los destinos correctos. (AWS., s.f.)

Además, tanto las LAN como las WAN utilizan conjuntos de reglas denominados protocolos de comunicación para administrar la transmisión de datos entre los dispositivos conectados. El protocolo más común es TCP/IP. También hay otros protocolos para diferentes tipos de comunicación, como el Protocolo de datagramas de usuario (UDP) y el Protocolo de mensajes de control de Internet (ICMP). (AWS., s.f.)

2.9.2 Seguridad

Puede proteger tanto las LAN como las WAN mediante diversos métodos, como firewalls, cifrado y control de acceso. Las medidas de seguridad evitan el acceso no autorizado a la red y protegen los datos confidenciales durante la transmisión. Si implementa medidas de seguridad sólidas, tanto las WAN como las LAN pueden proporcionar un entorno seguro para que los usuarios se comuniquen y compartan datos. (AWS., s.f.)

2.10 CENTROS DE PROCESAMIENTO DE DATOS.

Todas las empresas que tengan relación con la informática habrán oído hablar de los CPD o Centros de Proceso de Datos (también se les conoce como Data Center, o incluso Centros de Informática). (Rubio, 2016)

Un centro de datos se puede definir como la ubicación donde se encuentran los equipos informáticos necesarios para el procesamiento de la información de una empresa. Su tamaño puede variar de pequeñas salas a conjuntos de edificios. Los más habituales suelen ocupar grandes salas o un edificio entero. (Rubio, 2016)

En ellos se ubican grandes cantidades de componentes electrónicos que hacen posible el almacenamiento y proceso de la información. Es por esto que hay que tener un especial cuidado con estas instalaciones. Se construyen con el objetivo de garantizar la continuidad de servicio, o para gestionar informaciones críticas. Por ejemplo, todos los bancos cuentan con Centros de Proceso de Datos, manejan informaciones confidenciales y la seguridad es una prioridad. (Rubio, 2016)

Son elementos muy delicados que requieren de seguridad y mantenimiento. En todos los casos deben cumplir con unos aspectos básico. (Rubio, 2016)

2.10.1 Auditoría Técnica.

Consiste en un estudio exhaustivo y pormenorizado de todos los elementos del CPD y de su estado. Se requiere la realización de informes que aporten la suficiente confianza y disponibilidad. Como hemos dicho antes, esto nos permitirá la continuidad y calidad de los servicios. (Rubio, 2016)

2.10.2 Limpieza Técnica.

La limpieza es un aspecto fundamental, y debido a esto, la normativa vigente recomienda, al menos, una medición de suciedad y partículas al año. Los datos obtenidos juzgarán si es necesario o no una limpieza técnica. Este tipo de limpieza ha de hacerse por personal especializado. Si no se realiza de esta manera se corre el riesgo de contaminar la sala y no habrá servido de nada. (Rubio, 2016)

La acumulación de suciedad dentro de las salas puede llevar al sobrecalentamiento de los equipos y al mal funcionamiento de los mismos, incluso a la obstrucción de los filtros y a dificultar el flujo de aire. (Rubio, 2016)

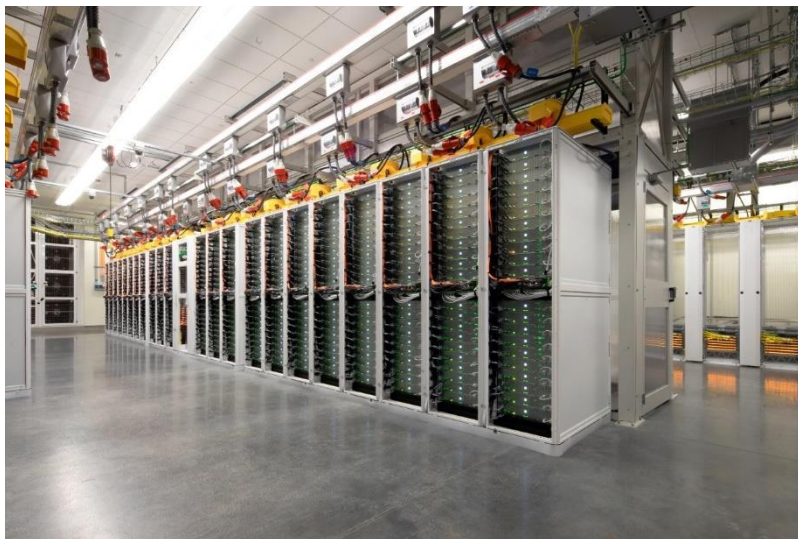
2.10.3 Mantenimiento.

Como todas las instalaciones delicadas de una empresa, uno de los servicios más importantes que hay que tener en cuenta es el mantenimiento. El correcto funcionamiento de la infraestructura, así como el constante cuidado y optimización evitará posibles fallos o desastres. Cuando se trata de información crítica, la prevención es prioritaria. (Rubio, 2016)

2.10.4 Instalaciones Anti vibraciones.

Todos los componentes electrónicos sufren enormemente con las vibraciones y empeoran su rendimiento. Pero no solo las debidas a terremotos o sismos. Una obra cercana, las vías del tren, una autovía o los mismos equipos de refrigeración, pueden perjudicar al sistema. Para evitar estos problemas debemos contar con una de las múltiples soluciones anti vibraciones que existen en el mercado. (Rubio, 2016)

Figura. 6 Centros de datos



FUENTE: <https://www.forbes.com.mx/crean-una-asociacion-de-data-centers-para-potenciar-el-mercado-mexicano/>

CAPÍTULO III DESARROLLO

3.1 INTRODUCCION AL CAPITULO.

A continuación, se describe el contenido del proyecto partiendo de la infraestructura de hardware que se utilizó para el diseño de la arquitectura de los 3 centros de datos, la configuración básica, el diseño de la topología de red de área local, el diseño de la topología de red área amplia, direccionamiento ip utilizado en la configuración, contextos virtuales de los dispositivos, el diseño de capa 2, la configuración de la capa de routing y por ultimo políticas de seguridad para controlar los flujos de red.

3.2 HARDWARE PARA LA IMPLEMENTACION.

3.2.1 Cisco Nexus 7K.

Por sus características y funcionalidad el hardware que se utilizó para esta implementación son equipos cisco Nexus 7K que fueron desarrollados para soportar grandes cargas de informacion de un Centro de Procesamiento de Datos.

Como se muestra en la figura 7. Dos equipos cisco Nexus 7K uno redundante del otro serán usados para interconectar cada centro de datos con el resto de regiones, cada chasis tendrá el siguiente equipamiento:

Figura. 7 Nexus 7k configuracion.



FUENTE: <https://www.cisco.com/c/en/us/products/switches/nexus-7700-6-slot-switch/index.html#>

1. 2 x Tarjetas supervisoras modelo N77-SUP2E.

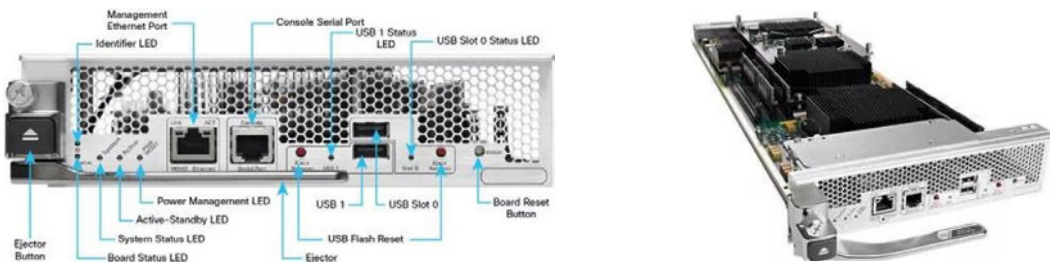
Este modulo esta diseñado para ofrecer funciones de gestión y plano de control, Las supervisoras controlan los servicios de capa 2 y capa 3, las capacidades de redundancia, la gestión de la configuración, el monitoreo del estado del hardware, la gestión ambiental y de energía.

Algunas características de estos sistemas son:

- Operación continua del sistema.
- Funciones de virtualización.
- Eficiencia operativa.

En la figura 8 se muestra la imagen de las tarjetas supervisoras

Figura. 8 N77-SUP2E.



FUENTE: https://www.cisco.com/c/dam/en/us/products/collateral/switches/nexus-7000-series-switches/data_sheet_c78-728591.doc/_jcr_content/renditions/data_sheet_c78-728591_0.jpg

2. 2 x line cards modelo N77-F324FQ-25.

Estos módulos ofrecen flexibilidad de funciones y rendimiento de velocidad en cada puerto, Estos módulos permiten la implementación de una arquitectura de centros de datos escalable, de alta densidad y baja latencia. Con estos módulos la plataforma cisco Nexus 7K ofrece hasta 384 puertos de 40gb de velocidad.

En la figura 9 se muestra la imagen de las tarjetas de puertos de fibra óptica.

Figura. 9 N77- F324FQ-25



FUENTE: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/data_sheet_c78-728410.html

3. 4 fuentes de poder N77-AC-3KW.

Las fuentes de poder son totalmente intercambiables en caliente lo que ayuda a garantizar que no se interrumpa el sistema durante la instalación, la salida máxima para estas fuentes de alimentación de CA de 3KW es de 1400 o 3000 W, estas fuentes de poder ofrecen tolerancia a fallas, alta eficiencia y carga compartida.

En la figura 10 se muestra la imagen de las fuentes de poder.

Figura. 10 N77-AC-3KW.



FUENTE: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/data_sheet_c78-729141.html

3.2.2 Módulos de fábrica.

Cada chasis deberá tener instalados 6 fabric modules modelo N77-C7706-FAB-2.

Los routers Nexus 7k cada fabric module proporciona 220 gbs de ancho de banda dedicado a cada una de las line cards, por lo tanto 1.3 Tb de ancho de banda estará disponible para cada linecard instalada.

En la figura 11 se muestra la imagen representativa de un módulo de fabrica.

Figura. 11 N77-C7706-FAB-2.



FUENTE: https://www.cisco.com/c/dam/en/us/products/collateral/switches/nexus-7000-series-switches/data_sheet_c78-728596.doc/_jcr_content/renditions/data_sheet_c78-728596_0.jpg

3.2.3 Redundancia de fuentes de poder.

4 x fuentes de poder serán instaladas en cada router el modo de redundancia que utilizaremos será redundant mode.

Tabla 1 Detalles de las fuentes de poder.

Modelo	Porcentaje de voltaje usado	Total de voltaje de PSU	Total de voltaje usado	Voltaje total Actual Restante
N77-AC-3KW modo redundante	30%	240	70	50

FUENTE: (Imagen creada por el autor)

Los consumos de las fuentes de poder que se muestran en la tabla 2 se consideraron usando la máxima capacidad de puertos de las line cards, los consumos podrían variar dependiendo del uso de las tarjetas line cards.

Tabla 2 Requerimientos de voltaje por router.

Slot	Line Card	Voltaje actual (A)	Capacidad de Voltaje (W)	Uso normal de voltaje (W)
SYSTEM-FAN	N77-C7706-FAN	6	300	40
SYSTEM-FAN	N77-C7706-FAN	6	300	40
SYSTEM-FAN	N77-C7706-FAN	6	300	40
FABRIC MODULE	N77-C7706-FAB-2	2	80	0
FABRIC MODULE	N77-C7706-FAB-2	2	80	0
FABRIC MODULE	N77-C7706-FAB-2	2	80	0
FABRIC MODULE	N77-C7706-FAB-2	2	80	0
FABRIC MODULE	N77-C7706-FAB-2	2	80	0
FABRIC MODULE	N77-C7706-FAB-2	2	80	0
1	N77-F324FQ-25	15	740	640
2	N77-F324FQ-25	15	740	640
3	N77-SUP2E	5.5	265	137
4	N77-SUP2E	5.5	265	137
5	SLOT VACIO	0	0	0
6	SLOT VACIO	0	0	0
	Total	71	3390	1674

FUENTE: (Imagen creada por el autor).

Abajo en la figura 12 se muestra la configuración aplicada para la redundancia de las fuentes de poder.

Figura. 12 Comando para configurar fuentes de poder.

```
Switch#(config)power redundancy-mode redundant
```

FUENTE: (Imagen creada por el autor)

Con el comando “Show environment power” validamos el tipo de redundancia configurado en las fuentes de poder, como se muestra en la figura 13.

Figura. 13 Comando “show enviroment power”.

```
switch# show environment power

Power Usage Summary:
-----
Power Supply redundancy mode (configured)      Redundant
Power Supply redundancy mode (operational)     Redundant
```

FUENTE: (Imagen creada por el autor)

3.2.4 Transceptores Ópticos.

Para esta implementación usaremos Cisco QSFP BiDi Transceivers (QSFP-40G-SR-BD=), los cuales se muestran en la figura 8.

Figura. 14 QSFP-40G-SR-BD.



FUENTE: https://www.cisco.com/c/dam/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-660083.docx/_jcr_content/renditions/data_sheet_c78-660083_0.png

Como se menciona en la página web de cisco, el transceptor bidireccional (BiDi) Cisco QSFP de 40 Gbps (Figura 1) es un transceptor óptico conectable con una interfaz de conector LC dúplex para comunicación de datos de corto alcance y aplicaciones de interconexión mediante fibra multimodo (MMF). El transceptor BiDi Cisco QSFP de 40 Gbps ofrece a los clientes una solución atractiva que permite la reutilización de su infraestructura MMF dúplex de 10 gigabits existente para la migración a conectividad Ethernet de 40 Gigabits. (Cisco 40GBASE QSFP Modules Data Sheet, 2022)

Tabla 3 Características de QSFP-40G-SR-BD

Producto	Tipo	Conector Tipo
QSFP-40G-SR-BD	40GBASE-SR-BiDi, duplex MMF	LC

FUENTE: (Imagen creada por el autor)

3.2.5 Versión de software.

El sistema operativo de que se utilizó es la versión 7.3 ya que cumple con las funcionalidades necesarias para esta implementación.

Tabla 4 Version de software para equipos Nexus 7K

Plataforma	Versión software
Nexus 7k	7.3

FUENTE: (Imagen creada por el autor)

Esta versión del software soporta funcionalidades de routing, switching y storage que cumplen las necesidades de un Data center, es capaz de soportar configuración en formato XML y a través de CLI (Command-line) interface similar a la versión de software de cisco IOS. (Cisco, 2022)

3.3 CONFIGURACION BASICA DE EQUIPO ROUTER CISCO NEXUS 7K.

A continuación, se describe la configuración básica aplicada a los equipos Nexus 7K, esta es la configuración necesaria para comenzar con la administración remota por SSH y por cable de consola a los equipos, para la configuración es necesario contar con un software de terminal como putty, secure crt, Moba Xterm etc. y un cable de consola para conectarnos directamente a cada router.

3.3.1 Configuración del nombre del equipo (hostname).

Lo primero que se requiere antes de iniciar con las configuraciones más complejas, será establecer una configuración básica en los equipos para dar seguridad y facilitar la administración de los equipos routers Nexus 7K.

En la figura 15 se muestran los comandos necesarios para configurar el hostname.

Figura. 15 Configuración hostname.

```
Switch# configure terminal
Switch(config)#
Switch(config)# hostname DCS1
Switch(config)# switchname DCS1
DCS1(config)# exit
DCS1# copy running-config startup-config
```

FUENTE: (Imagen creada por el autor)

1. En la primera línea se muestra el comando para ingresar al modo de configuración global.
2. En la segunda línea se puede observar que pasamos del modo privilegiado señalado con el símbolo “#” al modo de configuración global
3. En la tercera línea se muestra el comando para configurar el hostname del equipo
4. En la cuarta línea se muestra que opcionalmente se puede utilizar el comando switchname en lugar de hostname para configurar el nombre del equipo, cualquiera de los 2 comandos tiene la misma funcionalidad.
5. En la quinta línea con el comando exit salimos del modo de configuración global para pasar al modo privilegiado
6. En la sexta línea se muestra el comando para guardar los cambios realizados en el equipo.

3.3.2 Deshabilitar la traducción de nombres de dominio.

Este comando es muy útil al configurar un equipo cisco, su función es deshabilitar la traducción de nombres de dominio, cuando se ingresa un comando erróneamente al router el sistema operativo no lo reconoce y supone que se ingresó el nombre de algún dominio e intenta realizar la traducción. Esto desde luego retrasa el proceso

para corregir el comando y se tiene que tomar un lapso de tiempo para seguir configurando.

En la figura 16 se muestra la configuración del comando para deshabilitar esta traducción.

Figura. 16 Deshabilitar traduccion de nombres

```
DCS1# configure terminal
DCS1(config)# no ip domain-lookup
DCS1(config)# exit
DCS1(config)# copy running-config startup-config
```

FUENTE: (Imagen creada por el autor)

3.3.3 Mensaje de aviso contra intrusos.

Resulta importante configurar un mensaje en el router para informar a cualquier usuario que ingrese al sistema sin autorización, que solo personal autorizado puede entrar al router.

En la figura 17 se muestra el comando para realizar la configuración del mensaje de aviso, este está limitado solamente a 254 caracteres por línea y un máximo de 40 líneas permitidas.

Figura. 17 Mensaje de aviso contra intrusos.

```
DCS1# configure terminal
DCS1(config)# banner motd "ACCESO RESTRINGIDO SOLO PERSONAL AUTORIZADO"
DCS1(config)# exit
DCS1(config)# copy running-config startup-config
```

FUENTE: (Imagen creada por el autor)

3.3.4 Usuario local y contraseña.

En el modo de configuración global se puede crear un nombre de usuario y una contraseña las cuales agregan seguridad al equipo al momento de ingresar por consola o vía remota por SSH o Telnet

En la figura 18 se muestra el comando utilizado para la configuración de usuario y contraseña encriptada con el rol de administrador.

Figura. 18 Configuración usuario local y contraseñas.

```
DCS1# configure terminal
DCS1(config)# password strength-check
DCS1(config)# username admin password 5 djLDwfiojff role admin
DCS1(config)# exit
DCS1(config)# copy running-config startup-config
```

FUENTE: (Imagen creada por el autor)

Con el comando “password strength-check” se puede habilitar la verificación de la seguridad de la contraseña, lo que impide crear contraseñas débiles para las cuentas de usuario.

3.3.5 Protección del acceso a modo EXEC privilegiado

A continuación, se muestra la configuración para habilitar la contraseña secreta de enable, la cual es una contraseña que limita el acceso al modo privilegiado, el comando enable secret proporciona seguridad, dado que la contraseña es encriptada después de ejecutar el comando

La figura 19 muestra la configuración necesaria

Figura. 19 Proteccion del acceso a modo exec privilegiado.

```
DCS1# configure terminal
DCS1(config)# enable secret class
DCS1(config)# exit
```

```
DCS1(config)# copy running-config startup-config
```

FUENTE: (Imagen creada por el autor)

3.3.6 Protección del acceso a modo EXEC usuario.

El puerto de consola del equipo de red debe estar asegurado para evitar que cualquier persona que ingrese a la sala de datos y se conecte al equipo pueda acceder a la configuración, con una contraseña segura, se reducen las posibilidades de un ataque.

La figura 20 muestra la configuración necesaria

Figura. 20 Proteccion del acceso a modo exec usuario.

```
DCS1# configure terminal
DCS1(config)# line console 0
DCS1(config)# login local
DCS1(config)# logging synchronous
DCS1(config)# exit
```

FUENTE: (Imagen creada por el autor)

3.3.7 Contraseñas VTY.

Las líneas virtuales VTY permiten el acceso a un dispositivo cisco a través de telnet o SSH de manera predeterminada los routers y switches permiten hasta 16 accesos vía remota a la vez, Es necesario proteger el acceso remoto a cada equipo por seguridad.

