UNIVERSIDAD NACIONAL DEL CALLAO

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

TESIS

"DISEÑO DE UNA GESTIÓN CENTRALIZADA Y AUTOMATIZACIÓN DE LA RED LAN UTILIZANDO LA SOLUCIÓN CISCO SD-ACCESS EN UNA EMPRESA DE AERONAVEGACIÓN"

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO

AUTORES:

BACH. CHARA CONOCC, JUAN VICTOR ALBERTO

BACH. SAN MARTIN SORIA, FRANCO RENATO

ASESOR:

MSc. Ing. WILBERT CHAVEZ IRAZABAL

Callao – 2022

PERÚ

HOJA DE REFERENCIA DEL JURADO Y APROBACIÓN

PRESIDENTE : Dr. Ing. JACOB ASTOCONDOR VILLAR

SECRETARIO : MSc. Ing. JULIO CÉSAR BORJAS CASTAÑEDA

VOCAL : MSc. Ing. RUSSELL CÓRDOVA RUIZ

ASESOR : MSc. Ing. WILBERT CHÁVEZ IRAZÁBAL

DEDICATORIA

Yo Franco San Martin Soria dedico este trabajo a mis padres por siempre brindarme su apoyo incondicional y creer en mi desde el primer día que decidí estudiar esta hermosa carrera sacándome adelante a pesar de las adversidades, a mi hermana por sus consejos y su influencia en mi crecimiento como persona y profesional en el que me he convertido.

Yo Juan Víctor Alberto Chara Conocc dedico con todo mi corazón esta tesis a mi padre y madre pues sin ellos no lo habría logrado, ya que siempre me apoyaron en toda mi etapa universitaria, me aconsejaron cuando tenía dudas y me ayudaron a seguir adelante cuando se presentaba alguna dificultad. Gracias a ellos es que soy el profesional que soy ahora.

ÍNDICE

ÍNDICE DE CUADROS

ÍNDICE DE ILUSTRACIONES

RESUMEN

En la actualidad existen diversas soluciones de redes definidas por software tanto de código abierto como licenciado para el control total de la red LAN, el presente proyecto tiene como finalidad remplazar una infraestructura tradicional de red con la cual se venía administrando los servicios corporativos de una empresa de aeronavegación y facilitar a los administradores de red la gestión de la misma de manera inteligente e intuitiva.

El objetivo principal de esta tesis consiste en implementar una solución de redes definidas por software (SDN) para una red LAN de empresa de aeronavegación y otorgar al administrador de red una gestión centralizada y automatizada de la red lo cual se verá reflejado en la velocidad de realizar troubleshooting y el ingreso de manera segura a la red LAN.

Para la obtención del objetivo general de la investigación se tomó la decisión de implementar la solución SD-Access de Cisco entre una gran gama de soluciones SDN por su nivel de desarrollo constante y seguro por parte de la empresa CISCO. Previamente se realizó un estudio para la elección de los mejores dispositivos a utilizar en la solución mencionada basada en su nivel compatibilidad y capacidad.

Los resultados de la implementación muestran una manera eficiente de administrar la red LAN a nivel empresarial mediante la solución SD-Access por lo cual resulta importante su futura implementación y estudio para automatizar las redes en las distintas empresas de manera que se le permita tener un dominio total y seguro sobre toda la red interna.

Palabras claves: SD-Access, troubleshooting, automatizada, SDN.

ABSTRACT

Currently there are various software-defined network solutions both open source and licensed for total control of the LAN network, the present project aims to replace a traditional network infrastructure with which the corporate services of a company had been administered. of air navigation and make it easier for network administrators to manage it in an intelligent and intuitive way.

The main objective of this thesis is to implement a software-defined network (SDN) solution for an aircraft company LAN network and provide the network administrator with a centralized and automated management of the network, which will be reflected in the speed of perform troubleshooting and secure access to the LAN.

In order to obtain the general objective of the research, the decision was made to implement the Cisco SD-Access solution among a wide range of SDN solutions due to its constant and secure level of development by the CISCO company. Previously, a study was carried out to choose the best devices to use in the aforementioned solution based on their level of compatibility and capacity.

The results of the implementation show an efficient way to manage the LAN network at a business level through the SD-Access solution, which is why its future implementation and study is important to automate the networks in the different companies so that it is allowed to have a domain total and secure over the entire internal network.

Keywords: SD-Access, troubleshooting, automated, SDN.

INTRODUCCIÓN

El presente plan de trabajo tiene la finalidad de desarrollar el diseño de la solución SD-Access de CISCO que nos permitirá obtener una gestión centralizada y automatizada de la red LAN (Local Área Network) en este caso para una empresa de aeronavegación, para así poder solucionar los diferentes problemas tales como acceso y la escalabilidad de la infraestructura actual de forma más eficaz y al mismo tiempo nos permitirá reemplazar la red tradicional actual por una red inteligente que dote información precisa al administrador de la red para una facilidad en el diagnóstico de problemas que podrían causar un gran impacto en los usuarios y con esto una disminución en el desempeño de sus funciones. La gestión de las redes tanto cableada como inalámbrica se ha vuelto una prioridad en las empresas debido a que toda la información se transmite por dichos medios y por lo tanto se necesita mantener segura esa información del cual depende sus ganancias.

La escalabilidad es una propiedad importante a desarrollar en las redes LAN debido a que una empresa siempre busca su crecimiento continuo y de la mano a ese crecimiento tenemos que llevar la tecnología, por eso SD-Access nos permite automatizar las políticas de acceso a los usuarios y entregar a estos usuarios una experiencia estable en toda la red sin comprometer su seguridad.

Los beneficios que nos entrega implementar una infraestructura basada en SD-Access es una visibilidad de toda la red y poder transformar los datos de la misma para los fines más convenientes en cuanto a planificación; Por eso nosotros aprovecharemos de las virtudes que nos brinda tener una red centralizada y automatizada para obtener el mayor beneficio en cuanto a la reducción de tiempo para el acceso y ahorro de personal encargado del monitoreo de la red LAN para la empresa.

I. PLANTEAMIENTO DEL PROBLEMA

En el mundo entero las redes de telecomunicaciones proporcionan el acceso para la comunicación entre personas de distintas zonas geográficas que permite realizar un intercambio de información evitando las barreras de distancia, así también la importancia que hay en tener una red optima que permita esa comunicación fluida a través de los distintos medios comunicación alámbricos e inalámbricos.

En el Perú exactamente en una empresa de aeronavegación se es de manera sumamente importante la disponibilidad de una red segura y administrada de tal forma que permita a los usuarios realizar sus labores con total libertad y tener el control de cualquier dispositivo conectado dentro de la red corporativa que pueda causar algún perjuicio en el desarrollo de las labores de las distintas especialidades ubicadas en esta empresa de aeronavegación.

1.1. Descripción de la Realidad Problemática

Debido a la falta de gestión centralizada y automatización de la red LAN tradicional en una empresa de aeronavegación existen diversos problemas en cuanto a escalabilidad y acceso a la red, por ejemplo, cualquier dispositivo puede ser conectado a los puertos de los equipos de comunicación de la infraestructura de red para obtener un acceso a la red interna lo que no es óptimo tratándose de una empresa tan importante que ve el tráfico aéreo a diario.

En una red tradicional los switches cuentan con ciertas políticas para sus determinados puertos lo que no es de todo bueno ya que los usuarios suelen cambiar de ubicación por distintos factores y esto ocasiona una falta de control sobre esos equipos que acceden a la red sin antes comunicar los cambios, lo que lleva reorganizar la red cada vez que se realice este cambio así como también resulta casi imposible monitorear el tráfico de red de cada dispositivo individualmente para comprobar si se encuentran haciendo una actividad inusual a lo estipulado en el área de desempeño. También existe inconvenientes a la hora de ejercer escalabilidad sobre la red tradicional actual debido a que conlleva mucho tiempo en configurar cada equipo nuevo que se desea añadir a la red además de un gasto económico en personal especializado dedicado a la configuración de los diversos equipo a incorporar, con el tiempo esta red resulta cada vez más difícil de administrar por la gran cantidad de equipos pertenecientes a la

infraestructura de red y esto significa una pérdida de control a medida que vaya creciendo nuestra red.

SD-Access nos va permitir mejorar esos tiempos de configuración en lo que respecta a escalabilidad y automatización debido a que el control central nos brinda una visión de la red bien clara, especifica y detallada, además mejora los tiempos de respuesta ante los posibles problemas internos por los usuarios, nos permite administrar la red como un todo y nos brinda mayor seguridad al momento de segmentar la red y aprovechar la infraestructura.

Por todo lo mencionado resulta interesante la implementación de SD-Access en la Red LAN de una empresa de aeronavegación para mejorar la escalabilidad de la red y brindad un conocimiento de implementación a las futuras investigaciones.

1.2. Formulación del Problema

A manera de organizar la investigación se plantea el problema general y problemas específicos.

1.2.1. Problema General

¿Cómo el diseño de la solución SD-ACCESS gestiona de manera centralizada y automatizada la red LAN de una empresa de aeronavegación?

1.2.2. Problema especifico

- ¿Cómo la solución SD Access integra a los nuevos dispositivos de la red LAN en una empresa de aeronavegación?
- ¿Cómo optimizar la seguridad en la red LAN con la solución SD-Access?
- ¿Cómo administrar de manera centralizada la red LAN utilizando DNA CENTER?

1.3. Objetivos de la investigación

1.3.1. Objetivo General

Diseñar la solución SD Access para gestionar centralizadamente y automatizada la red LAN en una empresa de aeronavegación.

1.3.2. Objetivos Específicos

- Diseñar la infraestructura de red con la solución SD-Access de CISCO.
- Determinar políticas de seguridad conforme a los estándares de CISCO.
- Diseñar un control centralizado basado en los 3 niveles del fabricante (CORE, DISTRIBUTION, EDGE).

1.4. Limitantes de la investigación

- Una limitación que se presentó es que no se tenía permisos y accesos a ciertas zonas donde se necesitaran instalar los equipos, así que se necesitó tramitar los permisos y accesos a las áreas para la implementación final de proyecto.
- Al revisar como estaba diseñada la RED anterior, nos percatamos que muchos equipos de distintas redes están pasando por la VLAN 1, lo cual generó desorden con el nuevo diseño que se implementó.
- La migración física de los nuevos equipos de red llevo determinadas ventanas de tiempo para lo cual se tuvo que realizar cortes totales en la comunicación de los usuarios por rangos de horas, lo que generó demora en la implementación debido a que estas ventanas de tiempo eran programadas por la empresa de aeronavegación.

II. MARCO TEÓRICO

2.1. Antecedentes

2.1.1. Antecedentes nacionales

- Rodríguez (2020) en su tesis “Diseño y simulación de una red definida por software para la implementación de un laboratorio avanzado de datos para la EP de Telecomunicaciones de la Facultad de Ingeniería Electrónica y Eléctrica de la Universidad Nacional Mayor de San Marcos”.

  RESUMEN: En la presente tesis, para obtener el título de Ingeniero de Telecomunicaciones, se estudia la arquitectura de una Red Definida por Software-SDN, tanto a nivel de hardware: equipos requeridos y función de cada uno de ellos, como a nivel de Interfaz de Programación de Aplicaciones-API northbound y southbound. Con el fin de proponer una arquitectura de Red Definida por Software-SDN para la implementación de un laboratorio avanzado de datos en la Facultad de Ingeniería Electrónica y Eléctrica-FIEE de la Universidad Mayor de San Marcos-UNMSM, el cual cuente con la opción de conectividad remota para poder realizar las actividades de laboratorio (tanto evaluaciones como ensayos) a distancia. La propuesta de SDN se sustenta en las simulaciones realizadas en Mininet, previo estudio de las especificaciones de esta arquitectura SDN.

  Esta tesis pretende ser el primer paso para una futura implementación de un laboratorio de Red Definida por Software en la Facultad de Ingeniería Electrónica y Eléctrica de la UNMSN y con esto dar el salto tecnológico que permita colocar a nuestra facultad y casa de estudios como referente en investigación a nivel nacional, teniendo un laboratorio que permita preparar a los estudiantes de la universidad acorde con las necesidades actuales de investigación y adaptabilidad al cambio tecnológico.

  CONCLUSIONES: Como consecuencia del análisis de las especificaciones técnicas que definen la arquitectura de una Red Definida por Software se ha propuesto y simulado el funcionamiento y comportamiento con tráfico IPv4 e IPv6 de una red SDN para la Facultad de Ingeniería Electrónica y Eléctrica de la Universidad Nacional Mayor de San Marcos que facilitara

la enseñanza de los alumnos y les permitirá afrontar los retos del ámbito profesional conociendo la tecnología a la cual se están dirigiendo las redes de datos de las compañías operadoras más importantes del país. Las simulaciones de la red SDN propuesta fueron realizadas usando la herramienta Mininet tanto para escenarios en IPv4 como IPv6: observándose que IPv6 es un 76.216 % superior en throughput para su prueba TCP con ventana optimizada (caso 6, figura 4.25, valor promedio 163 mbps) respecto al mismo parámetro en IPv4 (caso 2, figura 4.14, valor promedio 92.5 mbps). De los tres controladores usados HP VAN SDN, OpenDayLight y FloodLight, se seleccionó el OpenDayLight ya que ofrece más flexibilidad, posee mayor documentación y es open source, teniendo más módulos desarrollados que el FloodLight. En estos complicados momentos por la pandemia, es de vital importancia considerar la conexión remota al laboratorio tanto para los docentes como los alumnos. Es esencial que se empiecen a desarrollar aplicaciones en SDN en investigaciones posteriores, teniendo como base esta tesis.

- Chafloque (2018) en su tesis “Propuesta de diseño de una red de datos de área local bajo la arquitectura de redes definidas por software para la Red Telemática de la Universidad Nacional Mayor de San Marcos”.

  RESUMEN: La presente tesis tiene como objetivo brindar una propuesta de diseño de una red de datos de área local bajo una arquitectura de redes definidas por software (SDN – Software Defined Network en sus siglas en ingles) para mejor la eficiencia de la gestión e interoperabilidad entre los diferentes dispositivos o equipos de red que conforman la red de datos de área local (LAN – Lan Area Network en sus siglas en ingles) de la Red Telemática de la Universidad Nacional Mayor de San Marcos - UNMSM-.

  Se explicará el funcionamiento de la arquitectura de redes definidas por software, los protocolos y plataformas que son utilizadas para su desarrollo. Se presenta un análisis de la forma de gestión de la red LAN tradicionales, como lo es la Red Telemática, y la arquitectura de los dispositivos de red tradicionales.

La propuesta del diseño de red se realizará de forma simulada bajo el software Mininet, se explicará la topología a diseñar, así como la descripción del controlador SDN a utilizar y finalmente se presentarán las pruebas y resultados obtenidos de la simulación.

Con los resultados obtenidos se comparará los beneficios que brinda la arquitectura SDN con respecto a la red LAN actualmente implementada, presentando las conclusiones y recomendaciones del proyecto de investigación.

CONCLUSIONES: El simulador de red Mininet permitió diseñar de una red LAN bajo la arquitectura SDN para la Red Telemática de la UNMSM en un entorno de simulación usando el controlador Opendaylight. Se logró observar el potencial de las redes SDN incluso en un entorno de red virtualizado. Mininet permitió ejecutarlas aplicaciones, módulos y comandos del sistema Linux desde los hosts virtuales sin inconvenientes. Se pudo poner en evidencia que el controlador Opendaylight es capaz de administrar todos los dispositivos de red que tengan habilitado Openflow, además el controlador tiene la total visibilidad de la red de manera centralizada permitiendo una gestión unificada. Las redes definidas por software permitirían a la Red Telemática habilitar la programación de la red mediante distintas APIs de programación. En el caso particular del controlador Opendaylight, se utilizó el lenguaje de programación XML a través de RESTCONF. De esta manera, no fue necesario la configuración a nivel local del dispositivo de la red a través de línea de comandos permitiendo la posibilidad de cambiar los dispositivos de red actuales (con un comportamiento predefinido por el fabricante) por dispositivos que permiten ser programados según las necesidades del administrador. Los resultados obtenidos en las pruebas conectividad nos permiten concluir que el controlador Opendaylight puede manejar tráfico TCP y UDP. Una vez establecida la conexión y la instalación de las tablas de flujo en los switches, los tiempos de respuesta son menores con respecto a los primeros paquetes enviados. SDN brinda la oportunidad a los investigadores de desarrollar las líneas de investigación en el campo de la automatización de la red, seguridad de las redes de forma proactiva, convergencia en la red y desarrollo de aplicaciones proactivas de QoS. La configuración de los dispositivos de red por CLI no es escalable

y presentan inconvenientes de integración debido a la diversidad de sintaxis exclusiva de cada fabricante. Por otra parte, SDN proporciona APIs de programación dinámicos y fluidos entre el software y la infraestructura de red. SDN brindaría a la red telemática la posibilidad de mantener la integración a medida que la infraestructura de red evoluciona, reduciendo la complejidad operativa y costes mediante la reducción de la complejidad al usuario, y haciendo un uso más eficiente de los recursos de red existente. La automatización de la gestión y provisión de la red, a través de SDN, es la siguiente fase en la virtualización de la infraestructura de tecnologías de la información y las telecomunicaciones ya que permite crea una red inteligente mucho más abierta, flexible, escalable y reprogramable.

- Cuba & Becerra (2015) en su tesis “Diseño e implementación de un controlador SDN/OpenFlow para una red de campus académica”.

  RESUMEN: La presente tesis se encuentra dividida en 5 capítulos: El primer capítulo contiene una introducción a las redes de campus académicas, como es el caso de la red de la PUCP, y a la problemática presentada a través de la evolución de la tecnología Ethernet en las redes de área local (LAN) desde sus inicios, hasta la aparición del paradigma de redes SDN.

  El segundo capítulo contiene la definición del paradigma de redes SDN, así como también las bases para poder entender las tecnologías aplicadas y las plataformas utilizadas en el despliegue de este.

  En el tercer capítulo, se desarrollan los requerimientos a considerar en el diseño del controlador y las principales limitaciones y dificultades que se pueden encontrar. Finalmente, se explica la operación del controlador, detallando los mecanismos que se implementarán.

  En el cuarto capítulo se detalla los factores determinantes para la elección de la plataforma base de controlador y el diseño del mismo, en base a los requerimientos planteados en el capítulo 3.

Finalmente, en el quinto capítulo, se presentan las distintas pruebas de concepto utilizadas para poder determinar la funcionalidad de los módulos más importantes del controlador diseñado; así como también el modelo analítico, y el análisis respectivo, utilizado para poder medir la escalabilidad del mismo.

CONCLUSIONES: Se cumplió con el objetivo principal de la tesis, se diseñó un controlador OpenFlow escalable, y se implementó una prueba de concepto sobre la plataforma Floodlight. El controlador implementado es escalable en para el tráfico unicast, mediante el mecanismo usado por el módulo Clustering. Se demostró que usando este mecanismo se obtiene un 25% de uso en las TCAM de los Switches y en la capacidad del controlador. El Timeout de las Flow Entries determina influye directamente en el porcentaje de uso de las TCAM de los Switches y de la capacidad del controlador, y por lo tanto, en la escalabilidad del sistema. Cuando la distribución de destinos tiene una alta concentración en unos pocos hosts, se logra escalabilidad de las TCAM de los Switches de acceso respectivos mediante el módulo Circuit Tree. Bajo el nuevo esquema de subnetting, el tráfico Broadcast aumentará. Ante esto, el controlador provee los módulos para evitar tormentas de broadcast y saturación de enlaces. Además, se comprueba que este enfoque otorga la información necesaria para optimizar el enrutamiento. El controlador puede coexistir con elementos Legacy. Puede usarse para iniciar una migración a OpenFlow gradual. El diseño del controlador soporta una migración total de la Red PUCP a SDN, evitando así el uso de un Router centralizado y consecuentemente, las desventajas de la red actual que se indicaron en el capítulo 1.

2.1.2. Antecedentes internacionales

- Intriago (2017) en su tesis “Estudio del protocolo Openflow usando el modelo de red definida por Software (Software Define Networks). Caso de estudio la Universidad Técnica de Manabí”.

  RESUMEN: Las redes de comunicaciones han tenido un crecimiento exponencial de tráfico que circula por la red y cada día a un ritmo mayor, lo cual demanda de métodos de comunicación más eficiente. Se propone una solución que

permita cambiar la forma de comunicación de las redes, en la cual se le proporcione mayor inteligencia a la misma es así que nace la arquitectura de redes definidas por software.

Esta herramienta ha revolucionado las comunicaciones con el control de dispositivos desde un software exterior, con la ayuda del protocolo OpenFlow lo que le permite la programabilidad de las redes sin necesita que se exponga la estructura interna de los equipos de networking para esto se han desarrollado herramientas para su experimentación para esta tesis se utiliza el emulador Mininet y el software OpenDaylight para la creación de los escenarios prácticos.

Teniendo en cuenta que esta arquitectura SDN en nuestro país es reciente en esta investigación de la tecnología del protocolo OpenFlow, se ha buscado información sobre sus características, funcionalidad, arquitectura, plataformas de desarrollo, para esta tesis se desarrollaron escenarios prácticos utilizando Mininet y OpenDaylight para la prueba de esta herramienta.

El efecto de la virtualización de servidores es que los flujos de tráfico difieren sustancialmente del modelo tradicional de cliente-servidor. Por lo general, existe una cantidad considerable de tráfico entre los servidores virtuales, para fines tales como el mantenimiento de imágenes consistentes de la base de datos y la invocación de funciones de seguridad como el control de acceso. Estos flujos de servidor a servidor cambian en ubicación e intensidad a lo largo del tiempo, lo que exige un enfoque flexible para administrar los recursos de la red.

Mediante la realización de este proyecto se pretende una descripción de SDN, teniendo como protagonista al protocolo OpenFlow y su aplicación mediante el diseño del escenario virtual sobre la herramienta Mininet y OpenDaylight que soporte este protocolo, en la red académica de la Universidad Técnica de Manabí el cual permitirá realizar un diseño de la red definida por software permitiendo mejorar la administración y el tráfico de la red.

Al Realizar un proyecto de esta magnitud será de gran aporte y nos dará una visión diferente al momento de construir redes, porque con las redes definidas por software SDN openflow, ya

no es necesarios el hardware sino el software el encargado de controlar la red obteniendo de esta manera que la evolución de las redes se realice a la misma velocidad que se desarrolla el software logrando la reutilización de código para dar solución a una alternativa abaratando costos de implementación y no estar limitado a utilizar equipos de un mismo fabricante.

CONCLUSIONES: Una vez finalizado el trabajo se concluye: Luego de una exhaustiva investigación se logró conocer a cabalidad el protocolo Openflow, comprobando los resultados de la aplicación en la herramienta SDN, con la utilización de dicha arquitectura permitirá el mejoramiento de las redes en la comunidad universitaria, asegurando así una comunicación eficaz entre las facultades y departamentos administrativos. La realización del estudio efectuado con la arquitectura del SDN permitió que los dispositivos conectados mediante la red, controlan remotamente las tablas de reenvió en una red de switches y routers, permitiendo así automatizar y controlar las redes altamente escalables y flexibles, que se adaptan rápidamente a los requerimientos de la institución. SDN y Openflow representa una revolución en el mundo de las redes de comunicaciones, como vemos en estas investigaciones las empresas que han implementado Google, Cisco, Huawei, Hp, empiezan a confiar cada día más en estas nuevas tecnologías porque son el futuro de las redes al permitir aprovechar mejor los recursos de las tecnologías actuales. Finalmente se ha probado el software de emulación Opendaylight y Mininet siendo una herramienta orientada a demostrar de manera sencilla y educativa las principales características de OpenFlow y el modo en el que interactúan sus diferentes elementos de red, sobre todo al controlador en este estudio, se realizaron tres escenarios similares a las redes de comunicaciones de la universidad, con lo que se demostró que estas herramientas pueden facilitar una mejor administración de nuestra red.

- Núñez (2015) en su tesis “Red Definida por Software (SDN) en base a una infraestructura de software de libre distribución”.

  RESUMEN: La presente investigación tiene como objetivo estudiar las redes definidas por software mediante el análisis de los diferentes aspectos que componen esta nueva arquitectura, llegando a diseñar e implementar un prototipo de red tanto con

dispositivos diseñados para trabajar con el protocolo OpenFlow como con aquellos que pueden ser habilitados para este propósito.

El estudio de esta nueva tecnología se debe a la gran demanda de servicios de red con mejor calidad, siendo esta la causa de que la mayoría de las empresas de redes estén reestructurando sus arquitecturas con el objetivo de dar cabida a una nueva propuesta que permita solucionar los problemas generados sin afectar totalmente sus infraestructuras.

Gracias a que se trata de una tecnología de código abierto se espera un gran desarrollo de la misma, con el propósito de encontrar soluciones que permitan minimizar costos de implementación y dejar de lado la dependencia de servicios de un solo fabricante de dispositivos de red, solucionando así problemas de incompatibilidad.

CONCLUSIONES: Al finalizar el presente proyecto de titulación se obtuvieron las siguientes conclusiones: Las redes definidas por software surgen debido a la incapacidad de las redes convencionales de permitir cambios en los patrones de tráfico de forma dinámica, mediante la adición, eliminación o modificación de reglas de flujo en los dispositivos de interworking que soporte OpenFlow. Previo a la implementación del prototipo de red se llevó a cabo la actualización del firmware del router TP-LINK modelo TL-WR1043ND Versión 2.1 concluyendo que esta versión del router si soporta OpenFlow. Al utilizar los controladores evaluados en el proyecto, se pudo concluir que Floodlight presenta mejores características que Beacon, debido a su facilidad para crear nuevos módulos, agregar dependencias y utilizar librerías. Además, presenta el servicio Rest Api para interactuar con los módulos del controlador en forma remota.

2.2. Bases Teóricas

2.2.1. Gestión Centralizada de una Red LAN

Desde los últimos años las empresas están intentando hacerse con un abanico de herramientas que les permitan conseguir una gestión más centralizada.

La característica de la gestión centralizada permite que usted maneje y configure los múltiples dispositivos al mismo tiempo, para proporcionar la mayor confiabilidad, flexibilidad y escalabilidad dentro de su Red, permitiendo que usted maneje de manera global mientras que cumple con las políticas locales.

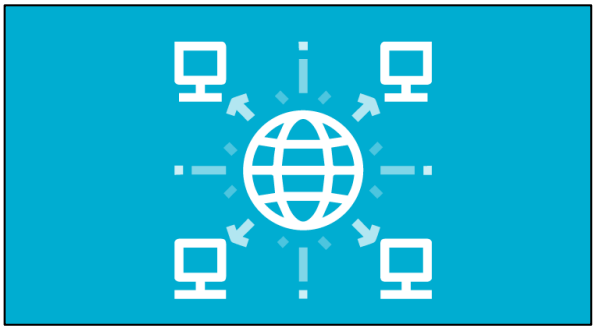

Figura 1 - Ilustración de Gestión Centralizada
Fuente: https://ehorus.com/es/gestion-centralizada/.

Principales ventajas de una Gestión Centralizada:

- Ahorro de tiempos:
  Esta es la principal ventaja al gestionar servicios de forma centralizada, ya que, si se desea configurar ciertos permisos en ciertos equipos en un esquema descentralizado, debería acudir equipo por equipo aplicando los cambios. En una red extensa (de 100 a 2000 equipos) este trabajo puede llevar incluso varios días. Sin embargo, si se gestiona desde un único servidor es posible realizar la tarea en unos pocos minutos.

- Mayor Seguridad:
  Al controlar todo desde un único punto de gestión, se minimiza la probabilidad de errores o configuraciones erróneas. Si un empleado debe visitar equipo por equipo para, por ejemplo, aplicar una configuración, puede ocurrir que se cometa un error al repetir una tarea tantas veces o incluso puede ocurrir que un equipo sea omitido. Con la gestión centralizada, se optimiza la

seguridad de los sistemas al ser más sencillo poder asegurar que todo “está como debe estar”.

- Mayor capacidad de análisis:
  Si se desea conocer cierta información sobre un servicio es posible obtenerla directamente desde el servidor, optimizando la capacidad de análisis. Suponga, por ejemplo, utilizar un servidor de red para verificar qué usuarios han usado los distintos aplicativos en la última semana. En cuestión de minutos puede obtenerse dicha información.

- Organizar los equipos en grupos:
  Independientemente de su ubicación física, es posible organizar los equipos en grupos, por ejemplo, según el departamento del que son parte, y así poder aplicar configuraciones específicas según los parámetros que se desee la empresa.

2.2.2. Automatización de una Red LAN

La automatización de la red utiliza la lógica programable para gestionar los servicios y los recursos de red. Permite que los equipos de operaciones de red configuren, ajusten, protejan e integren la infraestructura de red y los servicios de aplicaciones más rápido que cuando los usuarios lo hacen de forma manual. Elimina los pasos manuales que se necesitan para gestionar las redes, como iniciar sesión en enrutadores, conmutadores, equilibradores de carga y firewalls para cambiar las configuraciones manualmente antes de cerrar sesión. Este proceso se basa en scripts encadenados que se programan en la interfaz de la línea de comandos (CLI) de un sistema operativo (SO) o de un software de automatización definido previamente.

Figura 2 - Referencia a la Automatización en Redes
Fuente: https://www.auraquantic.com/es/guia-practica-para-la-automatizacion-de-procesos/.

La automatización consiste en usar la tecnología para realizar tareas, sin necesidad de una persona. La automatización de la TI se basa en el uso de sistemas de software para crear instrucciones y procesos repetibles, a fin de reemplazar o reducir la interacción humana con los sistemas de TI. El software de automatización funciona dentro de los límites de esas instrucciones, herramientas y marcos, para realizar las tareas con muy poca o sin ninguna intervención humana.

Figura 3 - Ilustración de la poca interacción humana en Redes Actuales. Fuente: https://www.ansible.com/products/automation-platform.

Es conveniente automatizar las redes, ya que, a pesar de que las tecnologías subyacentes han evolucionado, la gestión de las redes lleva décadas sin sufrir grandes cambios. Las redes por lo general se crean, operan y mantienen de forma manual. Sin embargo, los enfoques manuales tradicionales para la configuración y las actualizaciones de la red son demasiado lentos y propensos a errores para respaldar de forma efectiva las necesidades de las cargas de trabajo, que cambian rápidamente. Cuando se automatizan la gestión de servicios y los recursos de red, los equipos de operaciones de red adquieren más agilidad y flexibilidad para respaldar las demandas empresariales modernas de manera eficiente.

Para entender el correcto funcionamiento de la automatización de la red, tenemos que entender lo siguiente. No solo hay muchas maneras de automatizar una red, sino también muchos elementos de red que pueden automatizarse. La mayoría de las soluciones de automatización de la red se encuentran entre dos extremos: la automatización de la línea de comandos y el software de automatización.

En principio, puede automatizar los elementos de red mediante comandos y argumentos de CLI estándar. Por ejemplo, los administradores del sistema operativo Linux pueden utilizar operadores de Bash para encadenar eventos en función de los aciertos o los errores de los comandos anteriores. O bien, los usuarios podrían compilar listas de comandos en archivos de texto, conocidos como scripts de shell, que pueden tener lugar todos a la vez y reiteradamente con un solo comando de ejecución.

Figura 4 - Representación de la Interfaz de Línea de Comandos.
Fuente: https://pc-solucion.es/wp-content/uploads/2018/05/que-es-el-cli.jpg.

Los productos de software de automatización consolidan las tareas de red en programas predefinidos que se pueden seleccionar, programar y ejecutar desde el frontend de la aplicación. Por ejemplo, es posible utilizar algunos programas ya conocidos por los administradores de red para automatizar las redes y sus permisos. Para ello, las interfaces de programación de aplicaciones (API), los plugins, los inventarios y los módulos se empaquetan en playbooks que los usuarios pueden analizar, seleccionar y ejecutar para automatizar actividades como la configuración de la red, la seguridad, la organización de sistemas y la implementación, entre otras, en proveedores de servicios como AWS, Microsoft y Cisco.

Figura 5 - Representación del uso de un Software de Automatización en Redes.
Fuente: https://www.redhat.com/es/solutions/it-automation.