En la figura 21 se muestra la configuración necesaria

Figura. 21 Configuracion contraseña VTY.

```
DCS1# configure terminal
DCS1(config)# line vty 0 15
```

```
DCS1(config)# login local
DCS1(config)# transport input ssh
DCS1(config)# exit
```

FUENTE: (Imagen creada por el autor)

3.3.8 Contraseñas encriptadas.

Otra configuración de utilidad que sirve para encriptar todas las contraseñas que aparecen en texto plano cuando se visualizan los archivos de configuración. La figura 22 muestra la configuración necesaria.

Figura. 22 Configuración contraseñas encriptadas.

```
DCS1# configure terminal
DCS1(config)# service password-encryption
DCS1(config)# exit
DCS1# copy running-config startup-config
```

FUENTE: (Imagen creada por el autor)

El comando “service password-ecryption” encripta las contraseñas cuando estas se configuran en el equipo de red, este aplica una configuración mínima, ya que solo se ve reflejado en el archivo de configuración y no cuando se envía a través de los medios a otros dispositivos, el propósito de esta configuración es evitar que los usuarios no autorizados vean las contraseñas en el archivo de configuración.

3.3.9 Configuración manual de reloj en el dispositivo.

Es importante sincronizar el dispositivo de red con el horario de la región en la cual está operando el router, esto con la finalidad de que en caso de un evento que genere un log se tenga la hora exacta en la cual ocurrió, la figura 23 muestra la configuración necesaria.

Figura. 23 Configuración manual de reloj en router.

```
DCS1# configure terminal
DCS1(config)# clock time zone EST -5 0
DCS1(config)# clock summer-time PDT
```

```
DCS1(config)# clock set 15:00:00 30 June 2023
DCS1(config)# exit
DCS1# copy running-config startup-config
```

FUENTE: (Imagen creada por el autor)

3.3.10 Configuración de Autenticación por Tacacs+.

El protocolo de seguridad Tacacs+ provee autenticación centralizada de usuarios para acceder a un dispositivo con sistema operativo NX-OS, para realizar esta configuración será necesario que el router tenga comunicación con los servidores Tacacs+, El protocolo Tacacs utiliza el puerto TCP 49. A continuación en la figura 24 se muestra la configuración de tacacs+:

Figura. 24 Configuración de autenticación por tacacs+.

```
DCS1# configure terminal
DCS1(config)# feature tacacs+
DCS1(config)# tacacs-server key 7 cisco123
DCS1(config)# ip tacacs source-interface mgmt0
DCS1(config)# tacacs-server deadtime 30
DCS1(config)# tacacs-server host 1.5.3.4
DCS1(config)# tacacs-server host 1.5.3.2
DCS1(config)# aaa group server tacacs+ tacacs+
DCS1(config)# server 1.5.3.4
DCS1(config)# server 1.5.3.2
DCS1(config)# use-vrf management
DCS1(config)# source-interface mgmt0
DCS1(config)# aaa authentication login default group tacacs+
DCS1(config)# aaa authentication login console group tacacs+
DCS1(config)# aaa authorization config-commands default group tacacs+ local
DCS1(config)# aaa authorization commands default group tacacs+ local
DCS1(config)# aaa accounting default group tacacs+
```

```
DCS1(config)# aaa authentication login error-enable
DCS1(config)# tacacs-server directed-request
DCS1# copy running-config startup-config
```

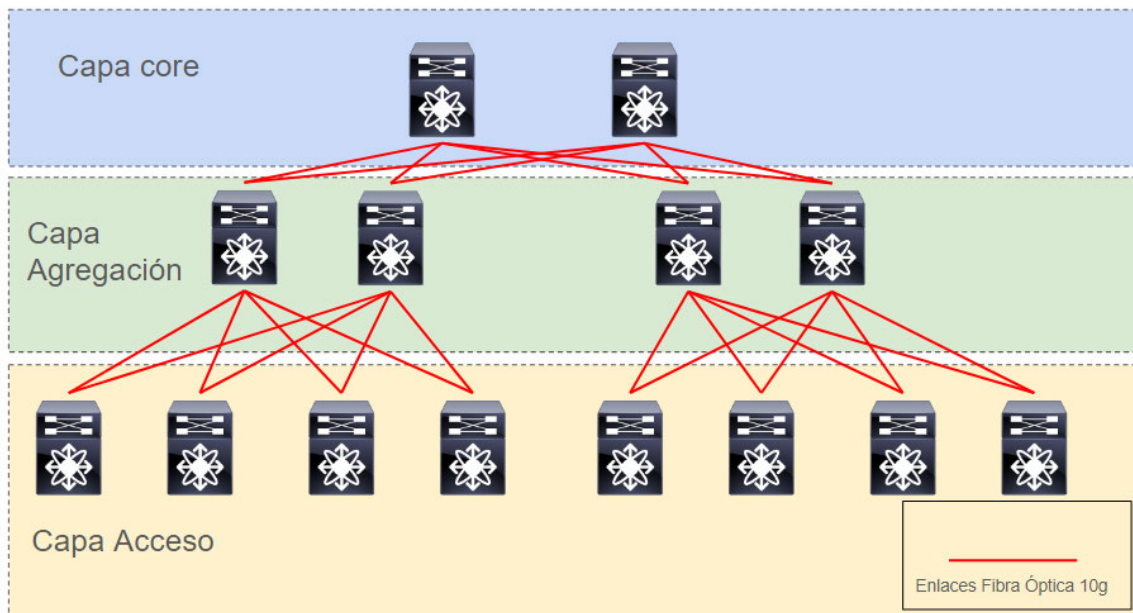
FUENTE: (Imagen creada por el autor)

El servicio de seguridad AAA te permite verificar la identidad, otorgar acceso y realizar un seguimiento de las acciones que realizan los usuarios que administran un router con sistema operativo NX-OS.

3.4 DISEÑO TOPOLOGIA RED DE AREA LOCAL.

Como se muestra en la figura 25. “Topología LAN” la arquitectura y diseño LAN de los centros de datos, es un modelo de 3 capas conocido como modelo Jerárquico, comenzando con la capa Core, capa de agregación y capa de acceso. A continuación, se detalla la funcionalidad de cada capa dentro de la red del centro de datos de la compañía.

Figura. 25 Topología LAN

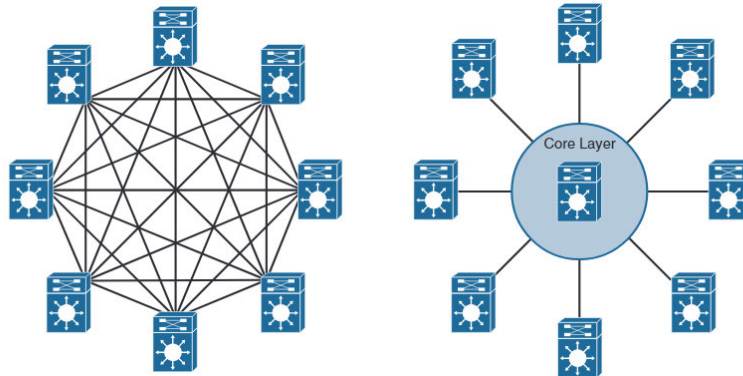


FUENTE: (Imagen creada por el autor)

3.4.1 Capa Core.

Esta capa se encarga de interconectar la red LAN de un sitio con otros sitios separados geográficamente, Los routers son capaces de transportar los datos de la red a velocidades muy altas.

Figura. 26 Capa Core

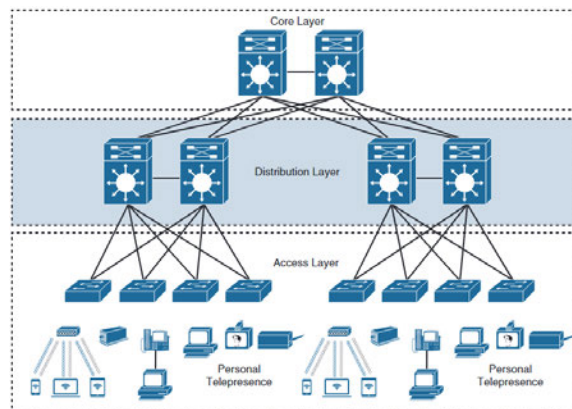


FUENTE: (Brad Edgeworth, 2020)

3.4.2 Capa Agregación.

En esta capa se define la configuración del InterVLAN routing para interconectar los diferentes segmentos de red, en esta capa también se definen políticas de seguridad y filtrado de redes como listas de control de acceso.

Figura. 27 Capa distribution

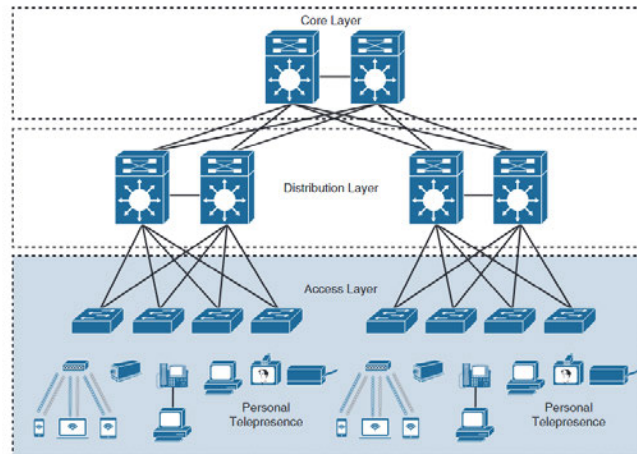


FUENTE: (Brad Edgeworth, 2020)

3.4.3 Capa Acceso.

En esta capa conectan todos los dispositivos finales como servidores, estaciones de trabajo, impresoras, Los switches de la capa de acceso garantizan que los datos se entreguen a los dispositivos finales.

Figura. 28 Capa Acceso

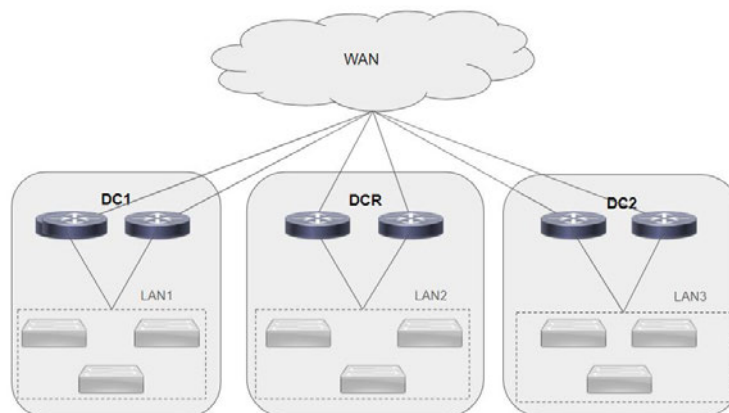


FUENTE: (Brad Edgeworth, 2020)

3.5 DISEÑO DE TOPOLOGIA RED DE AREA AMPLIA.

La figura numero 29 describe el diseño a alto nivel de la interconexión de los 3 centros de datos DC1 , DC2, DCR.

Figura. 29 Topologia WAN



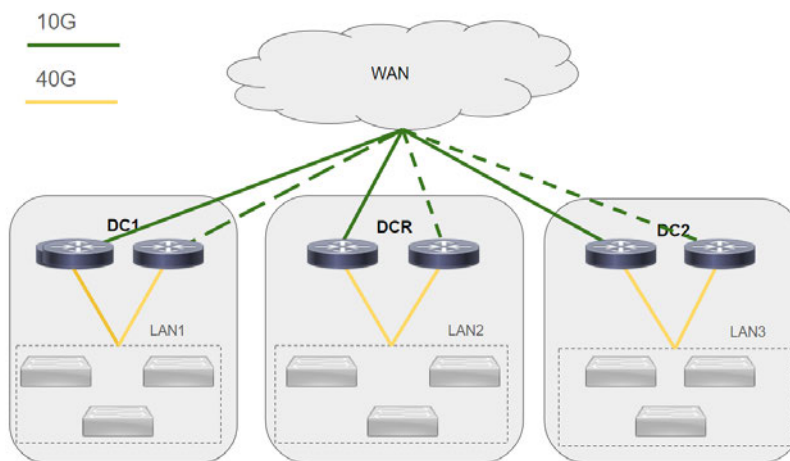
FUENTE: (Imagen creada por el autor)

En esta figura podemos observar que la distribución de la infraestructura es redundante en cada uno de los centros de datos, la redundancia eliminará un único punto de fallo en caso de un desastre, lo cual nos permitirá seguir otorgando el servicio de red entre las diferentes regiones de la compañía.

3.5.1 Topología física.

La figura 30 muestra el detalle de la topología física donde se detalla las velocidades de las interconexiones de fibra óptica en cada uno de los centros de datos:

Figura. 30 Topologia Fisica



FUENTE: (Imagen creada por el autor)

Características de la topología:

1. Todos los enlaces conectados entre los routers Nexus 7K serán a 10 gbs.
2. Todos los enlaces serán de capa 3 punto a punto (no subinterfaces, no SVI).
3. Existen 2 triángulos: uno entre DCR S1, DC1 S1 y DC2 S1, el segundo entre DCR S2, DC1 S2 y DC2 S2.
4. Las conexiones físicas de fibra óptica hacia las redes LAN en cada data center serán a 40G

En la tabla 5 se muestra el detalle de las conexiones WAN a 40G con su respectivo número de interfaz.

Tabla 5. Matriz de cableado

Equipo Origen	Puerto origen	Equipo Destino	Puerto destino	Tipo
SWTICH1_DC1S1	5/5	SWITCH1_DCRS1	5/5	40G
SWTICH1_DC1S1	3/5	SWITCH1_DC2S1	3/5	40G
SWITCH1_DCRS1	2/5	SWITCH1_DC2S1	2/5	40G
SWITCH2_DC1S2	5/5	SWITCH2_DCRS2	5/5	40G
SWITCH2_DC1S2	3/5	SWITCH2_DC2S2	2/12	40G
SWITCH2_DCRS2	2/5	SWITCH2_DC2S2	2/5	40G

FUENTE: (Imagen creada por el autor)

A continuación, en la figura 31 se muestra una representación de la distribución física de los equipos en Rack en cada uno de los centros de datos

Figura. 31 Equipos montados en Rack.



FUENTE: (Imagen creada por el autor)

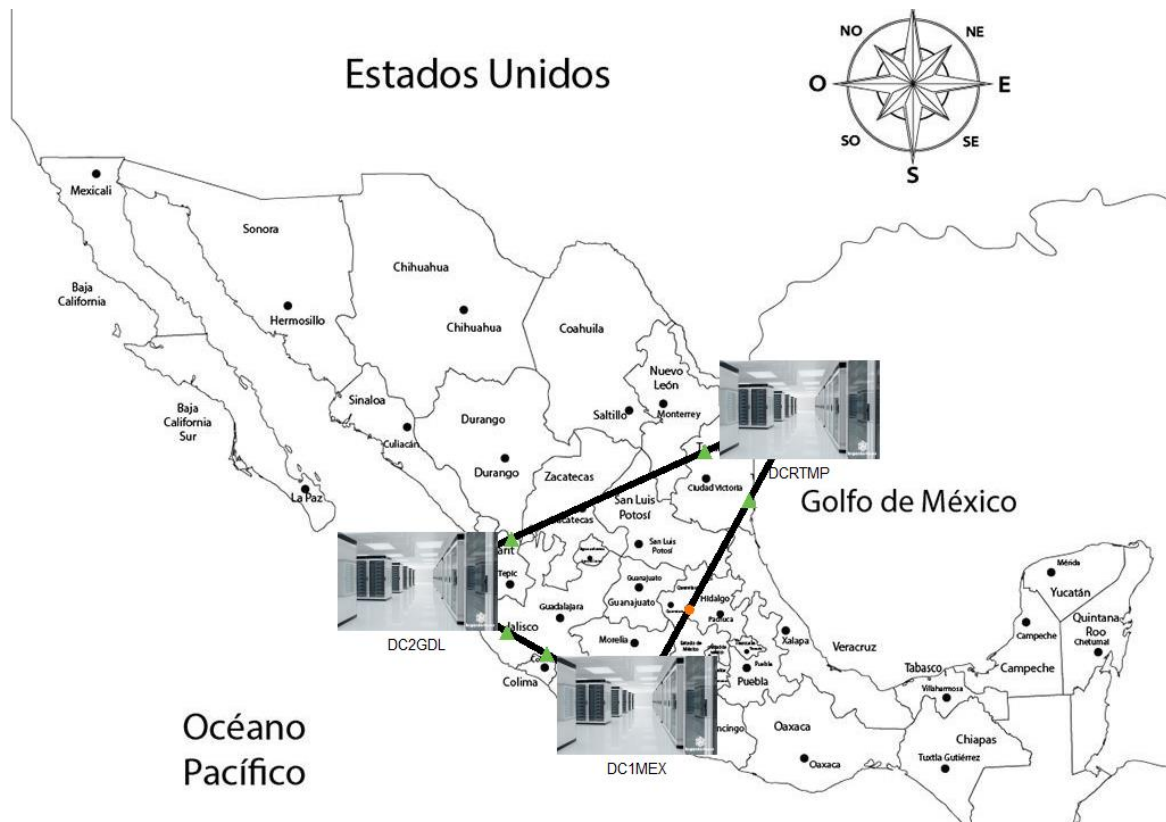
1. En el Rack 1 y 2 se encuentran instalados los equipos DCS 1 Y 2, los cuales son los encargados de interconectar con los otros centros de datos.
2. En el rack 3 se encuentran los equipos Core que pertenecen a la red LAN en cada centro de datos.

3. En el rack 4 se encuentran los equipos de agregación pertenecientes a la red LAN
4. En el rack 5 se encuentran los equipos de Acceso, encargados de dar conectividad a la red a los usuarios en cada región.

3.5.2 Distribución geográfica.

A continuación, en la figura 32 se muestra la representación de la distribución geográfica de cada centro de datos y la como están interconectados entre sí.

Figura. 32 Distribucion geografica de data centers



FUENTE: (Imagen creada por el autor)

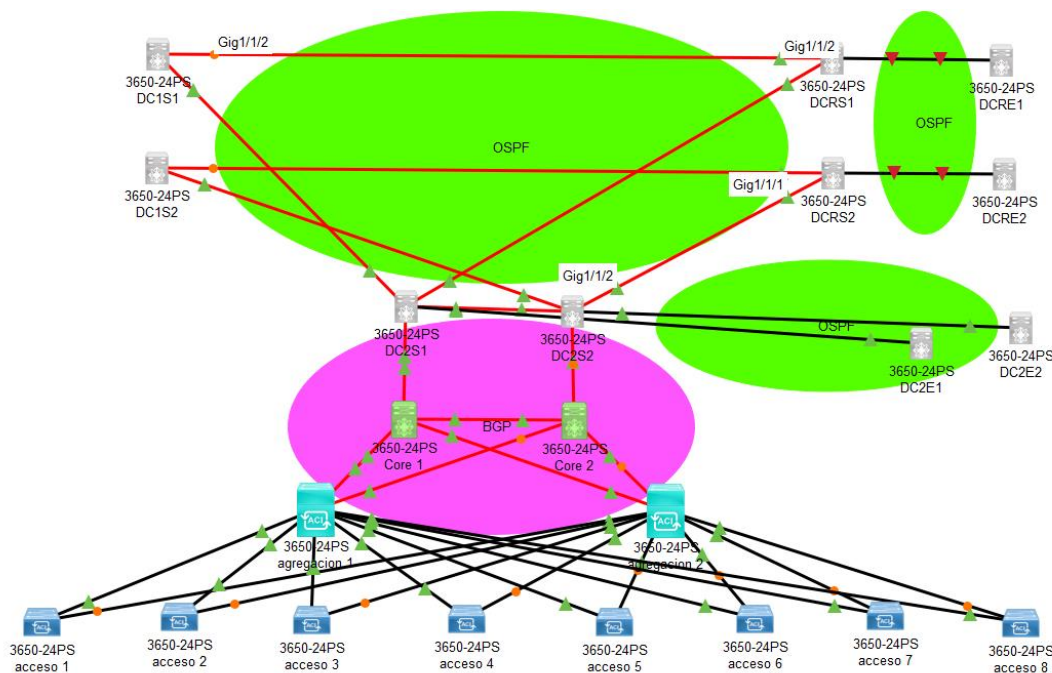
1. En la región del pacifico de encuentra el centro de datos 2 GDL, encargado de brindar servicio a Baja californiasur, baja californias, Hermosillo, chihuahua, Durango.

2. En la región del centro del país se encuentra el centro de datos 1 MEX encargado de soportar las cargas de trabajo de usuarios de la zona centro, sur y norte del país.
3. En la región del golfo se encuentra el centro de datos R TAMP, la función de este centro de datos es fungir como un desastre recovery es decir que en caso de que el centro de datos 1 o 2 por alguna razón dejen de funcionar, el centro de datos R deberá ser capaz de soportar las cargas de trabajo de usuarios de todo el país quien lo requiera.

3.5.3 Topología lógica.

A continuación, en la figura 33 se muestra una representación del diseño lógico de la topología WAN y su interconexión con las nubes públicas y las redes LAN en cada centro de datos.

Figura. 33 Topologia logica.



FUENTE: (Imagen creada por el autor)

1. El diseño lógico muestra la arquitectura y la configuración de los dispositivos cisco Nexus 7K

2. Los protocolos de ruteo dinámico OSPF para la interconexión WAN y BGP para el intercambio de rutas en las redes LAN.
3. La interconexión física entre dispositivos para las redes WAN y para redes LAN.

3.5.4 Características de la implementación.

A continuación, se describen los puntos más importantes para la implementación:

1. Cada DC deberá tener un par de Nexus 7K identificados por 1 y 2
2. Los routers cisco Nexus 7K conectaran la red LAN en cada centro de datos
3. Cada router cisco Nexus 7K conectara con los otros routers con el mismo número identificador (routers 1 conectaran con routers 1 y mismos casos con los routers 2).
4. El protocolo de ruteo usado para formar la WAN será OSPF en el área 0.
5. El protocolo BGP será utilizado entre los routers cisco Nexus 7K y las redes LAN en cada centro de datos.
6. El protocolo ULD será configurado entre los equipos routers cisco Nexus 7K 1 de cada centro de datos
7. El protocolo BFD será configurado entre los equipos routers cisco Nexus 7K 2 en cada centro de datos.
8. La recuperación de falla de enlace en el DWDM será 50 ms. Con la finalidad de que en caso de un fallo en los enlaces se conmute el tráfico lo antes posible.
9. Cada router tendrá un VDC de admin y de datos
10. El temporizador link debounce será fijado a su valor por default 100 ms in NX-OS.
11. Configuración de Jumbo Frames en los equipos routers cisco Nexus 7K.
12. Los protocolos CDP/LLDP serán habilitados.

3.6 DIRECCIONAMIENTO IP.

Cada Router switch tendrá una loopback interface la cual funcionará como router ID de cada equipo a continuación se muestra en la tabla 6:

Tabla 6 Direccionamiento Ip Loopback

Hostname	Loopback
SWTICH1_DC1	1.1.1.1/32
SWITCH2_DC1	2.2.2.2/32
SWITCH1_DC2	7.7.7.7/32
SWITCH2_DC2	8.8.8.8/32
SWITCH1_DCR	3.3.3.3/32
SWITCH2_DCR	4.4.4.4/32

FUENTE: (Imagen creada por el autor)

La administración de los equipos cisco Nexus 7K será a través de un de un equipo fuera de banda esto quiere decir que está aislado de la red interna con la finalidad de asegurar el acceso por CLI a los routers en caso de un problema severo, en la tabla número 7 se muestra el direccionamiento IP configurado en cada equipo para administración:

Tabla 7 Direccionamiento IP fuera de banda

Hostname vdc admin	mgmt	Mascara	Gateway
SWTICH1_ADM_DC1	192.168.1.11	/24	192.168.1.1
SWITCH2_ADM_DC1	192.168.1.12	/24	192.168.1.1
SWITCH1_ADM_DC2	192.168.2.11	/24	192.168.2.1
SWITCH2_ADM_DC2	192.168.2.12	/24	192.168.2.1
SWITCH1_ADM_DCR	192.168.3.11	/24	192.168.3.1
SWITCH2_ADM_DCR	192.168.3.12	/24	192.168.3.1

FUENTE: (Imagen creada por el autor)

El direccionamiento Ip que se usara para cada enlace punto a punto en la red WAN entre los equipos cisco Nexus 7K se muestra en la tabla 8 a continuación:

Tabla 8 Redes punto a punto entre enlaces WAN

switch origen	swtich destino	Ip Network	Mascara
SWTICH1_DC1	SWITCH1_DCR	192.168.5.0	/30
SWTICH1_DC1	SWITCH1_DC2	192.168.5.4	/30
SWITCH1_DCR	SWITCH1_DC2	192.168.5.8	/30
SWITCH2_DC1	SWITCH2_DCR	192.168.5.12	/30
SWITCH2_DC1	SWITCH2_DC2	192.168.5.16	/30
SWITCH2_DCR	SWITCH2_DC2	192.168.5.16	/30

FUENTE: (Imagen creada por el autor)

La asignación ip para cada rango deberá seguir la siguiente regla:

1. La primera dirección ip será asignada al uplink router 1 en cada data center
2. En el caso del enlace back to back, la primera dirección ip será asignada al router 1 en cada datacenter.

3.7 CONTEXTO VIRTUAL DEL DISPOSITIVO.

Los VDC son usados para particionar un router físico en “N” numero de dispositivos lógicos, Un VDC virtualiza el plano de control y el plano de datos dentro del switch, por lo tanto, cada vdc deberá ser tratado como un equipo físico independiente.

Para esta implementación serán creados un total de 2 VDC para cada swtich físico, el vdc 1 sera configurado con el role de activo mientras que el resto solo serán preconfigurados en caso de requerir su utilización en un futuro.

Adicionalmente el VDC de admin será usado para propósitos de administración. Ninguna interfaz de ninguna tarjeta de puertos puede ser asignado al vdc de admin, solamente la interfaz de mgmt puede ser asociada al vdc admin lo cual significa que solamente la administración fuera de banda es posible a través de la interface mgmt.

Ninguna feature puede ser habilitada en el admin VDC, el admini VDC deberá proveer solo administración permitiendo las siguientes tareas solamente:

1. Configuración CoPP
2. ISSU

3. Creación, suspensión y borrado de VDC
4. Mostrar tech-support, tac-pac, debugs
5. Balanceo de carga de port-channel
6. Administracion de licencias
7. Control de modulos (apagado y fuera de servicio)

3.7.1 Recursos para cada contexto virtual del dispositivo.

La configuración de recursos en cada vdc es usada para controlar los limites mínimos y máximos de recursos físicos por cada partición virtual, la tabla 9 muestra los recursos asignados a cada vdc por default.

Tabla 9 Limite de recursos por cada VDC

Recurso	Mínimo	Máximo
Ipv4 multicast route memory	8	8
Ipv6 multicast route memory	2	2
Ipv4 unicast route memory	8	8
Ipv6 unicast route memory	4	4
Port channels	0	768
SPAN sessions	0	2
ERSPAN sessions	0	23
VLANs	16	4094
VRFs	2	4096

FUENTE: (Imagen creada por el autor)

En la figura 34 se muestra la salida del comando “**show routing memory estimate**” en el equipo cisco Nexus 7K la cual indica que un vdc usando los recursos por default podría soportar aproximadamente 11000 rutas.

Figura. 34 Comando “”Show routing memory””.

```
Switch # show routing memory estimate route 12000 next-hops 8

Shared memory estimates:

Current max 8 MB; 6526 routes with 16 nhs
```

```
in-use 1 MB; 97 routes with 1 nhs (average)

Configured max 8 MB; 6526 routes with 16 nhs

Estimate 8 MB; 11000 routes with 8 nhs
```

FUENTE: (Imagen creada por el autor)

el comando show routing memory muestra los recursos de memoria asignados para las rutas, el rango de numero de rutas va de las 1000 a las 112000.

Por esta razón, en los equipos cisco Nexus 7k se usará la siguiente configuración la cual se muestra en la figura 35.

Figura. 35 Configuracion recursos VDC.

```
vdc swtich1 id 2

limit-resource module-type f3
cpu-share 8

allocate interface $INTERFACE$

limit-resource vlan minimum 3967 maximum 3967

limit-resource monitor-session-erspan-dst minimum 0 maximum 23

limit-resource vrf minimum 100 maximum 1000

limit-resource port-channel minimum 100 maximum 288

limit-resource u4route-mem minimum 96 maximum 96

limit-resource u6route-mem minimum 24 maximum 24

limit-resource m4route-mem minimum 8 maximum 8

limit-resource m6route-mem minimum 20 maximum 20

limit-resource monitor-session-inband-src minimum 0 maximum 1

limit-resource anycast_bundleid minimum 0 maximum 16

limit-resource monitor-session-extended minimum 0 maximum 12

limit-resource monitor-rbs-filter minimum 0 maximum 16

limit-resource monitor-rbs-product minimum 0 maximum 16
```

FUENTE: (Imagen creada por el autor)

Los recursos en cada vdc deberán de ser monitoreados para determinar si algún cambio es requerido en el futuro, para este monitoreo se usará el comando “**show vdc resource detail**” como se muestra a continuación en la figura 36.

Figura. 36 Comando “show vdc resource detail”.

```
Switch# show vdc resource detail
```

vlan	56 used	15836 unused	16327 free	491 avail	16383 total	

Vdc			Min	Max	Used	Unused Avail
---			---	---	----	-----
vdc_admin			16	4094	24	0 491
vdc_datos			3967	3967	8	3959 3959
VDC3			3967	3967	8	3959 3959
VDC4			3967	3967	8	3959 3959
VDC5			3967	3967	8	3959 3959
port-channel	0 used	400 unused	768 free	368 avail	768 total	

Vdc			Min	Max	Used	Unused Avail
---			---	---	----	-----
vdc_admin			0	768	0	0 368
vdc_datos			100	288	0	100 288
VDC3			100	288	0	100 288
VDC4			100	288	0	100 288
VDC5			100	288	0	100 288

FUENTE: (Imagen creada por el autor)

Se utilizará la funcionalidad de cpu-share que se encarga de controlar los recursos de CPU para cada vdc y permite al administrador de red priorizar los recursos depende el uso que se le dé a cada VDC, por defecto los vdc que no son de admin comparten la misma cantidad de CPU inicialmente para esta implementación se

usaran los valores por default, sin embargo, dependiendo de las necesidades puede ser ajustado como se muestra en la figura 37.

Figura. 37 Configuración de CPU en VDC.

```
vdc <nombre>

cpu-share <1-10>
```

FUENTE: (Imagen creada por el autor)

3.7.2 Asignación de interfaces en contextos virtuales.

La asignación de interfaces en cada VDC será hecha tomando en consideración los requerimientos específicos de ancho de banda y los requerimientos de diseño de alta disponibilidad, redundancia y escalabilidad, en las tablas 10,11y 12 se muestran las interfaces asignadas para cada centro de datos:

Tabla 10 Asignación de interfaces en switch router DC1

Numero VDC	Nombre	Interfaces
1	vcd_admin	N/A
2	vdc_datos	eth1/1-2, eth1/10-16 eth2/1-2, eth2/10-16

FUENTE: (Imagen creada por el autor)

Tabla 11 Asignación de interfaces en switch router DC2

Numero VDC	Nombre	Interfaces
1	vcd_admin	N/A
2	vdc_datos	eth1/1-2, eth1/10-16 eth2/1-2, eth2/10-16

FUENTE: (Imagen creada por el autor)

Tabla 12 Asignación de interfaces en switch DCR

Numero VDC	Nombre	Interfaces
1	vcd_admin	N/A
2	vdc_datos	eth1/1-2, eth1/10-16 eth2/1-2, eth2/10-16

FUENTE: (Imagen creada por el autor)

3.8 DISEÑO DE CAPA 2.

En la siguiente sección hablaremos sobre los protocolos de capa 2 del modelo OSI que se utilizaran para esta implementación.

3.8.1 Detección de link unidireccional.

El protocolo de enlace unidireccional UDLD monitorea la configuración física de los enlaces entre dispositivos. Este protocolo detecta la existencia de enlaces unidireccionales, cuando un enlace unidireccional es detectado, el protocolo pone los puertos afectados en error disable y alerta al usuario, este protocolo puede operar en modo normal o modo agresivo.

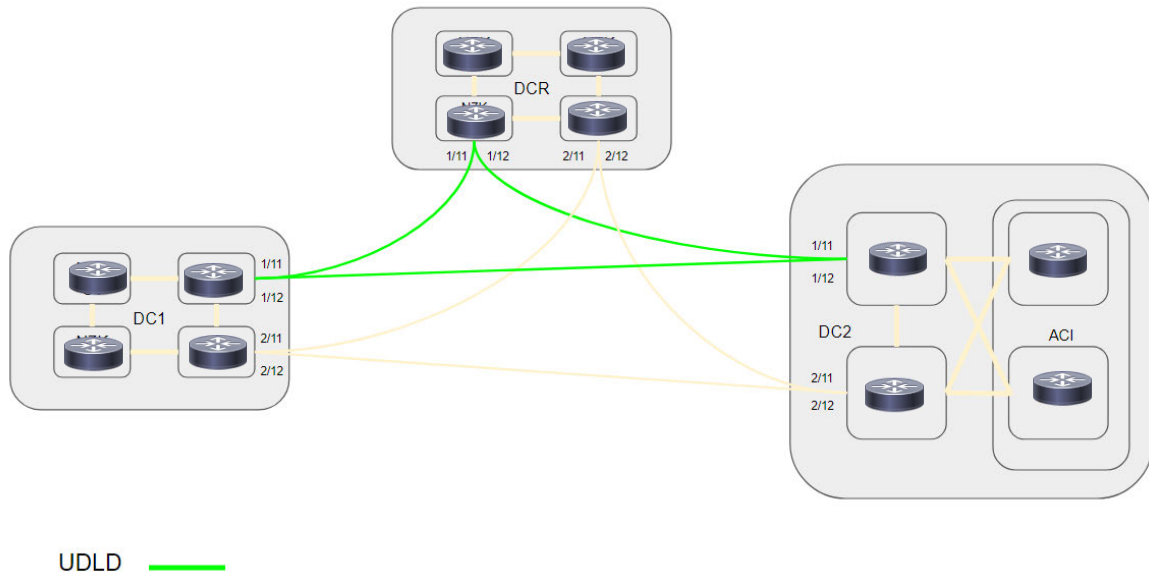
El modo agresivo del protocolo esta deshabilitado por default, se puede configurar solamente en enlaces punto a punto entre dispositivos de red que soporten este protocolo, si UDLD en modo agresivo es habilitado, cuando un puerto en un enlace bidireccional deja de recibir paquetes de UDLD, el protocolo intenta restablecer la conexión con el vecino después de 8 intentos fallidos el puerto es deshabilitado.

Cuando se habilita UDLD en modo agresivo ocurre lo siguiente:

1. Un lado del enlace tiene un puerto que transmite y recibe paquetes
2. Un lado del enlace permanece arriba mientras que el otro lado del enlace está apagado

En estos casos, el modo agresivo deshabilita uno de los puertos del enlace, lo cual previene que el tráfico sea descartado, En esta implementación se usara UDLD en modo agresivo en el triángulo entre los routers 1 como se muestra en la siguiente imagen:

Figura. 38 UDLD enlaces activos.



FUENTE: (Imagen creada por el autor)

A continuación, en la figura 39, se muestra la configuración en cada equipo cisco Nexus 7K:

Figura. 39 Configuración UDLD.

```
swtich (config)# feature udld
swtich (config)# udld aggressive
swtich (config)# interface ethernet <x/y>
swtich (config)# udld enable
```

FUENTE: (Imagen creada por el autor).

Se activará UDLD solamente en los routers 1, en los routers 2 se utilizará BFD en lugar de UDLD

La siguiente configuración se aplicará en los routers 2 para deshabilitar el protocolo UDLD como se muestra en la siguiente imagen:

Figura. 40 Configuración para deshabilitar protocolo UDLD.

```
switch(config)# no feature udld
```

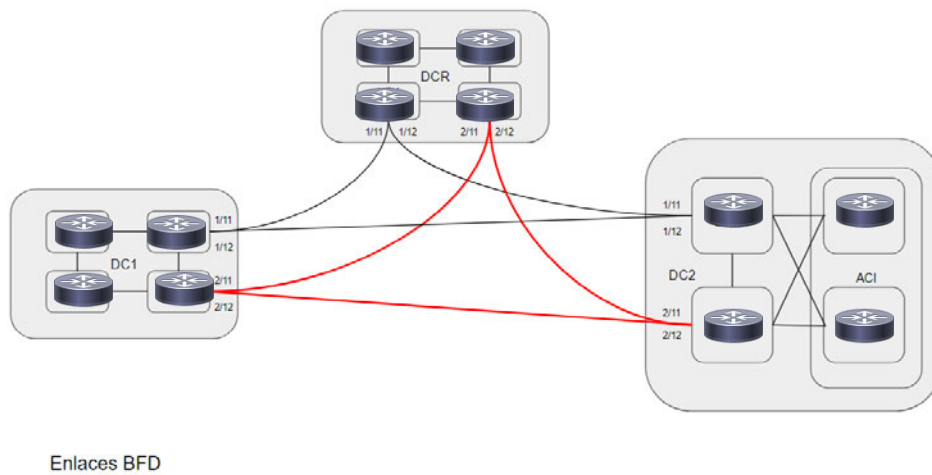
FUENTE: (Imagen creada por el autor).

3.8.2 Detección de reenvío bidireccional.

El protocolo de detección de reenvío bidireccional BFD es un protocolo de detección diseñado para proveer reenvío de paquetes rápidamente en caso de detectar una falla en el medio o en el protocolo de enrutamiento OSPF. Para esta implementación activaremos BFD en las conexiones de los routers 2.

BFD detecta fallas entre 2 dispositivos que forman una vecindad de OSPF, Para esta implementación activaremos BFD en las conexiones de los routers 2.

Figura. 41 Enlaces BFD.