El proceso de automatización de la red se dio debido a que, la configuración manual de la red puede generar falta de uniformidad, configuraciones erróneas e inestabilidad de la red, lo cual entorpece la capacidad de prestar un servicio con el alto nivel que requieren las operaciones empresariales digitales. Gracias a la automatización, podrá estandarizar los procesos de gestión de la red para aplicar las prácticas recomendadas. Los equipos de operaciones de red pueden prestar servicios según sea necesario de forma rápida y sencilla, así como reducir el tiempo medio de resolución (MTTR) de las interrupciones del servicio. Además, para poder optimizar el rendimiento y los costos, es necesario equilibrar las cargas de las aplicaciones en toda la infraestructura. El bajo rendimiento de las aplicaciones y las demoras en la conmutación por error cuando surgen problemas en el sistema son consecuencias del manejo manual de estas cargas. Sin embargo, gracias a la automatización, se elimina la necesidad de la intervención manual, lo cual permite efectuar la conmutación por error y realizar ajustes constantes con mayor rapidez para mejorar el rendimiento y la confiabilidad de las aplicaciones.

Si bien los proveedores de servicios de telecomunicaciones fueron de los primeros en adoptar la automatización de la red para mejorar las redes digitales, las empresas de todos los sectores pueden beneficiarse con esta herramienta.

2.2.3. SD-ACCESS

Es una solución diseñada para gestionar el acceso de usuarios a contenidos en la nube. Esta gestión, se puede realizar desde cualquier tipo de dispositivo móvil, desde teléfonos a ordenadores. El objetivo es proporcionar la posibilidad de que los usuarios entren bajo un control.

Esta herramienta multifuncional le puede ayudar a trabajar mejor en la empresa donde labora. No en vano, mejoraran los dispositivos de acceso, podrá acceder a datos de red para comprobar tendencias, tendrá una política de acceso común y, además, mejorara su eficiencia. En la actualidad, con la política de protección de datos global se hace imprescindible tener controles de acceso que cumplan con la legislación. Ya que no hay que arriesgarse a las sanciones que establece el

Reglamento Europeo de Protección de Datos (RGPD).

Las Tecnologías de la Información (TI) proporcionan una transferencia de datos rápida y eficaz. En consecuencia, le interesara utilizar este software si tiene una red con varios accesos.

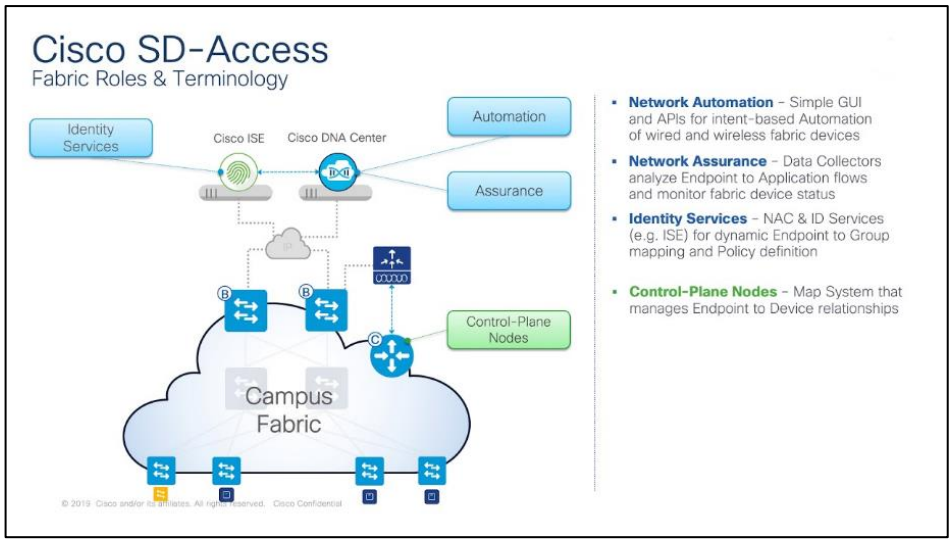

Figura 6 - Ilustración de los distintos componentes de SD-ACCESS.
Fuente: CISCO Live! 2019.

2.2.3.1. Network Automation

La automatización de redes es una metodología en la que el software configura, aprovisiona, administra y prueba automáticamente los dispositivos de una red. Es utilizado por empresas y proveedores de servicios para mejorar la eficiencia, reducir el error humano y reducir el Opex (Gastos Operacionales).

Las herramientas de automatización de red admiten funciones que van desde el mapeo de red básico y el descubrimiento de dispositivos hasta flujos de trabajo más complejos, como la gestión de configuración de red y el aprovisionamiento de recursos de red virtual.
La automatización de la red también juega un papel clave en las redes definidas por software, la virtualización de la red y la orquestación de la red, lo que permite el aprovisionamiento automatizado de los inquilinos y las funciones de la red virtual, como el equilibrio de carga virtual.

Tipos de automatización de redes.

La automatización se puede emplear en cualquier tipo de red, incluidas las redes de área local (LAN), la red de área amplia (WAN), las redes de centros de datos, las redes en la nube y las redes inalámbricas. Para resumir, cualquier recurso de red controlado a través de una interfaz de línea de comandos (CLI) o una interfaz de programación de aplicaciones (API) se puede automatizar.

- Automatización de red basada en scripts.
  La automatización de redes impulsada por scripts emplea lenguajes de programación y scripts para ejecutar tareas, idealmente aquellas con activadores precisos y procedimientos consistentes. Los lenguajes heredados, como Perl y TLC, siguen predominando en la automatización de redes debido a su familiaridad.

  A medida que las redes continúan volviéndose más complejas, los lenguajes de programación de código abierto más nuevos, como Ansible, Phyton y Ruby, han ganado popularidad por su facilidad de uso y flexibilidad. Otros lenguajes de programación para la automatización de redes incluyen Bash y Go.

- Automatización de redes basada en software.
  La automatización de red basada en software, a menudo denominada automatización de red inteligente, se coordina a través de un portal administrativo que elimina la necesidad de escribir comandos manualmente. Estas plataformas suelen proporcionar plantillas para crear y ejecutar tareas basadas en políticas de lenguaje sencillo.

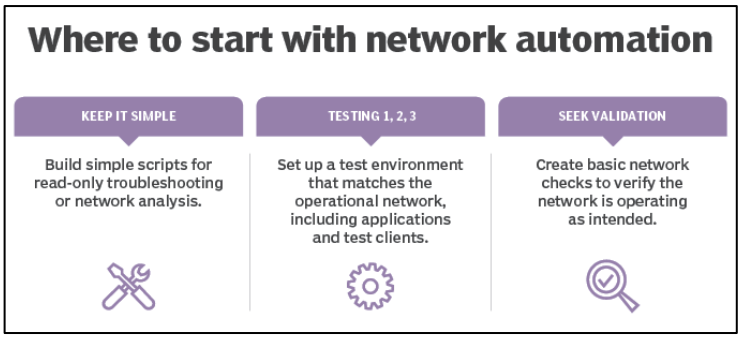

Figura 7 - Por dónde empezar con la automatización de la Red.
Fuente: https://www.techtarget.com/searchnetworking/tip/12-network-automation-ideas-to-incorporate-in-your-network.

2.2.3.2. Network Assurance

La garantía del servicio de red es la institución de políticas y procesos por parte de proveedores de red y proveedores de telecomunicaciones para garantizar una experiencia óptima del cliente. Mide el impacto que los cambios en la red tienen sobre la seguridad, la disponibilidad de la red y el cumplimiento. Una búsqueda que se ha vuelto más desafiante en los últimos años desde que las tendencias de virtualización y redes definidas por software (SDN) han cambiado la dinámica de las redes haciéndolas menos manejables usando técnicas tradicionales.

El aseguramiento del servicio de red intenta cuantificar el riesgo analizando los datos de la red (archivos de configuración, estado de la red, tráfico de la red, registros de errores y datos de rendimiento) e identificando errores dentro de estos datos, como configuraciones incorrectas en el equipo de red, que pueden resultar en problemas de conectividad, tráfico degradación o cortes de la red.

En última instancia, la experiencia del cliente es la medida principal del rendimiento de una red; sin embargo, los proveedores también deben cumplir los Acuerdos de nivel de servicio (SLA) objetivos que especifican los parámetros de rendimiento dentro de los cuales se proporciona un servicio. Son una parte integral de los contratos de proveedores de TI, incluida la protección de ambas partes en asuntos legales, los SLA brindan el entendimiento técnico entre el proveedor y el cliente, por lo tanto, es vital que el SLA esté alineado con los objetivos comerciales. La recopilación de políticas y procesos por parte de los proveedores de la red, denominada garantía de la red, intenta respaldar y cumplir o superar estos acuerdos entre los proveedores de la red y sus clientes finales.

Garantía de servicio de red impulsada por software de Cisco

En un nivel práctico, los grandes centros de datos de hoy están creciendo a tasas exponenciales, al igual que su complejidad. Estas empresas no pueden mantener sus redes sin la ayuda de la automatización. ¿Qué sucede si se cambia una política de nivel superior? ¿O un archivo de configuración cambió? ¿Cómo se puede garantizar la integridad de la red y mantenerla

operativa? ¿O cumplir con las regulaciones?

Cisco ha etiquetado estas incertidumbres en redes complejas como "brechas de garantía de red" y la forma tradicional de resolverlas era probar la red de forma exhaustiva y manual para cada escenario posible. Claramente, esto no es factible en la mayoría de las situaciones. Al tomar prestado del campo de la verificación formal, Cisco ha creado Network Assurance Engine, una solución de software que incorpora técnicas de verificación formal a la red.

Mediante el uso de la recopilación de datos, el modelado integral de redes y el análisis inteligente, Cisco Network Assurance Engine verifica y valida matemáticamente la corrección de redes enteras incluso cuando se reconfiguran. Esto acelera la resolución de problemas y permite a los administradores de red anticipar problemas potenciales antes de que afecten al negocio, manteniendo altos niveles de servicio con menos esfuerzo.

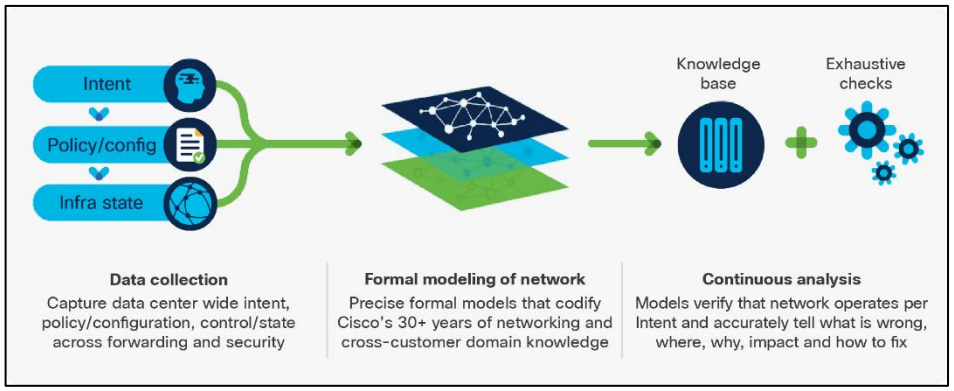

Figura 8 - Motor de Garantía de Red de Cisco.
Fuente: CISCO Live! 2019

2.2.3.3. Identity Services

La red de la empresa ya no está entre cuatro paredes seguras. Llega hasta donde viajen los empleados y los datos. Los empleados exigen poder acceder a los recursos profesionales desde más dispositivos y a través de más redes no corporativas que nunca. La movilidad y el concepto de Internet of Everything (IoE) están cambiando la forma en que vivimos y trabajamos. Las empresas deben hacer frente a la proliferación de nuevos dispositivos listos para conectarse a la red, mientras que la enorme cantidad de amenazas de seguridad y las brechas en

los datos de gran trascendencia pública demuestran claramente la importancia de garantizar la seguridad del acceso a una red empresarial en evolución.

A medida que se expanden las redes modernas, también aumenta la complejidad de administrar los recursos, gestionar soluciones de seguridad diversas y controlar los riesgos. Si añadimos la conectividad en cualquier lugar de IoE a unos recursos de TI limitados, el impacto potencial de no identificar y remediar las amenazas de seguridad aumenta notablemente.
Se requiere un enfoque diferente para la gestión y la protección de la red empresarial que no deja de evolucionar. La solución se llama Cisco Identity Services Engine (ISE).

Cisco Identity Services Engine (ISE) es su solución integral para la gestión de la política de seguridad simplificar y reducir los costos de operación. Con ISE, puede ver usuarios y dispositivos que controlan el acceso a través de conexiones cableadas, inalámbricas y VPN a la red corporativa.

Cisco ISE le permite proporcionar acceso de red altamente seguro a usuarios y dispositivos. Le ayuda a obtener visibilidad de lo que está sucediendo en su red, como quién está conectado, qué aplicaciones están instaladas y ejecutándose, y mucho más. También comparte datos contextuales vitales, como identidades de usuarios y dispositivos, amenazas y vulnerabilidades con soluciones integradas de los socios tecnológicos de Cisco, para que pueda identificar, contener y remediar las amenazas más rápidamente.

Ventajas para el cliente:

- Acceso empresarial y basado en el contexto altamente seguro basado en las políticas de su empresa.

- Visibilidad de red optimizada a través de una interfaz simple, flexible y altamente consumible.

- Aplicación de políticas extensiva que define reglas de acceso fáciles y flexibles que satisfacen sus requisitos comerciales en constante cambio.

- Experiencias sólidas para los huéspedes que brindan múltiples niveles de acceso a su red.

- Incorporación de dispositivos de autoservicio para las políticas de traiga su propio dispositivo (BYOD) o para invitados de la empresa.

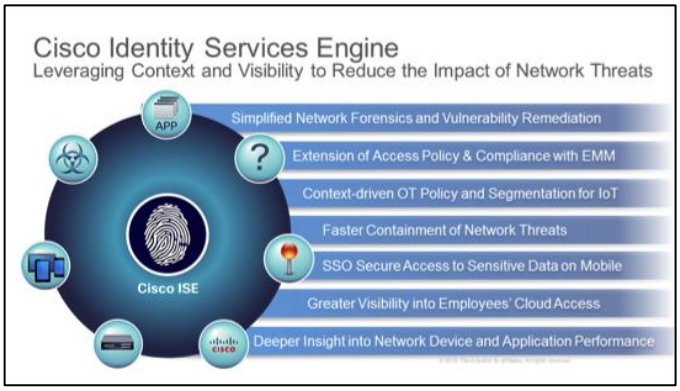

Figura 9 - Motor de Servicios de Identidad de Cisco.
Fuente: CISCO Live! 2019.

2.3. CONCEPTUAL

2.3.1. SOFTWARE DEFINED ACCESS (SD-ACCESS)

Cisco Software-Defined Access (SD-Access) es la evolución de Cisco DNA desde los diseños tradicionales de LAN del campus a las redes que implementan directamente la intención de una organización. La solución SD-Access está habilitada por un paquete de aplicaciones que se ejecuta como parte del software Cisco DNA Center y proporciona segmentación automatizada de un extremo a otro para separar el tráfico de usuarios, dispositivos y aplicaciones. Estas políticas de acceso de usuarios están automatizadas para que las organizaciones puedan garantizar que se establezcan las políticas correctas para cualquier usuario o dispositivo con cualquier aplicación en cualquier lugar de la red.

SD-Access utiliza bloques lógicos denominados fabric que aprovechan las overlay de redes virtuales que se controlan mediante la programación y la automatización para crear movilidad, segmentación y visibilidad. La virtualización de redes se vuelve fácil de implementar a través de la segmentación

definida por software y la política para redes de campus inalámbricas y cableadas. Las redes físicas individuales se abstraen y pueden albergar una o más redes lógicas que se organizan mediante software. Las operaciones manuales propensas a errores en estos entornos dinámicos se eluden por completo, proporcionando una política coherente para los usuarios a medida que se mueven por la red cableada e inalámbrica.

2.3.2. COMPONENTES SD-ACCESS

2.3.2.1. VXLAN

La tecnología principal utilizada para el Fabric Control Plane se basa en LAN virtual extensible (VXLAN), una encapsulación estándar IETF (RFC-7348, etc.).

La encapsulación VXLAN está basada en IP / UDP, lo que significa que puede ser reenviada por cualquier red basada en IP y crea efectivamente el aspecto de "overlay" del SD-Access Fabric.

Se utiliza la encapsulación VXLAN por dos razones principales, VXLAN incluye el encabezado de la capa 2 de origen (Ethernet), y también proporciona campos especiales para información adicional (como la VN o SGT).

Esta tecnología proporciona varias ventajas para SD-Access, como soporte de capa 2 y capa 3, topologías (overlay) y la capacidad de operar sobre cualquier red basada en IP con segmentación de red integrada (VRF / VN) y una política de grupo integrada.

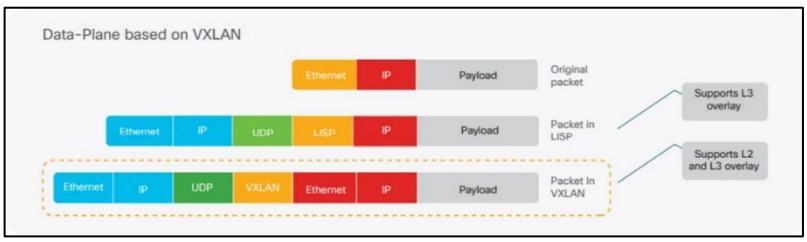

Figura 10 - Plano de datos del Fabric basado en VXLAN
Fuente: CISCO Live! 2019.

2.3.2.2. LISP

El protocolo de separación de ID de localizador (LISP) es un protocolo de red que implementa el uso de dos espacios de nombres en lugar de una única dirección IP:

- Endpoint identifiers (EID): Asignados a los hosts finales.
- Routing locators (RLOC): Asignados a dispositivos (principalmente enrutadores) que forman el sistema de enrutamiento global.

La división de las funciones de EID y RLOC ofrece varias ventajas, incluida la escalabilidad mejorada del sistema de enrutamiento y la eficiencia mejorada de multihoming, por esa razón LISP es el protocolo de plano de control de Cisco SDA, ayuda a automatizar la red del campus con la ayuda de DNA-Controller.

2.3.2.3. Fabric Border Node

Es un punto de entrada y salida para el tráfico de datos que entra y sale del Fabric. Se basa en un enrutador de túnel proxy lisp (pxtr), todo el tráfico que entra o sale del Fabric pasa por este tipo de nodo.

- Conecta redes L3 tradicionales y / o diferentes dominios de Fabric al dominio local.
- Donde dos dominios intercambian información sobre políticas y accesibilidad de endpoints.
- Responsable de la traducción de contexto (VRF y SGT) de un dominio a otro.
- Proporciona un punto de salida de dominio para todos los nodos perimetrales.

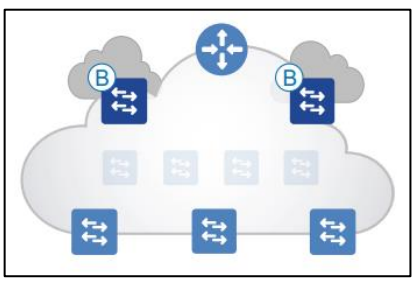

Figura 11 - Fabric Border Node.
Fuente: CISCO Live! 2019.

2.3.2.4. Fabric Control Plane

Ejecuta una base de datos de seguimiento de host para asignar información de ubicación de los dispositivos que se encuentran dentro y fuera del Fabric SDAccess.

- Una base de datos de host simple que asigna ID de punto final a una ubicación actual, junto con otros atributos.
- La base de datos del host admite múltiples tipos de punto final de búsqueda de ID (IPv4, IPv6 o MAC).
- Recibe registros de prefijo de Edge Nodes con Endpoints locales.
- Resuelve solicitudes de búsqueda equipos Edge y / o Border Nodes, para ubicar el ID de punto final de destino.

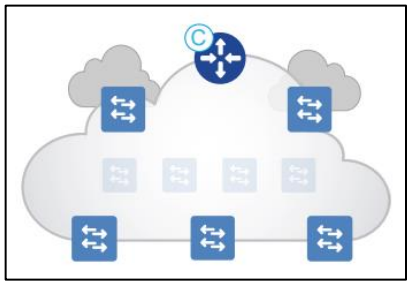

Figura 12 - Fabric Control-Plane Node.
Fuente: CISCO Live! 2019.

2.3.2.5. Intermediate Node

Este nodo intermedio (Intermediate Node) es parte de la red de Capa 3 que se utiliza para las interconexiones entre los dispositivos que operan en una función de fabric, como son las interconexiones entre el Border Node y el Edge Node. Estas interconexiones son creadas en la tabla de ruteo global de los dispositivos y se conoce como Underlay Network.

Por ejemplo, si una implementación de campus de tres niveles aprovisiona los Switches de Core como Border Node y los Switches de Acceso como Edge Nodes, los Switches de Distribución son los Intermediate Nodes.

2.3.2.6. Fabric Edge Node

El Edge Node es el equivalente a un switch de acceso en un diseño LAN de campus tradicional. La funcionalidad del Edge

Node se basa en los enrutadores de túnel de entrada y salida (xTR) en LISP. Los Edge Node deben implementarse utilizando un diseño de acceso enrutado de Capa 3. Proporciona los siguientes servicios para usuarios/dispositivos conectados al Fabric SD-Access:

- Responsable de identificar y autenticar endpoints.
- Proporcionar una puerta de enlace Anycast L3 para los endpoints conectados.
- Autenticador (AAA), el mapeo de puntos finales en VLAN se puede realizar de forma estática o dinámica mediante un servidor de autenticación.
- Realiza la encapsulación / des-encapsulación de datos en el tráfico hacia y desde todos los puntos finales conectados.

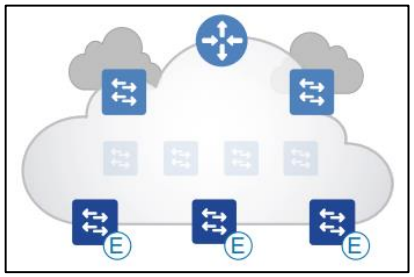

Figura 13 - Fabric Edge Node.
Fuente: CISCO Live! 2019.

2.3.2.7. Underlay Network

Las Underlay networks o llamadas redes físicas donde funcionan los protocolos tradicionales.

Esta es una infraestructura física sobre la cual se construye la Overlay network. Es la Underlay network responsable de la entrega de paquetes a través de redes.

La red física esta descrita por los dispositivos físicos y pueden ser conmutadores y enrutadores en la red. Todos los componentes de red de la capa Underlay deben determinar la conectividad IP mediante el uso de un protocolo de enrutamiento. El protocolo utilizado en los dispositivos Underlay es como OSPF, IS-IS, BGP para fines de enrutamiento.

Para que esta red configure una base de Capa 3 bien diseñada que incluya los conmutadores de borde del campus para

garantizar el rendimiento, la escalabilidad y la alta disponibilidad de la red.

Protocolos Underlay: BGP, OSPF, IS-IS, EIGRP.

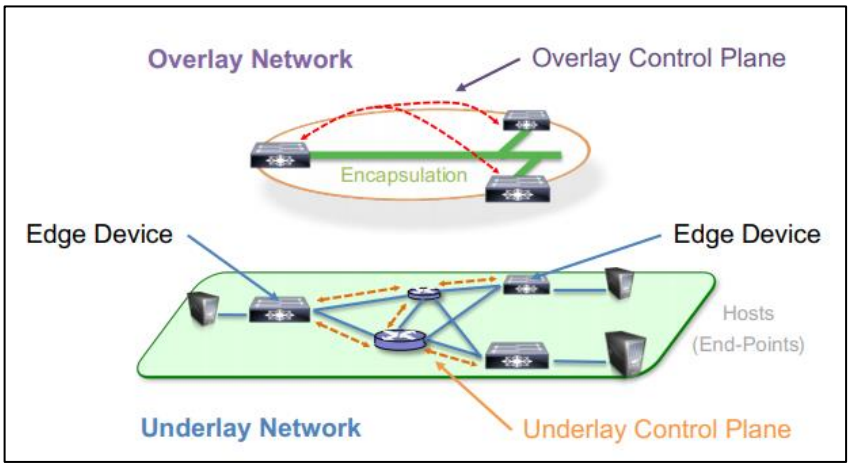

Figura 14 - Overlay Network y Underlay Network.
Fuente: CISCO Live! 2019.

2.3.2.8. Overlay Network

Se forma una overlay network sobre la capa Underlay en la dirección de construir una red virtualizada. El tráfico del plano de datos y la señalización del plano de control se controlan dentro de cada red virtualizada. Encapsular el tráfico de usuarios en Overlay networks mediante paquetes IP que se obtienen.

Usar Overlay network es un método de uso de software para crear capas de abstracción de red que se pueden usar para ejecutar múltiples capas de red virtualizadas independientes y discretas en la parte superior de la red física, lo que a menudo proporciona nuevas aplicaciones o beneficios de seguridad.

Esta es una red virtual que se enruta sobre la infraestructura de la Underlay network; la decisión de enrutamiento se tomaría con la ayuda de un software.

Protocolos de Overlay: VXLAN, NVGRE, GRE, OTV, OMP, MVPN.

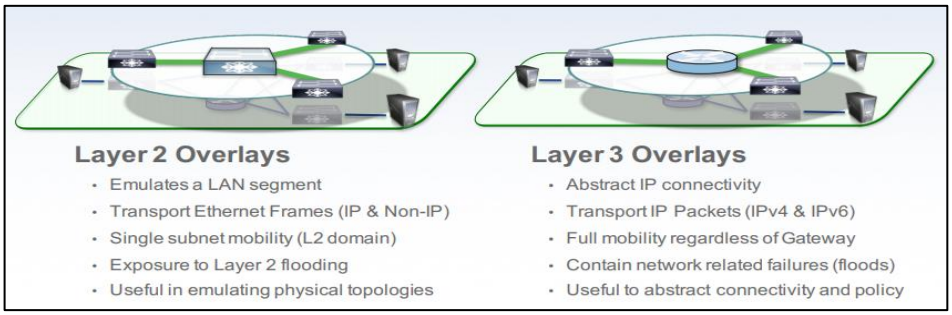

Figura 15 - Overlay Network de Capa 2 y Capa 3.
Fuente: CISCO Live! 2019.

2.3.3. Arquitectura basa en controladores

Las redes tradicionales se centran en la gestión por dispositivo, lo que lleva tiempo y crea muchas complejidades. Este enfoque es propenso a errores humanos. SD-Access utiliza DNA Center, el centro de comando y control para la red basada en DNA, para impulsar la intención empresarial en la orquestación y operación de los elementos de la red. Esto incluye la configuración del día 0 de los dispositivos y las políticas asociadas con los usuarios, los dispositivos y los puntos finales a medida que se conectan a la red. El controlador proporciona una capa de abstracción de red para arbitrar los detalles de varios elementos de red. Además, DNA Center expone API basadas en la transferencia de estado representacional (REST) en dirección norte para facilitar el desarrollo interno o de terceros de servicios significativos en la red.

2.3.4. Tejido de red

Con un elemento de controlador en su lugar, puede considerar construir la red en bloques lógicos llamados entramados. SD-Access Fabric aprovecha las superposiciones de redes virtuales para admitir la movilidad, la segmentación y la programación a gran escala. La superposición de red virtual aprovecha un plano de control para mantener actualizado el mapeo de los puntos finales a su ubicación de red a medida que los puntos finales se mueven por la red. La separación del plano de control del plano de reenvió reduce la complejidad, mejora la escala y la convergencia con respecto a las técnicas tradicionales de redes. SD-Access Fabric habilita varias capacidades clave, como la movilidad del host independientemente del volumen de movimientos y el tamaño de la red, segmentación de Capa 2 y

Capa 3 e integración inalámbrica. Otras capacidades incluyen servicios inteligentes para el reconocimiento de aplicaciones.

2.3.5. Infraestructura programable

Para construir una infraestructura moderna, Cisco está equipando sus dispositivos actuales y futuros con capacidades avanzadas para permitir la administración del ciclo de vida completo mientras es abierto, basado en estándares y extensible. Estas tecnologías clave incluyen:

a. Aprovisionamiento automatizado de dispositivos, que incorpora funciones bien conocidas como aprovisionamiento sin intervención y Plug and Play.
b. Interfaz API abierta.
c. Visibilidad granular, utilizando capacidades de telemetría como NetFlow.
d. Actualizaciones de software sin problemas con parches de software en vivo.

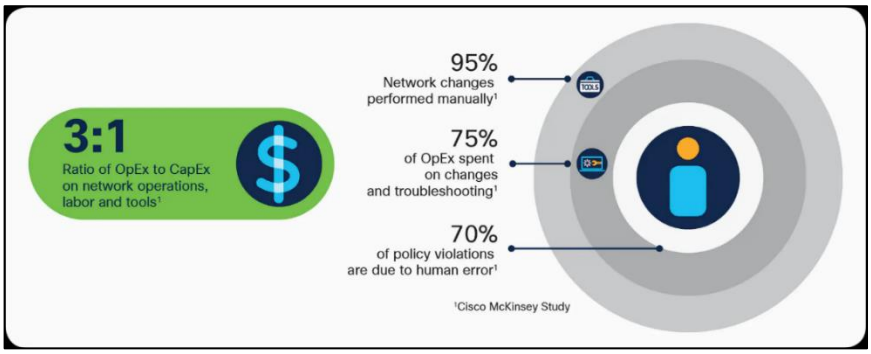

Figura 16 - El ritmo del cambio supera la escala humana.
Fuente: CISCO Live! 2019.

2.4. Definición de términos básicos

LAN AUTOMATION: Como parte de Cisco DNA Center, la automatización de LAN implementará un protocolo de enrutamiento IGP basado en estándares para activar automáticamente la red subyacente. Tradicionalmente, esto ha sido IS-IS, pero SD-Access ahora ofrece soporte para OSPF como el protocolo de enrutamiento subyacente automatizado**.**

MULTICAST (NATIVE): La multidifusión se utiliza para distribuir copias de datos a múltiples destinos de red diferentes. Cisco SD-Access ha

ofrecido superposición de multidifusión (replicación de cabecera) desde sus inicios. Ahora, SD-Access también ofrece soporte de multidifusión nativa, que proporciona replicación en la red subyacente como una opción. Esto mejora la eficiencia de la implementación de multidifusión para redes de estructura al distribuir la carga de replicación de multidifusión a múltiples elementos de red.

LAYER 2 FLOODING: SD-Access ofrece soporte para la inundación de Capa 2 al reenviar transmisiones para ciertos tipos de tráfico y aplicaciones que pueden requerir el aprovechamiento de la conectividad de Capa 2, como hosts silenciosos, lectores de tarjetas, cerraduras de puertas, etc. Tales dispositivos y aplicaciones pueden requerir una inundación de tráfico en un dominio de Capa 2, que ahora pueden acomodar las implementaciones de SD-Access.

LAYER 2 BORDER: Diseñada como una solución de migración, la función de borde de Capa 2 proporciona una funcionalidad que permite a los hosts comunicarse desde la estructura SD-Access basada en VXLAN a un puerto de conmutador VLAN tradicional conectado a la red empresarial (fuera de la estructura). Esta capacidad simplifica las migraciones al permitir que se utilice la misma subred IP tanto dentro como fuera de la estructura SD-Access.

FABRIC-IN-A-BOX: La función fabric-in-a-box permite utilizar un único dispositivo SD-Access para los tres roles de fabric (borde, plano de control y nodo de borde de fabric). Esta característica es especialmente valiosa para admitir sitios más pequeños y/o implementaciones de sucursales remotas.

EMBEDDED WIRELESS LAN CONTROLLER: Esta nueva y emocionante capacidad brinda la habilidad de soportar una capacidad de controlador de LAN inalámbrica incorporada en un conmutador de la familia Catalyst 9000, para usar con implementaciones de SD-Access. Esto simplifica las implementaciones inalámbricas con SD-Access fabric, especialmente para sitios más pequeños y sucursales.

IoT EXTENSION FOR SD-ACCESS: Esta capacidad se utiliza para conectar dispositivos de red de Capa 2 que no son de estructura descendente al nodo de borde de estructura de SD-Access (extendiendo así la estructura). Esto se hace mediante el uso de un dispositivo (como un conmutador de Capa 2 más pequeño) designado como nodo extendido, conectado y aprovechando el conmutador de

borde de la estructura ascendente para la conectividad de la estructura y la aplicación de políticas. Esto es especialmente útil en implementaciones industriales o implementaciones fuera del espacio tradicional “alfombrado”.