FUENTE: (Imagen creada por el autor)

La configuración será como se muestra en la siguiente imagen:

Figura. 42 Configuración de BFD.

```
feature bfd

router ospf <instance-tag>

interface ethernet <x/y> solo en enlaces WAN

ip ospf <instance-tag> bfd
```

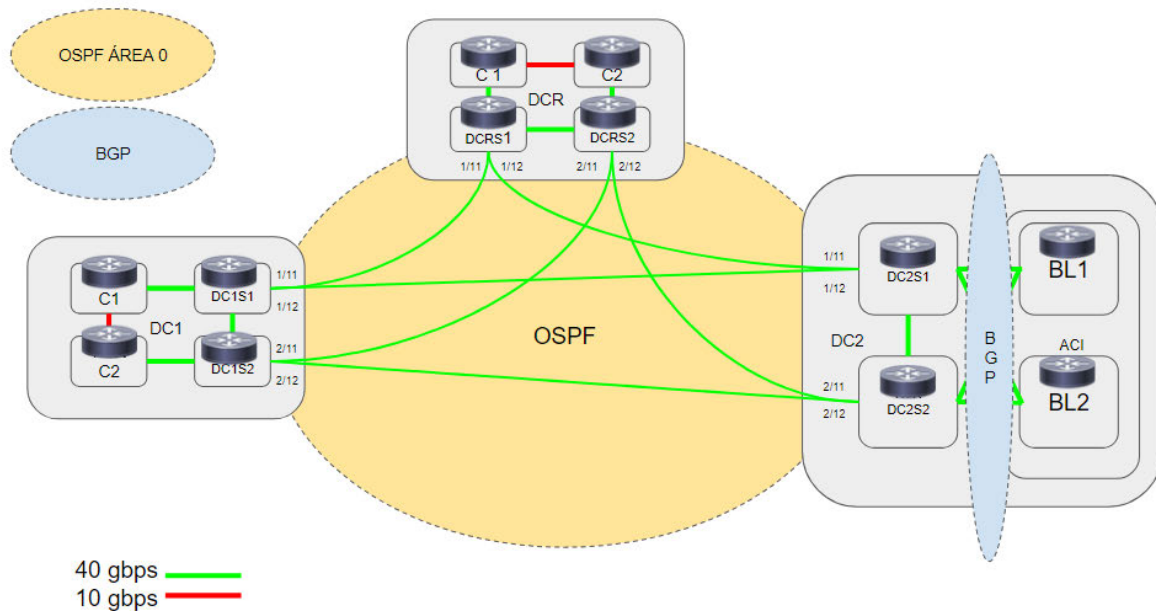
FUENTE: (Imagen creada por el autor)

3.9 CAPA ROUTING.

OSPF y BGP serán usados en los routers de la siguiente manera:

1. Se usará un solo dominio de OSPF, el dominio o instancia de OSPF será “2”.
2. OSPF área 0 se usará para interconectar los 3 centros de datos
3. BGP se usará para interconectar los router cisco 7K con las redes LAN en cada centro de datos, Las redes LAN darán el servicio de red interna en cada región, lo cual no cubre este proyecto.

Figura. 43 Ruteo dinamico vista general.



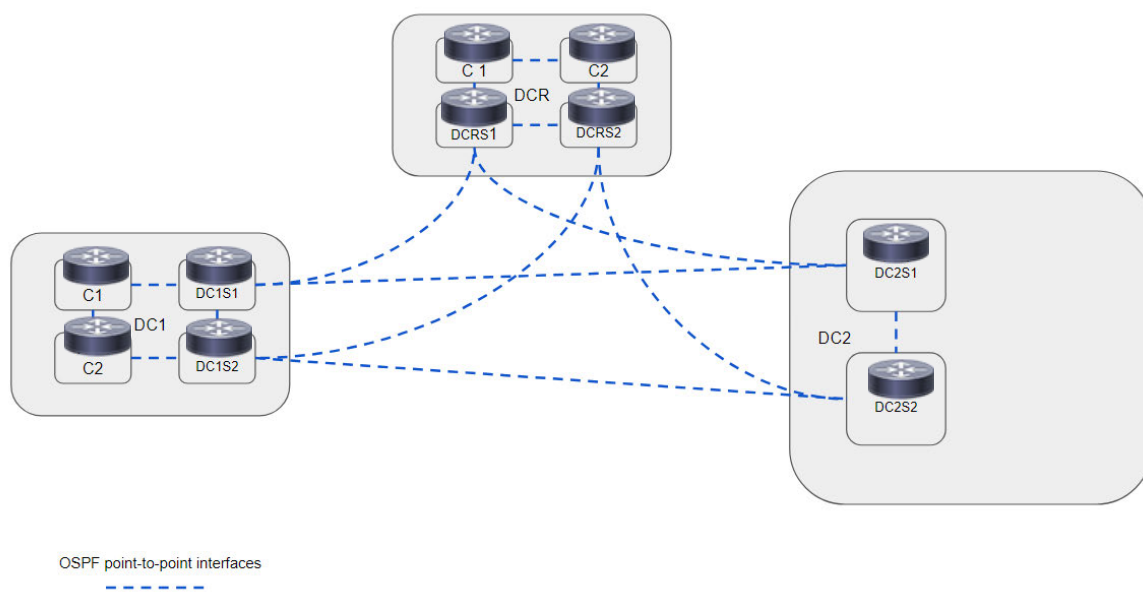
FUENTE: (Imagen creada por el autor)

El diseño de ruteo deberá cumplir las siguientes características:

1. La versión de OSPF que se usará será V2.
2. La versión de BGP que se usará para conectar con las redes LAN V4.
3. El router id de los equipos será la interfaz loopback.
4. Todo el ruteo será configurado en la VRF por default
5. Todas las interfaces en los routers conectaran al área 0 de OSPF, excepto las interfaces que conectan a la red LAN en cada centro de datos.

6. Cada router preferirá su propio enlace WAN para enviar tráfico a los centros de datos.
7. El MTU para las interfaces OSPF serán configuradas para soportar jumbo frames 9216 bytes
8. Las adjacencias de OSPF serán configuradas con el mecanismo de seguridad password-protected.
9. Todas las conexiones de OSPF serán configurados como enlaces point to point

Figura. 44 Ruteo interfaces punto a punto.



FUENTE: (Imagen creada por el autor)

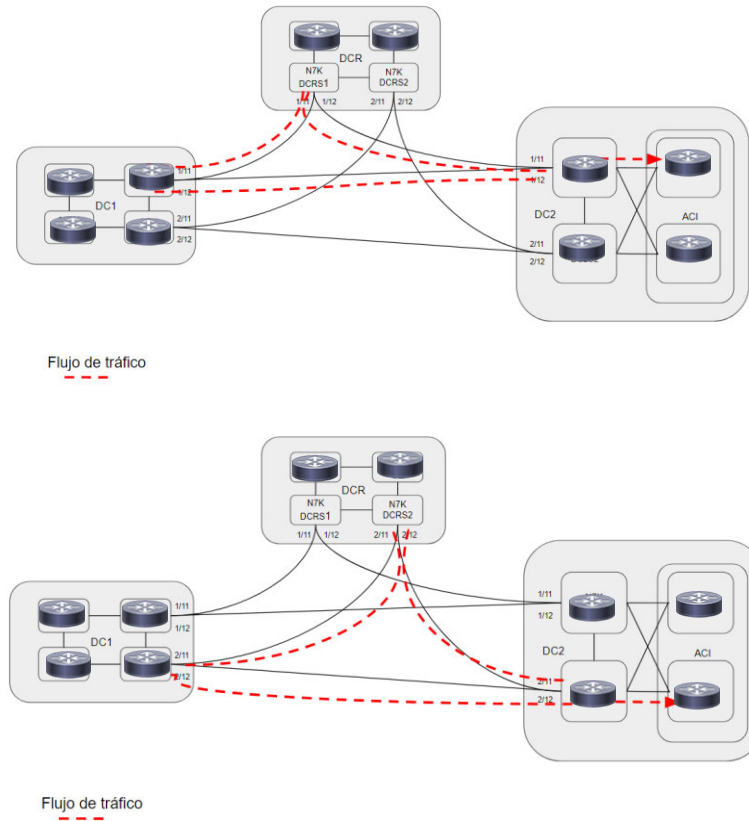
3.9.1 Costos protocolo de apertura de la ruta más corta primero.

EL flujo de tráfico entre los centros de datos deberá ser el siguiente:

1. Cada data center preferirá el router 1 enlace WAN para alcanzar los otros centros de datos.
2. Cada router preferirá el router 1 enlace LAN para conectar con la red interna de su propio centro de datos.
3. En DC2 los 2 routers principales enviarán tráfico al BL 1 en cada red LAN

Este comportamiento es válido cuando los enlaces principales estén activos en caso de que un enlace falle el flujo de tráfico será a treves del router 2 en cada centro de datos.

Figura. 45 Comportamiento del flujo de trafico.



FUENTE: (Imagen creada por el autor)

Para controlar los flujos de tráfico dentro de la red, se van a configurar los siguientes costos de OSPF como se muestra en la tabla 13.

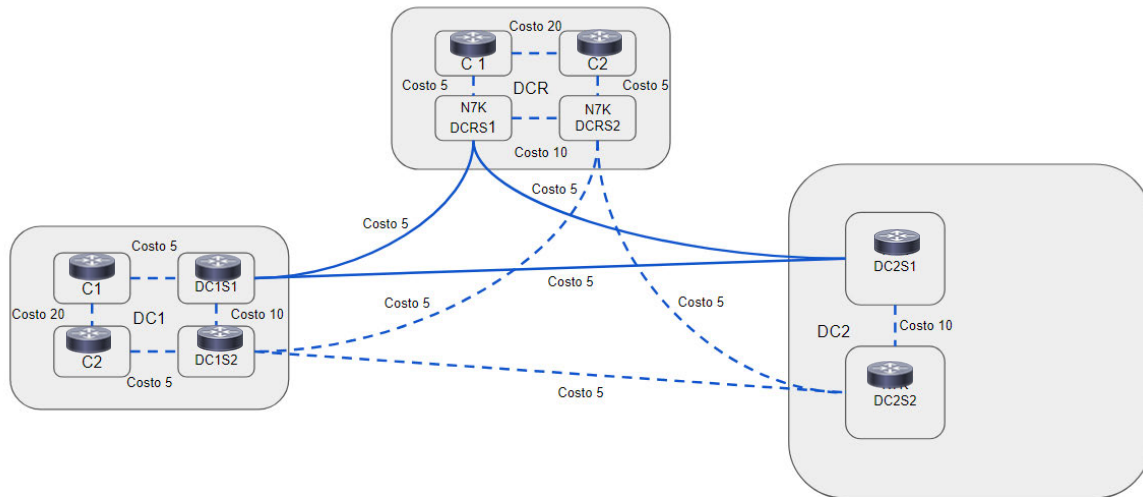
Tabla 13 Costos de enlaces de OSPF.

Enlaces Punto a punto	Descripción	Puerto destino
Entre routers de diferentes centros de datos	WAN Links	5
Entre routers en el mismo centro de datos	Enlaces back to back entre routers	10
Entre Routers y C routers	Enlaces internos	5
Entre C routers	Enlaces back to back entre C routers	20

FUENTE: (Imagen creada por el autor)

La figura 46 muestra la distribución de los valores en la topología:

Figura. 46 Costo de enlaces de OSPF.



FUENTE: (Imagen creada por el autor)

3.9.2 Configuración protocolo de apertura ruta más corta primero.

A continuación, se muestra en la figura 47 y 48 se muestra la configuración de OSPF necesaria para formar las vecindades de OSPF entre los routers cisco Nexus 7K en la región 2 con los otros centros de datos:

Figura. 47 Configuración de OSPF router 1.

```
feature ospf
feature udld
udld aggressive
router ospf 200
  router-ID 7.7.7.7
  redistribute bgp 5XXXX route-map BGP_TO_OSPF
  log-adjacency-changes detail
  passive-interface default
```

FUENTE: (Imagen creada por el autor)

A continuación, se muestra en la figura 48 la configuración de OSPF en el router cisco Nexus 7K 2.

Figura. 48 Configuración de OSPF router 2.

```
feature ospf
feature bfd
router ospf 200

  router-id 8.8.8.8

  redistribute bgp 5XXXX route-map BGP_TO_OSPF

  log-adjacency-changes detail

  passive-interface default
```

FUENTE: (IMAGEN CREADA POR EL AUTOR)

1. Con el comando “feature ospf” se activa la configuración de OSPF en el equipo, sin este comando no es posible configurar toda la suite de comandos siguiente para lograr establecer la conectividad.
2. Para la configuración de ospf será importante definir un ID del proceso de ospf que para este caso usaremos el 200 y no es necesario que sea idéntico en los routers vecinos ya que tiene valor local únicamente.
3. Con el comando “redistribute bgp” a través de una route-map, propagamos todas las redes aprendidas en la red LAN hacia la red WAN, esto quiere decir que desde otras regiones podremos acceder a redes LAN de otra región.
4. Con el comando “passive interface default” evitamos que se anuncien paquetes de OSPF por todas las interfaces del router, para habilitarlo en las interfaces necesarias usaremos el comando no ip ospf passive interface.

A continuación, en la figura 49 se muestra las configuraciones de las interfaces que participan en la negociación del protocolo OSPF, con esta configuración lograremos interconectar con todas las regiones.

Figura. 49 Configuración de interfaces con ospf.

<pre> interface Ethernet3/5 ip ospf authentication message-digest ip ospf message-digest-key 1 md5 3 215613e98e293359 ip ospf cost 5 ip ospf network point-to-point no ip ospf passive-interface ip router ospf 200 area 0 udld enable interface Ethernet4/5 ip ospf authentication message-digest ip ospf message-digest-key 1 md5 3 215613e98e293359 ip ospf cost 5 ip ospf network point-to-point no ip ospf passive-interface ip router ospf 200 area 0 udld enable interface Ethernet5/2 ip ospf cost 10 ip ospf network point-to-point no ip ospf passive-interface ip router ospf 200 area 0 </pre>	<pre> interface Ethernet3/5 ip ospf authentication message-digest ip ospf message-digest-key 1 md5 3 215613e98e293359 ip ospf cost 20 ip ospf network point-to-point no ip ospf passive-interface ip router ospf 200 area 0 ip ospf bfd interface Ethernet4/5 ip ospf authentication message-digest ip ospf message-digest-key 1 md5 3 215613e98e293359 ip ospf cost 20 ip ospf network point-to-point no ip ospf passive-interface ip router ospf 200 area 0 ip ospf bfd interface Ethernet5/2 ip ospf cost 30 ip ospf network point-to-point no ip ospf passive-interface ip router ospf 200 area 0 </pre>
--	--

FUENTE: (Imagen creada por el autor)

En la figura 50 se muestra la configuración del route-map “BGP_TO_OSPF”, esta configuración sirve para anunciar todas las redes permitidas en las prefix-list hacia las otras regiones, un route map es un mecanismo de seguridad que invoca una prefixlist solo las redes permitidas en estas listas serán anunciadas, las que no estén declaradas serán eliminadas y no lograrán establecer comunicación.

La prefix-list BGP_TO_OSPF_FROM_LANC invoca todas las redes de LANC con la sentencia permit, estamos indicando que se pueden propagar hacia la red

WAN, con la sentencia deny decimos que redes no se permiten en este caso se deniegan todas las que no aparecen como permit.

Mismo caso con la prefix-list BGP_TO_OSPF_FROM_LANP solo las redes declaradas en estas listas serán anunciadas desde la red LANP hacia las demás regiones.

Figura. 50 Configuración de route-map en router 1.

```
route-map BGP_TO_OSPF permit 10
  description Routes from LANC
  match ip address prefix-list BGP_TO_OSPF_FROM_LANC
  set tag 100
  set metric 2000
  set metric-type type-1

route-map BGP_TO_OSPF permit 20
  description Routes from PHYSICS
  match ip address prefix-list BGP_TO_OSPF_FROM_LANP
  set tag 101
  set metric 2000
  set metric-type type-1

ip prefix-list BGP_TO_OSPF_FROM_LANC seq 10 permit 1.0.0.0/16 le 32
ip prefix-list BGP_TO_OSPF_FROM_LANC seq 20 permit 2.0.0.0/32
ip prefix-list BGP_TO_OSPF_FROM_LANC seq 1000 deny 0.0.0.0/0 le 32
ip prefix-list BGP_TO_OSPF_FROM_LANP seq 10 permit 3.0.0.0/16 le 32
ip prefix-list BGP_TO_OSPF_FROM_LANP seq 20 permit 4.0.0.0/16 le 32
ip prefix-list BGP_TO_OSPF_FROM_LANP seq 1000 deny 0.0.0.0/0 le 32
```

FUENTE: (Imagen creada por el autor)

En la figura 51 se muestra la configuración del route map BGP_TO_OSPF

Con el comando `match ip address prefix-list` invocamos todas las redes permitidas en las prefixlist `BGP_TO_OSPF_FROM_LANC` y `BGP_TO_OSPF_FROM_LANP`, debemos asegurarnos que estén permitidas todas las redes que queremos interconectar con otras regiones de lo contrario será imposible establecer comunicación.

Figura. 51 Configuración de route map en router 2.

```
route-map BGP_TO_OSPF permit 10
  description Routes from LANC
  match ip address prefix-list BGP_TO_OSPF_FROM_LANC
  set tag 100
  set metric 2000
  set metric-type type-1
route-map BGP_TO_OSPF permit 20
  description Routes from LANP
  match ip address prefix-list BGP_TO_OSPF_FROM_LANP
  set tag 101
  set metric 2000
  set metric-type type-1

ip prefix-list BGP_TO_OSPF_FROM_LANC seq 10 permit 1.0.0.0/16 le 32
ip prefix-list BGP_TO_OSPF_FROM_LANC seq 20 permit 2.0.0.0/32
ip prefix-list BGP_TO_OSPF_FROM_LANC seq 1000 deny 0.0.0.0/0 le 32
ip prefix-list BGP_TO_OSPF_FROM_LANP seq 10 permit 3.0.0.0/16 le 32
ip prefix-list BGP_TO_OSPF_FROM_LANP seq 20 permit 4.0.0.0/16 le 32
ip prefix-list BGP_TO_OSPF_FROM_LANP seq 1000 deny 0.0.0.0/0 le 32
```

Fuente: (Imagen creada por el autor)

3.9.3 Puntos importantes protocolo de enlace de puerta fronteriza.

El diseño de configuración de los routers en DC2 hacia las fábricas de ACI en cada red LAN será la siguiente:

1. BGPv4 será el protocolo de ruteo que se usará para conectar los routers con las fábricas de ACI en cada data center.
2. El router ID de BGP en los routers será la interfaz loopback
3. Todo el ruteo será configurado en la VRF por default
4. El MTU que se configurara en las interfaces para BGP sera 1500 bytes
5. El sistema autónomo de BGP en los routers se 56005
6. Los enlaces que conectan los routers con las fábricas de ACI serán enlaces punto a punto de capa 3.
7. Las adyacencias de BGP serán creadas con la dirección Ip de las interfaces
8. Las adyacencias de BGP no usaran MD5 password protection
9. Solamente una ruta por default sera anunciada a las fábricas de ACI
10. Los routers preferirán el BL 1 para enviar el tráfico hacia ACI, para esto se configurará local preference de 600 en los BL1 en los BL2 300.

3.9.4 Configuración de protocolo de enlace fronteriza

A continuación, se muestra la configuración de BGP aplicada en los routers para conectar con las redes LAN.

Figura. 52 Configuración de BGP en router 1

<pre> feature bgp router bgp 65XXX router-id 7.7.7.7 log-neighbor-changes address-family ipv4 unicast neighbor 192.168.1.3 remote-as 74236 address-family ipv4 unicast route-map FROM_LANC_BL_1 in route-map TO_LANC_BL_1 out neighbor 192.168.1.7 remote-as 75935 address-family ipv4 unicast route-map FROM_LANP_BL_1 in route-map TO_LANP_BL_1 out neighbor 192.168.1.1 remote-as 74236 address-family ipv4 unicast route-map FROM_LANC_BL_02 in route-map TO_LANC_BL_02 out neighbor 192.168.1.10 remote-as 75935 address-family ipv4 unicast route-map FROM_LANP_BL_2 in route-map TO_LANP_BL_2 out </pre>	<pre> feature bgp router bgp 56632 router-id 8.8.8.8 log-neighbor-changes address-family ipv4 unicast neighbor 192.168.2.3 remote-as 74236 address-family ipv4 unicast route-map FROM_LANC_BL_1 in route-map TO_LANC_BL_1 out neighbor 192.168.2.7 remote-as 75935 address-family ipv4 unicast route-map FROM_LANP_BL_1 in route-map TO_LANP_BL_1 out neighbor 192.168.2.1 remote-as 74236 address-family ipv4 unicast route-map FROM_LANC_BL_02 in route-map TO_LANC_BL_02 out neighbor 192.168.2.10 remote-as 75935 address-family ipv4 unicast route-map FROM_LANP_BL_2 in route-map TO_LANP_BL_2 out </pre>
--	--

FUENTE: (Imagen creada por el autor)

1. En primer lugar, es importante definir un sistema autónomo para comenzar con la configuración de bgp, al no estar expuesto a internet estas conexiones será importante considerar que deberá estar en el rango de 64512 y 65534 reservado para para uso privado y pruebas.
2. Después se configuran las vecindades con el comando neighbor dirección ip del vecino seguido del sistema autónomo del otro extremo.

A continuación, Se muestra la configuración de las interfaces físicas que conectan con la red LANC Y LANP

Figura. 53 Configuración de interfaces BGP en router 1 y 2

<pre>interface Ethernet3/1 description DC2S1 TO LANC BL_1 mtu 9000 logging event port link-status no ip redirects ip address 192.168.1.4/30 no shutdown interface Ethernet2/1 description DC2S1 TO LANC BL_2 mtu 9000 logging event port link-status no ip redirects ip address 192.168.1.2/30 no shutdown interface Ethernet2/3 description DC2S1 TO LANP BL_1 mtu 9000 logging event port link-status no ip redirects ip address 192.168.1.8/30 no shutdown interface Ethernet3/3 description DC2S1 TO LANP BL_2 mtu 9000 logging event port link-status no ip redirects ip address 192.168.1.9/30 no shutdown</pre>	<pre>interface Ethernet3/1 description DC2S2 TO LANC BL_1 mtu 9000 logging event port link-status no ip redirects ip address 192.168.2.4/30 no shutdown interface Ethernet2/1 description DC2S2 TO LANC BL_2 mtu 9000 logging event port link-status no ip redirects ip address 192.168.2.2/30 no shutdown interface Ethernet2/3 description DC2S2 TO LANP BL_1 mtu 9000 logging event port link-status no ip redirects ip address 192.168.2.8/30 no shutdown interface Ethernet3/3 description DC2S2 TO LANP BL_2 mtu 9000 logging event port link-status no ip redirects ip address 192.168.2.9/30 no shutdown</pre>
---	---

FUENTE: (Imagen creada por el autor)

En la figura 54 se muestra la configuración de los route-maps configurados como filtro de seguridad para determinar que redes serán propagas a los otros data centers.

Figura. 54 Configuración de route-maps.

<pre> route-map FROM_LANC_BL_1 permit 10 match ip address prefix-list FROM_LANC set local-preference 800 route-map FROM_LANC_BL_02 permit 10 match ip address prefix-list FROM_LANC set local-preference 200 route-map FROM_LANP_BL_1 permit 10 match ip address prefix-list FROM_LANP set local-preference 800 route-map FROM_LANP_BL_2 permit 10 match ip address prefix-list FROM_LANP set local-preference 200 route-map TO_LANC_BL_1 permit 10 match ip address prefix-list TO_LANC route-map TO_LANC_BL_2 permit 10 match ip address prefix-list TO_LANC set as-path prepend 56631 route-map TO_LANP_BL_1 permit 10 match ip address prefix-list TO_LANP route-map TO_LANP_BL_2 permit 10 match ip address prefix-list TO_LANP set as-path prepend 56631 ip prefix-list FROM_LANC seq 5 permit 1.0.0.0/16 le 32 ip prefix-list FROM_LANC seq 10 permit 2.0.0.0/32 ip prefix-list FROM_LANC seq 1000 deny 0.0.0.0/0 le 32 ip prefix-list FROM_LANP seq 5 permit 3.0.0.0/16 le 32 ip prefix-list FROM_LANP seq 10 permit 4.0.0.0/16 le 32 ip prefix-list FROM_LANP seq 1000 deny 5.0.0.0/0 le 32 ip prefix-list TO_LANC seq 1000 deny 0.0.0.0/0 le 32 ip prefix-list TO_LANP seq 1000 deny 0.0.0.0/0 le 32 </pre>	<pre> route-map FROM_LANC_BL_1 permit 10 match ip address prefix-list FROM_LANC set local-preference 800 route-map FROM_LANC_BL_02 permit 10 match ip address prefix-list FROM_LANC set local-preference 200 route-map FROM_LANP_BL_1 permit 10 match ip address prefix-list FROM_LANP set local-preference 800 route-map FROM_LANP_BL_2 permit 10 match ip address prefix-list FROM_LANP set local-preference 200 route-map TO_LANC_BL_1 permit 10 match ip address prefix-list TO_LANC route-map TO_LANC_BL_2 permit 10 match ip address prefix-list TO_LANC set as-path prepend 56631 route-map TO_LANP_BL_1 permit 10 match ip address prefix-list TO_LANP route-map TO_LANP_BL_2 permit 10 match ip address prefix-list TO_LANP set as-path prepend 56631 ip prefix-list FROM_LANC seq 5 permit 1.0.0.0/16 le 32 ip prefix-list FROM_LANC seq 10 permit 2.0.0.0/32 ip prefix-list FROM_LANC seq 1000 deny 0.0.0.0/0 le 32 ip prefix-list FROM_LANP seq 5 permit 3.0.0.0/16 le 32 ip prefix-list FROM_LANP seq 10 permit 4.0.0.0/16 le 32 ip prefix-list FROM_LANP seq 1000 deny 5.0.0.0/0 le 32 ip prefix-list TO_LANC seq 1000 deny 0.0.0.0/0 le 32 ip prefix-list TO_LANP seq 1000 deny 0.0.0.0/0 le 32 </pre>
---	---

FUENTE: (Imagen creada por el autor)

Los mapas de ruta son una secuencia ordenada de instrucciones individuales, cada una tiene el resultado de permiso o rechazo, La evaluación de prefix-list y los mapas de ruta consiste en un escaneo de la prefixlist, en un orden predeterminado, y una evaluación de los criterios de cada sentencia que coincida. Una vez que se encuentra la primera coincidencia de instrucciones se realiza una acción asociada a la coincidencia de instrucciones.

3.9.5 Conexión con nubes publicas

A continuación, se muestra la configuración en los routers cisco Nexus 7K en DC2 para conectar con la nube publica de AWS he iniciar el intercambio de redes a través del protocolo OSPF.

Figura. 55 Configuración OSPF hacia nubes router 1

```
interface Ethernet1/4
  description DC2S1 to DCE2PROD1 3/2
  mtu 9216
  logging event port link-status
  no ip redirects
  ip address 192.168.20.1/30
  ip ospf cost 1000
  ip ospf network point-to-point
  no ip ospf passive-interface
  ip ospf priority 90
  ip router ospf 200 area 0
  ip arp timeout 300
  no shutdown
router ospf 200
  router-id 7.7.7.7
  redistribute bgp 56631 route-map BGP_TO_OSPF
  log-adjacency-changes detail
  passive-interface default
route-map BGP_TO_OSPF permit 10
  description Routes from LANC
  match ip address prefix-list BGP_TO_OSPF_FROM_LANC
  set tag 200
  set metric 2000
route-map BGP_TO_OSPF permit 20
  description Routes from LANP
  match ip address prefix-list BGP_TO_OSPF_FROM_LANP
  set tag 201
  set metric 3000
ip prefix-list BGP_TO_OSPF_FROM_LANC seq 5 permit 1.1.1.1/16 le 32
ip prefix-list BGP_TO_OSPF_FROM_LANC seq 10 permit 2.2.2.2/32
ip prefix-list BGP_TO_OSPF_FROM_LANC seq 1000 deny 0.0.0.0/0 le 32
ip prefix-list BGP_TO_OSPF_FROM_LANP seq 5 permit 1.1.1.1/16 le 32
ip prefix-list BGP_TO_OSPF_FROM_LANP seq 10 permit 2.2.2.2/16 le 32
ip prefix-list BGP_TO_OSPF_FROM_LANP seq 1000 deny 0.0.0.0/0 le 32
```

FUENTE: (Imagen creada por el autor)

Figura. 56 Configuración OSPF hacia nubes router 2

```
interface Ethernet1/4
  description DC2S2 to DCE2PROD2 3/2
  mtu 9216
  logging event port link-status
  no ip redirects
  ip address 192.168.20.5/30
  ip ospf cost 1000
  ip ospf network point-to-point
  no ip ospf passive-interface
  ip ospf priority 90
  ip router ospf 200 area 0
  ip arp timeout 300
  no shutdown
router ospf 200
  router-id 8.8.8.8
  redistribute bgp 56632 route-map BGP_TO_OSPF
  log-adjacency-changes detail
  passive-interface default
route-map BGP_TO_OSPF permit 10
  description Routes from LANC
  match ip address prefix-list BGP_TO_OSPF_FROM_LANC
  set tag 200
  set metric 2000
route-map BGP_TO_OSPF permit 20
  description Routes from LANP
  match ip address prefix-list BGP_TO_OSPF_FROM_LANP
  set tag 201
  set metric 3000
ip prefix-list BGP_TO_OSPF_FROM_LANC seq 5 permit 1.1.1.1/16 le 32
ip prefix-list BGP_TO_OSPF_FROM_LANC seq 10 permit 2.2.2.2/32
ip prefix-list BGP_TO_OSPF_FROM_LANC seq 1000 deny 0.0.0.0/0 le 32
ip prefix-list BGP_TO_OSPF_FROM_LANP seq 5 permit 1.1.1.1/16 le 32
ip prefix-list BGP_TO_OSPF_FROM_LANP seq 10 permit 2.2.2.2/16 le 32
ip prefix-list BGP_TO_OSPF_FROM_LANP seq 1000 deny 0.0.0.0/0 le 32
```

FUENTE: (Imagen creada por el autor)

1. Se configuro un MTU de 9216, es decir para soportar paquetes conocidos como jumbo frames por encima de los paquetes con MTU 1500 valor por default.
2. Con el comando logging event port link-status habilitamos el sistema de log de la interfaz, para que cada vez que ocurra un cambio de estado o algún otro evento específico sobre esta interfaz, se genere un log en el equipo.

3. Con el comando `no ip redirects`, este deshabilita los mensajes de redireccionamiento de ICMP sobre la interfaz, las redirecciones ocurren cuando un router reconoce un paquete que llega a una interfaz y la mejor ruta es salir de esa misma interfaz, en este caso el router envía un paquete de redireccionamiento icmp al origen informando sobre un camino mejor en la misma subred, los paquetes posteriores toman la ruta optima, si se desactiva esto los paquetes continúan usando la misma ruta.
4. Con el comando `ip address` se configura una dirección ip sobre la interfaz en este caso /30 con 2 direcciones ip utilizables para configurar una ip en cada extremo y formar un enlace P2P.
5. Con el comando `ip ospf cost`, se configura la métrica que utiliza OSPF para determinar la viabilidad de una ruta, Cuanto mayor sean los valores del ancho de banda de una interfaz, menor será el valor del costo.
6. Con el comando `ip ospf network point to point` configuramos una conexión entre dos routers específicos que hablan OSPF.
7. Con el comando `no ip ospf passive-interface` nos aseguramos que esta interfaz continuara recibiendo paquetes de hello de ospf, asegurándonos aside que se reciban todas las actualizaciones del protocolo de ruteo.
8. Con el comando `ip ospf priority` forzamos la elección del router DR en un dominio de OSPF entre mayor sea el valor de la prioridad de OSPF habrá más probabilidades de que el router se convierta en el router DR o BDR.
9. Con el comando `ip router ospf` se habilita OSPF versión 3, el valor del `process-id` representa un numero de entre 1 y 65535 seguido del número de área.
10. Con el comando `ip arp timeout` fijamos el contador a 5 minutos (300s) de esta manera nos aseguramos, que cualquier cambio dentro de la tabla de arp del equipo será actualizado después de los 5 minutos
11. Con el comando `redistribute bgp`, con un route map redistribuimos todas las redes que aprendemos de la LAN a los equipos DCE para que estas redes sean alcanzables desde las nubes públicas.

CAPÍTULO IV RESULTADOS

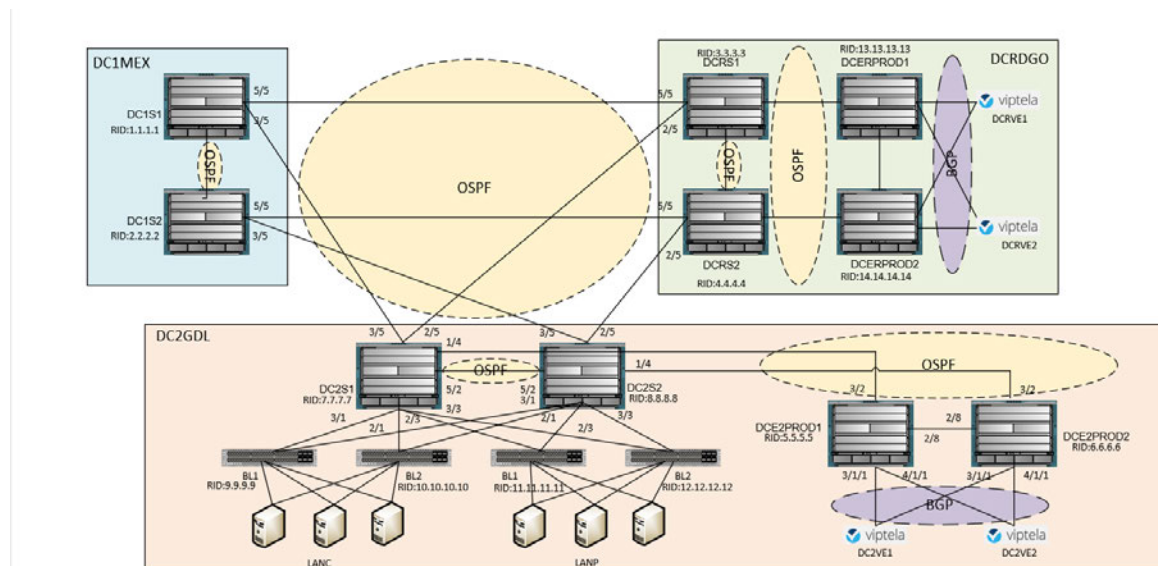
4.1 INTRODUCCION AL CAPITULO.

A continuación, se analizan los resultados obtenidos en este proyecto, topología final, validación de los equipos Data center cloud Edge y las validaciones de los equipos DC2S del centro de datos 2 que demuestran el resultado final de la implementación.

4.2 TOPOLOGIA FINAL.

A continuación, se muestra la topología final como resultado de la implementación “Red empresarial con router cisco Nexus 7k para la interconexión de centros de datos regionales en Bancomer”, en la topología se observa la interconexión de los 3 centros de datos regionales MEX, GDL y DGO.

Figura. 57 Topología Final.



FUENTE: (Imagen creada por el autor)

A continuación, se describen los procedimientos necesarios para validar el correcto funcionamiento del Routing en el data center DC2, Esto abarca los equipos, DC2S1C, DC2S2, DCE y los BL de LANC y LANP.

4.3 EQUIPOS DATA CENTER CLOUD EDGE (DCE).

El funcionamiento de estos equipos es dar salida a los usuarios del DC2 a los principales proveedores de nube publica como son AWS, AZURE y GCP, donde se encuentran alojados algunos de los servicios más importantes de la compañía.

Los procedimientos detallados a continuación se han validado entrando directamente a los contextos VDC de cada equipo. Los equipos DCE son equipos cisco Nexus 7k igual que los DCS en todos los centros de datos estos conectan a los equipos DCS1 y DCS2 en el DC2 con los DCVE (Data Center Virtual Edge) que dan acceso a la SD-WAN. Existen dos equipos por contexto (Producción y Desarrollo). La siguiente tabla describe los contextos virtuales que tiene configurado cada equipo.

Tabla 14 Infraestructura DCE.

Hostname	Descripción
DCE2ADM1	Contexto de administracion 1 DC2
DCE2ADM2	Contexto de administracion 2 DC2
DCE2PROD1	Contexto de produccion 1 DC2
DCE2PROD2	Contexto de produccion 2 DC2
DCE2DEV1	Contexto de desarrollo 1 DC2
DCE2DEV2	Contexto de desarrollo 2 DC2

FUENTE: (Imagen creada por el autor)

4.3.1 Interfaces UP

Para los contextos de producción en DC2 tienen que estar UP las interfaces:

Tabla 15 Conexiones físicas contexto visual DCEPROD.

Interfaz	Uso
Eth2/8	Conexión entre los DCE
Eth3/2	Conexión con DC2S1 y DC2S2
Eth3/1/1	Conexión con DC2VE1
Eth4/1/1	Conexión con DC2VE2

FUENTE: (Imagen creada por el autor)

Con el comando “show ip interface brief” se muestra el estado físico de las interfaces y la dirección ip configurada en cada extremo de la conexión, como se puede ver a continuación:

Figura. 58 Salida comando “show ip interface brief” DCE2PROD1

```
DCE2PROD1# show ip interface brief
```

IP Interface Status for VRF "default"(1)

Interface	IP Address	Interface Status
Lo0	50.55.XX.XXX	protocol-up/link-up/admin-up
Eth2/8	50.55.XX.XXX	protocol-up/link-up/admin-up
Eth3/2	50.55.XX.XXX	protocol-up/link-up/admin-up
Eth3/1/1.100	50.55.XX.XXX	protocol-up/link-up/admin-up
Eth4/1/1.100	50.55.XX.XXX	protocol-up/link-up/admin-up

FUENTE: (Imagen creada por el autor)

Para los contextos de desarrollo

En el centro de datos DC2 tienen que estar UP las siguientes interfaces:

Tabla 16 Conexiones físicas contexto visual DCEDEV.

Interfaz	Uso
Eth2/10	Conexión entre los DCE
Eth3/10	Conexión con DC2S1 y DC2S2
Eth3/9/1	Conexión con DC2VE1
Eth4/9/1	Conexión con DC2VE2

FUENTE: (Imagen creada por el autor).

Con el comando “show ip interface brief” se muestra el estado físico de las interfaces y la dirección ip configurada en cada extremo de la conexión, como se puede ver a continuación:

Figura. 59 Salida comando “show ip interface brief” DCEDEV1

```
DCE2DEV1# show ip interface brief
```

IP Interface Status for VRF "default"(1)

Interface	IP Address	Interface Status
Lo0	50.55.XX.XXX	protocol-up/link-up/admin-up
Eth2/10	50.55.XX.XXX	protocol-up/link-up/admin-up
Eth3/10	50.55.XX.XXX	protocol-up/link-up/admin-up
Eth3/9/1.200	50.55.XX.XXX	protocol-up/link-up/admin-up
Eth4/9/1.200	50.55.XX.XXX	protocol-up/link-up/admin-up

FUENTE: (Imagen creada por el autor).