EXTRANET: La extranet SD-Access proporciona un método flexible y escalable para lograr comunicaciones entre VN, simplificando la implementación de la estructura SD-Access y proporcionando un método de comunicación más eficiente y basado en políticas entre dispositivos y servicios ubicados en redes virtuales (VN) separadas.

VN ANCHORING: El anclaje de VN permite que el tráfico de un VN determinado en varios sitios dispersos se agregue nuevamente a una ubicación central, utilizando una sola subred común, en lugar de tener que definir y usar subredes por sitio para ese VN como sería el caso. Esto simplifica la implementación general para varios casos de uso clave, incluido el acceso de invitados centralizado e implementaciones similares.

IPv6 SUPPORT: SD-Access ahora admite el acceso basado en IPv6 para un cliente adjunto a la superposición de la red de estructura, un requisito crítico ya que cada vez más hosts admiten la próxima generación del Protocolo de Internet.

ACCESS CONTROL APPLICATION (ACA): La aplicación ACA, que reside en Cisco DNA Center, está diseñada para proporcionar un mayor nivel de interoperabilidad con soluciones de nube e identidad que no son de Cisco, así como para simplificar el diseño, la implementación y el uso de políticas dentro de una estructura.

VRF: En las redes informáticas basadas en IP, el enrutamiento y reenvío virtual (VRF) es una tecnología que permite que varias instancias de una tabla de enrutamiento coexistan dentro del mismo enrutador al mismo tiempo. Una o más interfaces lógicas o físicas pueden tener un VRF y estos VRF no comparten rutas, por lo que los paquetes solo se reenvían entre interfaces en el mismo VRF. Los VRF son el equivalente de capa 3 de TCP/IP de una VLAN. Debido a que las instancias de enrutamiento son independientes, se pueden usar las mismas direcciones IP o superpuestas sin entrar en conflicto entre sí. La funcionabilidad de la red se mejora porque las rutas de la red se pueden segmentar sin requerir varios enrutadores.

La forma más sencilla de implementación de VRF es VRF-Lite. En esta implementación, cada enrutador dentro de la red participa en el entorno de enrutamiento virtual de una manera basada en pares. Si bien es fácil de implementar y apropiado para pequeñas y medianas empresas y centros de datos compartidos, VRF-Lite no se escala al tamaño requerido por empresas globales o grandes operadores, ya que existe la necesidad de implementar cada instancia de VRF en cada enrutador, incluidos los enrutadores intermedios. Los VRF se introdujeron inicialmente en combinación con el cambio de etiquetas multiprotocolo (MPLS), pero el VRF demostró ser tan útil que finalmente evolucionó para vivir independientemente del MPLS.

VXLAN: VXLAN es una tecnología que permite superponer una red de CAPA 2 (L2) sobre una capa subyacente de CAPA 3 (L3) con el uso de cualquier protocolo de enrutamiento IP. Utiliza encapsulación MAC-in-UDP.

IS-IS: El protocolo de enrutamiento de sistema intermedio a sistema intermedio (IS-IS) es un protocolo de puerta de enlace interior (IGP) estandarizado por el Grupo de trabajo de ingeniería de Internet (IETF) y comúnmente utilizado en grandes redes de proveedores de servicios. IS-IS también se puede implementar en redes empresariales extremadamente grandes. IS-IS es un protocolo de enrutamiento de estado de enlace que proporciona una convergencia rápida y una escalabilidad excelente. Como todos los protocolos de estado de enlace, IS-IS es muy eficiente en el uso del ancho de banda de la red.

BGP: Border Gateway Protocol (BGP) es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos (AS). Entre los sistemas autónomos de los ISP se intercambian sus tablas de rutas a través del protocolo BGP. Este intercambio de información de encaminamiento se hace entre los routers externos de cada sistema autónomo, los cuales deben ser compatibles con BGP. Se trata del protocolo más utilizado para redes con intención de configurar un protocolo de puerta de enlace exterior (Exterior Gateway Protocol).

La forma de configurar y delimitar la información que contiene e intercambia el protocolo BGP es creando lo que se conoce como sistema autónomo o AS. Cada uno tendrá conexiones o sesiones internas (iBGP), así como sesiones externas (eBGP).

El protocolo de puerta de enlace de frontera (BGP) intercambia información de encaminamiento entre sistemas autónomos a la vez que garantiza una elección de rutas libres de bucles. Es el protocolo principal de publicación de rutas utilizado por las compañías más importantes de ISP en Internet.BGP4 es la primera versión que admite encaminamiento entre dominios sin clave (CIDR) y agregado de rutas. A diferencia de los protocolos de puerta de enlace internos (IGP), como RIP, OSPF y EIGRP, no usa métricas como número de saltos, ancho de banda o retardo. En cambio, BGP toma decisiones de encaminamiento basándose en políticas de la red o reglas que utilizan varios atributos de reta BGP.

ENCAPSULAMIENTO: La encapsulación de datos es el proceso que agrega la información adicional del encabezado del protocolo a los datos antes de la transmisión. En la mayoría de las formas de comunicaciones de datos, los datos originales se encapsulan o envuelven en varios protocolos antes de transmitirse.

Cuando se envían mensajes en una red, el stack de protocolos de un host opera desde las capas superiores hacia las capas inferiores.

ISE (identity Service Engine): Cisco ISE es la evolución de NAC de Cisco, donde permite crear políticas centralizadas para gestionar con seguridad los dispositivos de los usuarios finales, la gestión de estos dispositivos se realiza de acuerdo a perfiles teniendo en cuenta el contexto, quien es el usuario y a que recursos accede. Es un motor de políticas centralizado, el cual permite definir y gestionar de manera eficiente a las organizaciones, las políticas de seguridad corporativas en función del contexto que rodea a los dispositivos, distinguen de los dispositivos de la empresa y los hosts personales de los usuarios, automatiza la seguridad y políticas de acceso basadas en la red. Identifica el sistema operativo del dispositivo final, lo almacena en las sesiones activas y en los logs.

AAA: En seguridad informática, AAA significa comúnmente autentificación, autorización y contabilidad. Se refiere a una arquitectura de seguridad para sistemas distribuidos que permite control sobre que usuarios se les permite el acceso a qué servicios y que mantiene las pestañas en cuanto de los recursos que han utilizado. Dos protocolos de red que proporciona este son particularmente popular: el protocolo RADIUS y su nuevo diámetro contrapartida.

Redes de Área Local (LAN): Son redes de propiedad privada, de hasta unos cuantos kilómetros de extensión. Por ejemplo, una oficina o un centro educativo. Se usan para conectar computadoras personales o estaciones de trabajo, con objeto de compartir recursos e intercambiar información.

Protocolo de configuración dinámica de hosts (DHCP): Es un estándar TCP/IP que utiliza un servidor central para gestionar direcciones IP y otros datos de configuración para toda una red.Un servidor DHCP responde a las peticiones de los clientes, asignándoles propiedades de forma dinámica.

Sistema de nombres de dominio (DNS): Es un sistema de bases de datos distribuidas que permite gestionar los nombres de host y las direcciones de protocolo de Internet (IP) asociadas a ellos.

Dispositivo final (Host): El dispositivo es un hardware, el cual un usuario llega a utilizar, también se le dice host. Estos dispositivos se conectan a red, algunos cuentan con 802.1x para autenticar con el ISE y otros solo se autentican con la dirección MAC. Los Host pueden ser:

- Computadoras, laptops.
- Teléfonos VoIP.
- Cámaras de red, como las cámaras de seguridad.
- Impresoras IP.

Usuario Final: Es una persona la cual utiliza el dispositivo final (computadora, laptop, Tablet, teléfono IP, impresora IP). Los clientes están en constante contacto con la información y los servicios, como las páginas web, correo electrónico, ambos requeridos para los trabajadores, para realizar los trabajos en las empresas.

III. HIPOTESIS Y VARIABLES

3.1. Hipótesis

3.1.1. Hipótesis general

El diseño de la solución SD Access mejora la gestión centralizada y automatizada la red LAN en una empresa de aeronavegación.

3.1.2. Hipótesis específicas:

- La integración automatizada de nuevos dispositivos de red permite reducir el tiempo de configuración.
- La determinación de las políticas de seguridad mejora los estándares actuales de seguridad de la red LAN.
- El diseño de un control centralizado permite gestionar la red LAN de manera gráfica.

3.2. Definición conceptual de variables:

3.2.1. Variable dependiente:

- Diseño de la gestión centralizada de la red LAN
- Automatización de la red LAN

3.2.2. Variable independiente:

- Solución CISCO SD-ACCESS

3.2.3. Operacionalización de variables:

Variable	Tipo de Variable	Definición	Dimensiones	Indicadores
1. Solución CISCO SD-ACCESS	Independiente	El acceso definido por software (SD-Access), una solución dentro de la arquitectura de red digital de Cisco (Cisco DNA) que se basa en principios de redes basadas en la intención, proporciona un cambio transformacional en la construcción, administración y protección de redes, haciéndolas más rápidas y fáciles de operar, con una mayor eficiencia empresarial	Componente cognoscitivo	Experiencia y conocimiento en uso de esta nueva tecnología
			Accesibilidad Económica	Disponibilidad económica para cubrir ese gasto de implementación
2. Diseño de una gestión centralizada de la red LAN	Dependiente	Gestión centralizada significa manejar y configurar los dispositivos múltiples al mismo tiempo, para proporcionar la mayor confiabilidad, la flexibilidad, y la escalabilidad dentro de su red, permitiendo gestionarla de manera global mientras que cumple con las políticas locales.	Flexibilidad de la red LAN	Tiempo medido en horas y minutos que tarda el administrador de la RED en solucionar un incidente o requerimiento
3. Automatización de la red LAN	Dependiente	La automatización de red es el proceso de automatizar la configuración, la administración, las pruebas, la implementación y la operación de dispositivos físicos y virtuales en una red. La disponibilidad de los servicios en red mejora al automatizar las tareas y funciones de red cotidianas, y controlar y administrar automáticamente los procesos repetitivos.	Escalabilidad de la red LAN	Cantidad de tiempo utilizado en la configuración de nuevos dispositivos de red para continuar con la escalabilidad

IV. DISEÑO METODOLÓGICO

4.1. Tipo de investigación

- **Aplicada**

  El presente trabajo de investigación es de tipo aplicada debido a que la red actual de una empresa de aeronavegación utiliza la infraestructura de red tradicional y esta va ser reemplazada por una tecnología más eficiente en cuanto a escalabilidad y acceso a la red LAN.

- **Espacial**

  Este trabajo de investigación es de tipo espacial puesto que hemos tomado como referencia una empresa de aeronavegación ubicada en el Perú.

4.2. Diseño de la investigación

El diseño del proyecto está orientado a la implementación de la solución tecnológica de Cisco SD-Access a un sector específico, este es: La gestión centralizada y automatización de la red LAN. Por lo revisado, existen algunas alternativas de soluciones para la optimización de este servicio, las cuales se fundamentan en Software Defined Network (SDN). Este proyecto se desarrolló mediante los siguientes pasos y procedimiento

Analizar los dispositivos electrónicos que sean compatibles con la solución planteada para nuestro caso son los switches Catalyst 9300 y Catalyst 9500 así como también los Nexus 9300, además del servidor que alojara al software DNA Center.

En base a los objetivos planteados, se procede a investigar sobre los dispositivos electrónicos que se utilizaran para el óptimo desarrollo de la solución SD-Access

Desarrollar el diseño planteado para infraestructura de la red de una empresa de aeronavegación mediante un laboratorio con los equipos reales a utilizar

Se implementará la solución SD-Access en paralelo a la red tradicional para ir migrando poco a poco los diferentes servicios y dispositivos que

se encuentran operando

Finalizar la implementación dejando fuera de operatividad los equipos pertenecientes a la red LAN tradicional.

4.3. Población y muestra

Las muestras de información fueron tomadas de la red LAN tradicional de una empresa de aeronavegación de los cuales se obtuvieron los datos reales de la infraestructura anterior y comparar con la nueva infraestructura implementada con la solución SD-Access.

4.4. Lugar del estudio

UNA EMPRESA DE AERONAVEGACIÓN UBICADA EN EL PERÚ.

4.5. Técnicas e instrumentos para la recolección de la información

Las principales técnicas para poder realizar la recolección de información fue que se utilizaron los informes mensuales pertenecientes al proyecto de la red LAN generados por el proveedor anterior que administraba la red LAN tradicional en la empresa de aeronavegación.
Analizar los dispositivos pertenecientes a la infraestructura de red tradicional que se tenía en la empresa de aeronavegación para obtener datos sobre sus limitaciones de operatividad.

4.6. Desarrollo del Proyecto

4.6.1. Arquitectura de Red

4.6.1.1. Infraestructura Actual

Actualmente la empresa de aeronavegación cuenta con 21 nodos de comunicación distribuidos en aeropuerto los cuales cuentan con switches de la marca Cisco con software desactualizado y fuera de soporte (EOL). Los nodos se encuentran interconectados hacia los Core de la red y entre ellos mismos mediante tecnologías de fibra y radio en una arquitectura redundante de Capa 2.

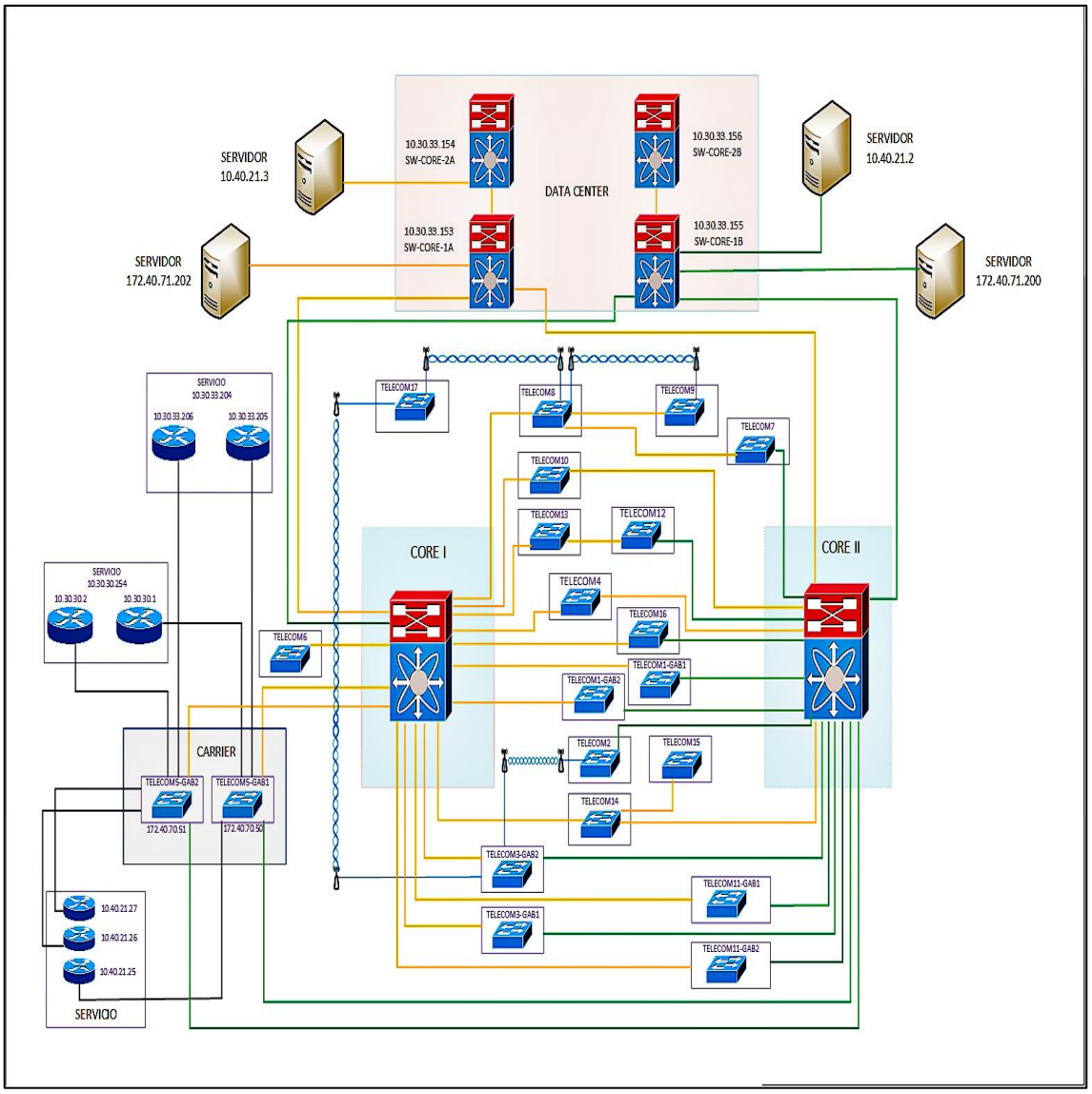

Figura 17 – Topología de Red Tradicional de una Empresa de Aeronavegación.
Fuente: Elaboración propia de los autores.

4.6.1.2. Infraestructura Propuesta

La Infraestructura Tecnológica para la red corporativa de una empresa de aeronavegación, estará compuesta por una solución de hardware con Switches Catalyst de la serie 9000, bajo la arquitectura de acceso a la red definida por software del fabricante Cisco Systems, denominada Cisco Software-Defined Access (SD-Access), la cual es una evolución de los diseños tradicionales de redes de campus.

De acuerdo a los Términos de referencia se implementó una red LAN Estrella en configuración con Enlaces de 100GE, 40GE, y 10GE de acuerdo al siguiente diagrama de Bloques:

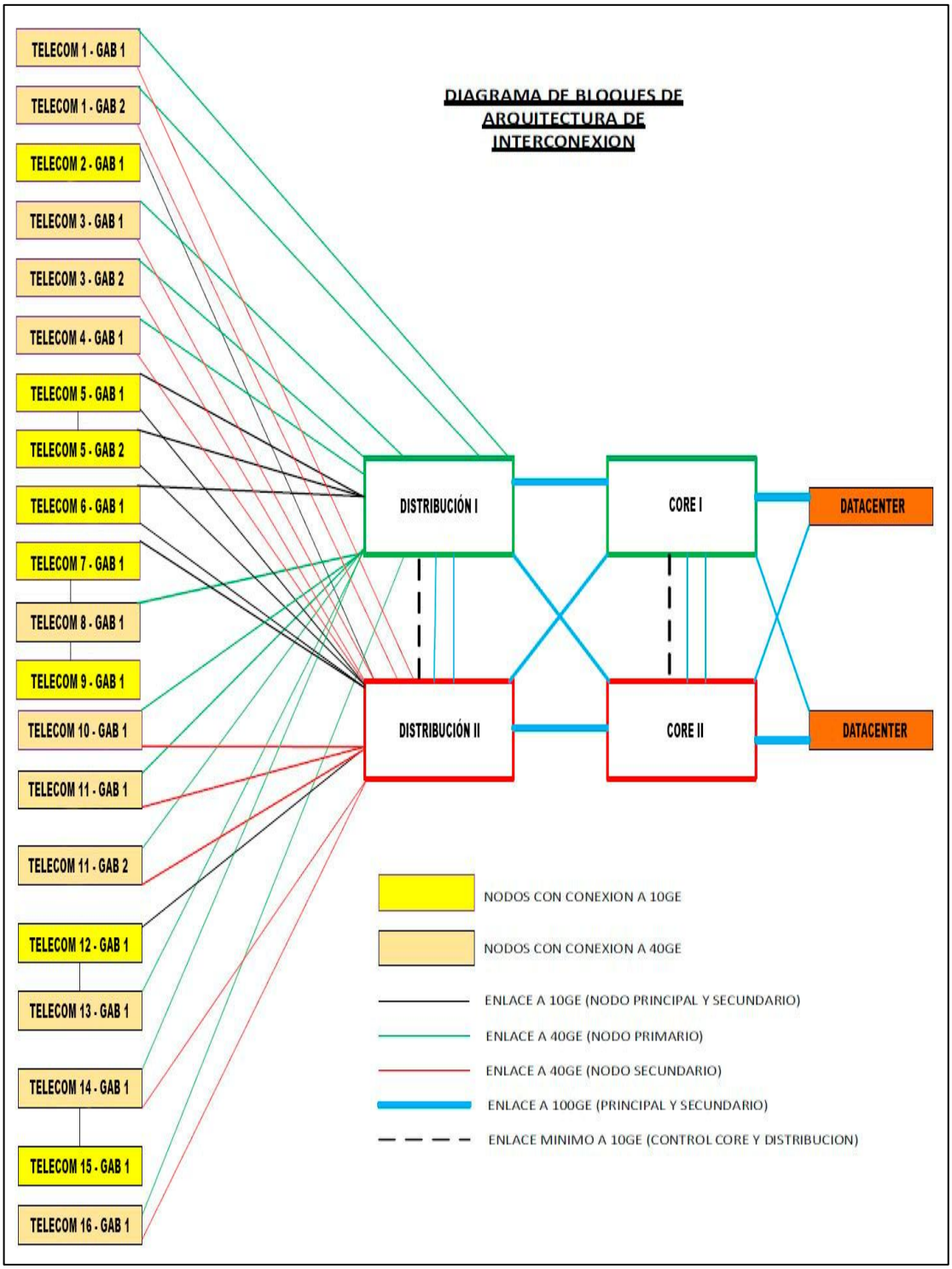

Figura 18 - Diagrama de Bloques de Arquitectura de Interconexión.
Fuente: Elaboración propia de los autores.

Para el Data Center se propone la implementación de 5 Switches Nexus 9k, los cuales estarán en redundancia y brindarán la conectividad a los servidores implementados también como parte del proyecto.

4.6.1.3. Topología Final

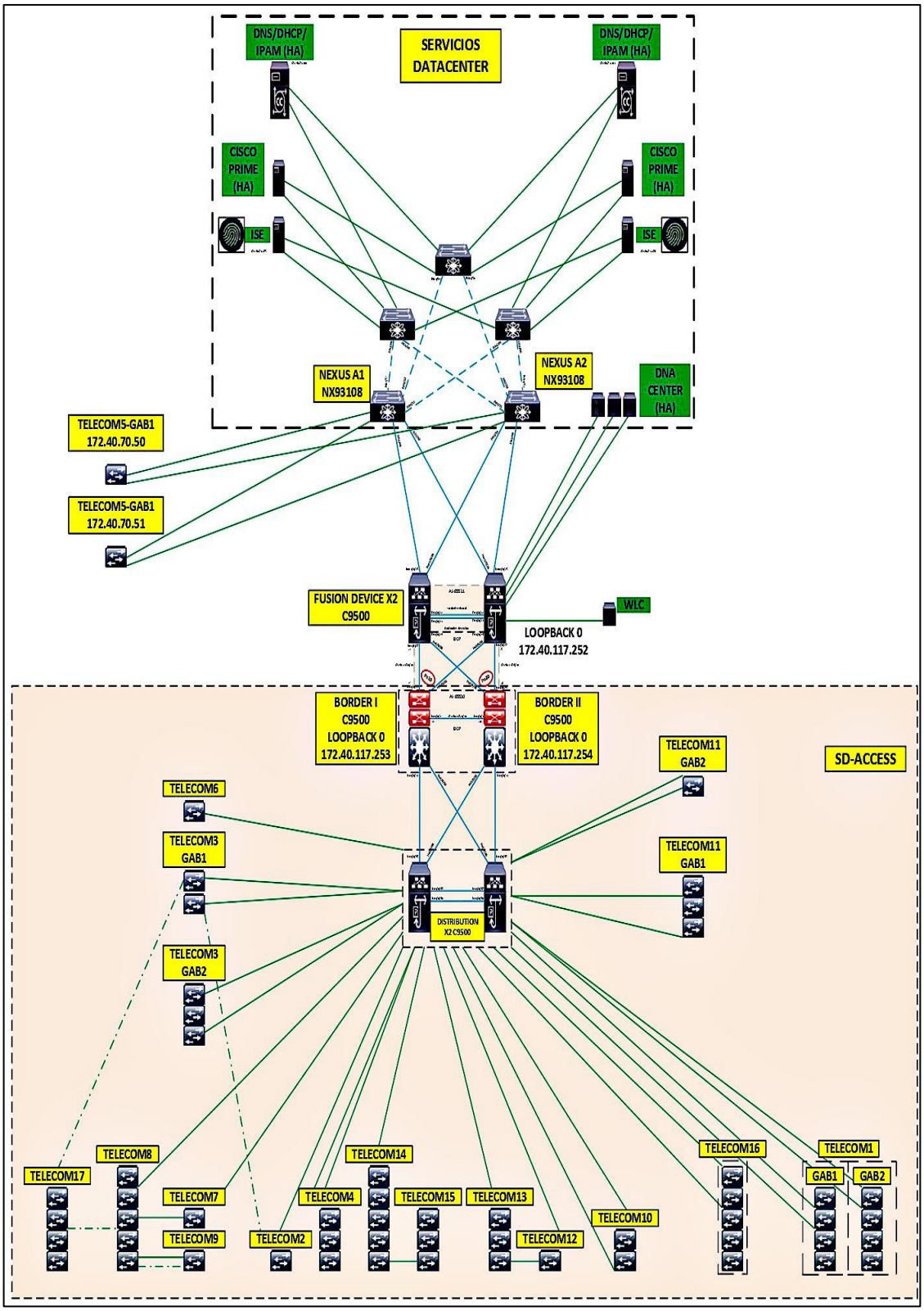

Figura 19 - Topología de Red SD-ACCESS de una Empresa de Aeronavegación.
Fuente: Elaboración propia de los autores.

4.6.2. Hardware

La red a implementar contará con el siguiente equipamiento:

- 05 Switches Datacenter Nexus 9300.
- 02 Fusion Device Catalyst 9500.
- 03 Servidores DNA Center DN2-HW APL.
- 02 Servidores ISE 3615.
- 02 Wireless LAN controllers C9800.
- 02 Switches Borde Catalyst C9500-32C-A.
- 02 Switches de Distribución Catalyst c9500-32QC-A.
- 28 Switches Catalyst C9300-24PA.
- 13 Switches Catalyst C9300-24UX.
- 48 Switches Catalyst C9300-48PA.

4.6.3. Distribución de Equipamiento

4.6.3.1. Equipamiento Sala Blanca

Implementación de los switches de Datacenter conformado por el siguiente equipamiento Nexus:

Tabla 1 - Switches Nexus - Data Center.

FUNCIONALIDAD	PART NUMBER	DESCRIPCION
SWITCH DATA CENTER	N9K-C93I08TC-EX	NEXUS 9300
SWITCH DATA CENTER	N9K-C93I08TC-EX	NEXUS 9300
SWITCH DATA CENTER	N9K-C93I08TC-EX	NEXUS 9300
SWITCH DATA CENTER	N9K-C93I08TC-EX	NEXUS 9300
SWITCH DATA CENTER	N9K-C93I08TC-EX	NEXUS 9300

Fuente: Elaboración propia de los autores.

Se habilito en esta sala los switches de Fusión (Quienes intercambian rutas entre el Fabric SD Access y el Data Center)

Tabla 2 - Switches Fusion - Data Center.

FUNCIONALIDAD	PART NUMBER	DESCRIPCION
FUSION DEVICE (DNA SWITCHING)	C9500-24Y4C-A	Cisco Catalyst 9500
FUSION DEVICE (DNA SWITCHING)	C9500-24Y4C-A	Cisco Catalyst 9500

Fuente: Elaboración propia de los autores.

Servidores en el Data Center: DNA Center, ISE, WLC.

Tabla 3 - Servidores Data Center.

FUNCIONALIDAD	PART NUMBER	DESCRIPCION
AUTOMATIZACION	DN2-HW-APL	DNA CENTER
AUTOMATIZACION	DN2-HW-APL	DNA CENTER
AUTOMATIZACION	DN2-HW-APL	DNA CENTER
SEGURIDAD	SNS-3615-K9	ISE
SEGURIDAD	SNS-3615-K9	ISE
CONTROLADOR WIRELESS	C9800-L-F-K9	Cisco Catalyst 9800-L
CONTROLADOR WIRELESS	C9800-L-F-K9	Cisco Catalyst 9800-L

Fuente: Elaboración propia de los autores.

4.6.3.2. Equipamiento de TELECOM 6 y TELECOM 11

El siguiente equipamiento se encuentra ubicados en los TELECOM 6 y TELECOM 11 los que tienen conexión hacia los Switches de acceso o Edge Nodes.

Tabla 4 - Equipamiento de TELECOM 6 Y TELECOM 11.

FUNCIONALIDAD	PART NUMBER	DESCRIPCION
SWITCH CORE	C9500-32C-A	Cisco Catalyst 9500
SWITCH CORE	C9500-32C-A	Cisco Catalyst 9500
DISTRIBUCION	C9500-32QC-A	Cisco Catalyst 9500
DISTRIBUCION	C9500-32QC-A	Cisco Catalyst 9500

Fuente: Elaboración propia de los autores.

4.6.3.3. Equipamiento de TELECOM Remotos

Equipamiento considerado para el reemplazo de los Switches antiguos de una empresa de aeronavegación por los SW CATALYST 9300

Tabla 5 - Equipamiento de TELECOMs Remotos.

DEPENDENCIA	NODOS	CANTIDAD	MODELO
UNA EMPRESA DE AERONAVEGACIÓN	TELECOM 15	3	CISCO CATALYST 9300
UNA EMPRESA DE AERONAVEGACIÓN	TELECOM 14	6	CISCO CATALYST 9300

UNA EMPRESA DE AERONAVEGACIÓN	TELECOM 8	5	CISCO CATALYST 9300
UNA EMPRESA DE AERONAVEGACIÓN	TELECOM 9	1	CISCO CATALYST 9300
UNA EMPRESA DE AERONAVEGACIÓN	TELECOM 3	5	CISCO CATALYST 9300
UNA EMPRESA DE AERONAVEGACIÓN	TELECOM 11	4	CISCO CATALYST 9300
UNA EMPRESA DE AERONAVEGACIÓN	TELECOM 16	5	CISCO CATALYST 9300
UNA EMPRESA DE AERONAVEGACIÓN	TELECOM 1	8	CISCO CATALYST 9300
UNA EMPRESA DE AERONAVEGACIÓN	TELECOM 4	3	CISCO CATALYST 9300
UNA EMPRESA DE AERONAVEGACIÓN	TELECOM 2	1	CISCO CATALYST 9300
UNA EMPRESA DE AERONAVEGACIÓN	TELECOM 7	1	CISCO CATALYST 9300
UNA EMPRESA DE AERONAVEGACIÓN	TELECOM 10	2	CISCO CATALYST 9300
UNA EMPRESA DE AERONAVEGACIÓN	TELECOM 12	1	CISCO CATALYST 9300
UNA EMPRESA DE AERONAVEGACIÓN	TELECOM 13	3	CISCO CATALYST 9300
UNA EMPRESA DE AERONAVEGACIÓN	TELECOM 17	4	CISCO CATALYST 9300

Fuente: Elaboración propia de los autores.

4.6.4. Equipamiento del Proyecto

4.6.4.1. DNA Center

En el corazón de la automatización de la solución SD-Access se encuentra Cisco DNA Center. SD-Access está habilitado con un paquete de aplicación que se ejecuta como parte del software en Cisco DNA Center para diseñar, aprovisionar, aplicar políticas y facilitar la creación de un Campus inteligente cableado e inalámbrico.

Se implementará un Cluster de (03) DNA Center DN2-HW-APL en configuración HA (High Availability), considerado como SISTEMA DE AUTOMATIZACIÓN DE LA RED.

4.6.4.1.1. Topología DNA Center

Se muestra la topología con el detalle de interconexiones de los tres servidores que forman parte del Cluster, cada servidor usa 3 interfaces: Enterprise, Cluster y CIMC para gestión fuer de banda.