En cualquier caso, si hay una caída de una interfaz se refleja en el log del equipo y normalmente se debería recibir una alerta en la herramienta de monitoreo

Figura. 60 Ejemplo log caída de interfaz

```
2019 Nov 8 19:12:13 DCE2PROD1 %ETHPORT-5-IF_DOWN_LINK_FAILURE: Interface Ethernet3/1/1.100 is down (Link failure)
2019 Nov 8 19:12:14 DCE2PROD1 %ETHPORT-5-IF_DOWN_LINK_FAILURE: Interface Ethernet4/1/1.100 is down (Link failure)
```

FUENTE: (Imagen creada por el autor).

4.3.2 Adyacencias Up

Los equipos DCE tienen que tener adyacencias de OSPF con los DCS y BGP con los DCVE

Con el DCS para producción:

Figura. 61 Salida de comando "show ip ospf neighbors" DCPROD1

```
DCE2PROD1# show ip ospf neighbors
```

```
OSPF Process ID 1 VRF default
```

```
Total number of neighbors: 2
```

Neighbor ID	Pri	State	Up Time	Address	Interface
50.55.XX.XXX	90	FULL/ -	10w3d	50.55.XX.XXX	Eth2/8
50.55.XX.XXX	100	FULL/ -	31w4d	50.55.XX.XXX	Eth3/2

FUENTE: (Imagen creada por el autor).

Con el DCS para desarrollo:

Figura. 62 Salida de comando "show ip ospf neighbors" DCEDEV1

```
DCE2DEV1# show ip ospf neighbors
```

```
111
```

```
OSPF Process ID 1 VRF default
```

```
Total number of neighbors: 2
```

Neighbor ID	Pri	State	Up Time	Address	Interface
50.55.XX.XXX	90	FULL/ -	10w3d	150.55.XX.XXX	Eth2/10
50.55.XX.XXX	100	FULL/ -	31w4d	150.55.XX.XXX	Eth3/10

FUENTE: (Imagen creada por el autor).

Con los DCVE producción:

Tiene que haber dos adyacencias de BGP con los equipos DCVE, además se puede comprobar que se establecen las adyacencias con los prefijos (si el número es 0 suele haber un problema)

Figura. 63 Salida de comando “show ip bgp summary” DCE2PROD1

```
DCE2PROD1# show ip bgp summary
```

BGP summary information for VRF default, address family IPv4 Unicast

BGP router identifier 150.55.XX.XXX, local AS number 6XXX0

BGP table version is 1134, IPv4 Unicast config peers 2, capable peers 2

88 network entries and 117 paths using 15344 bytes of memory

BGP attribute entries [5/720], BGP AS path entries [1/6]

BGP community entries [0/0], BGP clusterlist entries [0/0]

158 received paths for inbound soft reconfiguration

0 identical, 108 modified, 50 filtered received paths using 3664 bytes

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
50.55.XX.XXX	4	6XXX0	638553	637518	1134	0	0	7w5d	54
50.55.XX.XXX	4	6XXX0	638578	637537	1134	0	0	10w3d	54

FUENTE: (Imagen creada por el autor).

Con los DCVE desarrollo:

Figura. 64 Salida de comando “show ip bgp summary” DCEDEV1

```
DCE2DEV1# show ip bgp summary
```

BGP summary information for VRF default, address family IPv4 Unicast

BGP router identifier 150.55.XX.XXX, local AS number 65XX1

BGP table version is 1112, IPv4 Unicast config peers 2, capable peers 2

90 network entries and 110 paths using 14920 bytes of memory

BGP attribute entries [11/1584], BGP AS path entries [4/40]

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
50.55.XX.XXX	4	65XX0	638686	637554	1112	0	0	7w5d	50
50.55.XX.XXX	4	65XX0	638719	637573	1112	0	0	10w3d	50

FUENTE: (Imagen creada por el autor).

Para las interfaces que conectan a los DCVE, si hay pérdidas de adyacencias también se ve reflejado en el log.

Figura. 65 Salida de comando “show ip loggin last 50” DCEPROD1

```
DCE2PROD1# show loggin last 50
2020 Feb 18 18:23:02 DCE2PROD1 %BGP-5-ADJCHANGE: bgp-6XXX0 [16794] (default) neighbor XX.XX.XX.XXX
Down - other configuration change
2020 Feb 18 18:23:07 DCE2PROD1 %BGP-5-ADJCHANGE: bgp-6XXX0 [16794] (default) neighbor XX.XX.XX.XXX
Down - other configuration change
2020 Feb 18 18:23:13 DCE2PROD1 %BGP-5-ADJCHANGE: bgp-6XXX0 [16794] (default) neighbor XX.XX.XX.XXX
Up
2020 Feb 18 18:23:14 DCE2PROD1 %BGP-5-ADJCHANGE: bgp-6XXX0 [16794] (default) neighbor XX.XX.XX.XXX
Up
```

FUENTE: (Imagen creada por el autor).

Los mensajes de caída de BGP tienen un código que aporta información sobre el motivo de la caída. En el caso del ejemplo, el “other configuration change” es precisamente uno de los más genéricos, pero ya indica que ha habido un cambio en la configuración de BGP que implica un reseteo de las sesiones, en este caso se trató de un cambio de timers de keepalive del vecino, otros mensajes posibles pueden ser

1. Malformed attribute list in BGP update
2. Hold timer expired
3. Maximum number of prefixes reached
4. Peer de-configured
5. Administrative reset

4.3.3 Rutas aprendidas

4.3.3.1 Routing desde los equipos DCE2PROD1 y DCE2PROD2

Con el comando show ip route ospf-1 summary se validó que se reciba todas las rutas de los equipos DC2S aprendidas por OSPF al día de hoy unas 3222, tanto para desarrollo como para producción por que en los equipos DCS no se separan Producción de desarrollo. Se puede observar a continuación en la figura 57.

Figura. 66 Salida de comando “show ip route ospf-1 sum” DCE2PROD1

```
DCE2PROD1# show ip route ospf-1 summary

IP Route Table for VRF "default"

Total number of routes: 3222

Total number of paths: 3222

Best paths per protocol:      Backup paths per protocol:

  ospf-1      : 3222      None

Number of routes per mask-length:

  /8 : 38      /16: 49      /18: 9      /19: 14      /20: 8
  /21: 10      /22: 67      /23: 201     /24: 640     /25: 96
  /26: 139     /27: 135     /28: 107     /29: 20      /30: 118
  /31: 1       /32: 1570
```

FUENTE: (Imagen creada por el autor).

Figura. 67 Salida de comando “show ip route ospf-1” DCE2PROD1

```
DCE2PROD1# show ip route ospf-1

IP Route Table for VRF "default"

'*' denotes best ucast next-hop

'***' denotes best mcast next-hop

'[x/y]' denotes [preference/metric]

'%<string>' in via output denotes VRF <string>

X.0.0.0/8, ubest/mbest: 1/0

    *via 50.55.XX.XXX, Eth3/2, [110/1030], 10w3d, ospf-1, type-1, tag 100,

5.X.X.0/30, ubest/mbest: 1/0

    *via 50.55.XX.XXX, Eth3/2, [110/1021], 5d09h, ospf-1, inter

6.X.X.X/32, ubest/mbest: 1/0

    *via 50.55.XX.XXX, Eth3/2, [110/1022], 5d09h, ospf-1, intra

6.X.X.X/32, ubest/mbest: 1/0

    *via 50.55.XX.XXX, Eth3/2, [110/1022], 5d09h, ospf-1, intra
```

FUENTE: (Imagen creada por el autor).

4.3.3.2 Validar rutas desde los equipos DCVE

Con el comando “show ip bgp” se muestran las rutas que se reciben por bgp (las que están marcadas como external las aprendemos a través de los equipos DC2VE1 y DC2VE2).

Figura. 68 Salida de comando “show ip bgp” DCE2PROD1

```
DCEPROD1# show ip bgp

BGP routing table information for VRF default, address family IPv4 Unicast

BGP table version is 1134, local router ID is 1XX.XX.XX.13

Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best

Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist, I-injected

Origin codes: i - IGP, e - EGP, ? - incomplete, | - multipath, & - backup
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*>120.XX.XX.0/22	0.0.0.0		100	3XXX8	i
*>120.XX.XX.0/22	0.0.0.0		100	3XXX8	i
*>120.XX.XX.0/20	0.0.0.0		100	3XXX8	i
*>120.XX.XXX.0/23	0.0.0.0		100	3XXX8	i
*>a20.XX.0.0/16	0.0.0.0		100	3XXX8	i
*>120.XX.0.0/23	0.0.0.0		100	3XXX8	i
*>120.XX.X.0/23	0.0.0.0		100	3XXX8	i
*>120.XX.XX.0/23	0.0.0.0		100	3XXX8	i
*>120.XX.0.0/16	0.0.0.0		100	3XXX8	i
* e200.XX.0.0/19	50.55.XX.141	1000	400	0 6XXX0	?

FUENTE: (Imagen creada por el autor).

Sin embargo, que se reciban no significa que se importen en la tabla de enrutamiento, por los filtros de redistribución, por lo que también se puede revisar con el comando “show ip route bgp”, como se muestra a continuación:

Figura. 69 Salida de comando “show ip route bgp” DCEPROD1

```
DCE2PRO1# show ip route bgp

IP Route Table for VRF "default"

'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

100.XX.0.0/19, ubest/mbest: 1/0
    *via 50.55.XX.137, [20/1000], 6w5d, bgp-6XXX0, external, tag 6XXX0,
    via 50.55.XX.174, Eth2/8, [110/600], 7w2d, ospf-1, type-1, tag 202,
100.XX.0.0/24, ubest/mbest: 1/0
    *via 50.55.XX.137, [20/1000], 6w5d, bgp-6XXX0, external, tag 6XXX0,
    via 50.55.XX.174, Eth2/8, [110/600], 7w2d, ospf-1, type-1, tag 202,
100.XX.1.0/24, ubest/mbest: 1/0
    *via 50.55.XX.137, [20/1000], 6w5d, bgp-6XXX0, external, tag 6XXX0,
    via 50.55.XX.174, Eth2/8, [110/600], 7w2d, ospf-1, type-1, tag 202,
100.XX.4.0/24, ubest/mbest: 1/0
    *via 50.55.XX.137, [20/1000], 6w5d, bgp-6XXX0, external, tag 6XXX0,
    via 50.55.XX.174, Eth2/8, [110/600], 7w2d, ospf-1, type-1, tag 202,
```

FUENTE: (Imagen creada por el autor).

Nota: Aquí se ve la ruta que se aprende por BGP directamente del vecino, tanto como la que se aprende por OSPF desde el otro equipo DC2VE, De las dos rutas que se aprenden por BGP el algoritmo de selección elige la que tiene mayor local preference y la instala en la tabla de enrutamiento, es la ruta que tiene preferencia por tener menor distancia administrativa.

Nota: Las rutas con next-hop Null 0 se deben a que esos prefijos se anuncian agregados hacia los DCVE. Las crea automáticamente BGP para prevenir bucles.

Se pueden ver los cambios a nivel de BGP con el comando “show bgp event-history detail”, a un que hay poco buffer, por lo que si son muy recientes ya no los vemos en el log.

Figura. 70 Salida de comando “show bgp event-history” DCEPROD1

```
DCE2PROD1# show bgp event-history detail

BGP event-history detail

2020 Jun 15 18:17:14.903363: (default) BRIB: [IPv4 Unicast] Cleanup thread removed 1 prefix

2020 Jun 15 18:17:14.903356: (default) BRIB: [IPv4 Unicast] Prefix 1XX.2XX.XX.136/30 cleaned up
from BGP table

2020 Jun 15 18:17:14.903348: RNH: Cancelling pending requests for rnh 50.55.XX.141/32 (urib)

2020 Jun 15 18:17:14.903345: RNH: Rnh 50.55.XX.141/32 (urib) in use and added, nothing to do
```

FUENTE: (Imagen creada por el autor).

También podemos ver las rutas que se han añadido o borrado en las tablas de enrutamiento, pero ahí vamos a ver cualquier cambio en los equipos DC2S de la compañía ya que como comentamos, se reciben todas las rutas sin distinguir a que ambiente pertenecen

Figura. 71 Comando “show routing event-history delete-route” DCEPROD1

```
DCE2PROD1# show routing event-history delete-route

Dumping: delete-route

2020 Jun 16 00:23:45.203266 urib: "ospf-1": 50.XX.1.2/32, deleting nh 50.55.XX.178%Ethernet5/8,
metric [110/350] route-type type-2 tag 0x0000026c flags 0x00000000

2020 Jun 16 00:18:36.903178 urib: "ospf-1": 50.XX.1.2/32, deleting nh 50.55.XX.178%Ethernet5/8,
metric [110/350] route-type type-2 tag 0x0000026c flags 0x00000000

2020 Jun 15 23:21:17.073208 urib: "ospf-1": 50.XX.1.2/32, deleting nh 50.55.XX.178%Ethernet5/8,
metric [110/350] route-type type-2 tag 0x0000026c flags 0x00000000

2020 Jun 15 22:34:46.073262 urib: "ospf-1": 50.XX.1.2/32, deleting nh 50.55.XX.178%Ethernet5/8,
metric [110/350] route-type type-2 tag 0x0000026c flags 0x00000000
```

FUENTE: (Imagen creada por el autor).

Con el comando “show routing event-history add-route” podemos validar que rutas se van agregando a la tabla de enrutamiento de los equipos DCE como se muestra a continuación.

Figura. 72 Comando “show routing event-history add-route” DCEPROD1

```
DCE2PROD1# show routing event-history add-route

Dumping: add-route

2020 Jun 16 00:24:14.653291 urib: "ospf-1": 50.XX.1.2/32, new nh 50.55.XX.178%Ethernet3/2, metric
[110/350] route-type type-2 tag 0x0000026c flags 0x00000000 rt_o

2020 Jun 16 00:24:14.653256 urib: "ospf-1": 50.XX.1.2/32, adding nh 50.55.XX.178%Ethernet3/2, metric
[110/350] route-type type-2 tag 0x0000026c flags 0x00000000 r

2020 Jun 16 00:19:06.703270 urib: "ospf-1": 50.XX.1.2/32, new nh50.55.XX.178%Ethernet3/2, metric
[110/350] route-type type-2 tag 0x0000026c flags 0x00000000 rt_o

2020 Jun 16 00:19:06.703237 urib: "ospf-1": 50.XX.1.2/32, adding nh 50.55.XX.178%Ethernet3/2, metric
[110/350] route-type type-2 tag 0x0000026c flags 0x00000000 r

2020 Jun 15 22:28:35.833282 urib: "ospf-1": 50.XX.1.2/32, new nh 50.55.XX.178%Ethernet3/2, metric
[110/350] route-type type-2 tag 0x0000026c flags 0x00000000 rt_o
```

FUENTE: (Imagen creada por el autor).

También se puede comprobar si alguien ha cambiado algo en la configuración de los equipos DCE2, como por ejemplo anunciar una ruta con el comando show “accounting log” como se muestra a continuación.

Figura. 73 Salida de comando “show accounting log” DCEPROD1

```
DCE2PROD1# show accounting log

Fri Sep 13 20:53:51 2019:type=update:id=50.XXX.XXX.234@pts/0:user=XXX:cmd=switchto ; configure
terminal ; feature ospf (SUCCESS)

Fri Sep 13 20:53:57 2019:type=update:id=50.XXX.XXX.234@pts/0:user=XXX:cmd=switchto ; configure
terminal ; feature bgp (SUCCESS)

Fri Sep 13 20:54:05 2019:type=update:id=50.XXX.XXX.234@pts/0:user=XXX:cmd=netflow enabled

Fri Sep 13 20:54:05 2019:type=update:id=50.XXX.XXX.234@pts/0:user=XXX:cmd=switchto ; configure
terminal ; feature netflow (SUCCESS)

Fri Sep 13 20:54:52 2019:type=update:id=50.XXX.XXX.234@pts/0:user=XXX:cmd=switchto ; configure
terminal ; banner motd X (SUCCESS)
```

FUENTE: (Imagen creada por el autor).

4.3.4 Rutas propagadas

En los equipos DCE todas las que tengan el símbolo “*>”, son redes que se anuncian desde on-premise a la nube pública, esto podemos validarlos con el comando show ip bgp como se muestra a continuación.

Figura. 74 Salida de comando “show ip bgp” DCEPROD1

```
DCE2PROD1# show ip bgp
BGP routing table information for VRF default, address family IPv4 Unicast
BGP table version is 1134, local router ID is 50.XX.XX.133
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best
Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist, I-injected
Origin codes: i - IGP, e - EGP, ? - incomplete, | - multipath, & - backup
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*>110.XX.XX.0/22	0.0.0.0		100	3XXXX	i
*>110.XX.XX.0/22	0.0.0.0		100	3XXXX	i
*>110.XX.XX.0/20	0.0.0.0		100	3XXXX	i
*>110.XX.XX.0/23	0.0.0.0		100	3XXXX	i
*>110.XX.XX.0/16	0.0.0.0		100	3XXXX	i
*>110.XX.XX.0/23	0.0.0.0		100	3XXXX	i
*>110.XX.XX.0/23	0.0.0.0		100	3XXXX	i
*>110.XX.XX.0/23	0.0.0.0		100	3XXXX	i
*>110.XX.XX.0/16	0.0.0.0		100	3XXXX	i

FUENTE: (Imagen creada por el autor).

4.4 EQUIPOS DC2S EN CENTRO DE DATOS DC2.

Estos equipos conectan a las fábricas de ACI (Infraestructura LAN que da servicio a la red del centro de datos donde se albergan los principales servicios de la compañía) y con los equipos DCE (Data center cloud Edge) estos equipos controlan el tráfico de entrada y salida desde el centro de datos con los principales proveedores de nube publica AWS, AZURE y GCP.

Después de la implementación tenemos que verificar que las siguientes interfaces se encuentren en estado up (encendido)

DC2S1.

En la siguiente tabla podemos visualizar las conexiones físicas entre DC2S1 con los equipos DCS1 en DC1, con los equipos borde DCE1 en DC2 y con los equipos BL para la conexión con la red LANC y LANP.

Tabla 17 Conexiones físicas equipo DC2S1.

Interfaz	Conexión
Eth3/1	Conexión con BL1 LANC
Eth2/3	Conexión con BL1 LANP
Eth2/5	Conexión con DCS 1 de DCR
Eth1/6	Conexión con DCE2DEV1
Eth1/4	Conexión con DCE2PROD1
Eth2/1	Conexión con BL 2 LANC
Eth5/2	Interconexión con DC2S2
Eth3/2	Conexión con BL2 LANP
Eth3/5	Conexión con DCS 1 de DC1
Eth2/3	Conexión con BL2 LANC

FUENTE: (Imagen creada por el autor).

DCS2.

En la siguiente tabla podemos visualizar las conexiones físicas entre DCS1 con los equipos DCS1 en DC1, con los equipos borde DCE1 en DC2 y con los equipos BL para la conexión con la red LANC y LANP.

Tabla 18 Conexiones físicas equipo DC2S2.

Interfaz	Conexión
Eth3/1	Conexión con BL1 LANC
Eth2/3	Conexión con BL1 LANP
Eth2/5	Conexión con DCRS2
Eth1/6	Conexión con DCE2DEV2
Eth1/4	Conexión con DCE2PROD2
Eth2/1	Conexión con BL 2 LANC

Eth5/2	Interconexión DCS
Eth3/3	Conexión con BL2 LANP
Eth3/5	Conexión con DC1S2 de DC1

FUENTE: (Imagen creada por el autor).

4.4.1 Interfaces UP.

Con la salida del comando “show ip interface brief” se validó que todas las interfaces quedaran operando en modo up, y que el direccionamiento Ip configurado fuera el correcto.

Figura. 75 Salida de comando “show ip interface brief” DCS1

```
DCS1# show ip int brief

IP Interface Status for VRF "default"(1)

Interface

  IP Address      Interface Status
-----
Lo0               9.XX.XX.20      protocol-up/link-up/admin-up
Eth3/1            3.XX.XX.65      protocol-up/link-up/admin-up
Eth2/3            3.XX.XX.93      protocol-up/link-up/admin-up
Eth2/5            3.XX.XX.57      protocol-up/link-up/admin-up
Eth1/6            3.XX.XX.137     protocol-up/link-up/admin-up
Eth1/4            3.XX.XX.109     protocol-up/link-up/admin-up
Eth2/1            3.XX.XX.69      protocol-up/link-up/admin-up
Eth5/2            3.XX.XX.89      protocol-up/link-up/admin-up
Eth3/3            3.XX.XX.97      protocol-up/link-up/admin-up
Eth3/5            3.XX.XX.49      protocol-up/link-up/admin-up
```

FUENTE: (Imagen creada por el autor).

4.4.2 Adyacencias UP

Los equipos DCS en DC2 tienen adyacencias OSPF con los DCS en DC1, DCR y los equipos DCE en DC2, hablan BGP con los BL de LAN tanto para LANC como para LANP.

Con el comando “show ip ospf neighbors” se muestra que las vecindades de OSPF entre los DCS y los equipos DCE en DC2 se hayan formado correctamente.

Figura. 76 Salida de comando “show ip ospf neighbors” DCS1

```
DC2S1# show ip ospf nei
```

OSPF Process ID 1 VRF default

Total number of neighbors: 5

Neighbor ID	Pri	State	Up Time	Address	Interface
1.1.1.1	1	FULL/DR	49w4d	3.xx.xx.90	Eth3/5
8.8.8.8	90	FULL/ -	2y4w	3.xx.xx.50	Eth2/5
3.3.3.3	90	FULL/ -	2y4w	3.xx.xx.58	Eth5/2
5.5.5.5	90	FULL/ -	1y23w	3.xx.xx.138	Eth1/4

FUENTE: (Imagen creada por el autor).

Figura. 77 Salida de comando “show ip ospf neighbors” DCS2

```
DC2S2# show ip ospf nei
```

OSPF Process ID 1 VRF default

Total number of neighbors: 5

Neighbor ID	Pri	State	Up Time	Address	Interface
2.2.2.2	1	FULL/BDR	49w4d	3.XX.XX.89	Eth3/5
7.7.7.7	90	FULL/ -	2y4w	3.XX.XX.62	Eth5/2
4.4.4.4	90	FULL/ -	2y4w	3.XX.XX.70	Eth2/5
6.6.6.6	90	FULL/ -	1y23w	3.XX.XX.126	Eth1/4

FUENTE: (Imagen creada por el autor).

En la siguiente tabla se muestran los router-id de cada equipo con el cual se formó una vecindad de OSPF.

Tabla 19 Router ID de adyacencias OSPF DC2S1.

Neighbor ID	Equipo
1.1.1.1	DC1S1
8.8.8.8	DC2S2
3.3.3.3	DCRS1
5.5.5.5	DCE2PROD1

FUENTE: (Imagen creada por el autor).

Tabla 20 Router ID de adyacencias OSPF DC2S2.

Neighbor ID	Equipo
2.2.2.2	DC1S2
7.7.7.7	DC2S1
4.4.4.4	DCRSC2
6.6.6.6	DCEPROD2

FUENTE: (Imagen creada por el autor).

4.4.3 Adyacencias con LANC y LANP:

Con el comando `show ip bgp summary` se muestra que se establecieron correctamente las vecindades de BGP con la red LANC y LANP.

Figura. 78 Salida de comando “show ip bgp summary” DC2S1

```
DC2S1# show ip bgp summary

BGP summary information for VRF default, address family IPv4 Unicast

BGP router identifier 7.7.7.7, local AS number 6XXX0

BGP table version is 5423, IPv4 Unicast config peers 4, capable peers 4

Neighbor    V  AS  MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
9.9.9.9      4 6XXX0 1969414 1964728   5423    0    0   49w3d   27
10.10.10.10  4 6XXX0 1969427 1964747   5423    0    0   49w3d   27
11.11.11.11  4 6XXX1 1825162 1819857   5423    0    0   51w2d   44
12.12.12.12  4 6XXX1 1825091 1819855   5423    0    0   51w2d   44
```

FUENTE: (Imagen creada por el autor).

En la siguiente tabla se muestra la relación entre router-id y equipo con el cual se establece la vecindad de BGP.

Tabla 21 Router ID adyacencias de BGP DC2S1.

Neighbor ID	Equipo
9.9.9.9	BL1 LANC
10.10.10.10	BL2 LANC
11.11.11.11	BL1 LANP
12.12.12.12	BL2 LANP

FUENTE: (Imagen creada por el autor).

Figura. 79 Salida de comando “show ip bgp summary” DC2S2

```
DC2S2# show ip bgp summary

BGP summary information for VRF default, address family IPv4 Unicast
BGP router identifier 9.XX.XX.XX, local AS number 65050
BGP table version is 5680, IPv4 Unicast config peers 4, capable peers 4
71 network entries and 142 paths using 15904 bytes of memory
BGP attribute entries [8/1152], BGP AS path entries [2/12]
BGP community entries [0/0], BGP clusterlist entries [0/0]

Neighbor      V    AS MsgRcvd MsgSent   TblVer  InQ  OutQ  Up/Down  State/PfxRcd
9.9.9.9        4    6XXX1 1969393 1964707    5680    0    0    49w3d   27
10.10.10.10   4    6XXX2 1969406 1964725    5680    0    0    49w3d   27
11.11.11.11   4    6XXX3 1825172 1819861    5680    0    0    51w2d   44
12.12.12.12   4    6XXX4 1825053 1819818    5680    0    0    51w2d   44
```

FUENTE: (Imagen creada por el autor).

Tabla 22 Router ID adyacencias de BGP DC2S2.

Neighbor ID	Equipo
9.9.9.9	BL1 LANC
10.10.10.10	BL2 LANC
11.11.11.11	BL1 LANP
12.12.12.12	BL2 LANP

FUENTE: (Imagen creada por el autor).

4.4.4 Rutas aprendidas por ruteo dinámico.

A continuación, veremos el detalle de las rutas aprendidas a través del protocolo OSPF en los equipos DC2S:

Con el comando “show ip route ospf summary” se muestra el total de rutas aprendidas desde DC1 y DCR, que son los equipos que forman las vecindades de OSPF:

Figura. 80 Salida de comando “show ip route ospf summary” DC2S1

```
DC2S1# show ip route ospf summary

IP Route Table for VRF "default"

Total number of routes: 2494

Total number of paths: 2600

Best paths per protocol:      Backup paths per protocol:

  ospf-1          : 2600      None

Number of routes per mask-length:

/6 : 3      /7 : 2      /8 : 28      /12: 1      /14: 2
/16: 31     /17: 4      /18: 8      /19: 4      /20: 89
/21: 120    /22: 449    /23: 102    /24: 478    /25: 80
/26: 40     /27: 34     /28: 74     /29: 40     /30: 151
```

FUENTE: (Imagen creada por el autor).

Con el comando “show ip route ospf” se validó las rutas aprendidas como se muestra a continuación:

Figura. 81 Salida de comando “show ip route ospf” DC2S1

```
DC2S1 show ip route ospf

IP Route Table for VRF "default"

'*' denotes best ucast next-hop

'***' denotes best mcast next-hop

'[x/y]' denotes [preference/metric]

'%<string>' in via output denotes VRF <string>

1.X.XX.0/24, ubest/mbest: 1/0

    *via 1X.XXX.XX.50, Eth3/5, [110/21], 2y4w, ospf-1, type-1, tag 4,

3.X.X.110/32, ubest/mbest: 1/0

    *via 1X.XXX.XX.50, Eth3/5, [110/280], 4d23h, ospf-1, type-1, tag 2,

6.X.XX.0/22, ubest/mbest: 1/0

    *via 1X.XXX.XX.50, Eth3/5, [110/280], 2w4d, ospf-1, type-1, tag 2,

6.X.XX.0/22, ubest/mbest: 1/0

    *via 1X.XXX.XX.50, Eth3/5, [110/280], 2w4d, ospf-1, type-1, tag 2,

6.X.XX.0/22, ubest/mbest: 1/0

    *via 1X.1XX.XX.50, Eth2/5, [110/280], 2w2d, ospf-1, type-1, tag 2,

6.X.XXX.0/22, ubest/mbest: 1/0

    *via 1X.1XX.XX.50, Eth2/5, [110/280], 6d14h, ospf-1, type-1, tag 2,

6.X.X.0/22, ubest/mbest: 1/0

    *via 1X.XXX.XX.50, Eth2/5, [110/280], 2w4d, ospf-1, type-1, tag 2,

6.X.XXX.0/22, ubest/mbest: 1/0

    *via 1X.XXX.XX.50, Eth2/5, [110/280], 2w4d, ospf-1, type-1, tag 2,

6.X.XX.0/22, ubest/mbest: 1/0
```

FUENTE: (Imagen creada por el autor).

Para validar las rutas aprendidas a través de BGP desde las LANC y LANP se validó con el comando “show ip BGP”

DC2S VS LANC:

Figura. 82 Salida de comando “show ip bgp | i 6XXX0” DC2S1

```
DC2S1# show ip bgp | i 6XXX0
```

*>e10.XX.0.0/23	3.XX.XX.66	0	500	0 6XXX0 ?
* e	3.XX.XX.70	0	400	0 6XXX0 ?
*>e20.XX.X.0/23	3.XX.XX.66	0	500	0 6XXX0 ?
* e	3.XX.XX.70	0	400	0 6XXX0 ?
* e20.XX.X.0/23	3.XX.XX.70	0	400	0 6XXX0 ?
*>e	3.XX.XX.66	0	500	0 6XXX0 ?
*>e20.XX.X.0/23	3.XX.XX.66	0	500	0 6XXX0 ?
* e	3.XX.XX.70	0	400	0 6XXX0 ?
* e20.XX.XX.0/23	3.XX.XX.70	0	400	0 6XXX0 ?
*>e	3.XX.XX.66	0	500	0 6XXX0 ?
*>e20.XX.XX.0/23	3.XX.XX.66	0	500	0 6XXX0 ?
* e	3.XX.XX.70	0	400	0 6XXX0 ?
*>e20.XX.XX.0/23	3.XX.XX.66	0	500	0 6XXX0 ?
* e	3.XX.XX.70	0	400	0 6XXX0 ?
*>e20.XX.XX.0/23	3.XX.XX.66	0	500	0 6XXX0 ?
* e	3.XX.XX.70	0	400	0 6XXX0 ?
*>e20.XX.XX.0/23	3.XX.XX.66	0	500	0 6XXX0 ?

FUENTE: (Imagen creada por el autor).

DC2S VS LANP:

Figura. 83 Salida de comando "show ip bgp | i 6XXX1" DC2S1

```
DC2S1# show ip bgp | i 6XXX1
```

*>e10.XX.0.0/23	3.XX.XX.94	0	500	0 6XXX1 ?
* e	3.XX.XX.98	0	400	0 6XXX1 ?
*>e10.XX.2.0/23	3.XX.XX.94	0	500	0 6XXX1 ?
* e	3.XX.XX.98	0	400	0 6XXX1 ?
*>e10.XX.10.0/23	3.XX.XX.94	0	500	0 6XXX1 ?
* e	3.XX.XX.98	0	400	0 6XXX1 ?
*>e10.XX.12.0/23	3.XX.XX.94	0	500	0 6XXX1 ?
* e	3.XX.XX.98	0	400	0 6XXX1 ?
*>e10.XX.14.0/23	3.XX.XX.94	0	500	0 6XXX1 ?
* e	3.XX.XX.98	0	400	0 6XXX1 ?
*>e10.XX.16.0/23	3.XX.XX.94	0	500	0 6XXX1 ?
* e	3.XX.XX.98	0	400	0 6XXX1 ?
*>e10.XX.20.0/23	3.XX.XX.94	0	500	0 6XXX1 ?
* e	3.XX.XX.98	0	400	0 6XXX1 ?
*>e10.XX.22.0/23	3.XX.XX.94	0	500	0 6XXX1 ?
* e	3.XX.XX.98	0	400	0 6XXX1 ?
*>e10.XX.26.0/23	3.XX.XX.94	0	500	0 6XXX1 ?
* e	3.XX.XX.98	0	400	0 6XXX1 ?
*>e10.XX.30.0/25	3.XX.XX.94		500	0 6XXX1 ?
* e	3.XX.XX.98		400	0 6XXX1 ?
*>e10.XX.XX.128/25	3.XX.XX.94	0	500	0 6XXX1 ?

FUENTE: (Imagen creada por el autor).

También se validó que se estuvieran aprendiendo todas las redes desde la tabla de enrutamiento con el comando “show ip route bgp” como se muestra a continuación

Figura. 84 Salida de comando “show ip route bgp” DC2S1

```
DC2S1# show ip route bgp

IP Route Table for VRF "default"

'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

1.XX.0.0/23, ubest/mbest: 1/0
    *via 3.XX.XX.66, [20/0], 49w3d, bgp-6XXX0, external, tag 6XXX0,
    via 3.XX.XX.90, Eth5/2, [110/1005], 49w4d, ospf-1, type-1, tag 200,
1.XX.2.0/23, ubest/mbest: 1/0
    *via 3.XX.XX.66, [20/0], 49w3d, bgp-6XXX0, external, tag 6XXX0,
    via 3.XX.XX.90, Eth5/2, [110/1005], 49w4d, ospf-1, type-1, tag 200,
1.XX.4.0/23, ubest/mbest: 1/0
    *via 3.XX.XX.66, [20/0], 18w5d, bgp-65050, external, tag 65100,
    via 3.XX.XX.90, Eth5/2, [110/1005], 18w5d, ospf-1, type-1, tag 200,
1.XX.6.0/23, ubest/mbest: 1/0
    *via 3.XX.XX.66, [20/0], 49w3d, bgp-6XXX0, external, tag 6XXX0,
    via 3.XX.XX.90, Eth5/2, [110/1005], 49w4d, ospf-1, type-1, tag 200,
1.XX.10.0/23, ubest/mbest: 1/0
    *via 3.XX.XX.66, [20/0], 18w5d, bgp-6XXX0, external, tag 6XXX0,
    via 3.XX.XX.90, Eth5/2, [110/1005], 18w5d, ospf-1, type-1, tag 200,
1.XX.14.0/23, ubest/mbest: 1/0
    *via 3.XX.XX.66, [20/0], 49w3d, bgp-6XXX0, external, tag 6XXX0,
    via 3.XX.XX.90, Eth5/2, [110/1005], 49w4d, ospf-1, type-1, tag 200,
1.XX.16.0/23, ubest/mbest: 1/0
```

FUENTE: (Imagen creada por el autor).

Si se aprende por BGP y no se ve en la tabla de rutas es porque hay algún problema con los prefix-list y los route maps que son las políticas de seguridad encargadas de filtrar las rutas:

4.4.5 Validar rutas propagadas.

En los equipos DC2S el proceso de BGP está configurado para que origine una ruta por default hacia LANC y LANP, esto se puede comprobar por cada vecino BGP:

Figura. 85 Comando “show ip bgp nei 3.XX.XX.6 advertised-routes” DC2S1

```
DC2S1# show ip bgp nei 9.9.9.9 advertised-routes
Peer 3.XX.XX.X6 routes for address family IPv4 Unicast:
BGP table version is 5423, local router ID is 9.XX.XX.X0
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best
Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist, I-injected
Origin codes: i - IGP, e - EGP, ? - incomplete, | - multipath, & - backup
Originating default network 0.0.0.0/0
  Network          Next Hop          Metric      LocPrf      Weight Path
```

FUENTE: (Imagen creada por el autor).

4.4.6 Planeación de actividades.

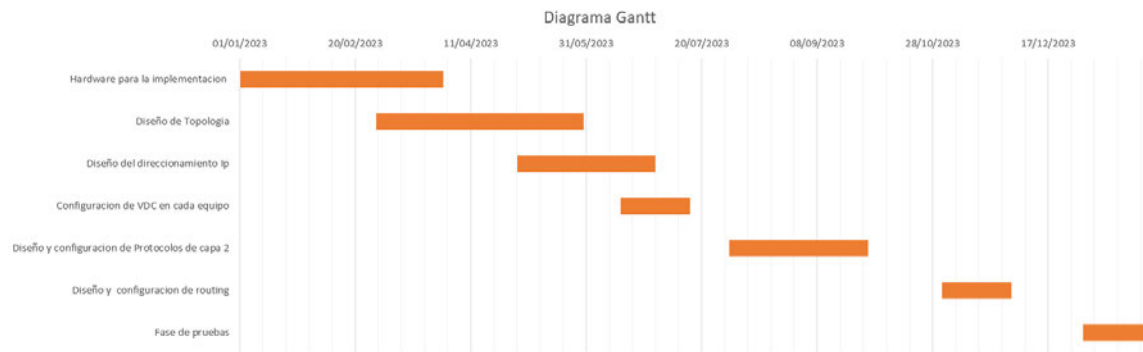
A continuación, se muestra la planeación de las actividades realizadas con fecha de inicio días de duración y fecha final de cada actividad, así como un diagrama de Gantt que representa el tiempo que tardo en ejecutarse en proyecto.

Tabla 23 Plan de actividades.

Nombre de la actividad	Fecha de Inicio	Duración de días	Fecha Fin
Hardware para la implementación	01/01/2023	88	30/03/2023
Diseño de Topología	01/03/2023	90	30/05/2023
Diseño del direccionamiento Ip	01/05/2023	60	30/06/2023
Configuración de VDC en cada equipo	15/06/2023	30	15/07/2023
Diseño y configuración de Protocolos de capa 2	01/08/2023	60	30/09/2023
Diseño y configuración de routing	01/11/2023	30	01/12/2023
Fase de pruebas	01/01/2024	31	01/02/2024

FUENTE: (Imagen creada por el autor).

Figura. 86 Diagrama Gantt “Cronograma de actividades”



FUENTE: (Imagen creada por el autor)

Conclusiones.

Para dar solución a este proyecto se realizó el estudio de diferentes protocolos y estándares de redes utilizando técnicas de networking tradicionales que han sido desarrolladas en el ámbito académico y en la actualidad se encuentran en pleno desarrollo en el ámbito comercial. Si analizamos los motivos que impulsan las arquitecturas de networking en las compañías podemos ver que detrás de estas hay objetivos importantes como disminuir costos operativos, mejorar los servicios a clientes externos e internos, hacer más eficientes y flexibles los procesos de negocio de la empresa.

Como se ha visto a lo largo de este trabajo, existen muchas tecnologías distintas para configurar, administrar o diseñar una red empresarial. Una ventaja de utilizar estas tecnologías tanto estándar como propietarias es que existen muchas maneras de utilizarlas para implementar una solución. A lo largo de este trabajo se han explorado de cada escenario LAN, WAN y Data center distintas soluciones para cumplir con el objetivo de interconectar 3 centros de datos regionales

Incorporar un data center como pieza clave en la estrategia de transformación digital o como recurso para fortalecer las actividades de una compañía puede traer grandes beneficios como la continuidad del negocio ya que con un centro de datos se puede ofrecer la garantía de que el negocio siga funcionando de manera correcta sin importar los eventos que se puedan suscitar, como por ejemplo un desastre natural.