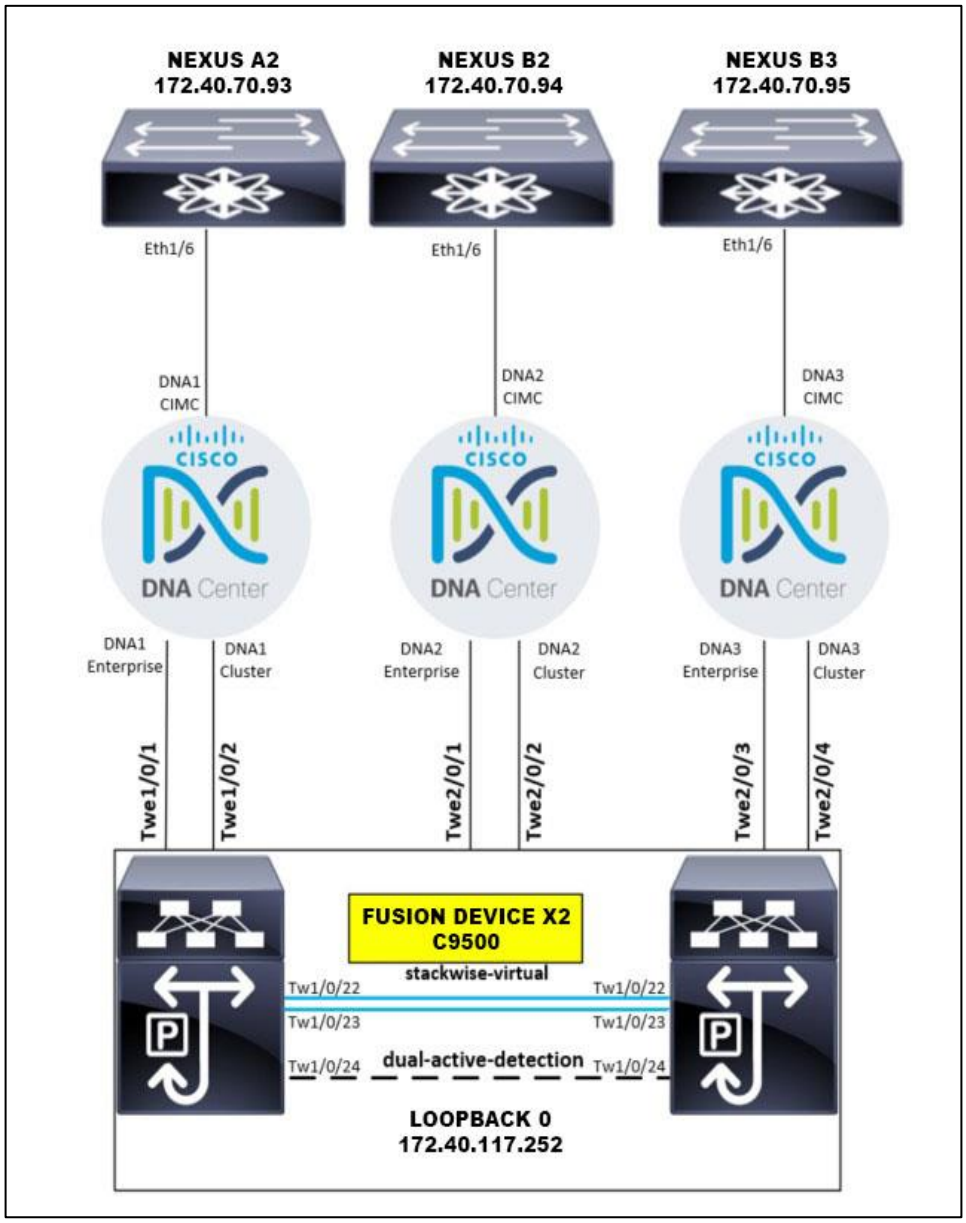

Figura 20 - Topología e Interconexiones DNA Center.
Fuente: Elaboración propia de los autores.

4.6.4.1.2. Direccionamiento DNA Center

Se presenta el direccionamiento IP asignado a los controladores del Cluster DNA en las siguientes tablas:

Tabla 6 - Direccionamiento IP DNA Center Fuera de Banda.

INTERFACE CIMC	Host IP address	Default Gateway
DNA1	172.40.119.171	172.40.119.1
DNA2	172.40.119.172	172.40.119.1
DNA3	172.40.119.173	172.40.119.1

Fuente: Elaboración propia de los autores.

Tabla 7 - Direccionamiento DNA Center Enterprise.

INTERFACE ENTERPRISE	VLAN	Host IP address	Default Gateway
DNA1	VLAN 71	172.40.71.171	172.40.71.1
DNA2	VLAN 71	172.40.71.172	172.40.71.1
DNA3	VLAN 71	172.40.71.173	172.40.71.1
DIRECCION VIRTUAL DEL CISCO DNA	VLAN 71	172.40.71.170	172.40.71.1

Fuente: Elaboración propia de los autores.

Tabla 8 - Direccionamiento Cluster DNA Center.

INTERFACE CISCO DNA - CLUSTER	Host IP address
DNA1	10.20.20.201
DNA2	10.20.20.202
DNA3	10.20.20.203
(VIP)	10.20.20.205

Fuente: Elaboración propia de los autores.

4.6.4.1.3. HA DNA Center

Cisco DNA Center admite una configuración de clúster de tres nodos, que proporciona alta disponibilidad tanto de software como de hardware. Se produce una falla de software cuando falla un servicio en un nodo. La alta disponibilidad del software implica la capacidad de reiniciar los servicios en el nodo o los nodos. Por ejemplo, si un servicio falla en un nodo en un clúster de tres nodos, ese servicio se reinicia en el mismo nodo o en uno de los otros dos nodos restantes.

Figura 21 - Alta disponibilidad Cluster DNA.
Fuente: Elaboración propia de los autores.

4.6.4.2. Identify Service Engine (ISE)

Cisco ISE es una plataforma seguridad de acceso a la red que permite una mayor gestión, control y consistencia para los usuarios y dispositivos que acceden a la red de una organización. ISE es una parte indispensable en el esquema de SD-Access para la implementación de políticas, perfilamiento y el control de acceso a la red.

La solución ISE a implementar consta de dos (02) servidores Cisco SNS-3615-K9 con versión de software 2.7 y parches 2 y 3 instalados.

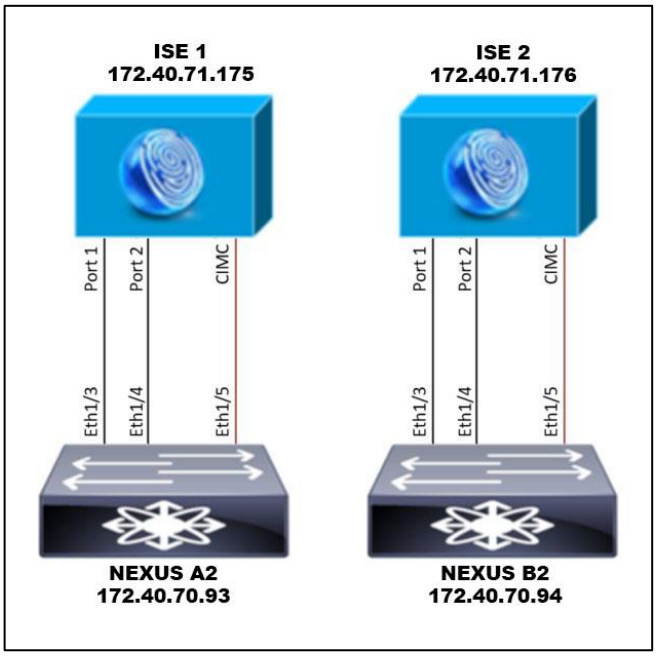

Figura 22 - Topología y conexiones Cisco ISE.
Fuente: Elaboración propia de los autores.

4.6.4.2.1. Direccionamiento ISE

Los servidores ISE estarán instalados en el Data Center con un direccionamiento perteneciente a la VLAN 71 como se muestra a continuación:

Tabla 9 - Direccionamiento IP CISCO ISE.

SOLUCION CISCO ISE	VLAN	Host IP address	Default Gateway
ISE1	VLAN 71	172.40.71.175	172.40.71.1
ISE2	VLAN 71	172.40.71.176	172.40.71.1

Fuente: Elaboración propia de los autores.

4.6.4.2.2. HA ISE

Un deployment que tiene más de un nodo Cisco ISE se denomina deployment distribuido. Para lograr el failover y mejorar el rendimiento, se puede configurar el deployment con varios nodos Cisco ISE de forma distribuida. En un deployment distribuido de Cisco ISE, las actividades de administración y supervisión están centralizadas y el procesamiento se distribuye entre las PSN (Policy Service nodes).

El registro de un nuevo nodo ISE para un deployment distribuído se realiza en la ruta *Administration/System/Deployment*

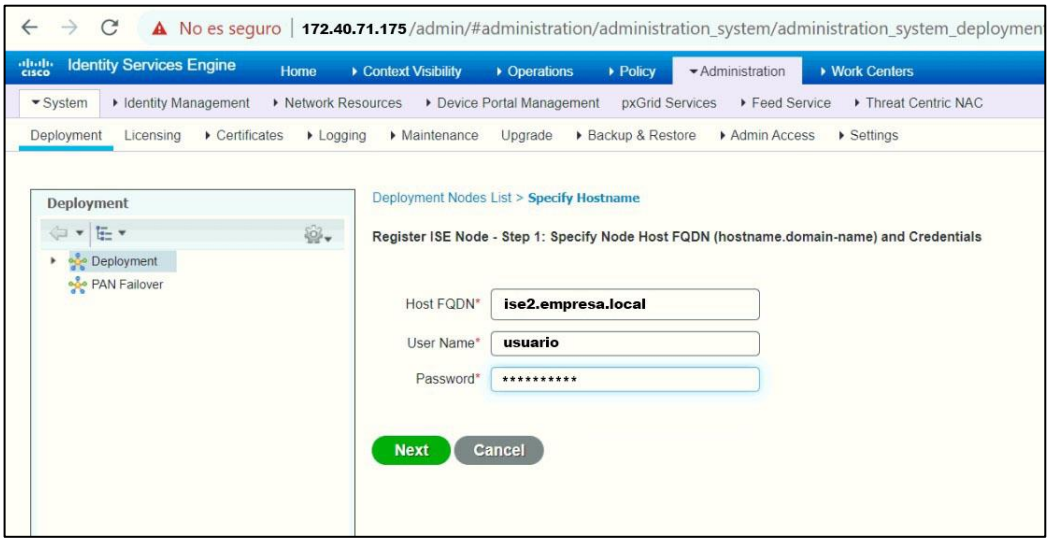

Figura 23 - Registro de Nodo ISE secundario – HA.
Fuente: Elaboración propia de los autores.

4.6.4.3. WLC

En una red inalámbrica podemos usar el Wireless LAN Controller para centralizar el control de los APs en lugar de delegar el control a cada uno de ellos.
Dicho rol está compuesto por dos (02) WLC Catalyst C9800-L-F-K9 con versión de software 16.12.02s.

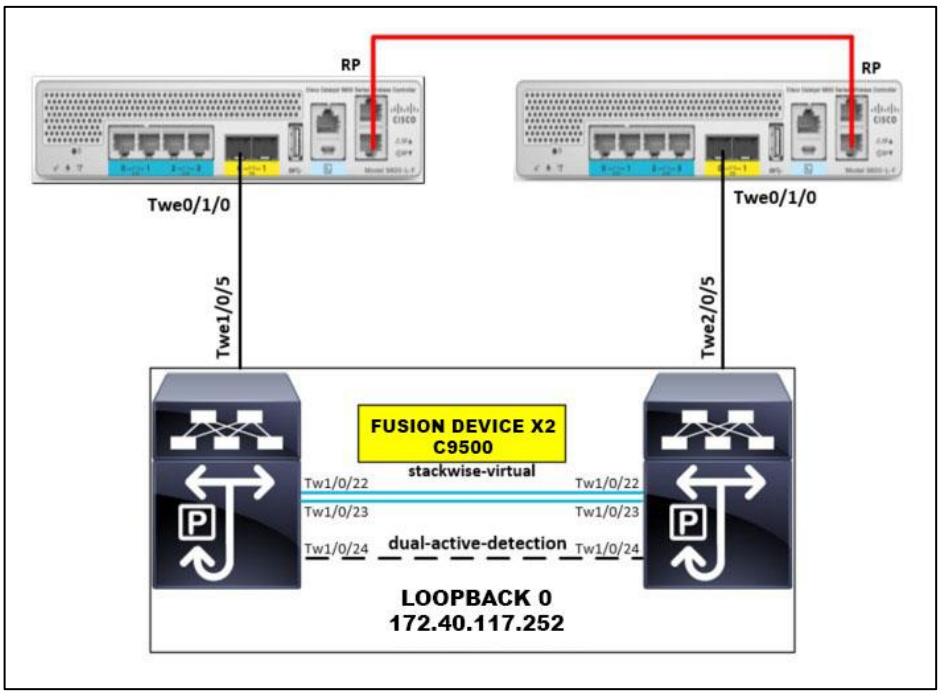

Figura 24 - Topología y conexiones WLC.
Fuente: Elaboración propia de los autores.

4.6.4.3.1. Direccionamiento WLC

Los WLC se encuentran en la VLAN 71 con el siguiente direccionamiento IP asignado:

Tabla 10 - Direccionamiento IP WLC.

CONTROLADORES DE ACCESO INALAMBRICO	VLAN	Host IP address	Default Gateway
WLC1	VLAN 71	172.40.71.191	172.40.71.1
WLC2	VLAN 71	172.40.71.192	172.40.71.1
DIRECCION VIRTUAL DE ESTOS EQUIPOS	VLAN 71	172.40.71.190	172.40.71.1

Fuente: Elaboración propia de los autores.

4.6.4.3.2. HA WLC

La capacidad SSO de alta disponibilidad en el WLC permite que los APs establezcan un túnel CAPWAP con el controlador inalámbrico activo para compartir una copia espejo del AP y la base de datos del cliente con el controlador inalámbrico Standby. Los APs no pasan al estado de descubrimiento y los clientes no se desconectan cuando falla el controlador inalámbrico activo y el controlador inalámbrico en espera toma el control de la red como WLC activo. Solo se mantiene un túnel CAPWAP a la vez entre los AP y el controlador inalámbrico que se encuentra en estado activo.

Los requerimientos para levantar HA entren dos WLC son los siguientes:

- El par HA solo se puede formar entre dos controladores inalámbricos del mismo factor de forma.
- Ambos controladores deben ejecutar la misma versión de software para formar el par HA.
- Latencia máxima del enlace RP = 80 ms RTT, ancho de banda mínimo = 60 Mbps y MTU mínimo = 1500.

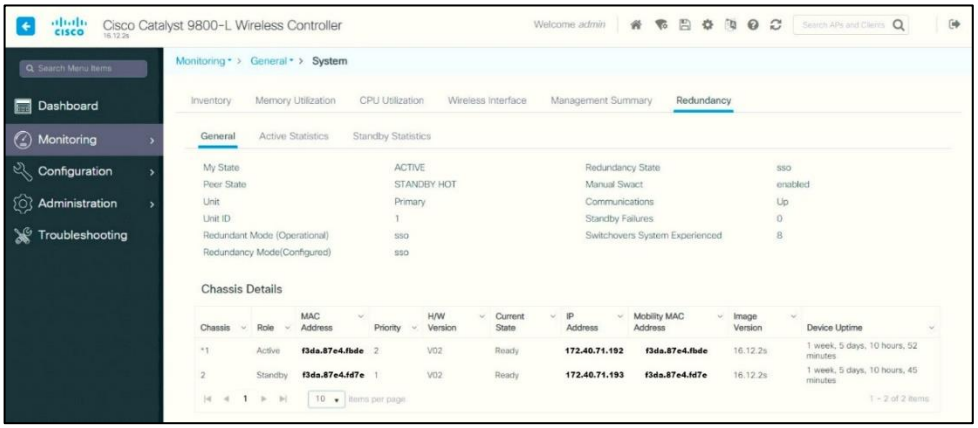

Figura 25 - Configuración HA WLC.
Fuente: Elaboración propia de los autores.

4.6.4.4. Nexus Data Center

Se están considerando cinco (05) switches de acceso data center, de los cuales dos (02) switches son para el Core data center y tres (03) son switches de servidores que cumplirán la

función de conexión de los servicios compartidos (DNA center, Cisco ISE, DNS/DHCP/IPAM).

Los switches a implementar son de la gama Nexus N9K-C93108TC-EX como switches de Data Center y servidores y estarán interconectados en un modelo de redundancia de capa 2 tradicional. Los dos Nexus principales brindarán la conexión hacia el Fusion Device y a su vez a otros servicios fuera del Datacenter (TELECOM 5).

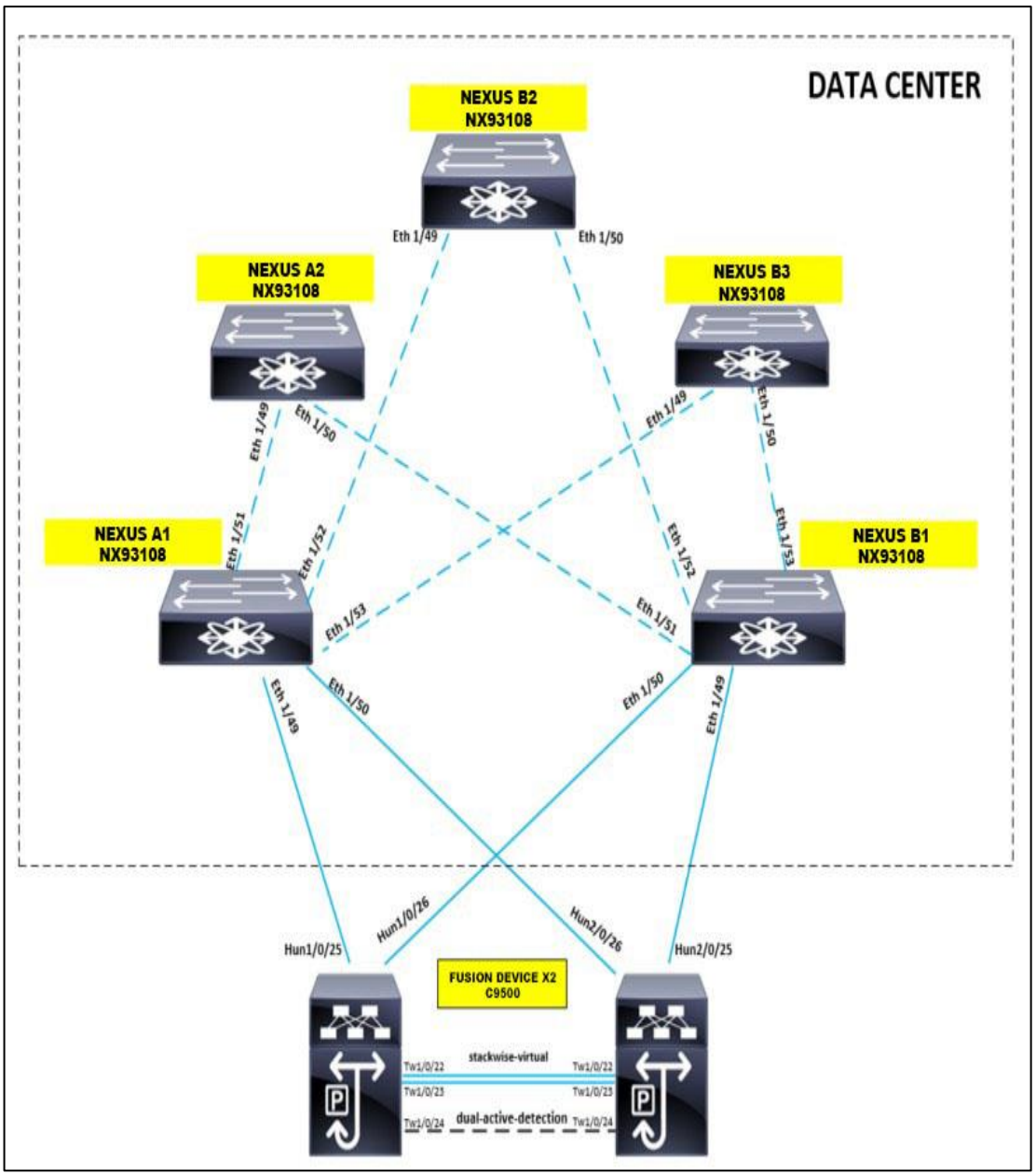

Figura 26 - Topología Data Center - Data Center.
Fuente: Elaboración propia de los autores.

4.6.4.4.1. Direccionamiento Nexus

Se muestra la configuración IP de los switches Nexus para fines de gestión. La gestión de los switches Nexus será a través de la VLAN 70.

Tabla 11 - Direccionamiento IP Switches Nexus.

HOST	VLAN	Host IP address	Default Gateway
NEXUS 1A	VLAN 70	172.40.70.91	172.20.70.1
NEXUS 1B	VLAN 70	172.40.70.92	172.20.70.1
NEXUS 2A	VLAN 70	172.40.70.93	172.20.70.1
NEXUS 2B	VLAN 70	172.40.70.94	172.20.70.1
NEXUS 3B	VLAN 70	172.40.70.95	172.20.70.1

Fuente: Elaboración propia de los autores.

4.6.4.5. Fusion Device

El término genérico enrutador de fusión o dispositivo de fusión, proviene de MPLS Layer 3 VPN. El concepto básico es que el enrutador de fusión es consciente de prefijos disponibles dentro de cada VPN (VRF), ya sea debido a la configuración de enrutamiento estático o a través del emparejamiento de rutas, y pueden, por lo tanto, fusionar estas rutas juntas. Las responsabilidades de un dispositivo de fusión genérico son enrutar el tráfico entre VRF separadas o para enrutar el tráfico hacia y desde una VRF a un grupo compartido de recursos en servidores globales como DHCP y DNS.

En una implementación de SD-Access, el dispositivo de fusión tiene una única responsabilidad: proporcionar acceso a servicios compartidos para los puntos finales en el fabric. Dicho rol estará cubierto por dos (02) switches Catalyst C9500-24Y4C-A

4.6.4.5.1. HA Fusion Device

Cisco StackWise Virtual es una tecnología de virtualización de sistemas de red que empareja dos switches en un switch virtual. Esta tecnología simplifica la eficiencia operativa ya que podemos tener el control en un plano para administrar los switches apilados. A través de Cisco StackWise Virtual, el switch de fusión utiliza dos conexiones para sincronización de información y una interface de control.

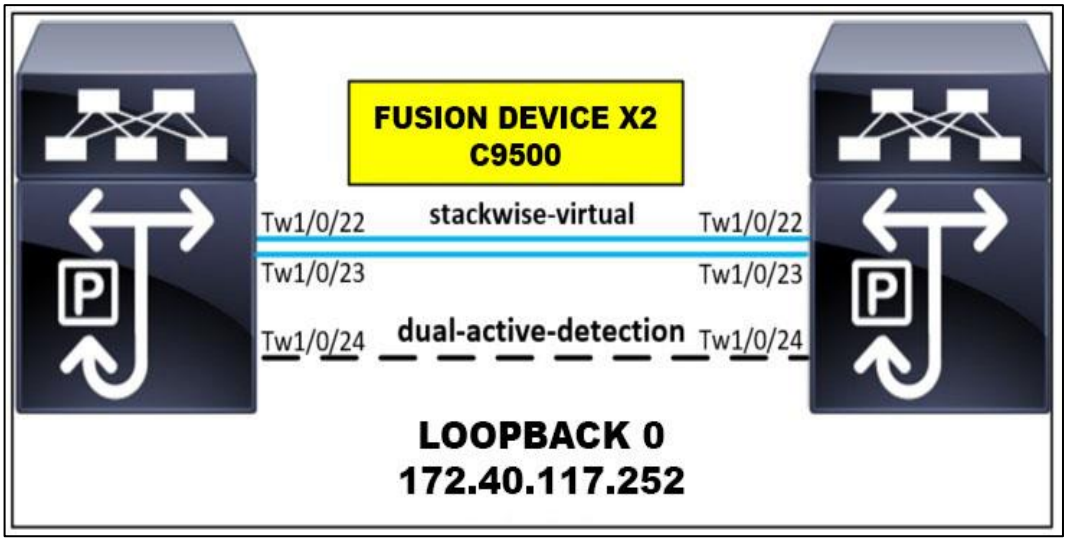

Figura 27 - Fusion Device HA Stackwise virtual.
Fuente: Elaboración propia de los autores.

4.6.5. Diseño

El primer paso luego de la instalación del DNA Center es ingresar al apartado de Diseño, con la finalidad planificar la jerarquía, ubicaciones, parámetros de red, repositorios de software, etc.

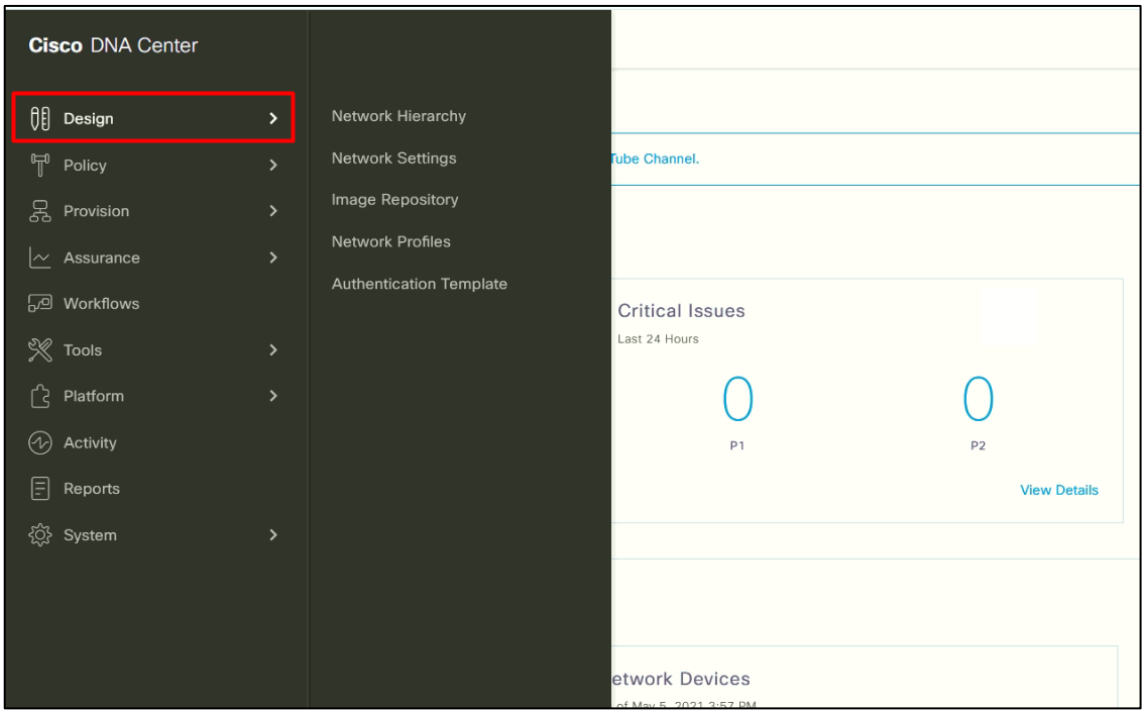

Figura 28 - DNA Center – Design.
Fuente: Elaboración propia de los autores.

4.6.5.1. Jerarquía

El primer paso de la implementación es diseñar una red empresarial con una jerarquía de ubicaciones, edificios y pisos. Con la creación de esta jerarquía, la red está lista para la gestión y los servicios básicos.

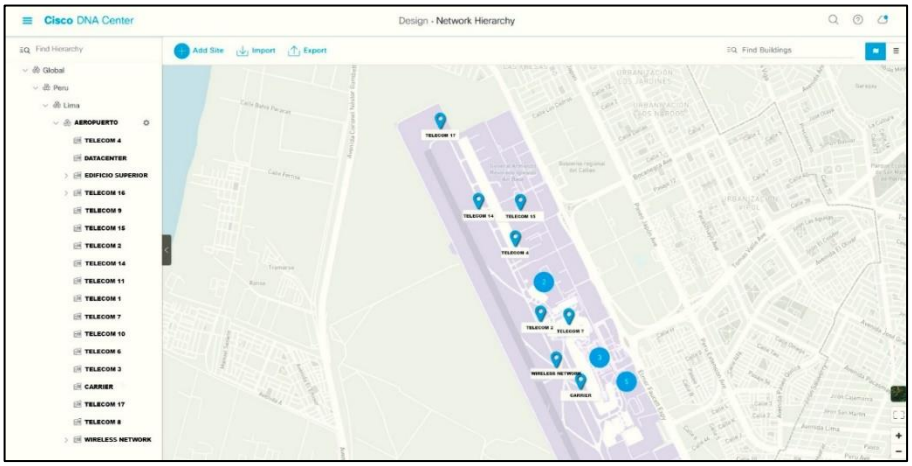

Figura 29 - DNA Center – Jerarquía.
Fuente: Elaboración propia de los autores.

4.6.5.2. Network Settings

Dentro de Network Settings se definen los parámetros y servicios generales de la red como DHCP, DNS, servidores AAA, NTP, zona horaria, etc. Estos servicios pueden ser configurados de forma global o asignar recursos por sitios de acuerdo a la Jerarquía creada en el paso anterior.

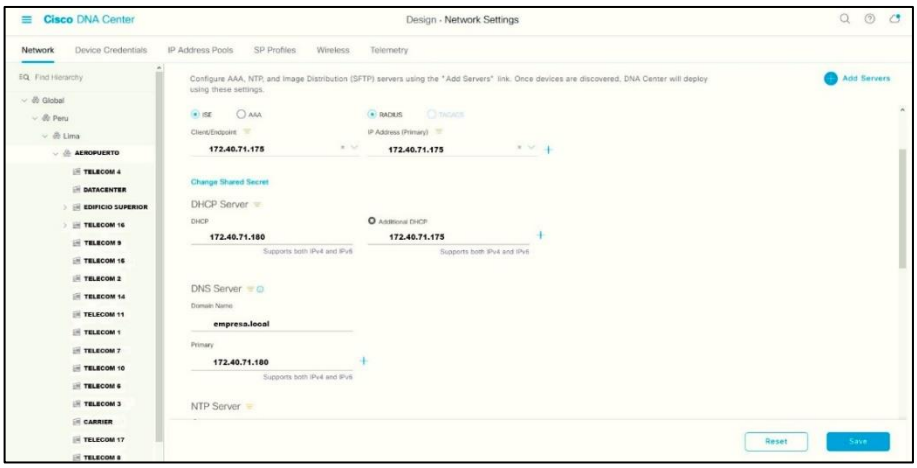

Figura 30 - DNA Center - Network Settings.
Fuente: Elaboración propia de los autores.

Una vez definidos los servicios de la red, DNA Center hará un push de la configuración a todos los switches del fabric durante el provisionamiento.

4.6.5.3. Credenciales

Aquí se configuran las credenciales de Usuario que usará DNA Center para ingresar remotamente a los equipos, así mismo las comunidades SNMP que serán agregadas durante el provisionamiento.

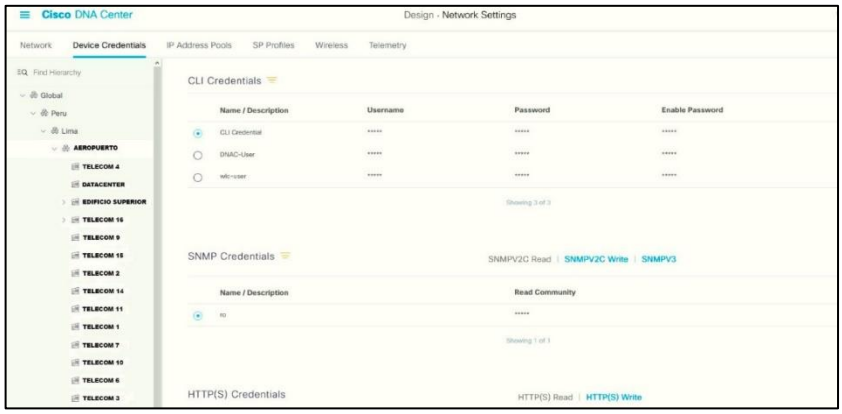

Figura 31 - DNA Center – Credenciales.
Fuente: Elaboración propia de los autores.

4.6.5.4. Pool de direcciones IP

La reserva de Pools de IPs es un paso muy importante durante la implementación de una infraestructura SD-Access. Sólo se podrá usar un pool de IPs en un Site si este ha sido reservado previamente para este Site.

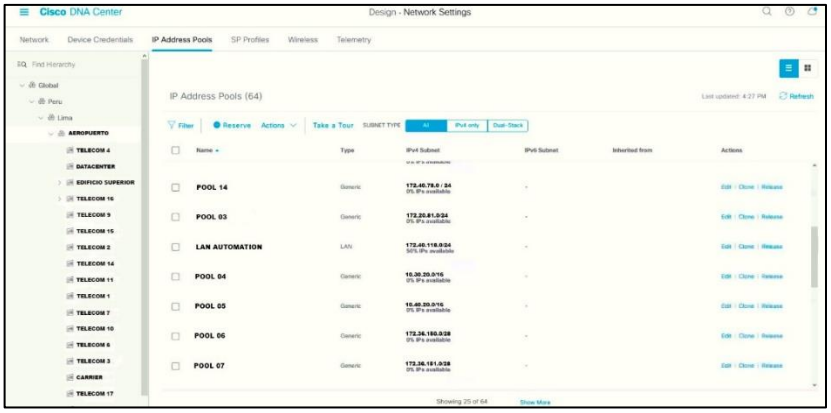

Figura 32 - Reserva Pool de IPs.
Fuente: Elaboración propia de los autores.

Para la reserva de pools en la red de una empresa de aeronavegación fue tomada en consideración la configuración actual de Vlans (Datos, voz, impresoras, infraestructura pasiva, SCADA, etc.). Adicionalmente se reservaron pools dedicados al funcionamiento del underlay y como se muestra en la siguiente tabla:

Tabla 12 - Pools Reservadas – Underlay.

POOL IP	NOMBRE	DESCRIPCIÓN
172.40.116.0/24	Border-Handoff	Por cada VN configurada se creará automáticamente una instancia de ruteo BGP en el border para el overlay, las ips para cada VN serán tomadas de este pool.
172.40.117.0/24	Global Routing Border - Fusion	Pool utilizado para la configuración de ruteo global entre los border-fusión y border1-border2. Adicionalmente se utilizan ips para las loopbacks de gestión de los border y fusión.
172.40.118.0/24	Lan Automation	DNA Center tomará ips disponibles de este pool para la asignación de loopbacks de los Edge nodes y configuración de ruteo entre las conexiones de los nodos dentro del Fabric.

Fuente: Elaboración propia de los autores.

4.6.5.5. Wireless

Dentro de la parte de Diseño también se encuentra la opción de crear redes inalámbricas. DNA se integra junto con los WLC y asume las funciones de administración de las redes inalámbricas. DNA no funciona como WLC, sino que hace un push de la configuración a los WLC mediante el protocolo Netconf, manteniendo así una gestión centralizada.

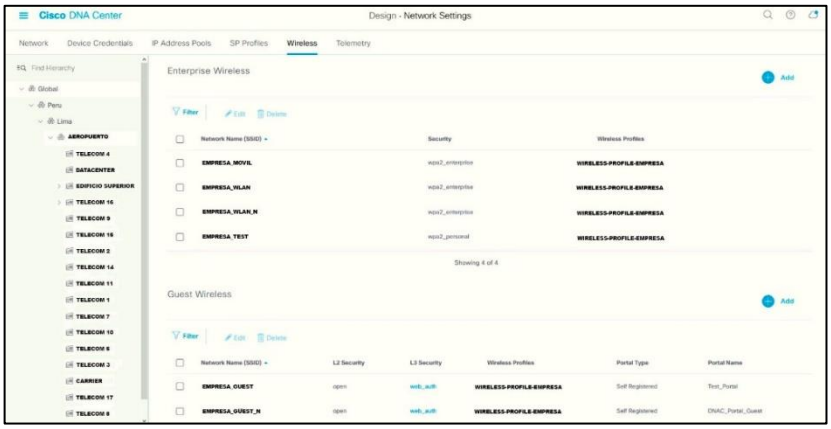

Figura 33 - Creación de SSIDs.
Fuente: Elaboración propia de los autores.

El detalle de la configuración de redes inalámbricas, así como la integración a otros servidores (WLC e ISE) será revisado en los capítulos posteriores de este documento.

4.6.6. Policy

Después de completar el diseño de la red SD Access se procede a configurar todo lo referente a políticas. El requisito importante es que en este punto el ISE esté integrado al DNA para la réplica de políticas entre ambos.

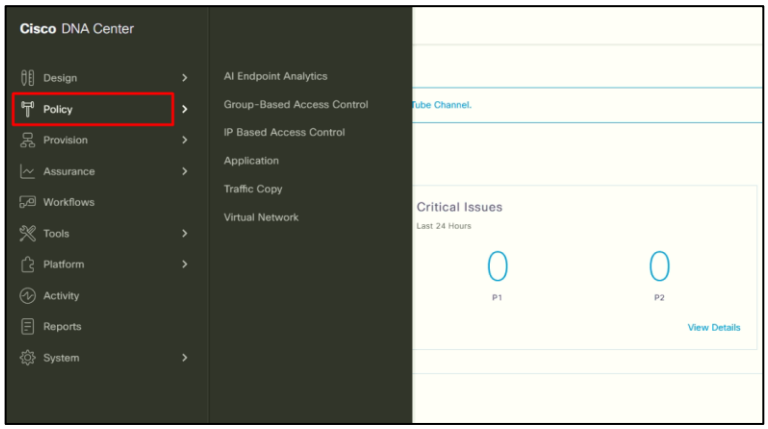

Figura 34 - DNA Center – Policy.
Fuente: Elaboración propia de los autores.

4.6.6.1. Policies

DNA Center proporciona una matriz de políticas muy intuitiva para la configuración de políticas de acceso similar a la de ISE, donde los filtros se aplican en base a un origen y un destino en base a identidades. Al igual que con un WLC, DNA hace el push

de las políticas a ISE y es este quien se encarga de la ejecución del control de acceso.

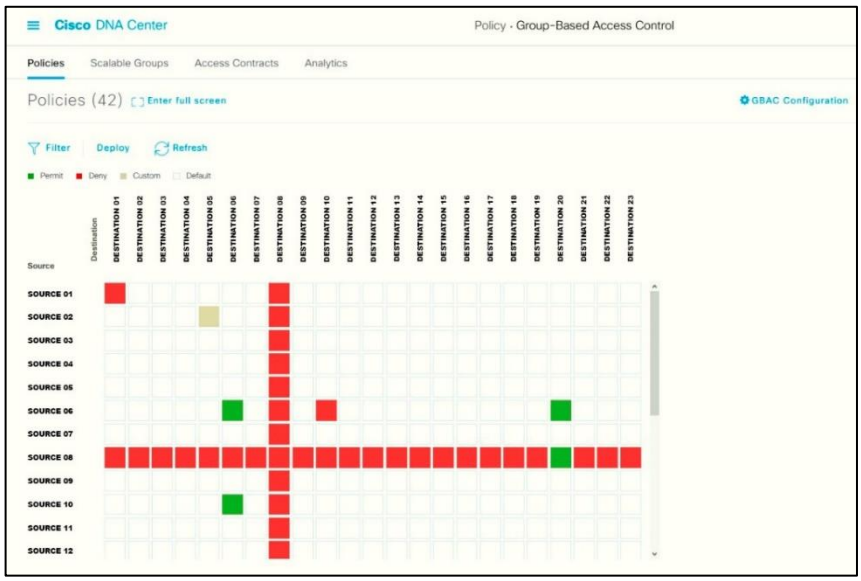

Figura 35 - Matriz de Políticas en DNA.
Fuente: Elaboración propia de los autores.

De igual forma se puede observar que la matriz ha sido desplegada en ISE por el DNA Center:

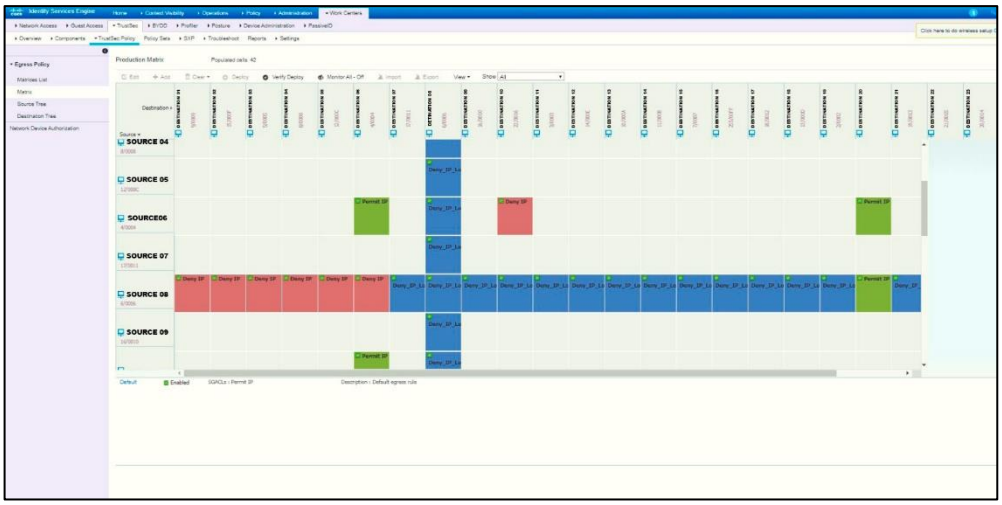

Figura 36 - Matriz de Políticas en ISE.
Fuente: Elaboración propia de los autores.

A diferencia de las Access-list convencionales, las políticas en SD-Access no se aplican en base a direcciones de red origen o destino, sino en base a identidades, dichas identidades están representadas por un tag conocido como “Scalable Group Tag”.

4.6.6.2. Scalabe Group Tag (SGT)

Una nueva forma de clasificar la identidad de los equipos finales es con el uso de etiquetas. Las etiquetas SGT se asignan a los endpoints que se conectan a la red que tienen políticas de red comunes. Cada SGT se identifica mediante un valor único. El SGT al que pertenece un host se puede asignar estática o dinámicamente (en base a perfilamiento en ISE) y se puede utilizar como clasificador en políticas de red.

Figura 37 - DNA Center - Lista de SGTs.
Fuente: Elaboración propia de los autores.

4.6.6.3. Virtual Network (VN)

Las Virtual Network brindan en un entorno SD-Access una segmentación a nivel macro, con la cual se pueden agrupar diferentes servicios y pools de IPs de acuerdo a las necesidades del campus. Una VN sería análogamente lo que es una VRF para una red tradicional.

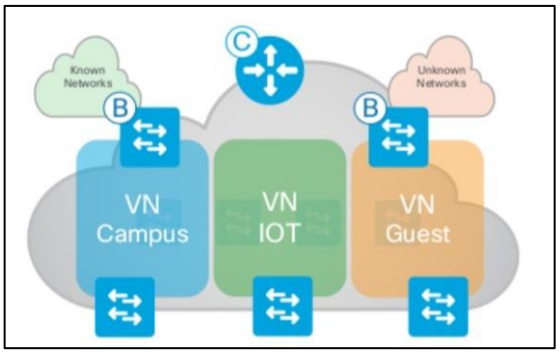

Figura 38 - Virtual Network – Esquema.
Fuente: CISCO Live! 2019.

Se crearon 7 Virtual Networks en la infraestructura de una empresa de aeronavegación para la macro-segmentación. Dos VNs se crean por default durante la instalación de DNA Center.

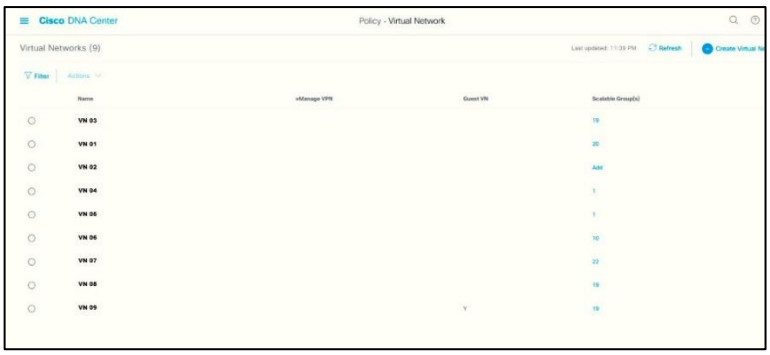

Figura 39 - DNA Center - Virtual Networks.
Fuente: Elaboración propia de los autores.

4.6.7. Provision

4.6.7.1. Inventario

En el inventario podremos ver la lista de los dispositivos que son administrados por DNA Center e información relevante como hostname, dirección IP, Site al que pertenece, serial number, versión de software, etc.

Por otro lado, desde el inventario se pueden realizar tareas básicas como provisionamiento de los equipos, programar upgrades de software o iniciar el proceso de LAN Automation.

Hay diversas formas de agregar dispositivos al inventario, las utilizadas para este proyecto son LAN Automation y Discovery manual.

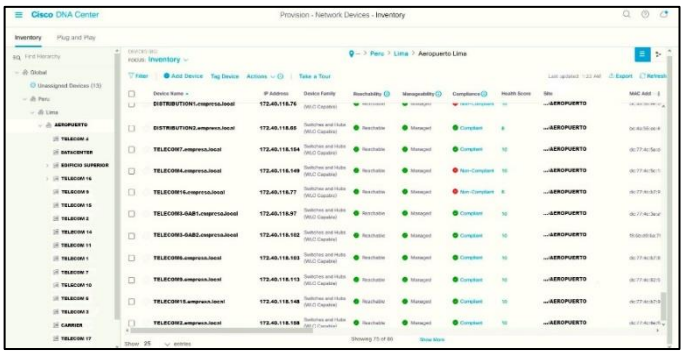

Figura 40 - Inventario DNA Center.
Fuente: Elaboración propia de los autores.

4.6.7.2. LAN Automation

LAN Automation es un proceso que ejecuta DNA Center para descubrir equipos nuevos sin configuración alguna, con la ayuda de un servidor DHCP y el proceso de Plug and Play. Una vez que el equipo ha sido descubierto se le aplica la configuración necesaria para levantar el underlay: Loopback, enlaces L3 y enrutamiento ISIS.

DNA Center solicita que se ingrese un dispositivo como semilla (en este caso el switch de distribución) y el puerto donde estará conectado el nuevo switch para iniciar el descubrimiento:

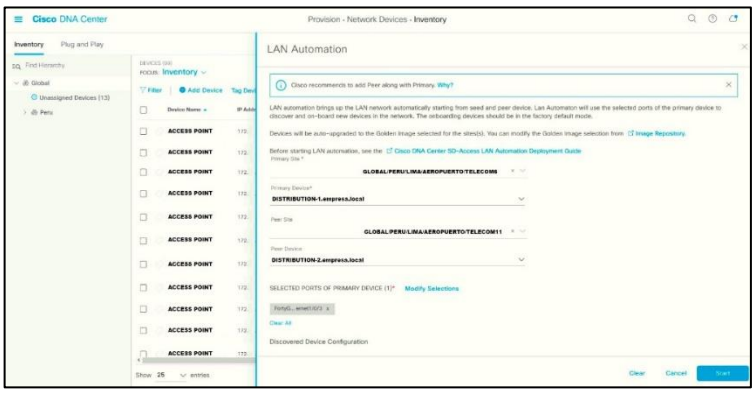

Figura 41 - Proceso LAN Automation.
Fuente: Elaboración propia de los autores.

Todas las conexiones entre los switches en SD-Access deben ser de capa 3, y LAN Automation se encarga de asegurar este requisito usando ips libres del pool reservado para LAN Automation en el proceso de Diseño.

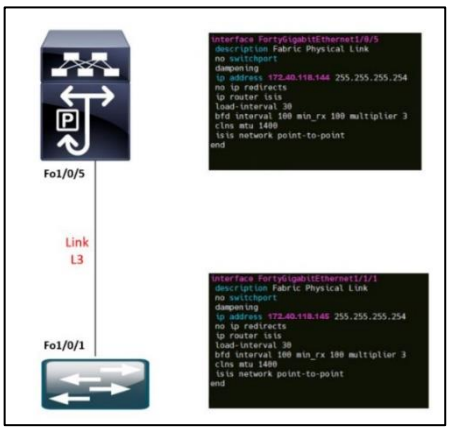

Figura 42 - Resultado LAN Automation.
Fuente: Elaboración propia de los autores.

4.6.7.3. Fabric

Una vez que los dispositivos han sido descubiertos por LAN Automation y agregados al inventario estos deben ser asignados al Fabric con un rol específico (Border, control, plane o Edge).

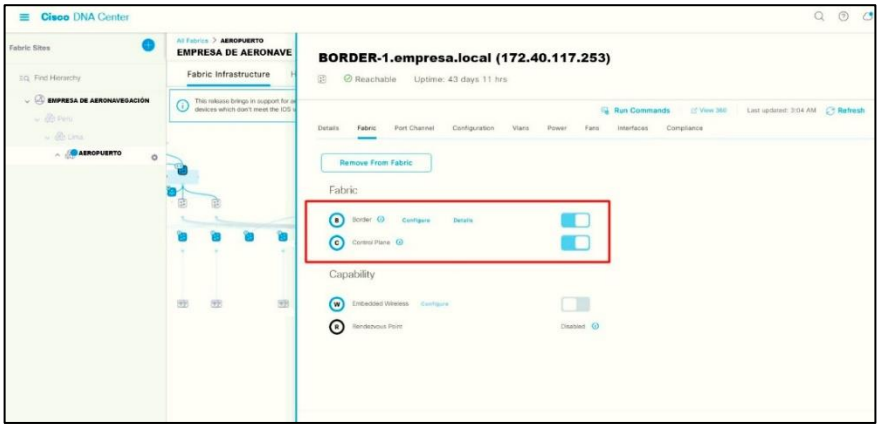

Figura 43 - Agregación de Dispositivo al Fabric.
Fuente: Elaboración propia de los autores.

Con el fabric levantado estamos listos para configurarlo: Asignación de pools a las VNs, asignación a los SSIDs y asignación de puertos de switch.

4.6.7.3.1. Virtual Networks

En este punto se configuran las VN que fueron creadas en fase de Policy. Aquí es donde se agregan los pools reservados y se asigna un SGT de forma manual.

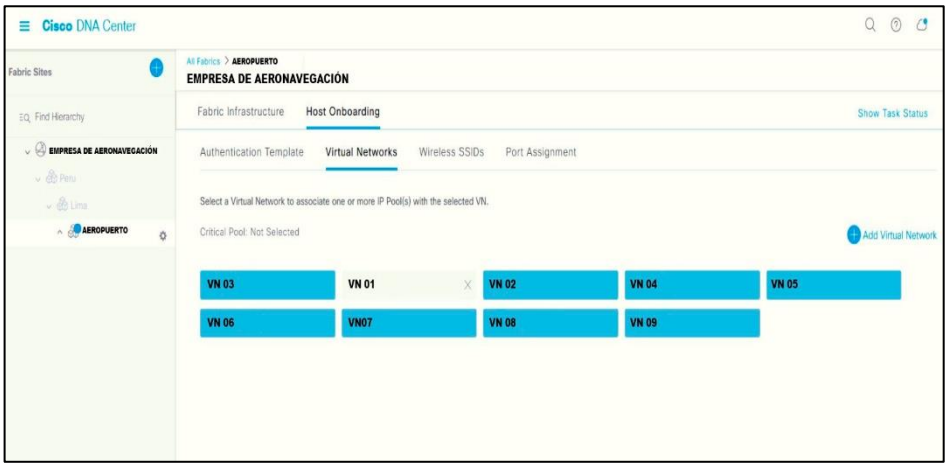

Figura 44 - VNs en el Fabric.
Fuente: Elaboración propia de los autores.

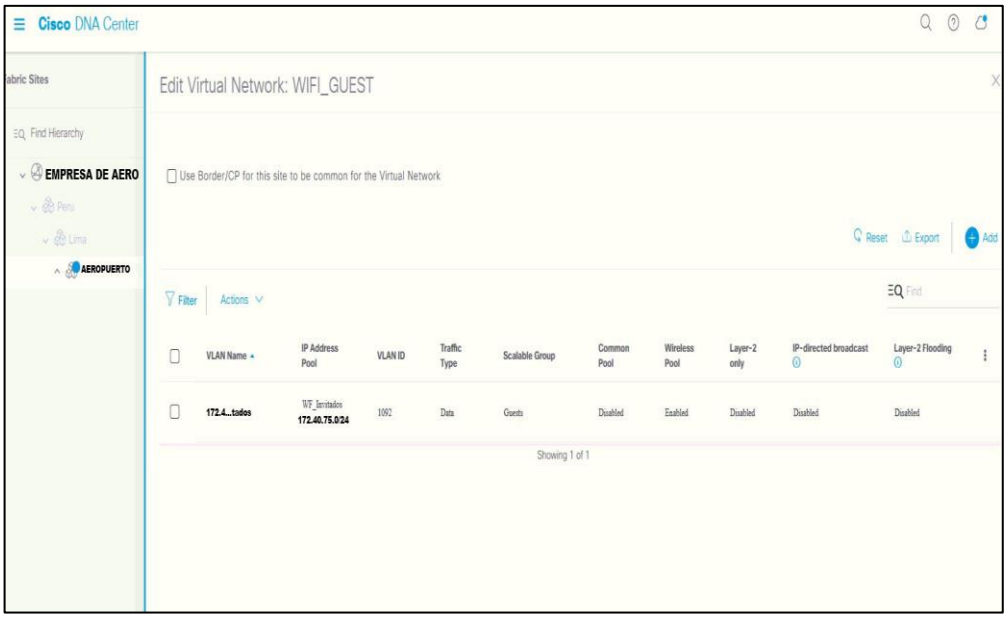

Figura 45 - Asignación de pool a VNs.
Fuente: Elaboración propia de los autores.

En la siguiente tabla se muestra la distribución de pools IP que tendrá cada VN dentro del Fabric.

Tabla 13 - Distribución de Pools en las VNs.

VN	Pool IP	Pool Name
VN 1	-	-
VN 2	172.40.76.0/24	Pool 1
	172.40.270.0/24	Pool 2
VN 3	172.40.81.0/24	Pool 3
	172.40.77.0/24	Pool 3
VN 4	10.30.20.0/16	Pool 4
	10.40.20.0/16	Pool 5
	172.36.150.0/28	Pool 6
	172.36.151.0/28	Pool 7
	172.70.25.0/24	Pool 8
	172.41.21.0/24	Pool 9
	172.40.79.0/24	Pool 10
VN 5	172.48.21.0/24	Pool 11
	172.49.21.0/24	Pool 12
VN 6	172.40.70.0/24	Pool 13
	172.40.78.0/24	Pool 14
	172.40.80.0/27	Pool 15
	172.41.60.0/24	Pool 16
	172.82.21.0/24	Pool 17

VN 7	172.40.30.0/23	Pool 18
	172.40.32.0/23	Pool 19
	172.40.34.0/23	Pool 20
	172.40.36.0/23	Pool 21
	172.40.38.0/23	Pool 22
	172.40.40.0/23	Pool 23
	172.40.42.0/23	Pool 24
	172.40.44.0/23	Pool 25
	172.40.46.0/23	Pool 26
	172.40.48.0/23	Pool 27
	172.40.50.0/23	Pool 28
	172.40.52.0/23	Pool 29
	172.40.54.0/23	Pool 30
	172.40.56.0/23	Pool 31
	172.40.58.0/23	Pool 32
	172.41.30.0/23	Pool 33
	172.41.32.0/23	Pool 34
	172.41.34.0/23	Pool 35
	172.41.36.0/23	Pool 36
	172.41.38.0/23	Pool 37
	172.41.40.0/23	Pool 38
	172.41.42.0/23	Pool 39
	172.41.44.0/23	Pool 40
	172.41.46.0/23	Pool 41
	172.41.48.0/23	Pool 42
	172.41.50.0/23	Pool 43
	172.41.52.0/23	Pool 44
	172.41.54.0/23	Pool 45
	172.41.56.0/23	Pool 46
	172.41.58.0/23	Pool 47
VN 8	172.40.73.0/24	Pool 48
	172.40.74.0/24	Pool 49
	172.40.82.0/24	Pool 50
	172.40.83.0/24	Pool 51
VN 9	172.40.75.0/24	Pool 52

Fuente: Elaboración propia de los autores.

4.6.7.3.2. Wireless SSIDs

Aquí se agregan los pools para cada SSID, se debe tener en cuenta que un SSID no va a ser irradiado por

los APs hasta que tenga un pool asignado.

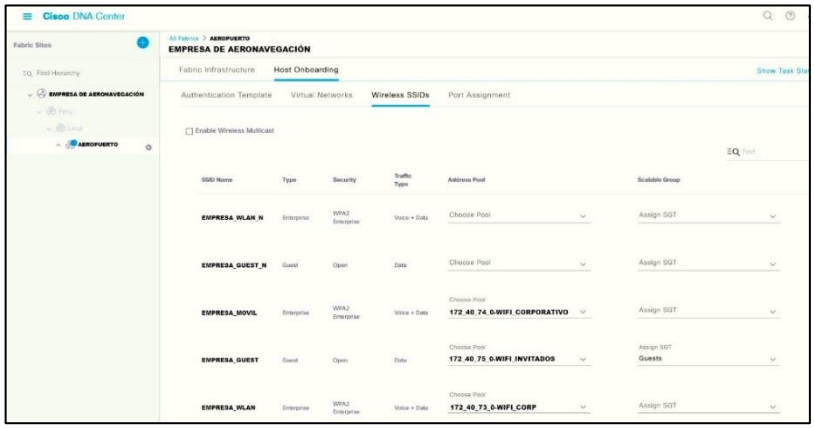

Figura 46 - Asignación de Pool y SGT a SSIDs.
Fuente: Elaboración propia de los autores.

4.6.7.3.3. Port Assignment

La asignación de un pool a un puerto puede realizarse de forma automática o manual, en ambos casos, el pool de be estar asignado a la VN correspondiente para poder tenerla disponible en el puerto.

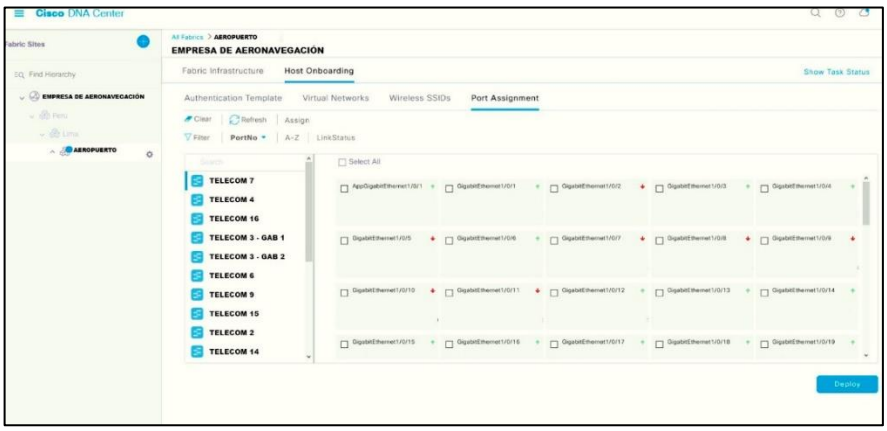

Figura 47 - Asignación / Configuración de puertos.
Fuente: Elaboración propia de los autores.

4.6.8. Assurance

Cisco DNA Analytics y Assurance prove visibilidad end-to-end en toda la red. La solución colecto data de multiples fuentes como dispositivos y aplicaciones para obtener una vista general de la salud de la red e incluso predecir degradaciones o problemas antes que sucedan.

Figura 48 - Network Assurance.
Fuente: Elaboración propia de los autores.

4.6.9. Layer 2 Handoff

Layer 2 handoff es un feature que permite a la red SD-Access extender una Vlan del Fabric SD Access hacia la red tradicional para propósitos de migración. Esto se logra conectando el Border con un dispositivo de la red tradicional en capa 2 (de preferencia el Switch Core actual).

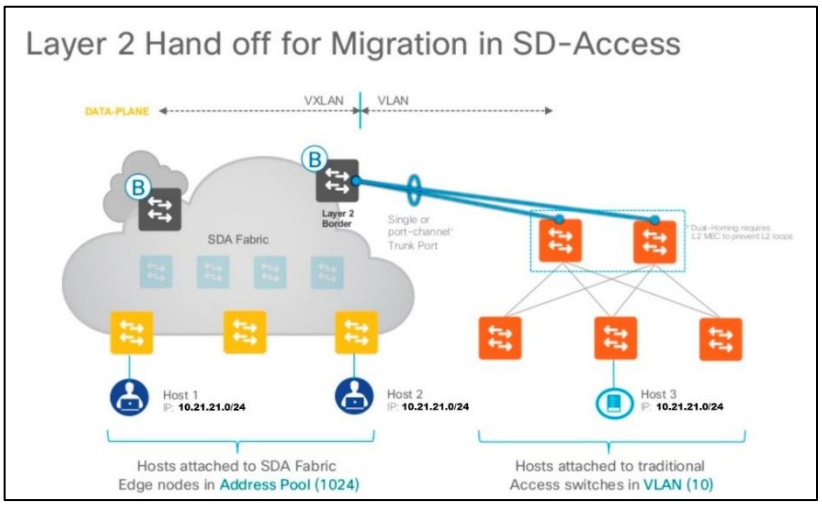

Figura 49 - Layer 2 Handoff General.
Fuente: CISCO Live! 2019.

Como bien se mencionó, esta funcionalidad debe ser usado con cautela y de forma temporal mientras dure la migración ya que se dejaría el acceso libre a problemas de capa 2 como tormentas de broadcast, además que tiene la limitante de sólo dejar pasar hasta 8000 direcciones MAC.

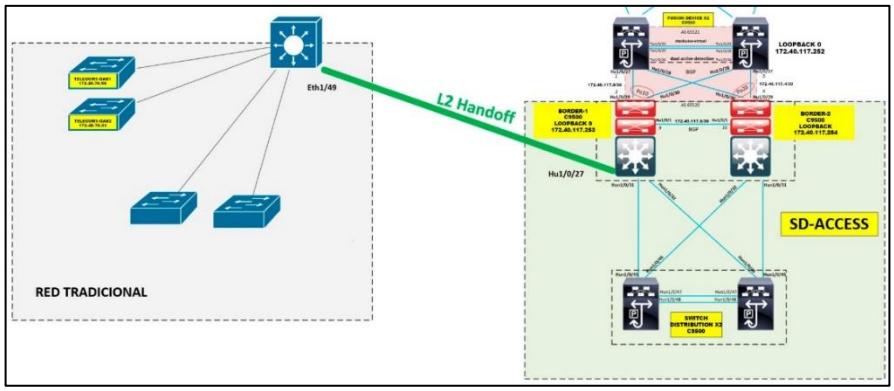

Figura 50 - Layer 2 Handoff.
Fuente: Elaboración propia de los autores.

4.6.10. Integraciones

DNA Center es un orquestador que trabaja en conjunto con otras soluciones para una tener una mejor visibilidad y control de la red. Estas soluciones pueden ser de la marca Cisco o cualquier otro vendor y el protocolo generalmente usado para la integración se conoce como PxGrid.

4.6.10.1. Integración DNA – ISE

Cisco ISE se integra a DNA usando PxGrid, una vez sincronizados ambos compartirán toda la información de dispositivos, políticas, SGTs, etc, con la finalidad de cumplir con las restricciones de acceso.

La configuración de esta integración se realiza en la Sección Settings de DNA Center:

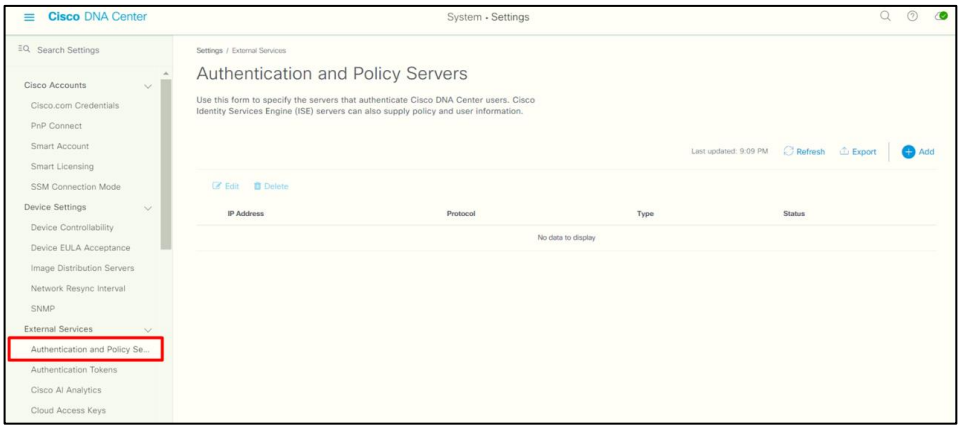

Figura 51 - Integración DNA-ISE - 1er Paso.
Fuente: Elaboración propia de los autores.

Rellenar los campos solicitados: Dirección IP, FQDN, credenciales:

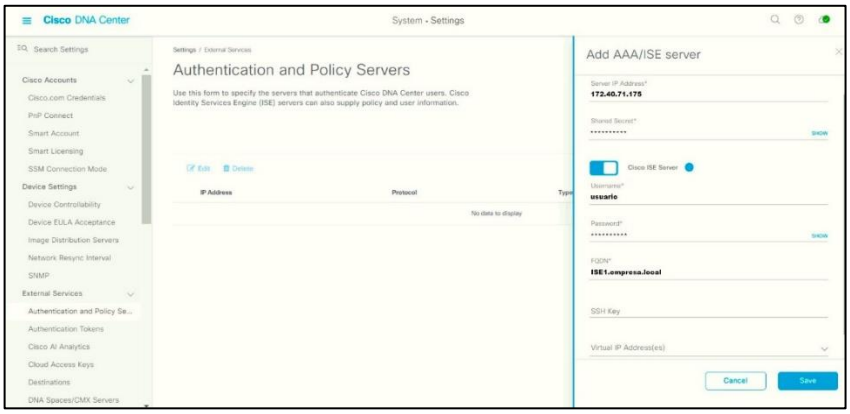

Figura 52 - Integración DNA-ISE - 2do Paso.
Fuente: Elaboración propia de los autores.

Finalmente ingresar al ISE, sección PxGrid Services y aprobar la solicitud de DNA Center:

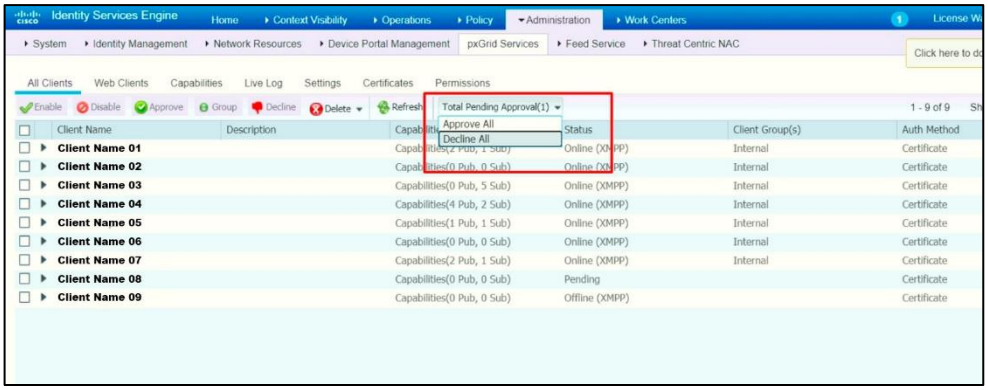

Figura 53 - Integración DNA-ISE - 3er Paso.
Fuente: Elaboración propia de los autores.

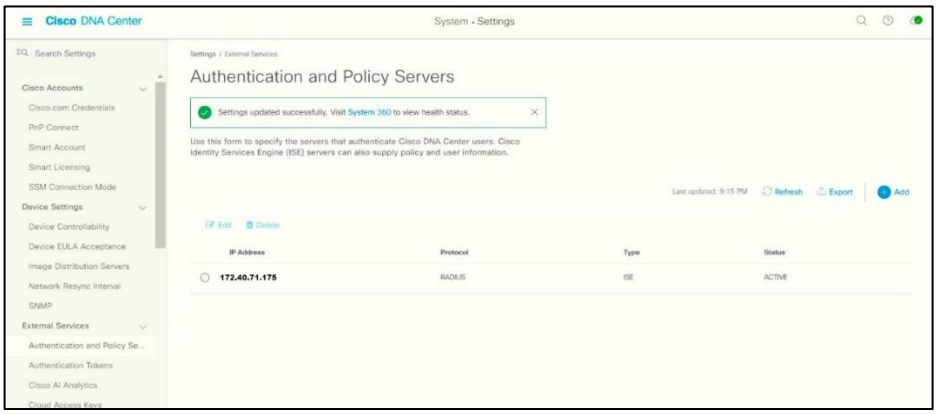

Figura 54 - Integración DNA-ISE – Finalizado.
Fuente: Elaboración propia de los autores.

4.6.10.2. Integración ISE – AD

Para aplicar políticas de autenticación y autorización en base a usuarios del dominio se procedió a integrar el ISE con el AD de una empresa de aeronavegación mediante el siguiente procedimiento:

Administration/Identity Management/External Identity Group

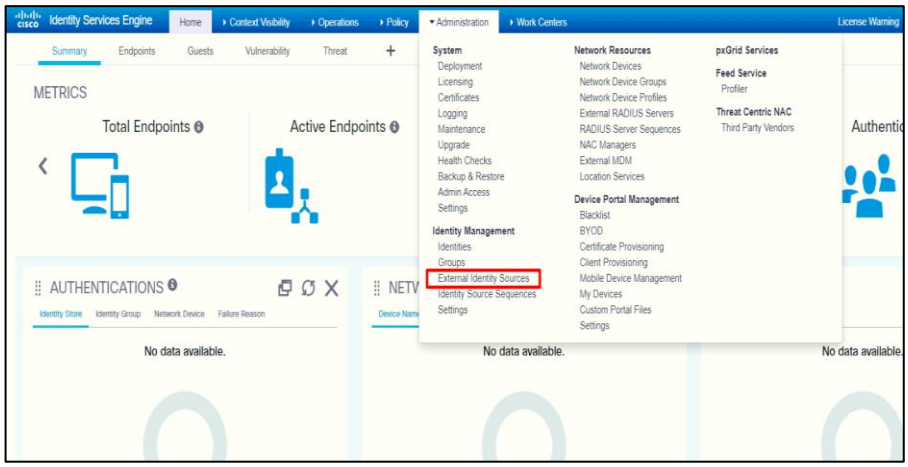

Figura 55 - Integración ISE-AD - 1er Paso.
Fuente: Elaboración propia de los autores.

En el menú izquierdo clic en Active Directory y luego clic en “Add” Para agregar un nuevo controlador de dominio.

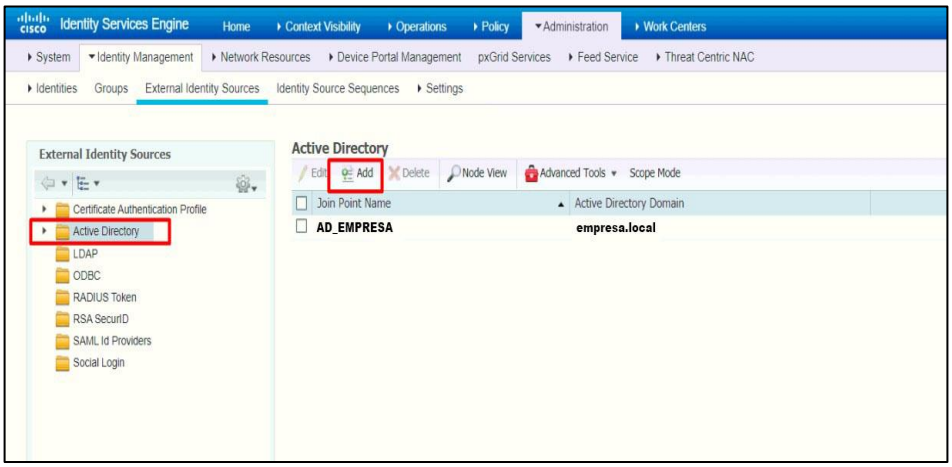

Figura 56 - Integración ISE_AD 2do Paso.
Fuente: Elaboración propia de los autores.

Se solicitará el usuario y password para integrar el controlador, puede utilizarse cualquier usuario que tenga privilegios de administrador.

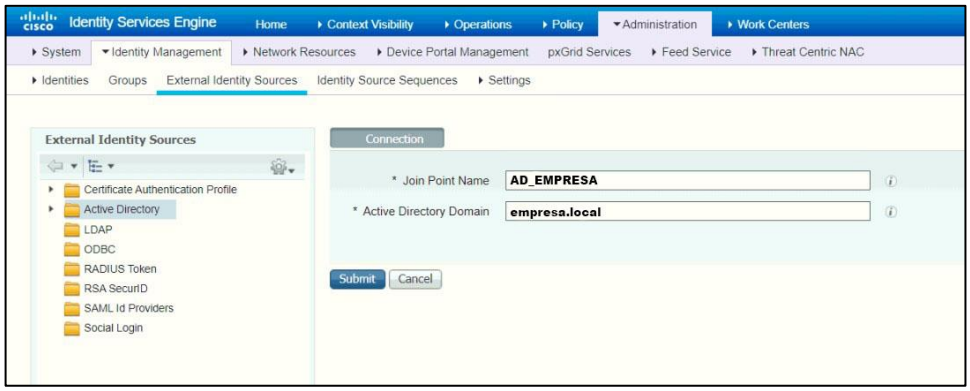

Figura 57 - Integración ISE-AD 3er Paso.
Fuente: Elaboración propia de los autores.

Luego de la validación del usuario aparecerá el nombre utilizado en la parte izquierda.

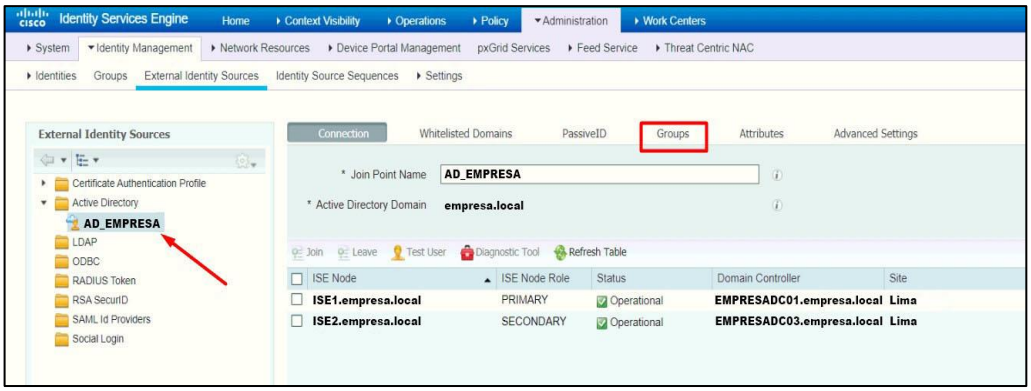

Figura 58 - Integración ISE-AD 4to Paso.
Fuente: Elaboración propia de los autores.

Finalmente ingresar a Grupos y clic en “Add” para seleccionar los grupos del AD que serán utilizados por el ISE.

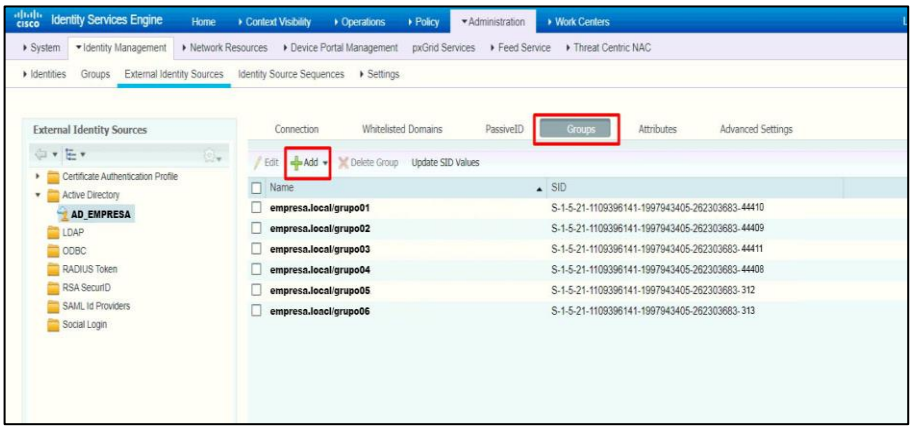

Figura 59 - Integracion ISE-AD – Finalizado.
Fuente: Elaboración propia de los autores.

4.6.10.3. Integración Wireless SD-Access

La configuración WIFI en SD Access se realiza desde al DNA Center, el cual provisionará al WLC mediante NETCONF, para esto el WLC debe ser descubierto mediante la herramienta Discovery del DNA Center:

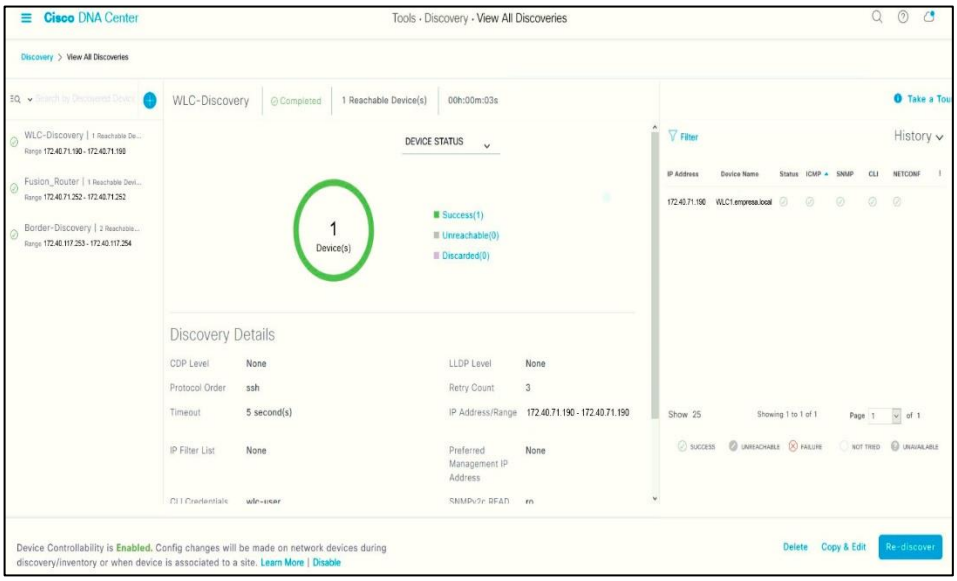

Figura 60 - Descubrimiento de Wireless LAN Controller.
Fuente: Elaboración propia de los autores.

La creación de SSIDs se realiza mediante la aplicación Design / Wireless:

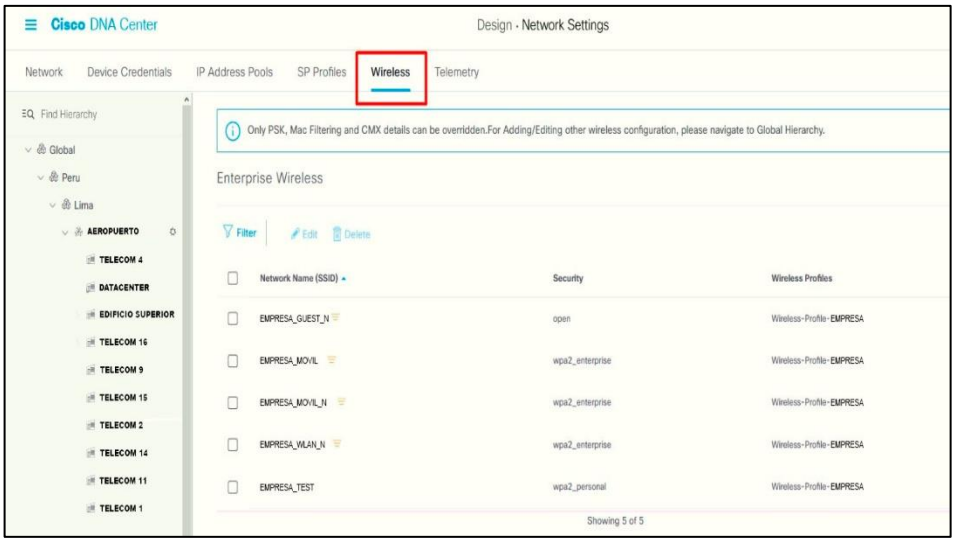

Figura 61 - Creación de SSIDs.
Fuente: Elaboración propia de los autores.

Las configuraciones realizadas en el DNA Center serán enviadas e implementadas automáticamente en el WLC:

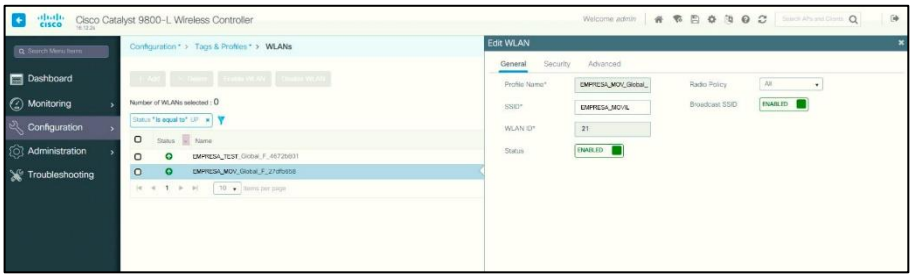

Figura 62 - WLC: Integración Wireless - SD Access Finalizada.
Fuente: Elaboración propia de los autores.

4.6.10.4. Integración SD-Access – Red Tradicional

La comunicación entre un dominio SD-Access y las redes externas se realiza mediante el Border Node y un dispositivo de Fusión, los cuales compartirán las rutas mediante el protocolo EBGP.

- Sistema Autónomo (AS) Border: 65520
- Sistema Autónomo (AS) Fusion: 65521

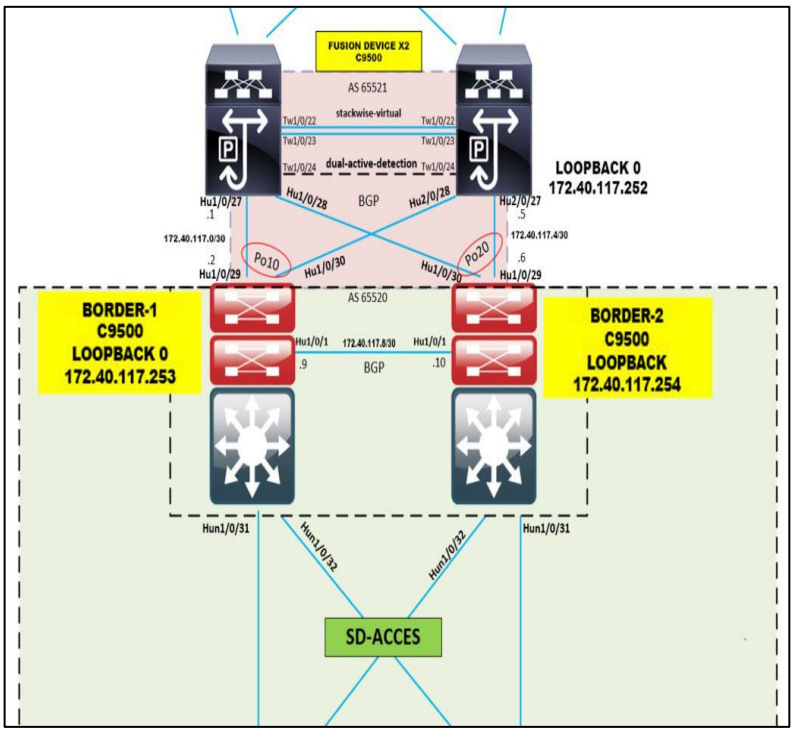

Figura 63 - Topologia y conexiones Border – Fusion.
Fuente: Elaboración propia de los autores.

Ya que cada VN es una VRF y representa una instancia de routing diferente, se debe levantar una vecindad bgp por cada vrf entre fusión-border y border1-border2.

4.6.11. Layer 3 Handoff

Layer 3 Handoff es el feature que DNA utiliza para configurar la conectividad con el dispositivo externo. El primer paso es crear un “Transit Peer Network” donde se define el Sistema Autónomo (SA) que va a tener el Fabric.

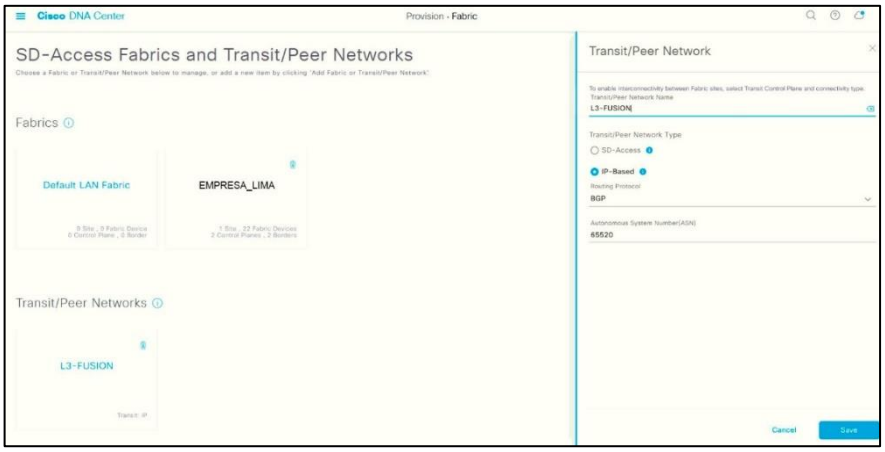

Figura 64 - Creación de Transit Network L3 Handoff.
Fuente: Elaboración propia de los autores.

Posteriormente se ingresa a la configuración de los border para habilitar L3 Handoff donde se solicita ingresar el Transit/Peer network creado en el paso anterior, la interface de conexión al Fusión y el Pool de IPs que fue reservado en la fase de Design.

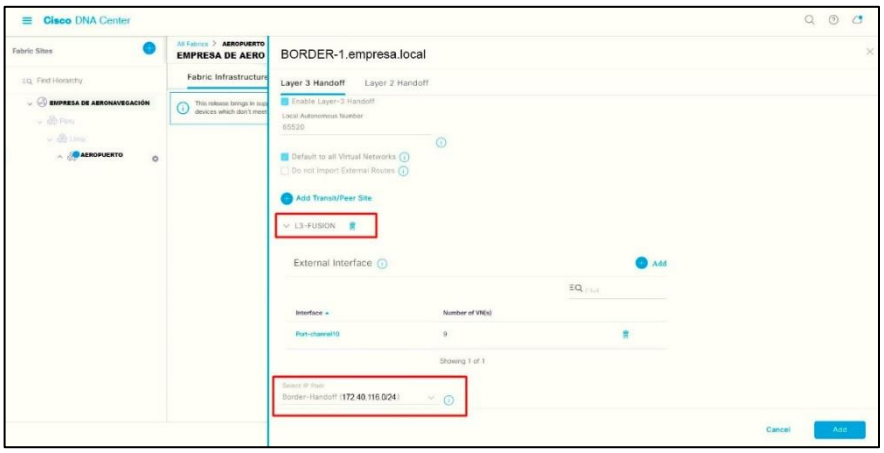

Figura 65 - Configuracion L3 Handoff Border Node.
Fuente: Elaboración propia de los autores.

4.6.12. Configuración Fusion Device

Una vez que DNA ha realizado el push de configuración a los borders, se tiene lista la información necesaria para el Fusion Device (Vlan ID, segmento de red). Ya que el Fusion device no pertenece al fabric, su configuración se realiza manualmente.

Los datos de configuración se obtienen del border y se distribuyen de acuerdo a las siguientes tablas:

Tabla 14 - Direccionamiento IP por VRF: Fusion - Border 1.

VLAN ID	VN	NETWORK	FUSION	BORDER 1
Vlan219	VN 1	172.40.117.0 /30	172.40.117.1	172.40.117.2
Vlan3021	VN 2	172.40.116.40 /30	172.40.116.42	172.40.116.41
Vlan3023	VN 3	172.40.116.48 /30	172.40.116.50	172.40.116.49
Vlan3024	VN 4	172.40.116.52 /30	172.40.116.54	172.40.116.53
Vlan3025	VN 5	172.40.116.56 /30	172.40.116.58	172.40.116.57
Vlan3032	VN 6	172.40.116.84 /30	172.40.116.86	172.40.116.85
Vlan3034	VN 7	172.40.116.92 /30	172.40.116.94	172.40.116.93
Vlan3036	VN 8	172.40.116.100 /30	172.40.116.102	172.40.116.101
Vlan3038	VN 9	172.40.116.108 /30	172.40.116.110	172.40.116.109

Fuente: Elaboración propia de los autores.

Tabla 15 - Direccionamiento IP por VRF: Fusion - Border 2.

VLAN ID	VN	NETWORK	FUSION	BORDER 2
Vlan220	VN 1	172.40.117.4 /30	172.40.117.5	172.40.117.6
Vlan3026	VN 2	172.40.116.60 /30	172.40.116.62	172.40.116.61
Vlan3028	VN 3	172.40.116.68 /30	172.40.116.70	172.40.116.69
Vlan3029	VN 4	172.40.116.72 /30	172.40.116.74	172.40.116.73

Vlan3030	VN 5	172.40.116.76 /30	172.40.116.78	172.40.116.77
Vlan3031	VN 6	172.40.116.80 /30	172.40.116.82	172.40.116.81
Vlan3033	VN 7	172.40.116.88 /30	172.40.116.90	172.40.116.89
Vlan3035	VN 8	172.40.116.96 /30	172.40.116.98	172.40.116.97
Vlan3037	VN 9	172.40.116.104 /30	172.40.116.106	172.40.116.105

Fuente: Elaboración propia de los autores.

Tabla 16 - Configuración eBGP Fusion Device.

Configuración eBGP Fusion Device
router bgp 65541 bgp log-neighbor-changes neighbor 172.40.116.41 remote-as 65540 neighbor 172.40.116.41 update-source Vlan3021 neighbor 172.40.116.49 remote-as 65540 neighbor 172.40.116.49 update-source Vlan3023 neighbor 172.40.116.53 remote-as 65540 neighbor 172.40.116.53 update-source Vlan3024 neighbor 172.40.116.57 remote-as 65540 neighbor 172.40.116.57 update-source Vlan3025 neighbor 172.40.116.61 remote-as 65540 neighbor 172.40.116.61 update-source Vlan3026 neighbor 172.40.116.69 remote-as 65540 neighbor 172.40.116.69 update-source Vlan3028 neighbor 172.40.116.81 remote-as 65540 neighbor 172.40.116.81 update-source Vlan3031 neighbor 172.40.116.85 remote-as 65540 neighbor 172.40.116.85 update-source Vlan3032 neighbor 172.40.116.93 remote-as 65540 neighbor 172.40.116.93 update-source Vlan3034 neighbor 172.40.116.101 remote-as 65540 neighbor 172.40.116.101 update-source Vlan3036 neighbor 172.40.116.109 remote-as 65540 neighbor 172.40.116.109 update-source Vlan3038 neighbor 172.40.117.2 remote-as 65540 neighbor 172.40.117.2 update-source Vlan219 neighbor 172.40.117.6 remote-as 65540

```
!
address-family ipv4
 network 0.0.0.0
 network 172.40.71.0 mask 255.255.255.0
 neighbor 172.40.116.41 activate
 neighbor 172.40.116.49 activate
 neighbor 172.40.116.53 activate
 neighbor 172.40.116.57 activate
 neighbor 172.40.116.61 activate
 neighbor 172.40.116.69 activate
 neighbor 172.40.116.81 activate
 neighbor 172.40.116.85 activate
 neighbor 172.40.116.93 activate
 neighbor 172.40.116.101 activate
 neighbor 172.40.116.109 activate
 neighbor 172.40.117.2 activate
 neighbor 172.40.117.2 route-map FROM-FABRIC in
 neighbor 172.40.117.2 route-map TO-FABRIC out
 neighbor 172.40.117.6 activate
 neighbor 172.40.117.6 route-map FROM-FABRIC in
 neighbor 172.40.117.6 route-map TO-FABRIC out
exit-address-family
```

Fuente: Elaboración propia de los autores.

4.6.13. Configuración Border1-Border2

La red de una empresa de aeronavegación cuenta con dos border nodes para una mayor redundancia. Para mantener la alta disponibilidad de la red se debe configurar enrutamiento interno (IBGP) para ambos dispositivos puedan compartir sus rutas por cada vrf. Esta configuración en particular se realiza de forma manual usando un pool de IPs reservado para este propósito de acuerdo al siguiente cuadro:

Tabla 17 - Direccionamiento IP por VRF: Border 1 - Border 2.

VLAN ID	VN	NETWORK	BORDER 1	BORDER 2
Vlan121	VN 1	172.40.117.8 /30	172.40.117.9	172.40.117.10
Vlan122	VN 2	172.40.117.12 /30	172.40.117.13	172.40.117.14
Vlan123	VN 3	172.40.117.16 /30	172.40.117.17	172.40.117.18

Vlan124	VN 4	172.40.117.20 /30	172.40.117.21	172.40.117.22
Vlan125	VN 5	172.40.117.24 /30	172.40.117.25	172.40.117.26
Vlan126	VN 6	172.40.117.28 /30	172.40.117.29	172.40.117.30
Vlan127	VN 7	172.40.117.32 /30	172.40.117.33	172.40.117.34
Vlan128	VN 8	172.40.117.36 /30	172.40.117.37	172.40.117.38

Fuente: Elaboración propia de los autores.

Se muestra a continuación la porción de configuración de un border para las rutas globales y una VN:

Tabla 18 - Configuración iBGP Border.

Configuración iBGP Border 1
router bgp 65540 bgp router-id interface Loopback0 bgp log-neighbor-changes bgp graceful-restart neighbor 172.40.116.102 remote-as 65541 neighbor 172.40.116.102 update-source Vlan3036 neighbor 172.40.117.1 remote-as 65541 neighbor 172.40.117.1 update-source Vlan219 neighbor 172.40.117.10 remote-as 65540 neighbor 172.40.117.10 update-source Vlan121 ! address-family ipv4 bgp aggregate-timer 0 network 172.40.76.1 mask 255.255.255.255 network 172.40.117.253 mask 255.255.255.255 network 172.40.117.254 mask 255.255.255.255 network 172.40.270.1 mask 255.255.255.255 aggregate-address 172.40.270.0 255.255.255.0 summary-only aggregate-address 172.40.118.0 255.255.255.0 summary-only aggregate-address 172.40.76.0 255.255.255.0 summary-only redistribute isis level-1-2 metric 10 redistribute lisp metric 10 neighbor 172.40.116.102 activate neighbor 172.40.116.102 weight 65555 neighbor 172.40.116.102 advertisement-interval 0

```
 neighbor 172.40.117.1 activate
 neighbor 172.40.117.10 activate
exit-address-family
!
address-family ipv4
 bgp aggregate-timer 0
 network 172.40.77.0 mask 255.255.255.0
 network 172.40.77.1 mask 255.255.255.255
 network 172.40.81.0 mask 255.255.255.0
 network 172.40.81.1 mask 255.255.255.255
 network 172.40.116.40 mask 255.255.255.252
 aggregate-address 172.40.81.0 255.255.255.0 summary-only
 aggregate-address 172.40.77.0 255.255.255.0 summary-only
 redistribute lisp metric 10
 neighbor 172.40.116.42 remote-as 65541
 neighbor 172.40.116.42 update-source Vlan3021
 neighbor 172.40.116.42 activate
 neighbor 172.40.116.42 weight 65555
 neighbor 172.40.117.22 remote-as 65540
 neighbor 172.40.117.22 update-source Vlan124
 neighbor 172.40.117.22 activate
exit-address-family
!
```

Fuente: Elaboración propia de los autores.

V. RESULTADOS

5.1. Resultado Descriptivo

Con la implementación de SD-Access logramos un control centralizado y automatizado obteniendo una visibilidad completa de la red permitiéndonos tomar acción desde el lugar que nos encontremos, así poder observar al detalle las aplicaciones que circulan por nuestra red LAN.

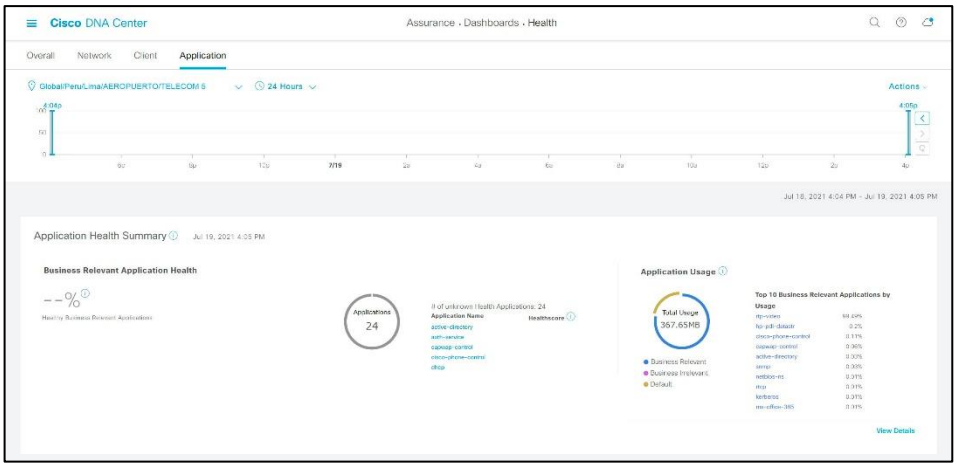

Figura 66 - Assurance - DashBoards - Health – Application.
Fuente: Elaboración propia de los autores.

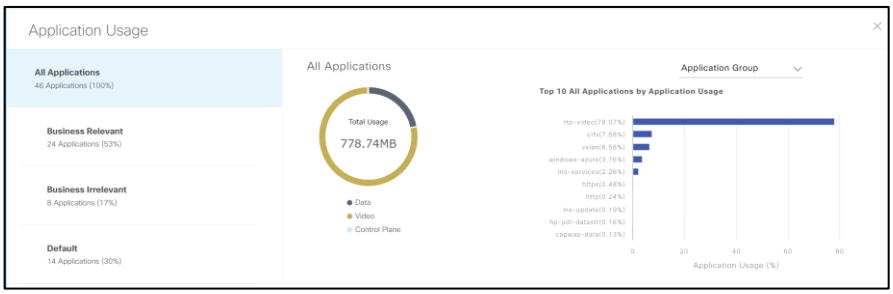

Figura 67 - Application Usage – All Application - Application Group.
Fuente: Elaboración propia de los autores.

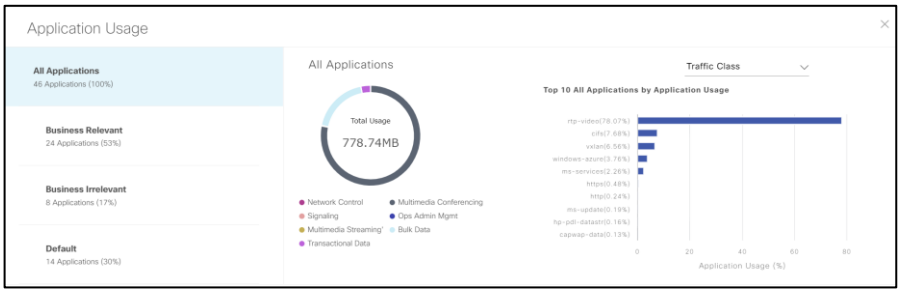

Figura 68 - Application Usage – All Application - Traffic Class.
Fuente: Elaboración propia de los autores.

También obtener de manera inteligente la clasificación de tráfico que está circulando por nuestra red para poder relacionarlos con el negocio y tomar acciones de mejora para el crecimiento del mismo, esto lo logramos gracias a la función de análisis que posees DNA Center y su clasificación de tráficos por grupos como son:

- **Relevante para el negocio**: (tráfico de alta prioridad) Las aplicaciones de este grupo contribuyen directamente a los objetivos de la organización y, como tales, pueden incluir una variedad de aplicaciones, incluidas aplicaciones de voz, video, streaming y multimedia colaborativas, aplicaciones de bases de datos, aplicaciones de recursos empresariales, correo electrónico, transferencias de archivos, distribución de contenido, etc. Las aplicaciones designadas como relevantes para el negocio se tratan de acuerdo con las recomendaciones de mejores prácticas de la industria, según lo prescrito en el Grupo de trabajo de ingeniería de Internet (IETF) RFC 4594.

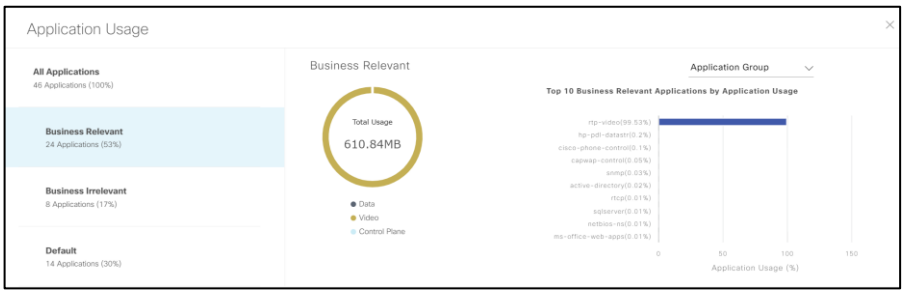

Figura 69 - Application Usage - Business Relevant - Application Group.
Fuente: Elaboración propia de los autores.

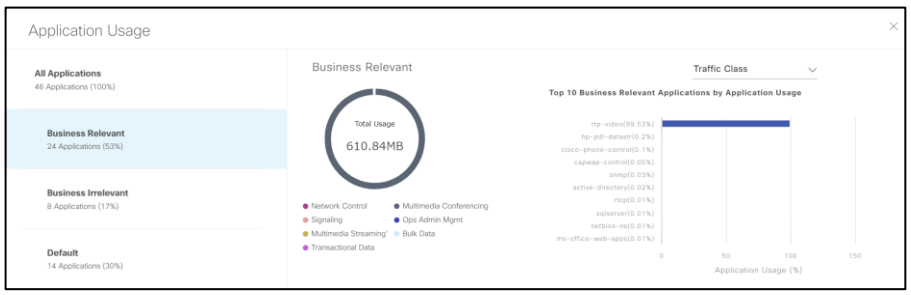

Figura 70 - Application Usage - Business Relevant - Traffic Class.
Fuente: Elaboración propia de los autores.

- **Predeterminado**: (Tráfico neutral) Este grupo está destinado a aplicaciones que pueden o no ser relevantes para el negocio, por ejemplo, el tráfico HTTP o HTTPS genérico puede contribuir a los objetivos de la organización en ocasiones, mientras que, en otras ocasiones, dicho tráfico puede que no. Es posible que no tenga una

idea del propósito de algunas aplicaciones, por ejemplo, aplicaciones heredadas o incluso aplicaciones recientemente implementadas. Por lo tanto, los flujos de tráfico para estas aplicaciones deben tratarse con el servicio de reenvío predeterminado, como se describe en IETF RFC 2747 y 4594.

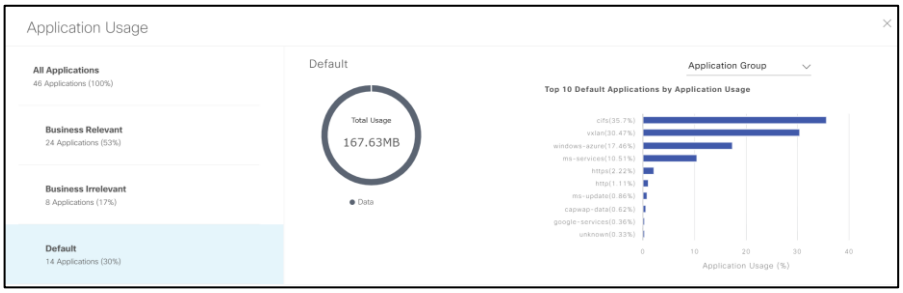

Figura 71 - Application Usage - Default - Application Group.
Fuente: Elaboración propia de los autores.

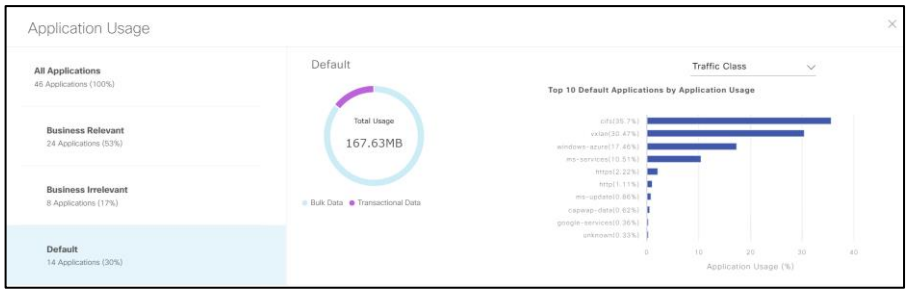

Figura 72 - Application Usage - Default - Traffic Class.
Fuente: Elaboración propia de los autores.

- **Irrelevante para el negocio**: (tráfico de baja prioridad) Este grupo está destinado a aplicaciones que se han identificado como que no contribuyen al logro de los objetivos de la organización. Están principalmente orientados al consumidor o al entretenimiento o ambos por naturaleza. Recomendamos que este tipo de tráfico se trate como un servicio Scavenger, como se describe en IETF RFC 3662 y 4594.

Figura 73 - Application Usage - Business Irrelevant - Application Group.
Fuente: Elaboración propia de los autores.

Figura 74 - Application Usage - Business Irrelevant - Traffic Class.
Fuente: Elaboración propia de los autores.

5.1.1. Despliegue de políticas de Calidad de Servicio (QoS).

Puede configurar QoS en su red mediante políticas de aplicación en Cisco DNA Center.

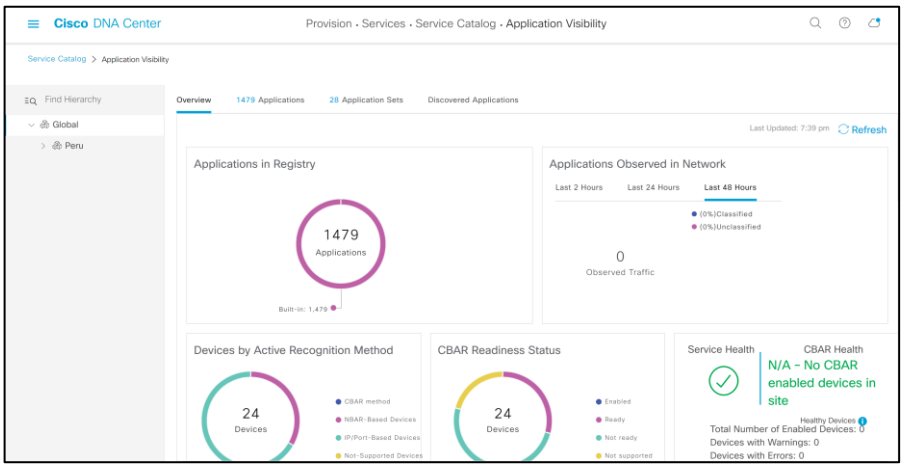

Figura 75 - Provision - Services - Service Catalog - Application Visibility – Overview.
Fuente: Elaboración propia de los autores.

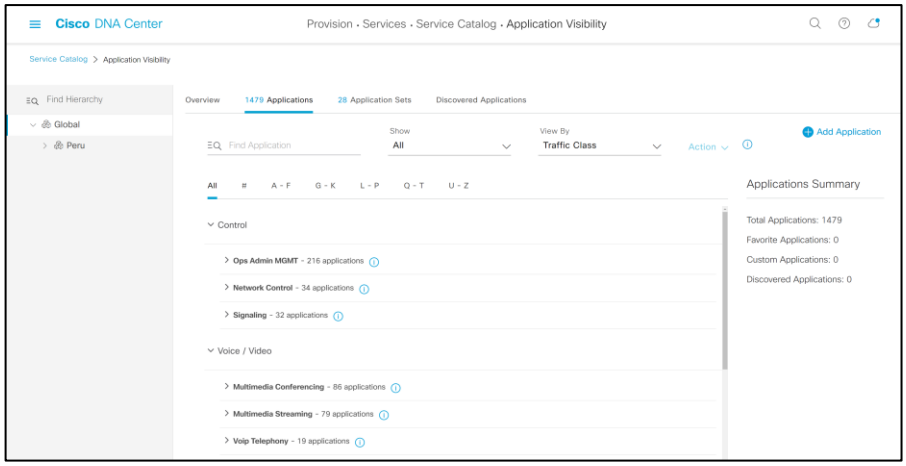

Figura 76 - Provision - Services - Service Catalog - Application Visibility – Applications.
Fuente: Elaboración propia de los autores.

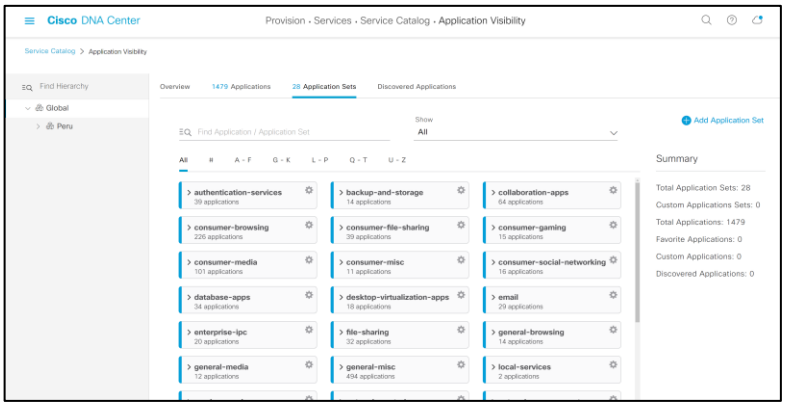

Figura 77 - Provision - Services - Service Catalog - Application Visibility - Application Sets.
Fuente: Elaboración propia de los autores.

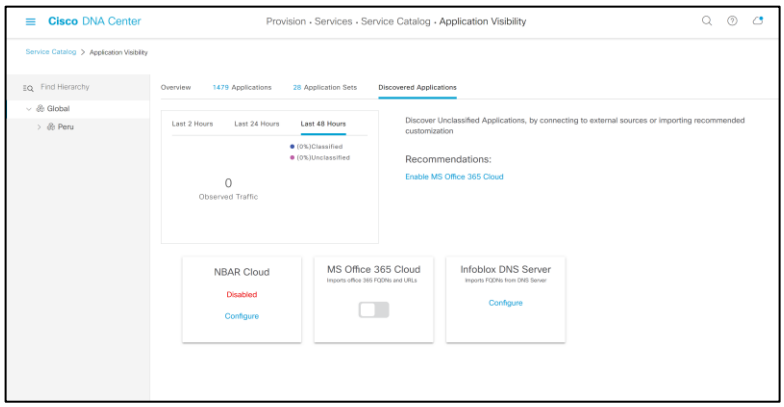

Figura 78 - Provision - Services - Service Catalog - Application Visibility - Discovered Applications.
Fuente: Elaboración propia de los autores.

5.1.2. Políticas de control de acceso.

- Control de acceso basado en grupos

Figura 79 - Policy - Group-Based Access Control – Policies.
Fuente: Elaboración propia de los autores.

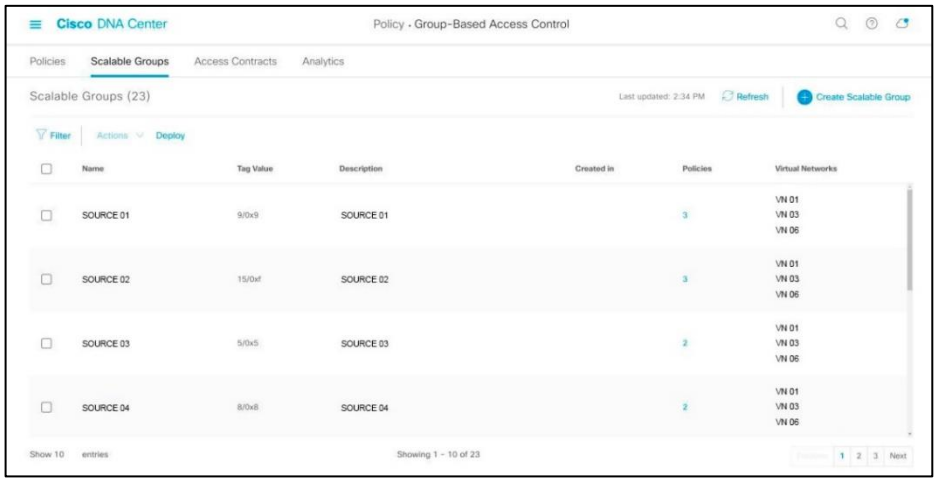

Figura 80 - Policy - Group-Based Access Control - Scalable Groups.
Fuente: Elaboración propia de los autores.

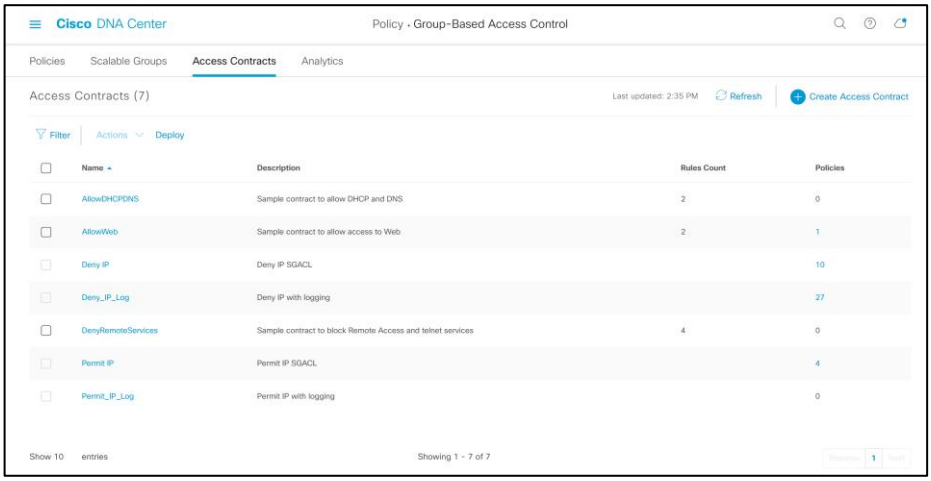

Figura 81 - Policy - Group-Based Access Control - Access Contracts.
Fuente: Elaboración propia de los autores.

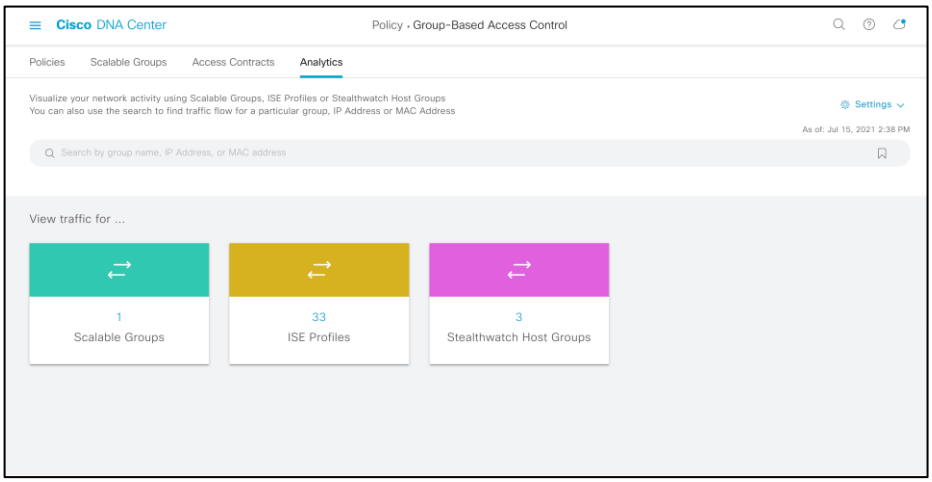

Figura 82 - Policy - Group-Based Access Control – Analytics.
Fuente: Elaboración propia de los autores.

- Control de acceso basado en IP

Figura 83 - Policy - IP Based Access Control - IP Based Access Control Policies.
Fuente: Elaboración propia de los autores.

Figura 84 - Policy - IP Based Access Control - IP Network Groups.
Fuente: Elaboración propia de los autores.

Figura 85 - Policy - IP Based Access Control - Access Contract.
Fuente: Elaboración propia de los autores.

5.1.3. Segmentación automatizada

Basada en políticas de usuarios, dispositivos y cosas usando un overlay o fabric de red automatizado. La segmentación de usuarios debe poder hacerse en base a sus respectivos roles en la organización. La configuración de estas políticas puede hacerse en un entorno gráfico, de manera centralizada y debe estar preparado para tener una misma política en redes cableadas e inalámbricas.

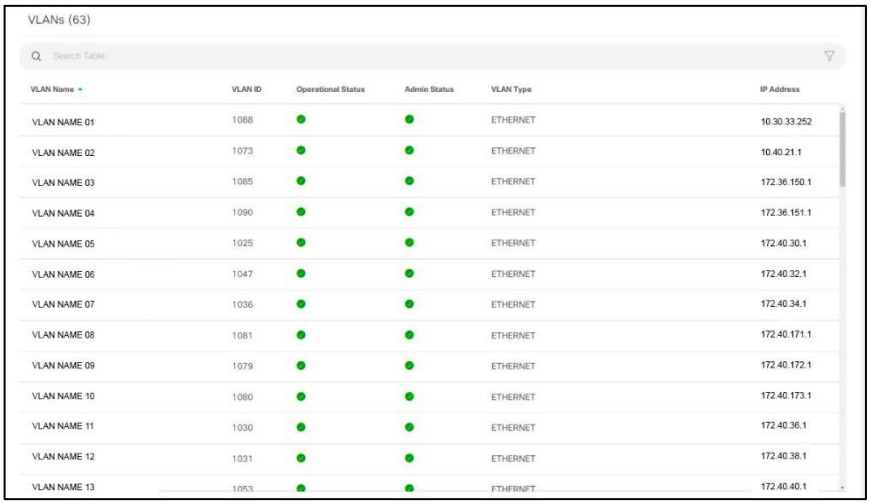

Figura 86 – VLANs.
Fuente: Elaboración propia de los autores.

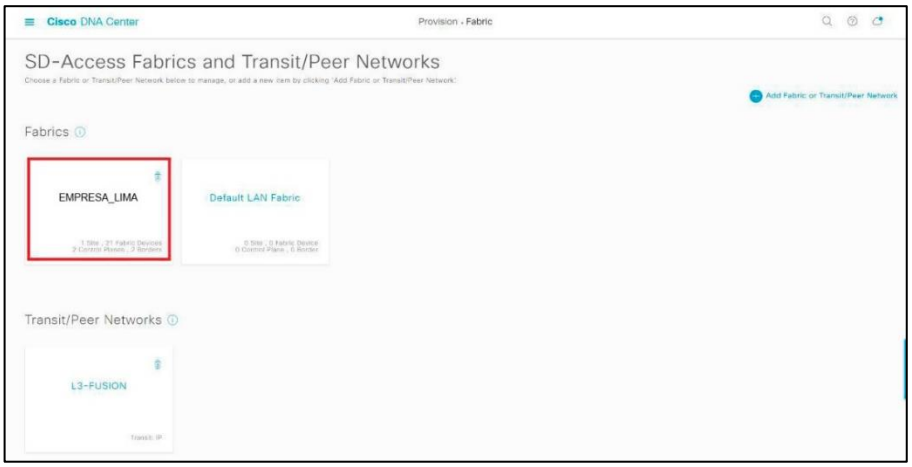

Figura 87 - Provision – Fabric.
Fuente: Elaboración propia de los autores.

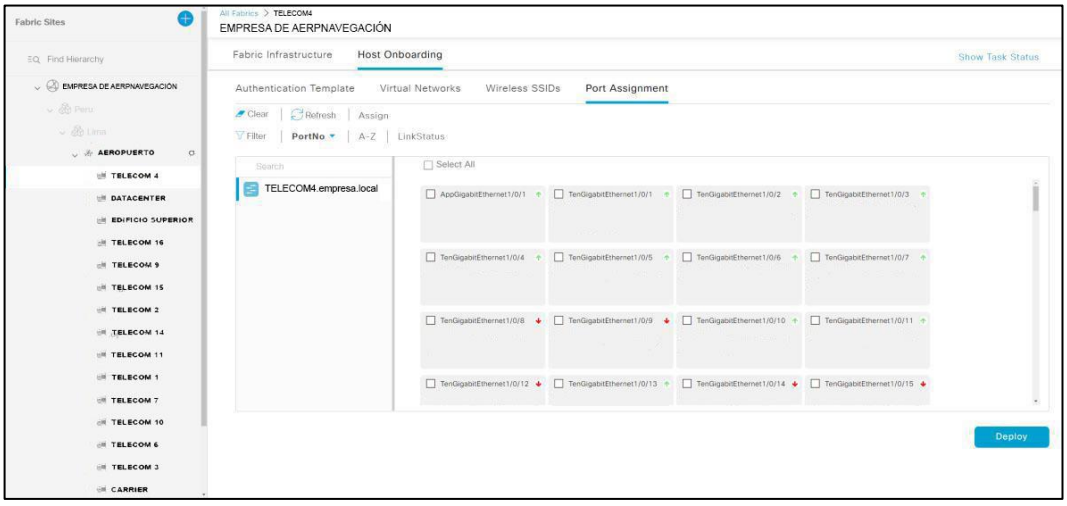

Figura 88 - Port Assignment.
Fuente: Elaboración propia de los autores.

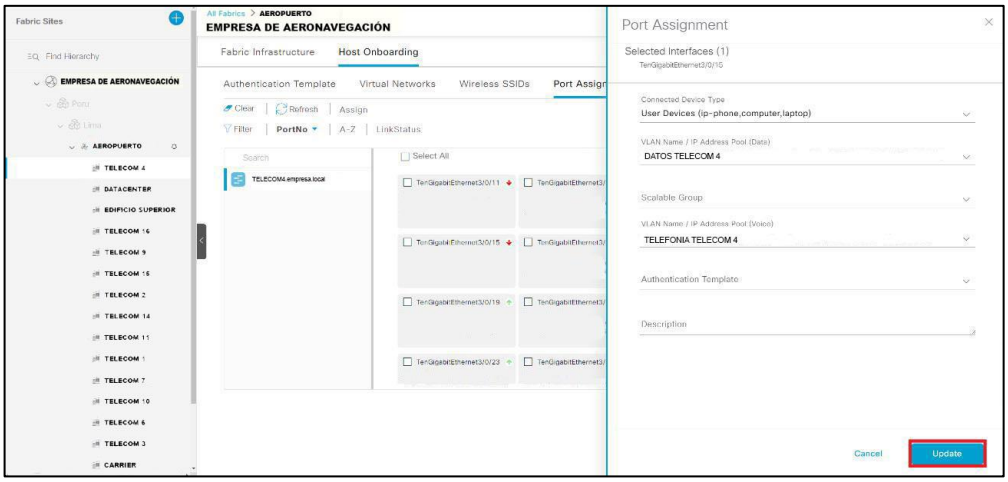

Figura 89 - Port Assignment - Designación de VLANs a un puerto de un Switch.
Fuente: Elaboración propia de los autores.

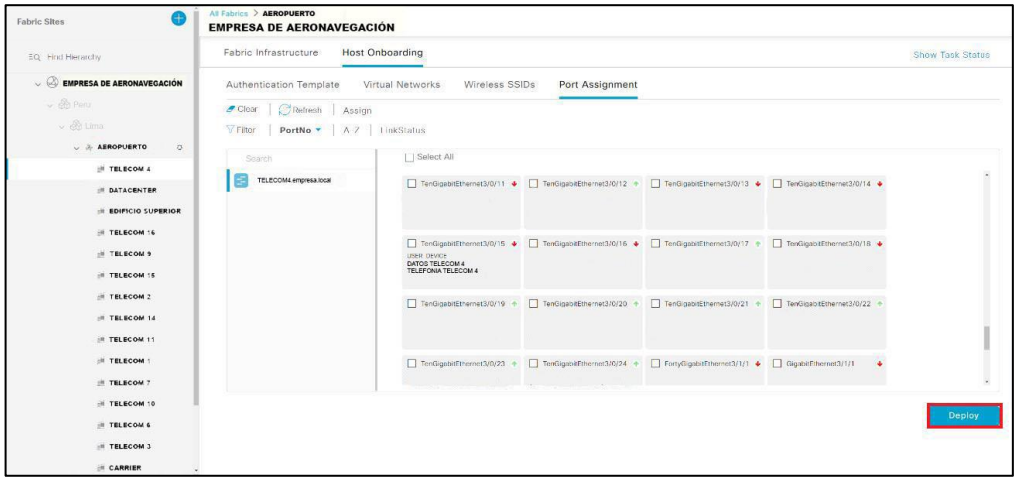

Figura 90 - Port Assignment - Desplegar la configuración.
Fuente: Elaboración propia de los autores.

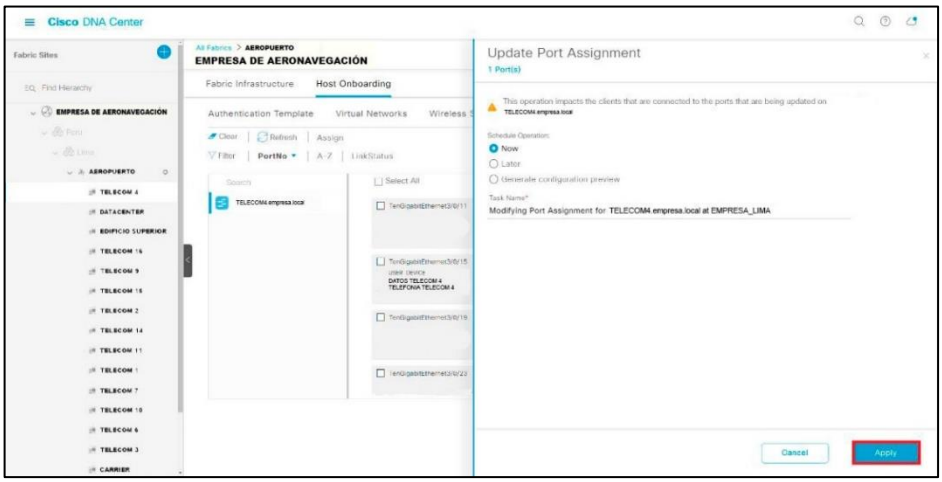

Figura 91 - Port Assignment - Aplicar los cambios realizados.
Fuente: Elaboración propia de los autores.

5.1.4. Analíticos de la salud general de los dispositivos de infraestructura de red.

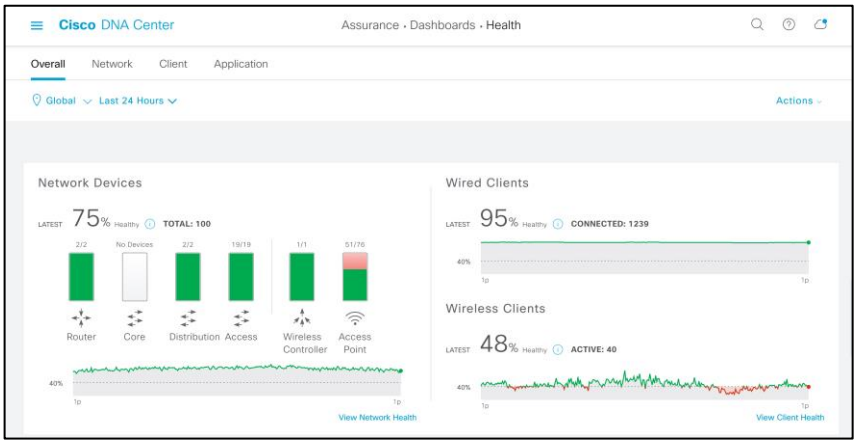

Figura 92 - Assurance - DashBoards - Health – Overall.
Fuente: Elaboración propia de los autores.

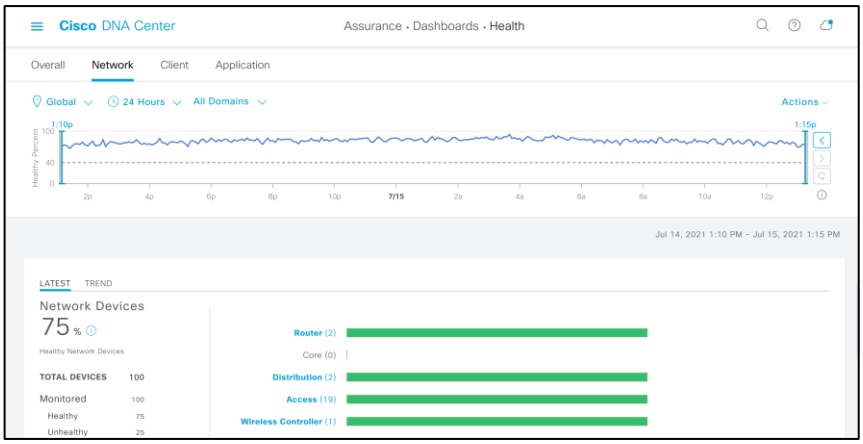

Figura 93 - Assurance - DashBoards - Health – Network.
Fuente: Elaboración propia de los autores.

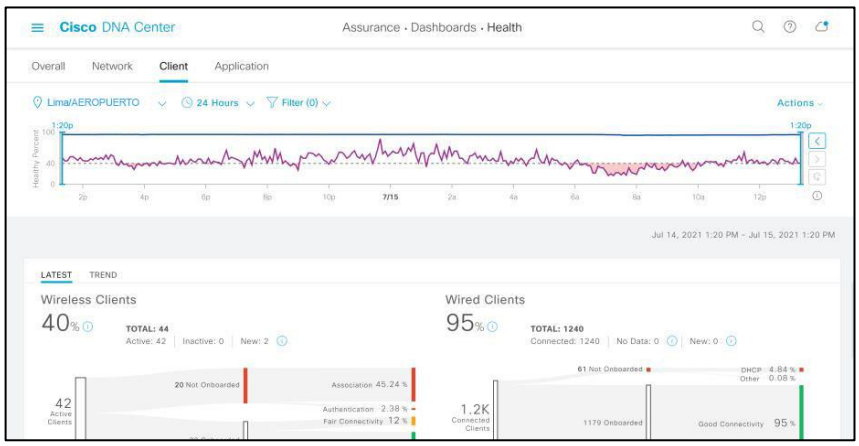

Figura 94 - Assurance - DashBoards - Health – Client.
Fuente: Elaboración propia de los autores.

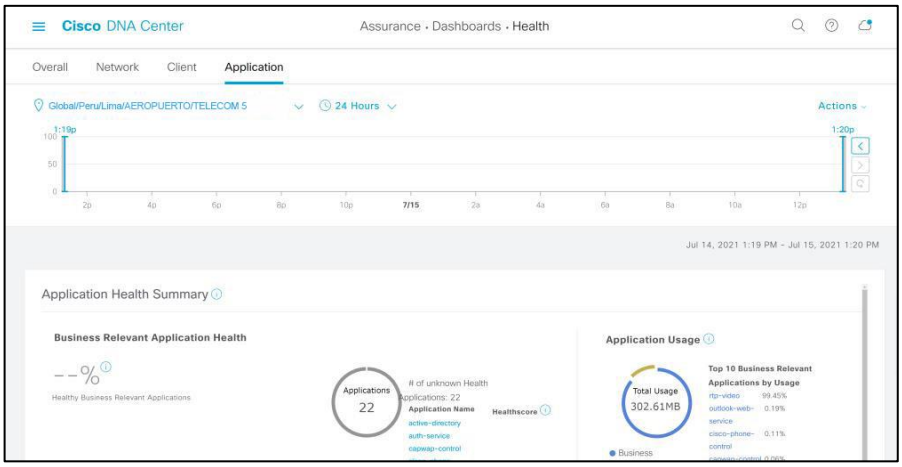

Figura 95 - Assurance - DashBoards - Health – Application.
Fuente: Elaboración propia de los autores.

- Analíticos de conectividad de los dispositivos finales conectándose a la red, mediante la recolección de información con respecto a DHCP, estado de los puertos, autenticación, etc.

Figura 96 - Assurance - DashBoards - Health - Client - Clientes Conectados e Inalámbricos.
Fuente: Elaboración propia de los autores.

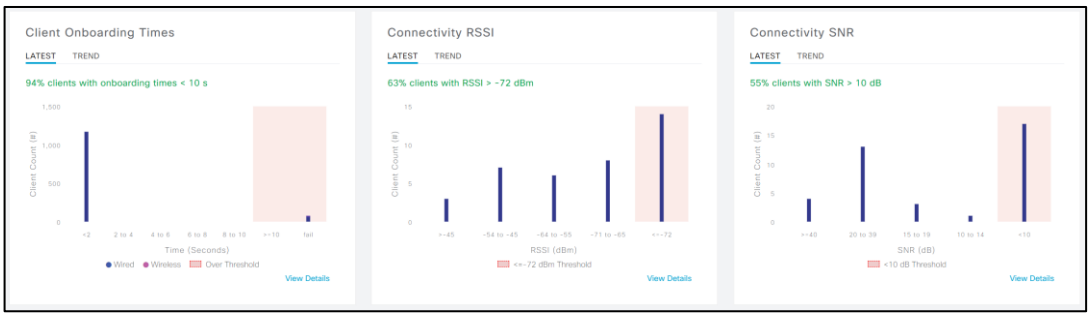

Figura 97 – Client Onboarding Times - Connectivity RSSI - Connectivity SNR.
Fuente: Elaboración propia de los autores.

Figura 98 - Client Roaming Times - Client Count per SSID - Conectivity Physical Link.
Fuente: Elaboración propia de los autores.

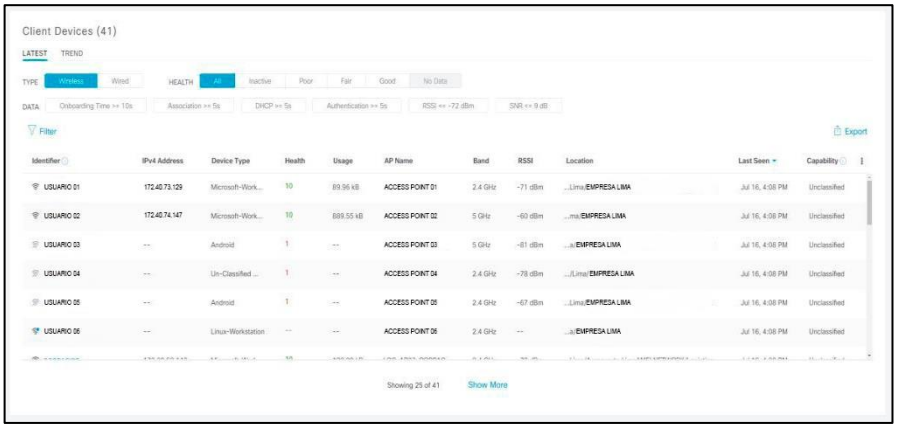

Figura 99 - Client Devices.
Fuente: Elaboración propia de los autores.

Figura 100 - Client Count per Band - Client Data Rate.
Fuente: Elaboración propia de los autores.

- Funcionalidad de búsqueda de dispositivos de infraestructura de red y usuarios.

Figura 101 - Assurance - DashBoard - Health - Client - Línea de Tiempo de Porcentaje de Salud.
Fuente: Elaboración propia de los autores.

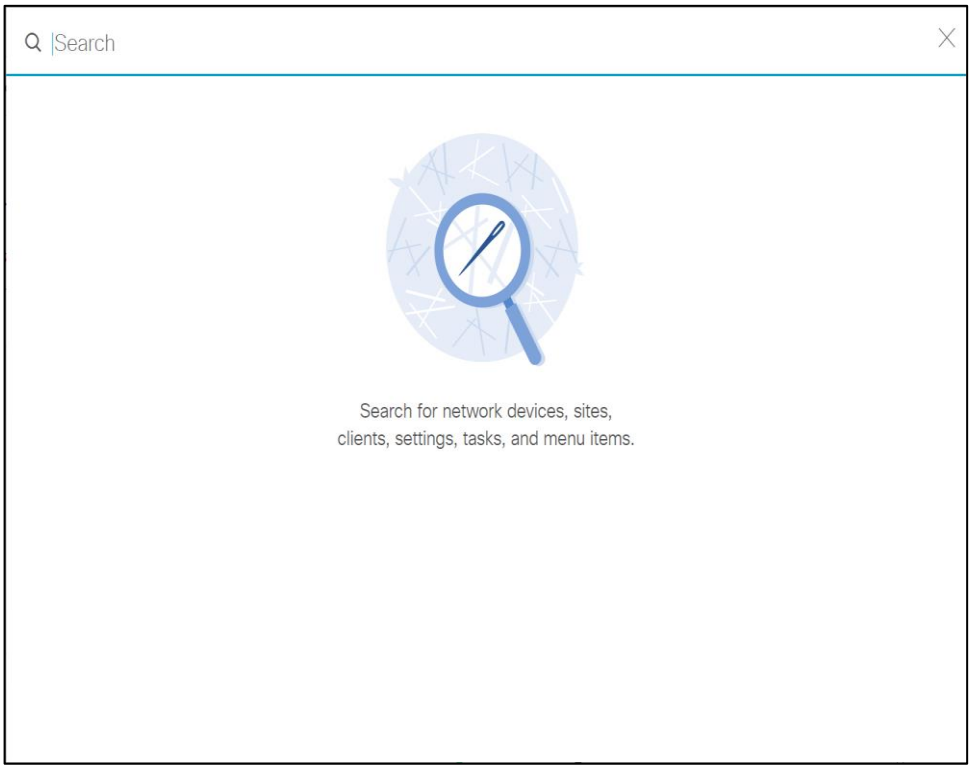

Figura 102 - Herramienta de Búsqueda del DNA Center.
Fuente: Elaboración propia de los autores.

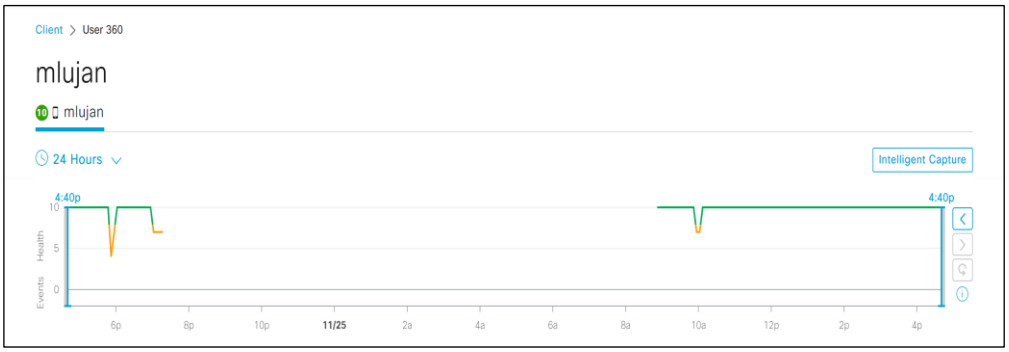

Figura 103 - Usuario de la RED.
Fuente: Elaboración propia de los autores.

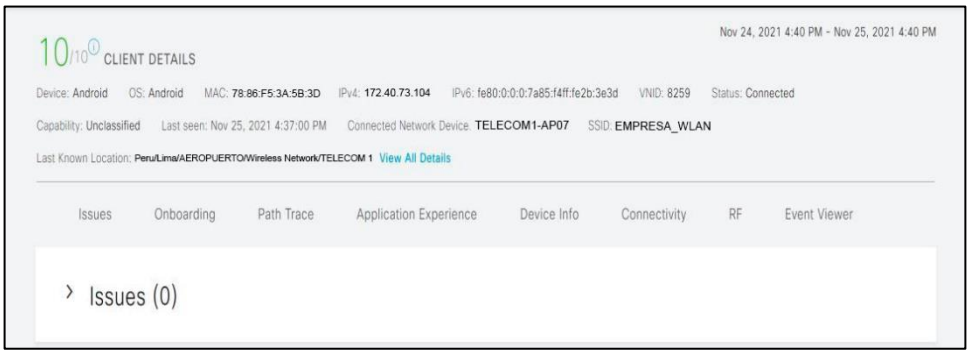

Figura 104 - Detalles del Cliente.
Fuente: Elaboración propia de los autores.

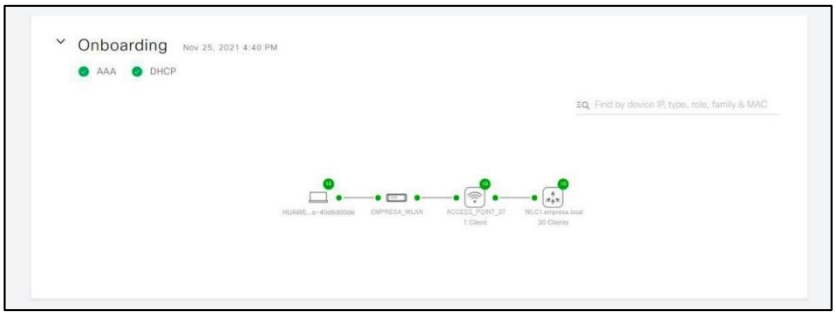

Figura 105 - Mapa de RED del Cliente.
Fuente: Elaboración propia de los autores.

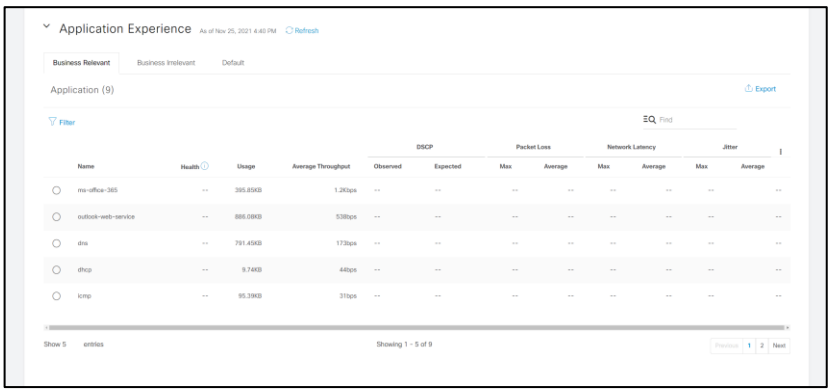

Figura 106 - Experiencia de las Aplicaciones del Cliente.
Fuente: Elaboración propia de los autores.

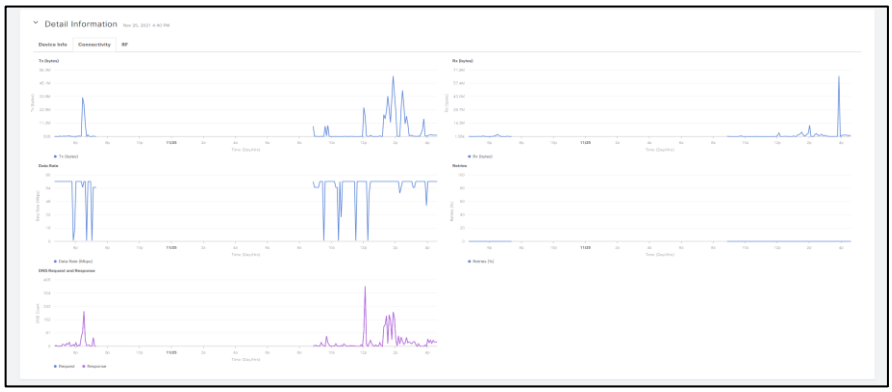

Figura 107 - Información Detallada del Cliente – Conectividad.
Fuente: Elaboración propia de los autores.

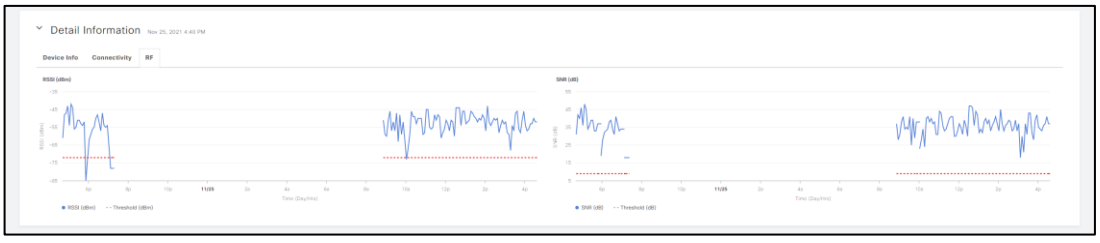

Figura 108 - Información Detallada del Cliente – RF.
Fuente: Elaboración propia de los autores.

VI. DISCUSION DE RESULTADOS

6.1. Contrastación y demostración de la hipótesis.

La implementación de la solución SD- Access funcionó correctamente al validar que se tiene una gestión centralizada y automatizada de la red LAN mediante el software DNA center (controlador) de Cisco pudiendo administrar la red en su totalidad en todas las ubicaciones donde se encuentran nuestros dispositivos de comunicación y logrando automatizar dicha red de manera que todo dispositivo de red es configurado automáticamente con solo conectarlo a la red, debido a que el controlador (DNA) de SD-Access gestiona y realiza la configuración completa de todos los parámetros correspondientes que están asociados a estos dispositivos, dichos parámetros pueden variar de acuerdo a la ubicación del dispositivo.

6.2. Contrastación de los resultados con otros estudios similares.

En Perú no se tiene referencia de un proyecto similar al implementado en este proyecto debido a que esta red SD-Access es la primera implementada en el país.

VII. CONCLUSIONES

1. Se logró el diseño e implementación de la solución SD-Access de Cisco en el presente trabajo dando buenos resultados en la gestión centralizada de la red LAN obteniendo una red que es fácil de administrar y al mismo tiempo automatizando sus procesos de configuración tanto de clientes como dispositivos finales.

2. Las políticas de seguridad se vuelven más robustas y automatizada al utilizar el nuevo concepto de microsegmentación, de esta manera dentro de un segmento de red se puede aislar el tráfico de acuerdo a las etiquetas (SGT) que nosotros asignemos a los distintos usuarios o grupos, esto se logra al integrar la nueva tecnología SD-Access con un controlador de políticas de seguridad (ISE) lo que faculta de mayor seguridad la red LAN.

3. Se logró diseñar un control centralizado de la red basado en los 3 niveles del fabricante (acceso, distribución y core) lo que permite distribuir correctamente los roles de SD-Access y cumplir con la finalidad que tiene esta tecnología de separar el plano de control del plano de datos mejorando la gestión de la red LAN.

VIII. RECOMENDACIONES

1. Para el caso que se necesiten migrar redes externas a SD-Access pero que se encuentren configuradas y funcionando en los nodos finales se debería proponer la implementación de un switch externo para realizar una conexión directa al switch de fusión perteneciente a la infraestructura externa de SD-Access, además de tener en cuenta que utilizar L2 handoff es solo una solución temporal a la hora de una migración.

2. Se debe tener en cuenta que los switch compatibles con la solución SD-Access, en este caso utilizamos la serie Catalyst 9300 posee un límite mínimo respecto a la velocidad de transmisión (100mb) pero al migrar una red tradicional tenemos equipos que funcionan a 10 Mb como son los Aires Acondicionados de Precisión para lo cual se debería realizar un estudio previo de las velocidades en que trabajan cada dispositivo perteneciente a la red para que al momento de migrar a SD-Access todos los dispositivos funcionen correctamente.

3. Para lograr el funcionamiento de telefónica analógica en una red SD-Access debería ser necesario solo configurar la VLAN de voz en el puerto que se conecten los Voice Gateway (VG) pero nos percatamos que estos equipos no se reconocen en SD-Access para lo cual sería importante su posterior investigación de como integrar telefonía analogía a una red SD-Access.

4. Es recomendable tener un mapeo completo de todos los segmentos de red que se tienen en la red LAN tradicional para que a la hora de la migración a SD-Access no pierdan conectividad los dispositivos que están en esa red, pero fuera de su ubicación, debido a que resulta de suma importancia que los usuarios no se queden sin conectividad a la red al momento de migrar su red tradicional a SD-Access.

REFERENCIAS BIBLIOGRAFICAS

[1] A. Nuñez, “Red Definida por Software (SDN) en base a una infraestructura de software de libre distribución”, Tesis de Pregrado, Universidad Técnica de Ambato, 2015. Disponible: **https://repositorio.uta.edu.ec/jspui/bitstream/123456789/10587/1/Tesis_982ec.pdf**

[2] Aprovisionamiento de fabric de Software-Defined Access. Guía de implementación prescriptiva, Cisco, 2019. Disponible: **https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/Localization/sda-fabric-deploy-2019jul_es_es.pdf**

[3] Authentication, Authorization, and Accounting Configuration Guide – Cisco IOS Release 15M&T, Cisco, 2016. Disponible: **https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-mt/sec-usr-aaa-15-mt-book.pdf**

[4] Cisco - Networking, Cloud, and Cybersecurity Solutions. Disponible: **https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/at-a-glance-c45-738181.pdf**

[5] Cisco - Networking, Cloud, and Cybersecurity Solutions. Disponible: **https://www.cisco.com/c/dam/global/es_es/solutions/enterprise-networks/software-defined-access/c45-738181-01_sda_aag_v7a_es.pdf**

[6] Cisco Catalyst 9300 Series Switches Data Sheet. Cisco. Disponible: **https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.pdf**

[7] Cisco data center spine-and-leaf architecture: Design overview white paper. Cisco. Disponible: **https://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/white-paper-c11-737022.pdf**

[8] Cisco DNA Center - Cisco DNA Center 2.2.2.0 Data Sheet. Cisco. Disponible: **https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-data-sheet-cte-en.pdf**

[9] Cisco Identity Services Engine - Cisco Identity Services Engine Data Sheet. Cisco. Disponible: **https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/data_sheet_c78-656174.pdf**

[10] Cisco Nexus 9300-EX Series Switches Data Sheet. Cisco. Disponible: **https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-742283.pdf**

[11] Cisco Prime Infrastructure - Cisco Prime Infrastructure 3.x Data Sheet.

Cisco. Disponible:
https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/prime-infrastructure/datasheet-c78-735696.pdf

[12] Cisco Prime Infrastructure - Cisco Prime Infrastructure 3.x Data Sheet. Cisco. Disponible:
https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/prime-infrastructure/datasheet-c78-735696.pdf

[13] Cisco Software-Defined Access - Cisco Software-Defined Access: Introducing an Entirely New Era in Networking Solution Overview. Cisco. Disponible:
https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/solution-overview-c22-739012.pdf

[14] Cisco Software-Defined Access – Enabiling intent-based networking, 2ed, Cisco, 2019. Disponible:
https://www.cisco.com/c/dam/en/us/products/se/2018/1/Collateral/nb-06-software-defined-access-ebook-en.pdf

[15] Cisco Software-Defined Networking: Different Solutions for Different Needs White Paper. Cisco. Disponible:
https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-735863.pdf

[16] Configure VXLAN. Cisco. Disponible:
https://www.cisco.com/c/en/us/support/docs/switches/nexus-9000-series-switches/118978-config-vxlan-00.pdf

[17] Data Collection Concepts – Cisco Prime Infrastructure 3.1, Cisco, 2017. Disponible: **https://www.cisco.com/c/dam/en_us/training-events/product-training/prime-infrastructure-31/ja-datacoll/PI31_DataCollectionConcepts.pdf**

[18] Design Zone for Campus - Cisco SD-Access Solution Design Guide (CVD). Cisco. Disponible:
https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.pdf

[19] E. Espinoza, “Desarrollo e implementación de un sistema de control de acceso a redes inalámbricas mediante RADIUS”, Tesis de Pregrado, Universidad Nacional Mayor de San Marcos, 2018. Disponible
http://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/10018/Espinoza_ae.pdf?sequence=1&isAllowed=y

[20] E. Rodríguez, “Diseño y simulación de una red definida por software para la implementación de un laboratorio avanzado de datos para la EP de Telecomunicaciones de la Facultad de Ingeniería Electrónica y Eléctrica de la Universidad Nacional Mayor de San Marcos”, Tesis de

Pregrado, Universidad Nacional Mayor de San Marcos, 2020. Disponible: **https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/16021/Rodriguez_ge.pdf?sequence=1&isAllowed=y**

[21] F. López, "El estándar IEEE 802.11 Wireless LAN", Trabajo de Investigación, Universidad Politécnica de Madrid, 2002. Disponible: **https://www.dit.upm.es/~david/tar/trabajos2002/08-802.11-Francisco-Lopez-Ortiz-res.pdf**

[22] F. Reina, & J. Ruiz, “Redes de área local”, Trabajo de Investigación, Universidad Nacional del Nordeste, 2002. Disponible: **http://ing.unne.edu.ar/pub/local.pdf**

[23] G. Cuba, & J. Becerra, “Diseño e implementación de un controlador SDN/OpenFlow para una red de campus académica”, Tesis de Pregrado, Pontificia Universidad Católica del Perú, 2015. Disponible: **https://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/7149**

[24] Guías de configuración de sistemas compatibles: Guía de configuración BGP. Cisco. Disponible: **https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/17612-bgp.pdf**

[25] Intermediate System-to-Intermediate System (IS-IS). Cisco. Disponible: **https://www.cisco.com/c/en/us/products/ios-nx-os-software/intermediate-system-to-intermediate-system-is-is/index.html#:~:text=IS%2DIS%20is%20a%20link,ongoing%20enhancements%20to%20the%20protocol**

[26] J. Chafloque, “Propuesta de diseño de una red de datos de área local bajo la arquitectura de redes definidas por software para la Red Telemática de la Universidad Nacional Mayor de San Marcos”, Tesis de Pregrado, Universidad Nacional Mayor de San Marcos, 2018. Disponible: **https://cybertesis.unmsm.edu.pe/handle/20.500.12672/10017**

[27] K. Karmarkar, “DNA Software Defined-Access – Integrating with Existing Network”. Cisco Live!, 2017. Disponible: **https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2017/pdf/BRKCRS-2812.pdf**

[28] L. Aguilar, “Propuesta de Diseño de una red privada de telecomunicaciones para accesos a aplicaciones de una entidad bancaria a través de Internet”. Tesis de Pregrado, Universidad Tecnológica del Perú, 2020. Disponible: **https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/3495/Luis%20Aguilar_Tesis_Titulo%20Profesional_2020.pdf?sequence=1&isAllowed=y**

[29] L. Hernández, R. García & C. Macías, "Tutorial para diseño y configuración de redes WLAN considerando el estándar 802.11n", Tesis de Pregrado, Universidad Cooperativa de Colombia, 2017. Disponible:

https://repository.ucc.edu.co/bitstream/20.500.12494/7481/1/2017_tutorial_configuracion_wlan.pdf

[30] López, “Diseño y simulación con ISE (identity services engine) para mitigar accesos no autorizados a una red corporativa”, Tesis de Pregrado, Universidad Tecnológica del Perú, 2017. Disponible: **https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/935/Carlos%20Lopez_Tesis_Titulo%20Profesional_2017.pdf?sequence=1&isAllowed=y**

[31] M. Hospina, “Diseño e implementación de VLANS para mejorar la eficiencia en la transmisión de datos en la Municipalidad Provincial de Huancayo”, Tesis de Pregrado, Universidad Nacional del Centro del Perú, 2017. Disponible: **http://repositorio.uncp.edu.pe/bitstream/handle/UNCP/5038/T010_47190108_T.pdf?sequence=1&isAllowed=y**

[32] Nakao, L. Peterson & A. Bavier, “A Routing Underlay for Overlay Networks”, Paper, Princeton University, 2003. Disponible: **https://www.cs.princeton.edu/courses/archive/fall06/cos561/papers/nakao03.pdf**

[33] NSX-T Data Center Quick Start Guide. VMware Docs Home. Disponible: **https://docs.vmware.com/es/VMware-NSX-T-Data-Center/3.1/nsxt_31_admin.pdf**

[34] Redes – Sistema de nombres de dominio (DNS), IBM, 2014. Disponible: **https://www.ibm.com/docs/es/ssw_ibm_i_72/rzakk/rzakkpdf.pdf**

[35] Seguridad en redes wifi: una guía de aproximación para el empresario, INCIBE – Instituto Nacional de Ciberseguridad. Disponible: **https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-de-seguridad-en-redes-wifi.pdf**

[36] T. Hess, & N. Matau, “Enterprise Network Virtualization using IP and MPLS Technologies: Introduction”. Cisco Live!, 2016. Disponible: **https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2016/pdf/LTRMPL-2102.pdf**

[37] V. Hafner, “Cisco SD-Access – Connecting to the Data Center, Firewall, WAN and More”, Cisco IMAGINE INTUITIVE, 2019. Disponible: **https://www.cisco.com/c/dam/m/hr_hr/training-events/2019/cisco-connect/pdf/VH-Cisco-SD-Access-Connecting.pdf**

[38] Virtual route forwarding design guide. Cisco. Disponible: **https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/vrf/design/guide/vrfDesignGuide.pdf**

[39] VXLAN Configuration - S7700 V200R011C10 Configuration Guide - VXLAN – Huawei. Disponible: **https://support.huawei.com/enterprise/en/doc/EDOC1000178306/2f28023c/vxlan-configuration**

[40] W. Intriago, “Estudio del protocolo Openflow usando el modelo de red definida por Software (Software Define Networks). Caso de estudio la Universidad Técnica de Manabí”, Tesis de Pregrado, Pontificia Universidad Católica del Ecuador, 2017. Disponible: **http://repositorio.puce.edu.ec/bitstream/handle/22000/14424/TESIS%20WILSON%20-%20PUCE-10-11-17.pdf?sequence=1&isAllowed=y**

ANEXOS

- Anexo N° 1: Matriz de Consistencia.

TITULO: "DISEÑO DE UNA GESTION CENTRALIZADA Y AUTOMATIZACION DE LA RED LAN UTILIZANDO LA SOLUCION CISCO SD-ACCESS EN UNA EMPRESA DE AERONAVEGACIÓN"				
PROBLEMA **Problema general** ¿Cómo el diseño de la solución SD-ACCESS gestiona de manera centralizada y automatizada la red LAN de una empresa de aeronavegación? **Problemas específicos A** ¿Cómo la solución SD Access integra a los nuevos dispositivos de la red LAN de una empresa de aeronavegación? **Problemas específicos B** ¿Cómo optimizar la seguridad en la red LAN con la solución SD-Access? **Problemas específicos C** ¿Cómo administrar de manera centralizada la red LAN utilizando DNA CENTER?	**OBJETIVOS** **Objetivo general** Implementar el diseño de la solución SD Access para gestionar centralizadamente y automatizada la red LAN en una empresa de aeronavegación **Objetivos Específicos A** Diseñar la infraestructura de red con la solución SD Access **Objetivos Específicos B** Determinar políticas de seguridad conforme a los estándares de Cisco **Objetivos Específicos C** Diseñar un control centralizado basado en los 3 niveles del fabricante (Core, distribución y acceso)	**HIPOTESIS** **Hipótesis general** La implementación del diseño de la solución SD Access mejora la gestión centralizada y automatizada la red LAN en una empresa de aeronavegación **Hipótesis especificas A** La integración automatizada de nuevos dispositivos de red permite reducir el tiempo de configuración **Hipótesis especificas B** La determinación de las políticas de seguridad mejora los estándares actuales de seguridad de la red LAN **Hipótesis especificas C** El diseño de un control centralizado permite gestionar la red LAN de manera grafica	**VARIABLE** **Variable Independiente** Solución CISCO SD-ACCESS **Variable Dependiente** Diseño de una gestión centralizada de la red LAN Automatización de la red LAN	**METODOLOGIA** **Tipo de investigación** Investigación tecnológica con niveles de aplicación **Diseño de investigación** • Gestionar de manera centralizada y automatizada la red LAN • Integra a los nuevos dispositivos de la red LAN • Optimizar la seguridad en la red LAN • Administrar de manera centralizada la red LAN utilizando DNA CENTER