Los recursos, información y procesos indispensables en una empresa deben estar disponibles siempre y cuando se necesiten para seguir ofreciendo los productos o servicios y no perder dinero por la inestabilidad o indisposición de los sistemas.

Un centro de procesamiento de datos debe tener altos estándares de seguridad de la información, así como personal calificado para evitar filtraciones y pérdidas, contar con un centro de datos para recuperación frente a desastres o una solución de disaster recovery es una de las mejores decisiones que puede tomar una

empresa moderna, en especial si es de un sector de alta confidencialidad como la banca, gobierno y seguros.

El campo profesional de las telecomunicaciones es muy extenso y hay muchas áreas de oportunidad donde puedes desarrollar diferentes habilidades técnicas, Cisco es un líder en esta rama y tiene un sin fin de soluciones tecnológicas que se pueden implementar de acuerdo a las necesidades de cada compañía, Como la tecnología cisco Nexus diseñada para soportar robustas cargas de trabajo como las de un data center. A lo largo de mi experiencia profesional he tenido la oportunidad de trabajar con infraestructura de campus y equipos de centros de datos mucho más robustos.

Las comunicaciones son una parte fundamental de todas las compañías en la actualidad gracias a estas podemos transportar grandes cantidades de información de un site a otro site en cuestión de segundos incluso en ubicaciones geográficas diferentes.

Competencias desarrolladas.

El objetivo general de la carrera Ingeniería en Sistemas Computacionales, es formar profesionistas líderes, analíticos, críticos y creativos, con visión estratégica y amplio sentido ético, capaces de diseñar, implementar y administrar infraestructura computacional para aportar soluciones innovadoras en beneficio de la sociedad, en un contexto global, multidisciplinario y sustentable.

Gracias a las materias Fundamentos de Investigación, Fundamentos de Telecomunicaciones, Redes de computadoras, Conmutación y enrutamiento en redes de datos y Administración de redes cursadas en los semestres 1,5,6,7 y 8 fue que se obtuvieron los conocimientos necesarios para ejecutar este proyecto.

Al ejecutar este proyecto se alcanzaron las siguientes competencias adquiridas en el transcurso de la carrera:

1. Diseñar, configurar y administrar redes computacionales aplicando las normas y estándares vigentes.
2. Coordinar y participar en proyectos interdisciplinarios
3. Diseñar e implementar interfaces hombre-máquina y máquina-máquina para la automatización de sistemas
4. Identificar y comprender las tecnologías de hardware para proponer, desarrollar y mantener aplicaciones eficientes
5. Integrar soluciones computacionales con diferentes tecnologías, plataformas o dispositivos
6. Desarrollar una visión empresarial para detectar áreas de oportunidad que le permitan emprender y desarrollar proyectos aplicando las tecnologías de la información y comunicación
7. Desempeñar sus actividades profesionales considerando los aspectos legales, éticos, sociales y de desarrollo sustentable
8. Seleccionar y aplicar herramientas matemáticas para el modelado, diseño y desarrollo de tecnología computacional.

Fuentes de Información.

1. ABC de la Fibra Óptica - MINTIC - Vive Digital. (n.d.). . (s.f.). *ABC de la Fibra Óptica*. Obtenido de ABC de la Fibra Óptica: <https://mintic.gov.co/portal/vivedigital/612/w3-article-5342.html>
2. Albarran, C. (2022). *Cableado estructurado, qué es, tipos y utilidades*. . Obtenido de Redes&Telecom: <https://www.redestelecom.es/infraestructuras/cableado-estructurado-que-es-tipos-y-utilidades/>
3. AWS. (s.f.). *¿Qué es el enrutamiento? - Explicación del enrutamiento de redes*. Obtenido de [https://aws.amazon.com/](https://aws.amazon.com/es/what-is/routing/#:~:text=Un%20protocolo%20de%20enrutamiento%20es,de%20puerta%20de%20enlace%20exterior): <https://aws.amazon.com/es/what-is/routing/#:~:text=Un%20protocolo%20de%20enrutamiento%20es,de%20puerta%20de%20enlace%20exterior>.
4. AWS. (s.f.). *¿Qué significa BGP? .* Obtenido de Explicación del Protocolo de Puerta de Enlace Fronteriza en Redes - AWS.: <https://aws.amazon.com/es/what-is/border-gateway-protocol/>
5. AWS., W. y. (s.f.). *Amazon Web Services, Inc.* Obtenido de <https://aws.amazon.com/es/compare/the-difference-between-lan-and-wan/>
6. *Black Box Mexico*. (s.f.). Obtenido de Cable de fibra óptica multimodo vs. monomodo: <https://www.blackbox.com.mx/mx-mx/page/28535/Recursos/Technical/black-box-explica/Fibre-Optic-Cable/Cable-de-fibra-optica-multimodo-vs-monomodo>
7. Brad Edgeworth, R. G. (2020). *CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide*. Cisco Press.
8. Brad Edgeworth, R. G. (2020). *CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide*. En R. G. Brad Edgeworth, *CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide*. Cisco Press.

9. Cabarcas Martínez, A., & Marrugo Castro, A. (2008). *Diseño y arquitectura de redes wan*.
10. Cisco. (2014). *Cómo Comprender VLAN Trunk Protocol (VTP)*. Obtenido de <http://www.cisco.com>
11. CISCO. (18 de Marzo de 2015). *Bidirectional forwarding detection*. Obtenido de Bidirectional forwarding detection.: https://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/fs_bfd.html#wp1199384
12. CISCO. (6 de Julio de 2021). *Cisco*. Obtenido de Cisco: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/vdc/config/cisco_nexus7000_vdc_config_guide_8x/overview.html
13. Cisco. (19 de Abril de 2022). *Cisco Nexus 7000 Series NX-OS*. Obtenido de Cisco Nexus 7000 Series NX-OS: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/7_x/nx-os/release/notes/7x_nx-os_release_note.html#pgfId-1418241
14. Cisco. (3 de Diciembre de 2023). *Apertura De La Ruta Más Corta Primero (OSPF): Guía De Diseño*. Obtenido de <https://www.cisco.com>: Apertura de la ruta más corta primero (OSPF): guía https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/7039-1.html
15. Cisco 40GBASE QSFP Modules Data Sheet. (2 de Mayo de 2022). *CISCO*. Obtenido de CISCO: https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-660083.html
16. Cisco Nexus 7700 6-Slot Switch. (16 de Diciembre de 2021). *Cisco*. Obtenido de Cisco: <https://www.cisco.com/c/en/us/products/switches/nexus-7700-6-slot-switch/index.html>

17. Cisco Nexus 7700 F3-Series 24-Port 40 Gigabit Ethernet Module Data Sheet. (2 de Marzo de 2017). CISCO. Obtenido de CISCO: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/data_sheet_c78-728410.html
18. Cisco Nexus 7700 Supervisor 2E Module Data Sheet. (13 de Enero de 2016). CISCO. Obtenido de CISCO: www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/data_sheet_c78-728591.html
19. Diferentes tipos de fibra óptica | Grupo COFITEL. (n.d.). (s.f.). *Diferentes tipos de fibra óptica*. Obtenido de Diferentes tipos de fibra óptica: <https://www.c3comunicaciones.es/diferentes-tipos-de-fibra-optica/>
20. HUAWEI. (15 de Enero de 2020). *Que es y Cómo Funciona OSPF (Open Shortest Path First) Parte 1*. Obtenido de <https://forum.huawei.com/enterprise/es/que-es-y-como-funciona-ospf-open-shortest-path-first-parte-1/thread/667218535828570112-667212882523336704>
21. IBM. (F. de S.). *Routing open shortest path first*. Obtenido de IBM documentation: <https://www.ibm.com/docs/es/i/7.2?topic=routing-open-shortest-path-first>
22. IPCISCO. (Junio de 9 de 2023). *BFD (Bidirectional Forwarding Detection)*. Obtenido de BFD (Bidirectional Forwarding Detection): <https://ipcisco.com/lesson/bfd/>
23. JM, C. (s.f.). *UDLD – UniDirectional Link Detection*. Obtenido de UDLD – UniDirectional Link Detection: <https://www.jmcristobal.com/es/2021/01/18/udld/>
24. Marcelo. (2020). *Introducción a OSPF*. Obtenido de CCNA desde Cero: <https://ccnadesdecero.com/curso/ospf/>

25. Molenaar, R. (2015). *How to Master CCNP ROUTE*. Idaho, USA: Click Sales, Inc.
26. Molenaar, R. (19 de Mayo de 2020). *Bidirectional Forwarding Detection (BFD)*. . Obtenido de NetworkLessons.com: <https://networklessons.com/cisco/ccie-routing-switching/bidirectional-forwarding-detection-bfd>
27. Netalit. (16 de Mayo de 2023). *What is the Border Gateway Protocol (BGP)*. Obtenido de <https://www.checkpoint.com>: <https://www.checkpoint.com/es/cyber-hub/network-security/border-gateway-protocol/>
28. Pavón, B. C. (2012). *Diseño de una red WAN para una compañía nacional*. UOC, Integración de redes telemáticas ETT Telemática.
29. Protected, E. (s.f.). *¿Qué es la fibra óptica? y su funcionamiento*. Obtenido de Fibras Ópticas de México: <https://fibrasopticasdemexico.com/que-es-la-fibra-optica-y-su-funcionamiento/>
30. Rubio, R. D. (14 de Noviembre de 2016). *¿Qué es un CPD, centro de Proceso de Datos o data Center?* . Obtenido de Soluciones e infraestructuras Tecnológicas.: <https://unitel-tc.com/que-es-cpd-centro-proceso-datos-data-center/>
31. Santos, O., & Stuppi, H. (2015). *CCNA Security 210-260*. Indianapolis, In: Pearson Education, Inc.
32. Sepulveda, M. (5 de Febrero de 2023). *Tipos de enrutamiento*. Obtenido de eClassVirtual - Cursos Cisco en línea: <https://eclassvirtual.com/tipos-de-enrutamiento/>
33. Tolosa, G. (2014). *Protocolos y modelo OSI*. Obtenido de Protocolos y modelo OSI: <http://www.tyr.unlu.edu.ar/TYR-publica/02-Protocolosy-OSI>.
34. Walton, A. (15 de Febrero de 2018). Obtenido de CCNA desde Cero: <https://ccnadesdecero.es/enrutamiento-routing-dinamico/>

35. Walton, A. (17 de Enero de 2020). *CCNA desde cero*. Obtenido de ¿Qué es el protocolo BGP?: https://ccnadesdecero.es/bgp-border-gateway-protocol/#2_Como_funciona_BGP
36. Walton, A. (19 de Octubre de 2022). *Tipos comunes de redes (LAN, WAN)*. Obtenido de CCNA desde cero. CCNA desde Cero: <https://ccnadesdecero.es/tipos-redes-informaticas-lan-wan-man/>
37. Wendell Odom. (2013). CISCO CCENT /CCNA ICND1 100-101 Official Cert Guide. Indianapolis, IN: Pearson Education, Inc.
38. Wendell Odom. (2013). CISCO CCNA Routing and Switching ICND2 200-101 Official Cert Guide. Indianapolis, IN: Pearson Education, Inc.
39. Omar Santos y Hohn Stuppi. (2015). CCNA Security 210-260. Indianapolis, In: Pearson Education, Inc.

Anexos.

Como parte de los requisitos para el proceso de titulación por estancias a continuación se comparten los anexos A, B, C Y D.

1. Anexo A contienen la carta de antigüedad de recursos humanos.
2. Anexo B Carta de autorización de jefe inmediato.
3. Anexo C primer recibo de nómina.
4. Anexo D último recibo de nómina.

Anexo A

**BBVA AXIAL TECH,
S.A. DE C.V.**

Ciudad de México a 17 de Julio de 2023

ING. RIGOBERTO SALINAS CORTES - JEFE DE DIVISIÓN SIC TESCO PRESENTE

Por medio de la presente nos es grato presentar al Sr(a). CARLOS HERNANDEZ MENESES quien forma parte del personal de la empresa BBVA AXIAL TECH, S.A. DE C.V. desde el 15 de Abril de 2019 a la fecha.

Actualmente se encuentra en el Departamento de BATCH & DATABASES desempeñando el puesto de INFRASTRUCTURE SENIOR EXPERT BUSINESS EXECUTION I MX 5.

Expedimos la presente a petición del Sr.(a) HERNANDEZ MENESES para los fines que juzgue convenientes.

Atentamente



RECURSOS HUMANOS

**BBVA AXIAL TECH, S.A. DE C.V.
LAGO ALBERTO #320, COLONIA ANÁHUAC I SECCIÓN, CP. 11320
DEL MIGUEL HIDALGO, CIUDAD DE MÉXICO**

AUTENTICIDAD: 153f263e1c8f2718c932c032891fda59

Anexo B



Ciudad de México a 12 de Junio de 2023.

A quien corresponda:

PRESENTE:

Por medio de la presente les informo que el C. Carlos Hernandez Meneses quien forma parte del proyecto IaaS-Networking América en Arquitectura Global Deployment bajo la dirección de Engineering en BBVA, desempeña las siguientes funciones dentro del equipo las cuales enlisto a continuación:

- Implementa Tecnología de los fabricantes de Telecomunicaciones Cisco, F5, Infoblox en el CCR (Centro de Cómputo Regional/Engineering) TIER 4, ubicados en el Estado de México, Monterrey y Querétaro, donde se almacenan las cargas de trabajo (servicios internos, servicios externos, aplicaciones para los clientes) de la región de América.
- Implementa tecnologías de nube pública como AWS, manteniendo el esquema híbrido del centro de datos.
- Administración y soporte a las diferentes tecnologías de TI : Cisco "ACI", F5 "Load Balancer", Infoblox "DNS", Red Hat "Virtual Machine".
- Automatización de tareas scripting/shell de Networking con Ansible
- Implementa herramientas de monitoreo Check_mk y Telegraf para detectar incidentes en la infraestructura
- Análisis de flujos de tráfico, troubleshooting con herramientas de analítica con cisco Tetration
- Atención de incidentes en el CCR
- Actualización del sistema operativo de toda la infraestructura de Telecomunicaciones en el Data Center (Upgrade)
- Implementa nuevos proyectos de comunicación en los diferentes países de américa (Colombia, Argentina, Perú)

Expendo la presente a petición del C. Carlos Hernandez Meneses para los fines que juzgue convenientes.

Atentamente,

Ing. Carlos Soto Islas

Tech Manager - IaaS Networking America

CCR (Centro de Cómputo Regional/Engineering)

Movil. (55) 50 981147 e-mail: carlos.soto2.next@bbva.com

Tel. 52 55 56 21 34 34 - Ext 6354

Calz. Gral. Mariano Escobedo 303, Granada, Miguel Hidalgo 11520 Ciudad de México, CDMX, Planta 23, Torre Polanco BBVA

EMISOR

Nombre o Razón Social: BBVA AXIAL TECH

RFC: ATA0304299DA

Régimen Fiscal: 601

Tipo de comprobante: N - Nómina

Expedido en: 11320

RECIBO DE NOMINA

FOLIO FISCAL

FECHA EMISIÓN 2023-05-26T18:30:26

FECHA TIMBRE 2023-05-26T18:36:11

CERTIFICADO EMISOR

CERTIFICADO SAT

RECEPTOR

Nombre: CARLOS HERNANDEZ MENESES

RFC:

CURP:

Fecha de Ingreso: 2019-04-15

Fecha de Pago: 2023-05-30

Fecha Inicial de Pago: 2023-05-16

Registro:

NSS IMSS:

Días: 16

Quincena: 10

Fecha Final de Pago: 2023-05-31

CANTIDAD	UNIDAD DE MEDIDA	DESCRIPCIÓN	OBJETO DE IMPUESTO	CLAVE DE SERVICIO	CLAVE DE UNIDAD	PRECIO UNITARIO	SUBTOTAL
1		Pago de nómina	01	84111505	ACT		
Tipo de cambio: Moneda: MXN Condiciones de pago: Uso de CFDI Receptor: CN01 - Nómina Forma de pago: Método de pago: PUE Régimen fiscal Receptor: 605 - Sueldos y Salarios e Ingresos Asimilados a Salarios Código postal de Domicilio fiscal: 11520 Exportación: 01 - No aplica							

PERCEPCIONES			
Concepto	Gravado	Exento	Total
Sueldo {16 dias}		0.00	
Retroactivo Prima Vacaciones		0.00	
Compensacion extraordinaria por unica vez		0.00	
Cuotas Obrero IMSS pagadas por el Patron	0.00		
Cuotas Obreras CYV pagadas por el Patron	0.00		
Subtotal			

SUBSIDIO AL EMPLEO	
Subsidio Causado	0.00

DEDUCCIONES			
Concepto	Gravado	Exento	Total
ISR	0.00		
Subtotal	0.00		

EMISOR

Nombre o Razón Social: BBVA AXIAL TECH

RFC: ATA0304299DA

Régimen Fiscal: 601

Tipo de comprobante: N - Nómina

Expedido en: 11320

RECIBO DE NOMINA

FOLIO FISCAL

FECHA EMISIÓN2024-05-28T18:30:19

FECHA TIMBRE2024-05-28T18:36:47

CERTIFICADO EMISOR

CERTIFICADO SAT

RECEPTOR

Nombre: CARLOS HERNANDEZ MENESES

RFC:

CURP:

Fecha de Ingreso: 2019-04-15

Fecha de Pago: 2024-05-30

Fecha Inicial de Pago: 2024-05-16

Registro:

NSS IMSS:

Días: 16

Quincena: 10

Fecha Final de Pago: 2024-05-31

CANTIDAD	UNIDAD DE MEDIDA	DESCRIPCIÓN	OBJETO DE IMPUESTO	CLAVE DE SERVICIO	CLAVE DE UNIDAD	PRECIO UNITARIO	SUBTOTAL
1		Pago de nómina	01	84111505	ACT		
Tipo de cambio: Moneda: MXN Condiciones de pago: Uso de CFDI Receptor: CN01 - Nómina Forma de pago: Método de pago: PUE Régimen fiscal Receptor: 605 - Sueldos y Salarios e Ingresos Asimilados a Salarios Código postal de Domicilio fiscal: 11520 Exportación: 01 - No aplica							

PERCEPCIONES			
Concepto	Gravado	Exento	Total
Sueldo {16 días}		0.00	
Retroactivo Prima Vacaciones		0.00	
Compensacion extraordinaria por unica vez		0.00	
Ingreso en Servicio IVA Interes Consumo {2147483647}		0.00	
Ingreso en Servicio Interes Consumo		0.00	
Cuotas Obrero IMSS pagadas por el Patron	0.00		
Cuotas Obreras CYV pagadas por el Patron	0.00		
Pago de Servicios Teletrabajo	0.00		
Subsidio para el empleo pagado	0.00	0.00	0.00
Subtotal			

SUBSIDIO AL EMPLEO	
Subsidio Causado	0.00

DEDUCCIONES			
Concepto	Gravado	Exento	Total
ISR	0.00		
Comedor 1era Mayo {1}	0.00		
Prima de Seguro de Grupo Temporal	0.00		
Cuotas Obrero IMSS pagadas por el Patron	0.00		
Cuotas Obreras CYV pagadas por el Patron	0.00		
Subtotal	0.00		

Total:

CADENA ORIGINAL:

SELLO DIGITAL EMISOR:

SELLO DIGITAL SAT: