Universitat Oberta de Catalunya

Software Defined Network
(Solución Cisco SDA)

Juan Pedro Zárate Díaz

Administración de redes y sistemas operativos

Grado de Ingeniería Informática

Tutor: Joaquín López Sánchez-Montañés

Año académico: 2022/23-2

FICHA DEL TRABAJO FINAL

Título del trabajo:	Software Defined Network (Solución Cisco SDA)
Nombre del autor:	Juan Pedro Zárate Díaz
Nombre del consultor:	Joaquin Lopez Sanchez-Montañes
Fecha de entrega (dd/mm/aaaa):	18/06/2023
Titulación:	Grado de Ingeniería Informática
Área del Trabajo Final:	Administración de redes y sistemas operativos
Idioma del trabajo:	Castellano
Palabras clave:	SDN, Automatización, Overlay/Underlay,VXLAN,DNAC

Resumen del trabajo:

La tecnología SDN [(1)] llega finalmente a las actualmente conocidas como Redes de Acceso (LAN+WLAN) [(1)] después de demostrar sus relevantes beneficios tanto en el Datacenter como en las redes WAN. Sin duda alguna, es el mayor cambio disruptivo que enfrentan a éstas en casi tres décadas. Conllevan un importante cambio de paradigmas tanto en su diseño como en su explotación y mantenimiento. Su mayor aporte lo constituye el hecho de responder a la necesidad de alinearse con las “intenciones” del negocio (intention based networking) y que por tanto representen una herramienta para crear valor dentro de cualquier compañía.

La arquitectura DNA [(2)] de Cisco, elemento central de esta memoria, está especialmente adelantada en la incorporación de SDN en las redes empresariales, por lo que su despliegue asegura los máximos beneficios para la organización como lo son una mayor simplificación, agilidad y eficacia en la implementación de nuevos servicios y la reducción de riesgos mediante la seguridad integrada.

Con este TFG pretendo facilitar comprensión e introducir a todos los lectores a las redes definidas por software en su capa de acceso (SDA), basándome en un caso práctico de migración de una red tradicional/ legacy a una red SDN.

SDN technology finally arrives to what is currently known as Access Networks (LAN+WLAN) after demonstrating its significant benefits in both the Datacenter and WAN networks. Without a doubt, this is the biggest disruptive change these networks have faced in almost three decades. It involves a significant shift in paradigms both in their design and operation and maintenance. Its greatest contribution is the fact that it responds to the need to align with the business's "intentions" (intention based networking) and therefore represents a tool for creating value within any company.

Cisco's DNA architecture, a central element of this memo, is particularly advanced in incorporating SDN in enterprise networks, so its deployment ensures maximum benefits for the organization such as greater simplification, agility, and effectiveness in implementing new services and reducing risks through integrated security.

With this TFG I intend to facilitate understanding and introduce all readers to Software Defined Networking in its access layer (SDA), based on a practical case of migration from a traditional/legacy network to an SDN network.

Índice

1. Introducción

1.1 Contexto y justificación

En la actualidad, la gestión de la red se enfrenta a numerosos retos debido a la configuración manual y a la fragmentada oferta de herramientas. Las operaciones manuales son lentas y propensas a errores, y estos problemas se verán agravados por el entorno en constante cambio, con más usuarios, dispositivos y aplicaciones. Con el crecimiento de usuarios y diferentes tipos de dispositivos que llegan a la red, es más complejo configurar las credenciales de usuario y mantener una política coherente en toda la red. Si su política no es coherente, existe la complejidad adicional de mantener políticas separadas entre las redes inalámbricas y las cableadas.

Como los usuarios se mueven por la red, también es difícil localizarlos y resolver problemas. La conclusión es que las redes actuales no responden a las necesidades existentes. El acceso definido por software (SD-Access) es la primera solución de red basada en la intención de la industria, fundamentada en los principios de la arquitectura de red digital (DNA) de Cisco.

SD-Access automatiza la política de acceso de los endpoints [2], por lo que las compañías pueden garantizar que las políticas correctas se establecen para cualquier usuario o dispositivo que se conecta a la red.

Las redes LAN tradicionales, disponen de mecanismos de seguridad bastante estáticos y manuales. Por lo general, más allá de disponer de una seguridad física para conectarse a la red desde la infraestructura interna, sea por el medio de acceso cableado o wireless, las redes de acceso suelen desplegarse en base a la ubicación o toma de red a la que se conecta el usuario o el dispositivo, debiendo haber configurado previamente el puerto al que se van a conectar junto a las restricciones de acceso, una vez que ya se ha conectado a la red.

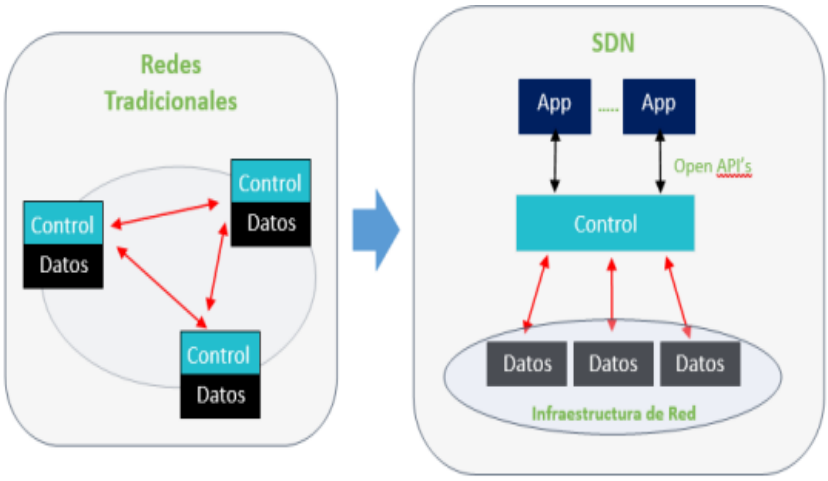

Imagen 1. Comparativa Redes Tradicionales vs SDN

Las ventajas fundamentales que nos proporciona la solución SDA son las siguientes:

1. Se simplifica el Onboarding [3] de dispositivos (Profiling [4] Posture [5], etc), donde ya no es necesaria una configuración manual del puerto del switch, o la toma de red donde se conecta el dispositivo o el usuario, sino que mediante estos mecanismos se identifica el tipo de endpoint y en base a ello, de manera inmediata se le aplica las restricciones o los permisos que hayan sido identificados o tipificados para ese tipo de dispositivo/ usuario.

Se controla qué se ha conectado y desde dónde se ha conectado.

2. Se simplifica la segmentación y microsegmentación. Se mejora la seguridad de la información, al poder controlar qué habla con qué (sensores vs control accesos, cartelería digital vs impresoras, etc) o quién habla con quién (RRHH con Marketing, IT con todos,..)
3. Se mejora la movilidad. Con esta tecnología, la dirección de red (IP) ya no está vinculada a la ubicación física donde se encuentra el endpoint, sino que es éste el que tiene la identidad (IP) independientemente de su ubicación.

4. Las políticas aplicadas se basan en la identidad del dispositivo o incluso en la de usuario y NO en la ubicación, tal y como sucede en el punto anterior.

La continua evolución de las tecnologías, sumado al cambio de paradigma que acompaña a las últimas innovaciones en el camino de la transformación digital hacía las redes SDN, ha hecho que la solución SDA del fabricante Cisco, centre toda nuestra atención y sea razón más que suficiente para protagonizar el proyecto de fin de grado que nos ocupa.

1.2 Objetivos

Construir una base sólida sobre la que se soporte el despliegue de una red SDN. En donde el equipo de red simplemente se encargue de definir lo que quiere conseguir (intención) y sería la "red" con la solución SDA quien se encargaría de traducir ese objetivo a un lenguaje simple y transparente, aplicando las políticas y las configuraciones necesarias a todos los elementos de red para llevarlo a cabo con éxito.

Los objetivos principales que se persiguen con este proyecto son:

- Evaluación y adquisición de hardware de red compatible con la solución SDA
- Automatización y simplificación de la gestión
- Tiempos de respuesta/ despliegues más rápidos ante la necesidad de nuevos servicios
- Mejorar la visibilidad de la red y de los endpoints
- Incrementar la disponibilidad de la red
- Control de acceso a la red basado en roles
- Políticas de acceso a la red consistentes en toda la compañía
- Estandarización

Para conseguirlos, y siempre en el contexto de un proyecto, se han aplicado los grupos de procesos de la dirección de proyectos.

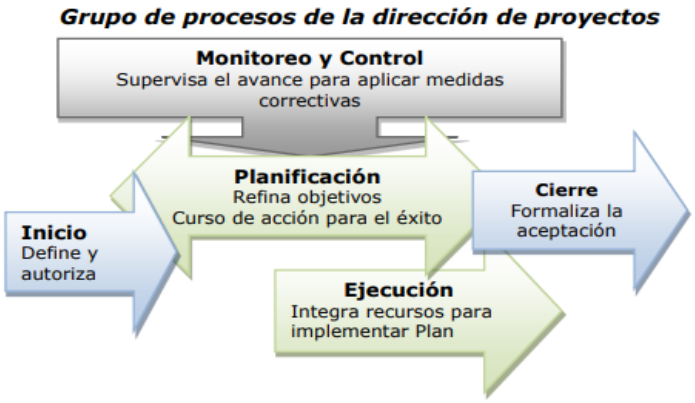

Imagen 2. Procesos de la Dirección de Proyectos

1.3 Alcance

El alcance de este proyecto engloba la migración y renovación de la infraestructura LAN/WLAN multiservicio, actualmente desplegada en una oficina ubicada en Málaga, estando las oficinas generales de la compañía en Barcelona.

Dentro del proyecto existen dos partidas económicas diferenciadas:

1. Servicios de Diseño, Instalación, Configuración y Mantenimiento dedicadas al integrador, en este caso, yo mismo.
2. Servicios profesionales del fabricante, en los que se englobaría el soporte y acompañamiento durante todas las fases del proyecto.

1.4 Enfoque y método seguido

En primer lugar, comenzaremos con una visión global de las redes SDN y más concretamente de la solución SDA que protagoniza este TFG, con el objetivo de comprender y diferenciar el comportamiento y la arquitectura de esta solución frente a las redes tradicionales.

En el segundo enfoque, pasaremos a desarrollar/ explicar los componentes en detalle de nuestra solución SDA, para que el entendimiento durante los diferentes "capítulos" sobre el Diseño Físico, Underlay [6] y Overlay [7], junto con la integración con las redes externas sea el máximo posible.

En tercer lugar, nos centraremos en detallar los dos elementos principales (Ciso ISE [3] y DNA Center) de la solución SDA.

Finalmente, elaboraremos un pequeño informe que recoja las conclusiones obtenidas sobre la simulación de un proyecto real de migración, en donde se incluirá un pequeño análisis de los riesgos y su posible mitigación.

1.5 Planificación

Incluimos dos planificaciones diferenciadas:

1. Planificación del Trabajo
2. Planificación del Proyecto (Alcance)

Planificación del Trabajo

Seguimiento de entregas:

Descripción de Entregas	Planificado	Entregado
Confirmar tema de trabajo con el consultor	12/03/2023	03/03/2023
PEC-1 Propuesta de Plan de Trabajo	19/03/2023	12/03/2023
PEC-2 Primera parte de la memoria	23/04/2023	21/04/2023
PEC-3 Segunda parte de la memoria	28/05/2023	27/05/2023
Elaboración presentación virtual	18/06/2023	12/06/2023
Entrega final del TFG	18/06/2023	12/06/2023

Tabla 1. Planificación de entregas del TFG

Cronograma:

Nombre de tarea	Duración	Comienzo	Fin	Predecesora
Software Define Network (Solución Cisco SDA)	**83 días?**	**vie 03/03/23**	**dom 18/06/23**	
Revisión tema de trabajo con el consultor	1 día	vie 03/03/23	vie 03/03/23	
PEC-1 Propuesta de Plan de Trabajo	**7 días**	**sáb 04/03/23**	**dom 12/03/23**	
Recopilación de información	2 días	sáb 04/03/23	lun 06/03/23	
Conceptualización	3 días	mar 07/03/23	jue 09/03/23	
Elaboración	2 días	vie 10/03/23	dom 12/03/23	
Entrega de la propuesta del Plan de Trabajo	1 día	dom 12/03/23	dom 12/03/23	
PEC-2 Primera parte de la memoria	**28 días?**	**dom 19/03/23**	**dom 23/04/23**	7
Recopilación de documentación	7 días	dom 19/03/23	dom 26/03/23	
Arquitectura solución SDA	**6 días**	**lun 27/03/23**	**lun 03/04/23**	
Añadir información a la memoria	6 días	lun 27/03/23	lun 03/04/23	9
Componentes solución SDA	**5 días?**	**mar 04/04/23**	**lun 10/04/23**	
Añadir información a la memoria	9 días	mar 04/04/23	vie 14/04/23	11
Diseño Físico de SDA	**6 días?**	**sáb 15/04/23**	**vie 21/04/23**	
Añadir información a la memoria	6 días	sáb 15/04/23	vie 21/04/23	13
Revisión de la primera parte de la memoria	2 días	vie 21/04/23	dom 23/04/23	
Entrega de la primera parte de la memoria	1 día	dom 23/04/23	dom 23/04/23	
PEC-3 Segunda parte de la memoria	**27 días?**	**lun 24/04/23**	**dom 28/05/23**	17
Recopilación de documentación	6 días	lun 24/04/23	lun 01/05/23	
Diseño y despliegue del Underlay	**4 días**	**mar 02/05/23**	**vie 05/05/23**	
Añadir información a la memoria	4 días	mar 02/05/23	vie 05/05/23	19
Diseño y despliegue del Overlay	**5 días?**	**sáb 06/05/23**	**jue 11/05/23**	
Añadir información a la memoria	5 días	sáb 06/05/23	lun 15/05/23	21
Integración redes externas	**0 días?**	**vie 12/05/23**	**vie 12/05/23**	
Añadir información a la memoria	2 días	vie 12/05/23	lun 15/05/23	23
ISE	**5 días?**	**mar 16/05/23**	**dom 21/05/23**	
Añadir información a la memoria	5 días	mar 16/05/23	dom 21/05/23	25
DNA Center	**4 días?**	**lun 22/05/23**	**jue 25/05/23**	
Añadir información a la memoria	1 día	lun 22/05/23	lun 22/05/23	27
Conclusiones	**2 días**	**mar 23/05/23**	**mié 24/05/23**	
Añadir información a la memoria	2 días	mié 24/05/23	jue 25/05/23	
Revisión de la segunda parte de la memoria	2 días	vie 26/05/23	dom 28/05/23	33
Entrega de la segunda parte de la memoria	1 día	dom 28/05/23	dom 28/05/23	
Elaboración presentación virtual	**16 días?**	**lun 29/05/23**	**dom 18/06/23**	
Realizar la pesentación en Power Point	16 días	lun 29/05/23	dom 18/06/23	35
Entrega final del TFG	23 días	jue 18/05/23	dom 18/06/23	

Imagen 3. Cronograma del TFG

Diagrama de Gantt:

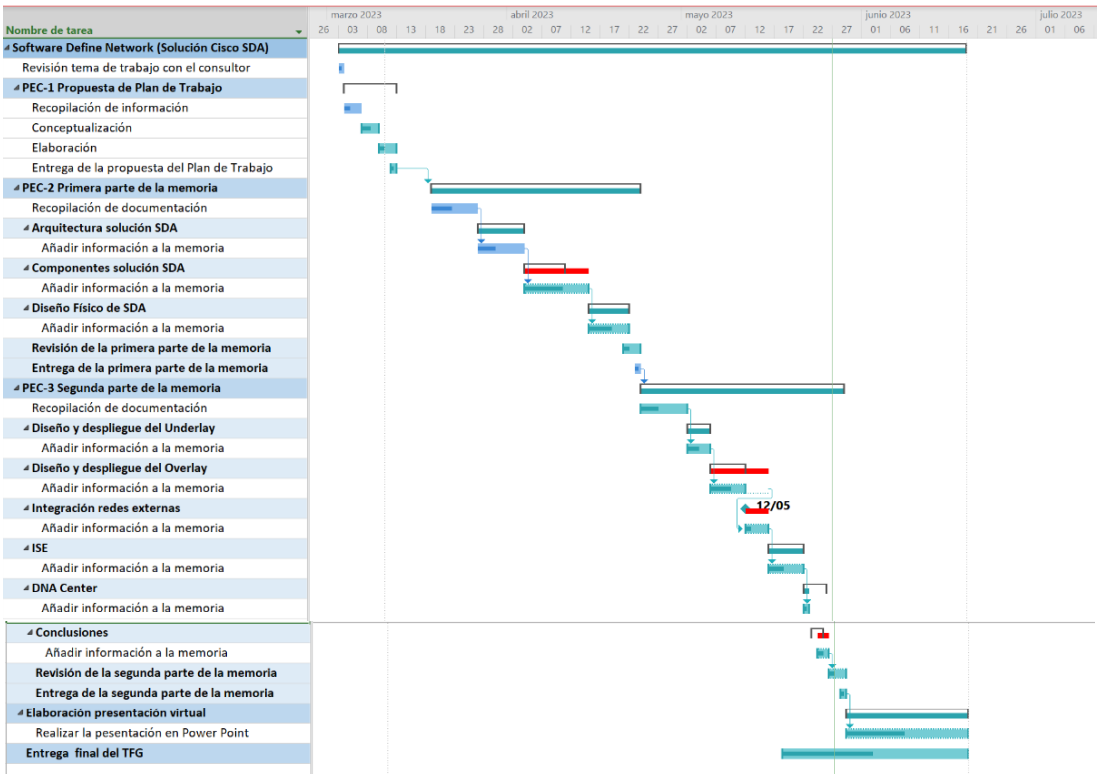

Imagen 4. Diagrama de Gantt del TFG

Planificación del Proyecto

A continuación, se muestra la planificación general de todo el proyecto, cuya duración se estima que sea de 6 meses.

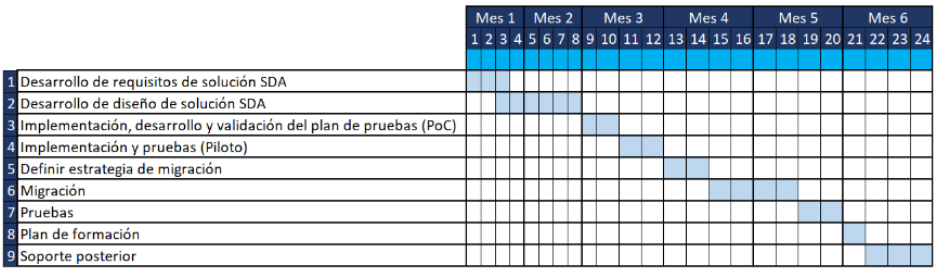

Imagen 5. Planificación del proyecto

Pasando a detallar las diferentes fases en las que hemos dividido todas las actividades a realizar:

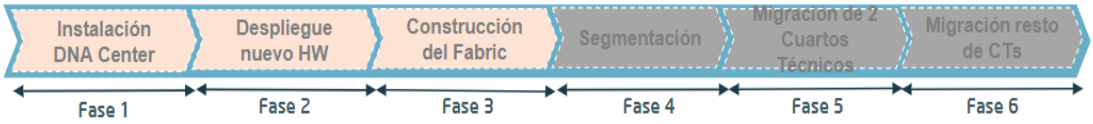

Imagen 6. Fases del proyecto

FASE 1: Instalación y configuración del DNA-Center, e integración con Cisco ISE.

FASE 2: Despliegue e interconexión de los nuevos equipos de red.

- Instalación de Border Nodes [8] y Control Plane Nodes [9]
- Despliegue de Intermediates Nodes [10] e interconexión con Border Nodes
- Instalación de Edge Nodes [11]

FASE 3: Construcción del Fabric

- Configuración desde DNA-Center de la nueva electrónica de red para construir el Fabric SDA.

FASE 4: Segmentación

- Configuración de macro y microsegmentación
- Configuración de políticas de acceso en ISE

FASE 5: Migración de 2 CT [4]

- Migración física y lógica de los endpoints de los dos cuartos técnicos seleccionados desde la electrónica actual a los nuevos Edge Nodes.

FASE 6: Migración del resto de CT

- Migración física y lógica de los endpoints del resto de cuartos técnicos desde la electrónica actual a los nuevos Edge Nodes.

1.6 Breve sumario de productos obtenidos

El producto obtenido es un documento que sirve de aproximación o de referencia para afrontar el reto de llevar a cabo un proyecto de migración real desde una red legacy hacía una red SDN o la implantación desde cero; enfocado en la solución SDA.

Además de servir como introducción a la propia solución SDA de Cisco, ya que se analiza/ desglosa todos sus componentes, facilitando su compresión, y la capacitación para llevar a cabo cualquier actividad relacionada con este nuevo enfoque con la mayor garantía de éxito.

1.7 Breve descripción de los otros capítulos de la memoria

La memoria se organiza en 3 bloques principales, además de un apartado final de conclusiones y los anexos.

Primer bloque:

Se compone de los capítulos 2,3 y 4, en donde nos centramos por completo en la solución SDA de Cisco. Comenzando por la arquitectura, pasando por la descripción detallada de sus componentes y finalización con el diseño físico.

Segundo Bloque:

Lo integran los capítulos 5,6 y 7, en donde ponemos el foco en el propio despliegue de la solución SDA, tanto del underlay como del overlay, así como con la integración con las redes externas.

Tercer Bloque:

Formado por los capítulos 8 y 9. Aquí, realizamos un análisis exhaustivo de los dos actores principales: Cisco ISE y Cisco DNA Center.

Conclusiones:

Al igual que indiqué en el punto 1.4, en este apartado recogeremos las conclusiones sobre la simulación de un proyecto real de migración, en donde se incluirá un pequeño análisis de los riesgos y sus posibles mitigaciones.

Anexos:

Donde se recogen toda la información que ayuda a la comprensión de la memoria (Acrónimos y Glosario), facilita el seguimiento o acceso directo a determinadas imágenes y tablas (Listado de Imágenes y Lisado de Tablas), se documentan todas las referencias bibliográficas en las que nos hemos apoyado para la elaboración del proyecto.

1.8 AS-IS (Situación actual)

1.8.1 Infraestructura de red

La arquitectura de red actual de la sede de la compañía QUARTZ en Málaga está formada por tres capas, y ha servido para satisfacer las necesidades y requerimientos de los servicios durante muchos años.

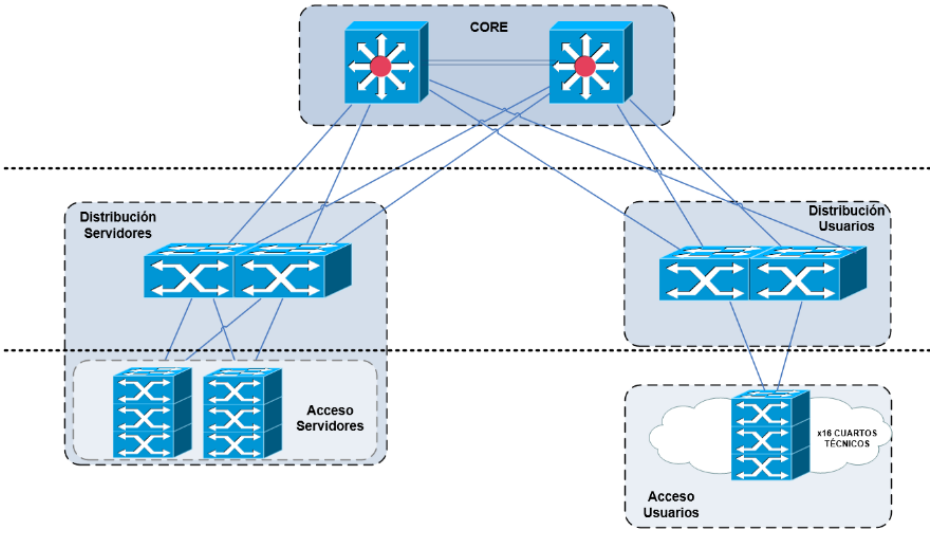

Imagen 7. Topología de red inicial

Existen dos equipos funcionando como el **núcleo/ backbone** de la red (Capa Core), dos bloques diferenciados dentro de la capa de **distribución** (Bloque de Distribución de Usuarios vs Distribución de Servidores) y del mismo modo, dos bloques para la parte de **acceso** (Acceso de Usuarios vs Acceso de Servidores). La ubicación física es la siguiente:

- Data Center: Core + Distribución de Servidores y de Usuarios + Acceso de Servidores
- Cuartos Técnicos repartidos por la sede: Acceso usuarios

Describimos brevemente el papel que desempeña cada una de las capas mencionadas:

Core

Proporciona un transporte rápido entre los dispositivos de la capa de distribución y es un punto de consolidación para el resto de la red.
Asegura el reenvío de paquetes de datos a alta velocidad y con redundancia.

Distribución

También llamada capa de agregación. Es un lugar de tránsito de tráfico apropiado para aplicar políticas, como QoS [5], enrutamiento o seguridad.

Acceso

Proporciona conexión física para que los dispositivos terminales accedan a la red.

Nuestra red también dispone de infraestructura Wireless compuesta por una controladora WLC [6] y 100 Access Points repartidos por toda la sede para proporcionar cobertura WiFi a los endpoints.

El resto de los servicios fundacionales como, por ejemplo: NAC [7] (Cisco ISE) y DNS [8] y DHCP[9] (InfoBlox [12]), se encuentran en la sede principal de Barcelona.

1.8.2 Conceptualización

La estimación de costes del proyecto la dividimos en 3 apartados:

1. BoM [10]
2. Estimación de esfuerzos y sus costes asociados
3. Servicios Profesionales

BoM

El equipamiento de red necesario para llevar a cabo la memoria es el siguiente:

- 34 nodos Edge Catalyst 9300 para Acceso
  - 32 x Acceso Usuarios
  - 2 x Acceso Servidores
- 4 nodos Catalyst 9500 para Distribución
  - 2 x Distribución Usuarios
  - 2 x Distribución Servidores
- 2 nodos Catalyst 9800 como WLC
- 100 puntos de acceso Catalyst 9120I
- 2 routers ISR4331
- 2 nodos Catalyst 9500 para Border
- 1 DNA Center

Role	Part Number	Descripción	Cantidad	Coste Unitario	Coste Total
Acceso Usuario/ Fabric Edge	C9300-48UN-A	Catalyst 9300 48-port of 5Gbps Network Advantage	32	15.873,00 USD	507.936,00 USD
Acceso Servidores/ Fabric Edge	C9300-24UX-A	Catalyst 9300 24-port mGig and UPOE, Network Advantage	2	16.006,00 USD	32.012,00 USD
Distribución Usuarios/ Intermediate Node	C9500-48Y4C-A	Catalyst 9500 48-port x 1/10/25G + 4-port 40/100G, Advantage	2	28.637,00 USD	57.274,00 USD
Distribución Servidores/ Intermediate Node	C9500-24Y4C-A	Catalyst 9500 24x1/10/25G and 4-port 40/100G, Advantage	2	26.319,00 USD	52.638,00 USD
Wireless Lan Controller	C9800-40-K9	Cisco Catalyst 9800-40 Wireless Controller	2	50.864,00 USD	101.728,00 USD
Access Point	C9120AXI-E	C9120AX Internal 802.11ax 4x4:4 MIMO;IOT;BT5;mGig;USB;RHL	100	2.164,00 USD	216.400,00 USD
Control Plane Node	ISR4331/K9	Cisco ISR 4331 (3GE,2NIM,1SM,4G FLASH,4G DRAM,IPB)	2	5.222,00 USD	10.444,00 USD
Border Node	C9500-24Y4C-A	Catalyst 9500 24x1/10/25G and 4-port 40/100G, Advantage	2	26.319,00 USD	52.638,00 USD
DNA Center	DN2-HW-APL-XL-U	DNA Center Appliance (Gen 2)- 112 core for Promos	1	368.739,00 USD	368.739,00 USD
				Total	1.399.809,00 USD

Imagen 8. BoM del proyecto

** No se tienen en cuenta otros ítems como doble fuente de alimentación, network modules para los uplink [13] de fibra, transceivers[14], etc.*

*** Precios obtenidos de la web https://itprice.com/ donde se encuentra el precio de lista de los ítems indicados.*

Estimación de esfuerzos y sus costes asociados

Se realiza en base a la planificación del proyecto del punto 1.5, considerando los perfiles requeridos para llevar a cabo el proyecto.

Actividad	Descripción	Esfuerzo	Coste
Responsable	Coordinación y gestión	200 Horas	20000 USD
Jefe de Proyecto	Coordinación del proyecto	700 Horas	56000 USD
Ingeniero Senior de Redes	Configuración y validación	400 Horas	24000 USD
Ingeniero Junior de Redes	Configuración y validación	600 Horas	27000 USD
Instalador	Montaje/conexionado del equipamiento	160 Horas	4800 USD
		Total:	131800 USD

Tabla 2. Estimación esfuerzos y costes del proyecto

Servicios Profesionales

Se han contratado los servicios profesionales del fabricante Cisco para que supervise y ayude durante todas las fases del proyecto, disponiendo de acceso completo al soporte avanzado de los expertos de la solución SDA. De este modo, garantizamos la correcta implantación e implementación de esta solución durante toda la duración del proyecto.

Actividad	Descripción	Coste
Fabricante	Soporte y acompañamiento	50000 USD

Tabla 3. Servicios profesionales del proyecto

Presupuesto final:

Actividad	Descripción	Coste
BoM	Contextualización	1.399.809 USD
Estimación de esfuerzos	Coordinación del proyecto	131.800 USD
Servicios Profesionales	Configuración y validación	50.000 USD
	Total:	**1.581.609 USD**

Tabla 4. Presupuesto final del proyecto

2. Arquitectura de la solución SDA

2.1 Visión general

La Arquitectura de Red Digital de Cisco (Cisco DNA) proporciona una hoja de ruta para la digitalización y un camino para lograr beneficios inmediatos de automatización de redes, garantía y seguridad. La arquitectura de Acceso Definido por Software (SD-Access) de Cisco es la evolución de Cisco DNA desde diseños tradicionales de LAN en el campus a redes que implementan directamente la intención de una organización. La aplicación SD-Access se ejecuta en el controlador Cisco DNA Center para diseñar, aprovisionar, aplicar políticas y proporcionar a la red cableada e inalámbrica del campus el contexto que permite una red intuitiva basada en la intención.

Proporciona segmentación de un extremo a otro, automatizada y basada en la visibilidad para separar el tráfico de usuarios, dispositivos y aplicaciones sin rediseñar la red física (underlay) y trabajando siempre sobre el overlay. Se definen unos nuevos criterios de segmentación (Macrosegmentación vía VNs [(11)], Microsegmentación vía SGTs [(12)]) y que en conjunto con la solución ISE (NAC ya existente) y un DNA-Center, permitirán gestionar y orquestar la nueva red (fabric) y sus servicios.

SD-Access automatiza la política de acceso de usuarios para que se pueda asegurar que se establecen las políticas correctas para cualquier usuario o dispositivo con cualquier aplicación en la red. Esto se logra aplicando políticas de acceso unificadas en LAN y WLAN, lo que crea una experiencia de usuario consistente en cualquier lugar sin comprometer la seguridad.

2.2 Componentes

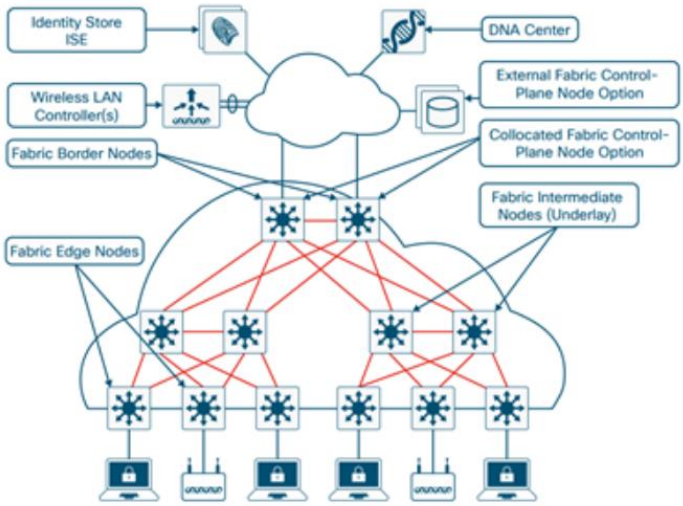

Imagen 9. Componentes de la solución SDA

DNA Center

El corazón de la automatización de la solución SD-Access se encuentra Cisco DNA Center. DNA Center es un controlador para la planificación y preparación, instalación e integración. SD-Access (SDA) es una de las muchas aplicaciones de software que se ejecutan en DNA Center.

Identity Services Engine (ISE)

Provee los servicios de autenticación, gestión de identidad y el cumplimiento de las políticas de seguridad (lo que permite el mapeo dinámico de usuarios y dispositivos a grupos escalables y simplifica la aplicación de políticas de seguridad de extremo a extremo). ISE se integra con DNA Center utilizando el Cisco Platform Exchange Grid (pxGrid) [15] y las API [13] REST para facilitar el intercambio de información del cliente y la automatización de las configuraciones relacionadas con el Fabric de SDA.

Fabric Wireless Lan Controller

Los WLC se integran con el plano de control del Fabric de SDA, y es en donde se centraliza el control de los Puntos de Acceso, dado que es en donde se registran los mismos a través del protocolo CAPWAP.

Access Point

Proporcionan acceso WiFi a todos los endpoints que tengan la capacidad de comunicarse por este medio de acceso.

Fabric Border Node "BN"

Es la puerta de entrada/salida entre el Fabric de SDA y las redes externas. Es el responsable de encapsular y entregar el tráfico entre el Fabric y el resto de la red. Y también, tiene la función de traducir el contexto (mapeo e identidad de usuario / dispositivo) dentro del propio Fabric.

Fabric Control Plane "CP"

Sirve como una base de datos central, rastreando a todos los usuarios y dispositivos a medida que se conectan a la red del Fabric y mientras se desplazan. El Fabric control plane permite que los componentes de la red (switches, enrutadores, WLC, etc.) consulten esta base de datos para determinar la ubicación de cualquier usuario o dispositivo conectado al fabric

Fabric Intermediate Node "IN"

Son los dispositivos más simples en la arquitectura de fabric de SD-Access. Ayudan a completar la capa del underlay, aglutinando todos los uplinks de los Fabric Edge hacia los Border Nodes.

Fabric Edge Node "FE"

Son responsables de conectar los endpoints al fabric y de encapsular / desencapsular y reenviar el tráfico desde estos endpoints hacia y desde el Fabric. Los Fabric Edge Nodes operan en el perímetro de Fabric y son los primeros puntos de conexión de los usuarios y la implementación de la política.

Un punto importante para tener en cuenta sobre los Fabric Edge Nodes es cómo manejan las subredes utilizadas para la conexión del endpoint. Todas las subredes alojadas en un Fabric SD-Access se aprovisionan, de forma predeterminada, en todos los Fabric Edge Nodes. Por ejemplo, si una subred 10.10.10.0/24 se aprovisiona en un fabric determinado, esta subred se definirá en todos los Edge Nodes de ese fabric, y los hosts ubicados en esa subred se pueden colocar en cualquier Edge Node dentro de ese fabric. Básicamente, esto "extiende" estas subredes en todos los Edge Nodes en ese fabric, lo que simplifica la asignación de direcciones IP, haciendo posible implementar menos subredes IP, aunque más grandes.

Aunque no hemos contemplado la parte de IoT como componente de nuestro proyecto, si vamos a comentar brevemente las opciones disponibles en caso de ser necesario, para extender nuestra red SDA más allá del entorno oficina (CPD, Cuartos Técnicos, Racks de pared, etc) en donde debido a las condiciones ambientales como: polvo, humedad, frío, calor, etc se requiere el despliegue de soluciones de red más robustas.

- **Extended Node** "EN**"**

Se conectan directamente a los Fabric Edge en modo trunk 802.1Q y funciona como un switch de nivel 2.

Admiten la autenticación del endpoint con 802.1x o MAB [(14)]. Cuando la autenticación del punto final se realiza correctamente, ISE aplica la política de autorización y la VLAN [(15)] adecuada se transfiere al puerto de acceso de origen. Para la microsegmentación, DNAC puede configurar un IP-SGT estático y enviarlo a la FE a la que está conectada la EN.

- **Policy Extended Node** "PEN**"**

Los puntos finales conectados a PEN pueden ser autenticados por ISE con 802.1x o MAB. Cuando la autenticación del punto final se realiza correctamente, el ISE aplica la política de autorización y la VLAN y el SGT adecuados se introducen en el puerto de acceso de origen del PEN, como se muestra en la Figura 9. Esto permite ampliar la microsegmentación hasta el PEN.

En la imagen siguiente vemos la diferencia entre ambos:

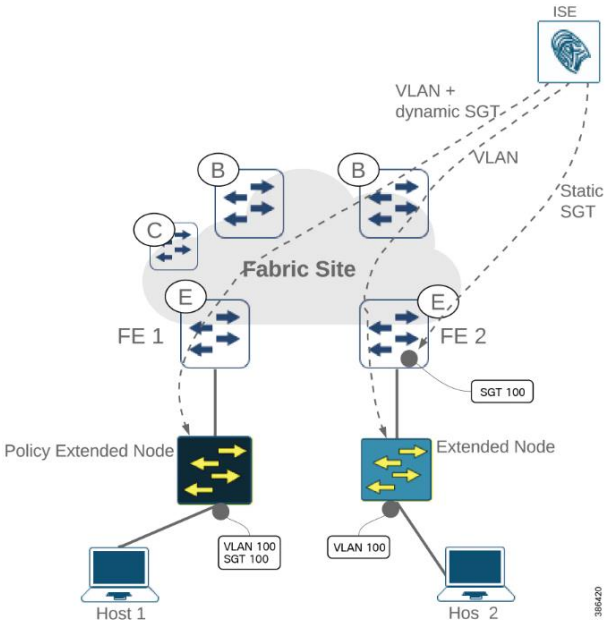

Imagen 10. Extended & Policy Extended Node

2.3 Capa del Overlay

Una red de Overlay se ejecuta sobre una capa subyacente/ física para crear una red virtualizada.

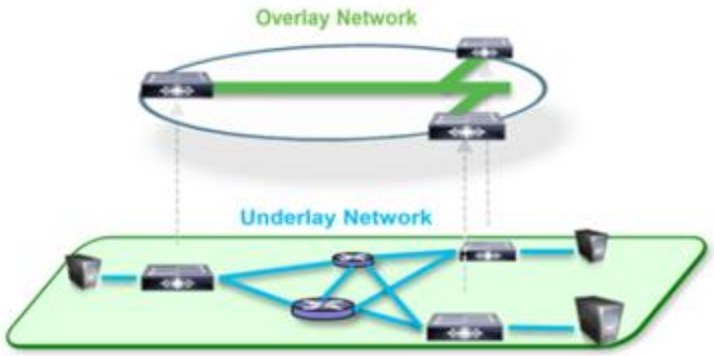

Imagen 11. Red Underlay y Red Overlay

Y se compone de 3 planos de operación:

1. Plano de control
2. Plano de datos
3. Plano de políticas

2.3.1 Plano de datos

Se basa en VXLAN. Es un método de encapsulación/ tunelización (basado en IP/UDP) que transporta tramas de capa 2 a través de paquetes de capa 3.

El objetivo principal es conectar dos redes separadas físicamente utilizando el mismo bloque de direccionamiento IP y la misma Vlan-ID si así fuera necesario; eliminando la limitación del número

de Vlans disponibles (4096/ 12 bits) al ofrecer más de 16 millones de Vlans-ID (24 bits) y la ineficiencia de los enlaces debido al uso del protocolo de spanning-tree [16].

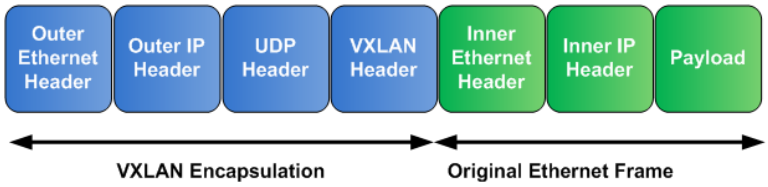

Imagen 12. Encapsulación VXLAN

Los segmentos VXLAN se crean entre los puntos finales del túnel VXLAN (VTEP [16]). Los VTEP admiten el protocolo VXLAN y realizan encapsulación y desencapsulación VXLAN. Puede pensar en un segmento VXLAN como un túnel entre dos VTEP, donde un VTEP encapsula una trama Layer2 con un encabezado UDP y un encabezado IP y lo envía a través del túnel. El otro VTEP recibe y desencapsula el paquete para obtener el marco de Capa 2.

En SD-Access, se han agregado algunas mejoras a las especificaciones VXLAN originales, en particular el uso de etiquetas de grupo de seguridad (SGTs) conocido en SDA como microsegmentación y el Virtual Nework Identity (VNI) o comúnmente conocido como VRF que en el entorno SDA sería la macro-segmentación.

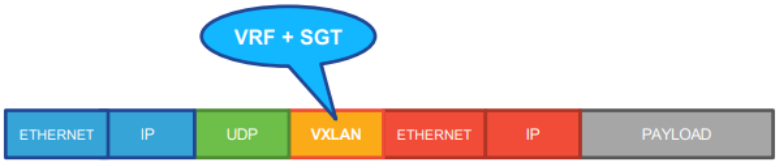

Imagen 13. Encapsulación VXLAN (VRF + SGT)

2.3.2 Plano de control

Se basa en LISP. Protocolo que crea dos identificadores:

1. EID == > Asignada al dispositivo final (endpoint)
2. RLOC == > Asignada a los dispositivos de red que ubican físicamente al dispositivo final

y cuyo uso cambia por completo el concepto de IP tradicional, con el que se podía conocer ambos identificadores, pero con grandes limitaciones que se evitan con LISP.

Tradicionalmente, cuando movemos un endpoint (Ejemplo: laptop) de ubicación, por lo general (siempre que hablamos de redes de nivel 3) es necesario cambiar el direccionamiento IP del dispositivo por uno nuevo.

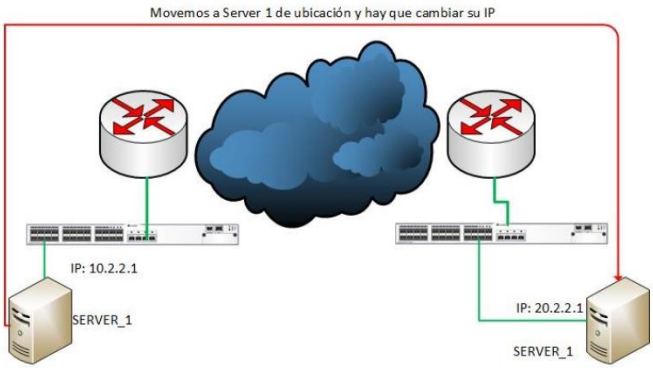

Imagen 14. Funcionamiento LISP -1

Sin embargo, esta necesidad desaparece con LISP[17]. Dado que el server_1 conserva su dirección IPv4 que en términos de LISP sería el EID[18], cambiando únicamente y de modo transparente el RLOC[19] para identificar el equipo de red al que está conectado.

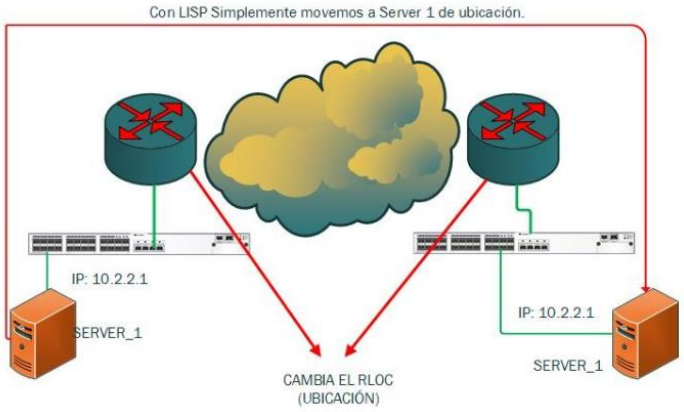

Imagen 15. Funcionamiento LISP -2

Para conseguir que este mecanismo funcione correctamente, se requiere de un mecanismo que almacene y traduzca EID a RLOC (similar al funcionamiento del servicio DNS).

Ese mecanismo se ejecuta en el nodo de Plano de Control, quien tiene la funcionalidad de MAP-Server (MS) y MAP-Resolver (MR).

- Los prefijos de EID (Direcciones IPv4 con máscaras /32) se registran en el MAP-Server junto con sus RLOC asociados en el momento de conectarse a la red.
- El MAP-Resolver entra en juego cuando se requiere establecer una comunicación entre un equipo A (10.10.10.1) y un equipo B (10.10.10.20), y el dispositivo de red al que está conectado no conoce el RLOC al que está conectado el equipo B.

2.3.3 Plano de políticas

Se basa en Cisco TrustSec [17]. Es una solución de seguridad integrada en los elementos de red (switches, routers, dispositivos inalámbricos y de seguridad como Cisco ISE) que permite segmentar dinámicamente el tráfico de red, clasificando los endpoints en grupos que pueden ser usados en cualquier lugar de la red, permitiendo desvincular las políticas de segmentación de la red del underlay.

La segmentación definida por software es mucho más fácil de habilitar y gestionar que la segmentación basada en VLAN y evita el impacto de procesamiento asociado en los dispositivos de red. La asignación de endpoints a un grupo no se realiza tomando como base su direccionamiento IP o pertenencia a una VLAN en particular sino a partir de decisiones de gestión alineadas con los requerimientos del negocio y las políticas de seguridad definidas. Esto facilita la gestión de la seguridad y brinda una mayor flexibilidad independizando la implementación de políticas de la pertenencia o no a una determina sección de la infraestructura (subred o VLAN). Cuando un usuario o dispositivo se conecta a la red, es esta (la red) la que le asigna un grupo de seguridad específico. Este mecanismo se denomina clasificación, y se realiza mediante el uso de Etiquetas de Grupo Escalables (SGT, por sus siglas en inglés) en la red del overlay.

El uso de SGT proporciona la capacidad de etiquetar el tráfico de puntos finales según las políticas de membresía de grupo en ISE. Se pueden crear asignaciones de grupo basadas en el rol laboral,

que se pueden utilizar para crear políticas de segmentación y reglas de asignación de redes virtuales.

Cisco TrustSec minimiza el riesgo reduciendo la superficie de ataque mediante una segmentación mejorada, aumenta la eficacia operativa y hace que sea más fácil alcanzar los objetivos de cumplimiento

2.4 Integración con redes externas

Cuando un endpoint es autorizado en el Fabric SDA, obtiene un SGT para que su tráfico esté siempre etiquetado con él. Por lo tanto, las comunicaciones Este-Oeste dentro del Fabric se pueden reforzar con SGACLs [(20)], ya que los switches Fabric Edge conocen tanto el SGT de origen como el de destino. Los SGT se transportan siempre con los paquetes de datos dentro de la cabecera VXLAN.

Imagen 16. SGACLs

Sin embargo, cuando los puntos finales se comunican con un destino fuera del Fabric, la cabecera VXLAN del paquete es desencapsulada en el nodo fronterizo del Fabric (Border Node) y desaparece cualquier referencia al valor del SGT. Lo mismo ocurre con el tráfico que entra al Fabric de inicio o de retorno por el Border-Node ya que desconoce el SGT y sólo recibe paquetes IP (sin etiquetar) procedente de los destinos externos.

Por ello, existen dos modos de propagar los SGTs:

1. Inline Tagging:
2. SXP

Inline Tagging

El etiquetado en línea es el proceso en el que el SGT se transporta dentro de un campo especial conocido como CMD (Cisco Meta Data) insertado en una cabecera L2, y requiere que todos los dispositivos por los que se transita (Del origen al destino) sean compatibles con TrustSec.

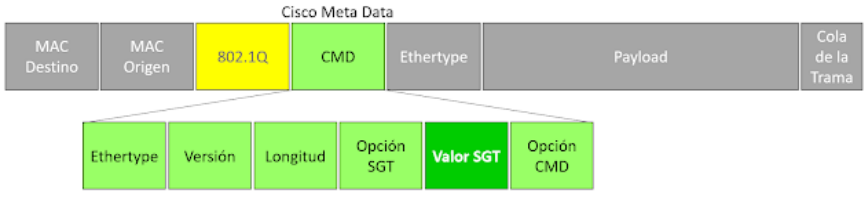

Imagen 17. Cisco Meta Data

Scalable Group Tag eXchange Protocol (SXP)

Protocolo de interconexión basado en TCP que se usa para anunciar la BBDD con la información de mapeo IP-to-SGT, a través del puerto 64999.

Se pueden establecer relaciones: Speaker, Listener o ambas

El servidor ISE puede actuar como SXP Speaker y los dispositivos de red como SXP Listeners, pudiendo descargar cuando así lo requieran los enlaces IP a SGT desde ISE para reforzar la seguridad entre endpoints tanto dentro como fuera del Fabric.

3. Componentes de la solución SDA del proyecto

Un Fabric SDA es una red superpuesta (overlay) compuesta por elementos de red como: switches, routers para la parte cableada y Access Point, Wireless Lan Controller para el medio de acceso Wireless.

Los diferentes roles de todos estos componentes son:

- Fabric Border (BN)
- Control Plane (CP)
- Intermediate Node (IN)
- Fabric Edge (FE)
- Wireless Lan Controller (WLC)
- Wireless Access Point (AP)
- Cisco DNA Center (DNAC)
- Cisco Identity Services Engine (ISE)

3.1 Border Node

Contiene la configuración, los protocolos y las tablas para proporcionar enrutamiento interno y externo entre el overlay y las redes externas (conocidas o desconocidas).

El equipamiento elegido para este role dentro de nuestro proyecto es el modelo: C9500-24Y4C

Imagen 18. Vista Frontal C9500-24Y4C

Se puede ver el detalle y el datasheet [18] en el siguiente link:

- Cisco Catalyst 9500 Series Switches Data Sheet - Cisco

3.2 Control Plane Node

Responsable de mantener la funcionalidad LISP Map-Server (MS) y Map-Resolver (MR). Aunque este rol puede ser ejecutado por el mismo equipo que tiene el rol de Border, siempre que sea posible es preferible que sea un hardware independiente.

El equipamiento elegido para este rol dentro de nuestro proyecto es el modelo: ISR4331

Imagen 19. Vista Trasera ISR 4331

Se puede ver el detalle y el datasheet en el siguiente link:

- Cisco 4000 Family Integrated Services Router Data Sheet - Cisco

3.3 Intermediate Node

En una arquitectura de 3 capas tradicional (Core, Distribución y Acceso), equivalen a los nodos de Distribución. En SDA simplemente se encargan de enrutar el tráfico IP, ni tan si quiera necesitan encapsular/desencapsular VXLAN, siendo su único requisito la capacidad de poder manejar Jumbo Frames para que sí puedan conmutar tráfico VXLAN.

El equipamiento elegido para este role dentro de nuestro proyecto son los modelos:

- C9500-48Y4C
- C9500-24Y4C

Imagen 20. Vista Frontal C9500-48Y4C

Imagen 21. Vista Frontal C9500-24Y4C

Se puede ver el detalle y el datasheet de ambos modelos en el siguiente link:

- Cisco Catalyst 9500 Series Switches Data Sheet - Cisco

3.4 Edge Node

Son equivalentes a los nodos de la capa de Acceso en una red legacy de 3 capas. Es decir, donde se conectan los endpoints (laptops, servidores, cámaras, impresoras, los puntos de acceso inalámbricos, etc).

El equipamiento elegido para este role dentro de nuestro proyecto son los modelos:

- C9300-48UN-A
- C9300-24UX-4

Imagen 22. Vista Frontal C9300-48UN-A

Imagen 23. Vista Frontal C9300-24UX-A

Se puede ver el detalle y el datasheet de ambos modelos en el siguiente link:

- Cisco Catalyst 9300 Series Switches Data Sheet - Cisco

La arquitectura StackWise permite ampliar hasta ocho switches en stack, con el objetivo de aumentar la capacidad y simplificar la administración. En nuestro proyecto se despliega esta arquitectura para los equipos con el rol:

- Fabric Edge
- Intermediate Node

Se conectan mediante cables especiales de stacking, comparten una única configuración de red, facilitando así la gestión y proporcionan una mayor resiliencia para la red, dado que el fallo de uno de los miembros del stack, no afecta a los endpoints que están conectados al otro switch, permitiendo que la red siga funcionando mientras se remplaza el switch sin afectar al funcionamiento general del stack.

Todo apilamiento de switches (stack) tiene un miembro master, que es el que se encarga de administrar el stack y coordinar el funcionamiento de todos los miembros del stack. El resto son miembros del stack (slave) pero siempre es recomendable configurar la prioridad en uno de ellos para que sea elegido como nuevo master, en caso de fallo del switch maestro. En nuestro caso, dispondremos de stack formados únicamente por dos switches, por lo que siempre estarán en modo activo/standby siendo uno de ellos el master y el otro el slave.

Esta arquitectura proporciona una solución escalable y de alta disponibilidad para las redes de datos.

Imagen 24. Conexión Cables de Stack

La configuración de los equipos que se encuentren en stack tendrán la siguiente configuración:

- Siwtch 1: 10 (Master)
- Switch 2: 8 (Standby)

```
i
switch 1 priority 10
switch 2 priority 8
i
```

3.5 Wireless Lan Controller

Nuestro modelo C9800-40-K9 es un controlador de red inalámbrica de alta capacidad diseñado para redes medianas y de gran tamaño.

Es compatible con el estándar WiFi 6 (802.1ax) lo que proporciona conexiones más rápidas y confiables que su homólogo WiFi 5.

Imagen 25. Vista frontal del C9800-40-K9

Se puede ver el detalle y el datasheet de ambos modelos en el siguiente link:

- Cisco Catalyst 9800-40 Wireless Controller Data Sheet - Cisco

3.6 Access Point

Hemos elegido el modelo de antenas integradas C9120AXI por las características de la oficina en donde se va a desplegar, al no permitir la instalación de antenas externas. Este punto de acceso también soporta el estándar WiFi 6 (802.1ax) siguiendo las funcionalidades del WLC al que se va a registrar, en las que destacamos su diseño para entornos de alta densidad y su flexibilidad con respecto al uso de sus dos radios (FRA).

Imagen 26. Punto de Acceso C9120AXI

Mostramos algunas de las principales capacidades:

Capacidad	Descripción
Compatible con Wi-Fi 6 (802.11ax)	Permite una mayor velocidad de transferencia de datos y una mejor eficiencia en el uso del espectro de radiofrecuencia.
Antena Flexible (FRA)	Mayor flexibilidad en la implementación del punto de acceso y una mejor cobertura inalámbrica para la ubicación específica del AP.
Tecnología MU-MIMO y OFDMA	Permiten al punto de acceso atender a múltiples dispositivos simultáneamente, lo que mejora la eficiencia y el rendimiento de la red inalámbrica.
Seguridad	Encriptación de datos de extremo a extremo, la autenticación de usuarios y la detección de intrusiones, que protegen la información confidencial de la empresa.
Power over Ethernet (PoE)	Permite la alimentación del AP y su conexión a la red a través de un único cable Ethernet.
Funciones avanzadas de movilidad/ roaming	Permiten a los dispositivos inalámbricos moverse sin interrupción entre diferentes puntos de acceso y mantener una conexión ininterrumpida.

Tabla 5. Capacidades Punto de Acceso C9120AXI

Se puede ver el detalle y el datasheet de ambos modelos en el siguiente link:

- Cisco Catalyst 9120AX Series Access Points Data Sheet - Cisco

3.7 DNA Center

La plataforma de administración y automatización elegida para nuestro proyecto es el modelo DN2-HW-APL-L, dado que nuestro objetivo después de finalizar este proyecto es el de añadir e integrar el resto de las sedes de nuestra compañía y el modelo elegido es el que mejores prestaciones nos ofrece en base al diseño y dimensión de nuestra organización.

	DN2-HW-APL	DN2-HW-APL-L	DN2-HW-APL-XL
Hardware description	Cisco UCS C220 M5 Rack Server 44 cores	Cisco UCS C220 M5 Rack Server 56 cores	Cisco UCS C480 M5 Rack Server 112 cores
Cisco DNA Center system scale			
Number of devices[1] (switch, router, wireless controller)	1000	2000	5,000
Number of wireless access points	4000	6000	13,000
Number of wireless sensors	600	800	1600
Number of concurrent endpoints	25,000	40,000	100,000
Number of transient endpoints (over 14-day period)	75,000	120,000	250,000
Ratio of endpoints: wired wireless	Any Any	Any Any	Any Any
Site Elements	1500	3000	6000
Number of wireless controllers	500	1000	2000
Number of ports[2]	48,000	192,000	768,000
API rate limit	50 APIs/min	50 APIs/min	50 APIs/min
NetFlow	30,000 flows/sec	48,000 flows/sec	120,000 flows/sec

Imagen 27. Escalabilidad y especificaciones hardware de DNA

Imagen 28. Vista Frontal de DN2-HW-APL-L

Se puede ver el detalle y el datasheet de ambos modelos en el siguiente link:

- Cisco DNA Center 2.3.3 Data Sheet - Cisco

3.8 ISE

Es nuestra plataforma de seguridad de red que proporciona una solución de gestión de identidad y acceso para dispositivos y usuarios que se conectan a la red. ISE permite a las organizaciones asegurar el acceso de los usuarios y los dispositivos a la red, aplicar políticas de seguridad y hacer cumplir los requisitos de cumplimiento.

Nuestra empresa ya dispone de un despliegue distribuido de ISE a nivel nacional, formado por 10 nodos:

- 2 ud x Nodos PAN
- 2 ud x Nodos MNT
- 5 ud x Nodos PSN

Hostname	Role	Model-VM	Status	Sede
BARPAN01	Admin	SNS-3655	Primary	Central Barcelona
BARMNT01	Monitor	SNS-3655	Secondary	Central Barcelona
BARPSN01	Policy Service	SNS-3655	PSN	Central Barcelona
BARPSN02	Policy Service	SNS-3655	PSN	Central Barcelona
MADPAN01	Admin	SNS-3655	Secondary	Sede Madrid
MADMNT01	Monitor	SNS-3655	Primary	Sede Madrid
MADPSN01	Policy Service	SNS-3615	PSN	Sede de Madrid
MADPSN02	Policy Service	SNS-3615	PSN	Sede de Madrid
VALPSN01	Policy Service	SNS-3615	PSN	Sede de Valencia
MALPSN01	Policy Service	SNS-3655	PSN	Sede de Málaga

Tabla 6. Despliegue de Nodos ISE

La topología de nuestro entorno ISE es el siguiente:

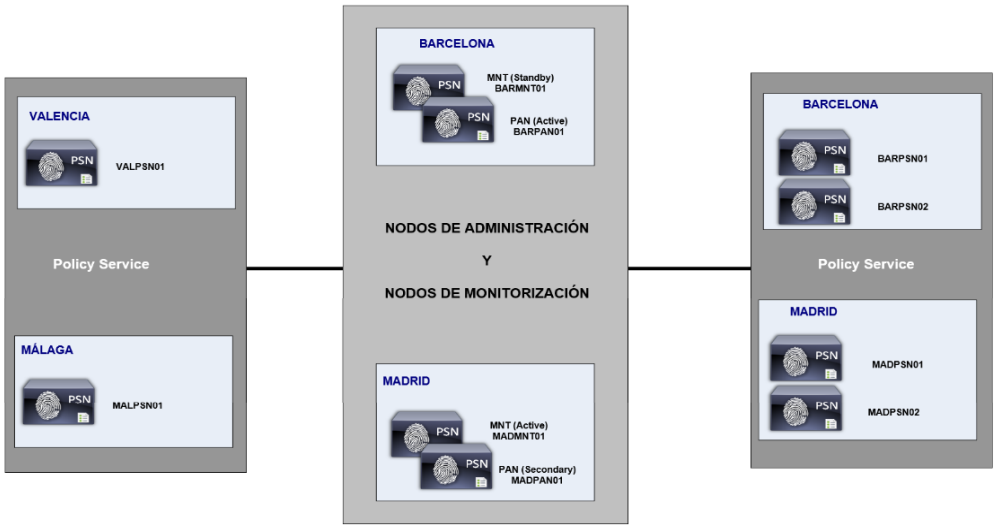

Imagen 29. Despliegue ISE

Se puede ver el detalle y el datasheet de ambos modelos en el siguiente link:

- https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/data_sheet_c78-656174.html

4. Diseño físico de la solución SDA (Topología de Red)

4.1 DNA Center

Aunque ya existe la alternativa de virtualizar el DNA Center, aún no es una solución muy extendida, por eso hemos decidido tal y como especificamos en el punto 3.7 elegir el modelo DN2-HW-APL-L en su opción física.

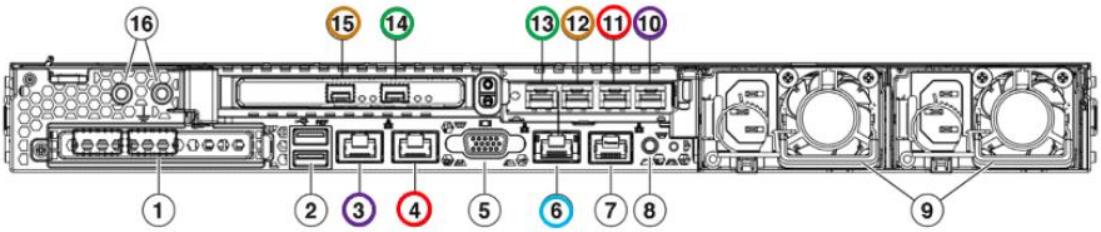

Imagen 30. Vista Trasera de DN2-HW-APL-L

Ports	Description
1	Modular LAN-on-motherboard (mLOM) card bay (x16 PCIe lane)
2	Two USB 3.0 ports
3,10	1-Gbps/10-Gbps **Management Port** (Network Adapter 3) • The primary instance (callout 3) is labelled 1 on the rear panel. • The secondary instance (callout 10) is the fourth port on the Intel X710-DA4 NIC in the appliance's PCIe riser 2/slot 2.
4,11	1-Gbps/10-Gbps Internet Port (Network Adapter 4) • The primary instance (callout 4) is labelled 2 on the rear panel. • The secondary instance (callout 11) is the third port on the Intel X710-DA4 NIC in the appliance's PCIe riser 2/slot 2.
5	VGA video port (DB-15).
6	1-Gbps **Cisco IMC** Port
7	Serial port (RJ-45 connector)
8	Rear unit identification button and LED
9	Power supplies (up to two: redundant as 1+1)
12,15	10-Gbps **Enterprise Port** (Network Adapter 1) • The primary instance (callout 15) is the left-hand port on the Intel X710-DA2 NIC in the appliance's PCIe riser 1/slot 1. • The secondary instance (callout 12) is the second port on the Intel X710-DA4 NIC in the appliance's PCIe riser 2/slot 2.
13,14	10-Gbps **Intra-Cluster Port** (Network Adapter 2) • The primary instance (callout 14) is the right-hand port on the Intel X710-DA2 NIC in the appliance PCIe riser 1/slot 1. • The secondary instance (callout 13) is first port on the Intel X710-DA4 NIC in the appliance's PCIe riser 2/slot 2.
16	Threaded holes for dual-hole grounding lug.

Tabla 7. Puertos de DNA Center

En nuestro proyecto, los puertos que van a ser conectados son:

- **Enterprise Port:** Dos puertos de fibra (12 y 15) conectados en modo LACP[(21)] a los switches del Data Center ubicados en Barcelona.
- **Intra-Cluster Port**: Un puerto de fibra (14) conectado al switch del Data Center ubicado en Barcelona.
- **Management Port**: Un puerto de cobre (3) conectado a un switch de OOB [(22)] en el Data Center ubicado en Barcelona.
- **CIMC** [(23)] **Port**: Un puerto de cobre (6) conectado a un switch de OOB en el Data Center de Barcelona.

Todos los puertos son conectados en modo acceso:

Port Name	Port	Port Type	IP & MASK	Connected to
Enterprise	Network Adapter 1 (15 and 12)	Fiber/10G	10.74.180.6/27 10.74.180.5	15: BARSWSAC001-T1/0/13 12: BARSWSAC001-T2/0/13
Intra-Cluster	Network Adapter 2 (14 and 13)	Fiber/10G	10.74.180.38/27 10.74.180.37	14: BARSWSAC001-T1/0/14 13: Not in use
Management	Network Adapter 3 (3 and 10)	Copper/1G/10G Fiber/1/10G	10.76.49.32/24 10.76.49.31	3: BARSWOAC001-G1/0/37 10: Not in use
Internet	Network Adapter 4 (4 and 11)	Copper/1G/10G Fiber/1/10G	N/A	4: Not in use 11: Not in use
CIMC	CIMC port (6)	Copper/1G	10.76.49.35/24	6: BARSWOAC001-G1/0/36

Tabla 8. Conexiones del DNAC a la infraestructura de red

La topología física de la conexión de nuestro DNA Center es la siguiente:

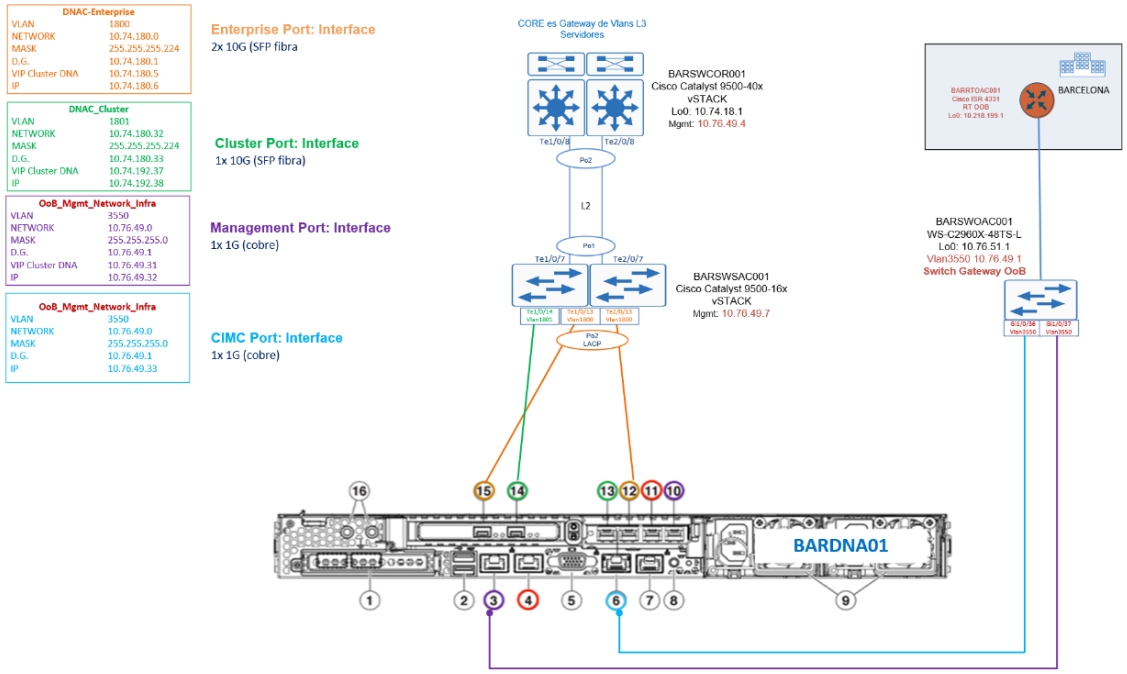

Imagen 31. Topología Física DNAC

Como el puerto Enterprise se usa para todas las comunicaciones requeridas por DNAC, se configura una ruta por defecto a través de esta interfaz. La puerta de enlace por defecto para DNAC será 10.74.180.1.

El puerto Cluster se configura en nivel 2, por lo que no requiere ninguna configuración de nivel 3 ni ruta alguna.

El puerto de Internet no lo usamos porque las comunicaciones con Internet se realizarán a través del proxy corporativo.

El puerto de Management se conecta a una red independiente del tráfico de producción, conocida como Out Of Band.

El puerto de la CIMC es el puerto de gestión remota, que al igual que con el puerto de Management lo vamos a conectar a la red OOB.

4.1.1 Modos de despliegue

El modo recomendado para desplegar un clúster DNA Center de 3 nodos se muestra en la siguiente figura. Todos los dispositivos DNAC deben estar ubicados en el mismo centro de datos y conectados de la siguiente forma:

- Cada dispositivo DNAC conecta todos sus enlaces primarios al mismo conmutador.

Esta topología proporciona los siguientes tipos de escenarios de fallo en los que el clúster seguirá operativo.

- Fallo de nodo único
- Fallo del enlace de red de la empresa para un único nodo
- Fallo del enlace del clúster para un único nodo
- Fallo del servicio para un único nodo
- Fallo del conmutador de red para un único nodo

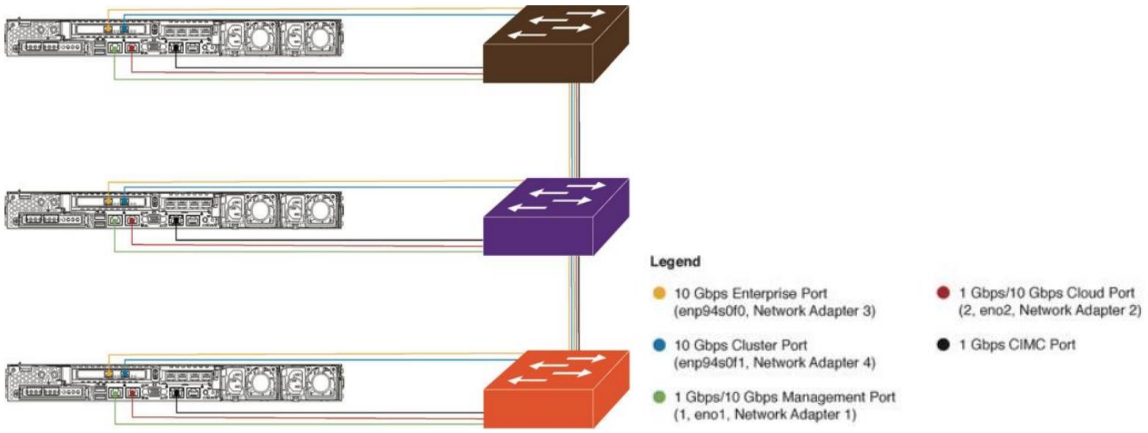

Imagen 32. DNA Center cluster deployment (single NIC)

En caso de habilitar la NIC [(24)] secundaria, los puertos de la NIC primaria se conectarán a un conmutador y los puertos de la NIC secundaria a otro conmutador, como se muestra en la figura siguiente.

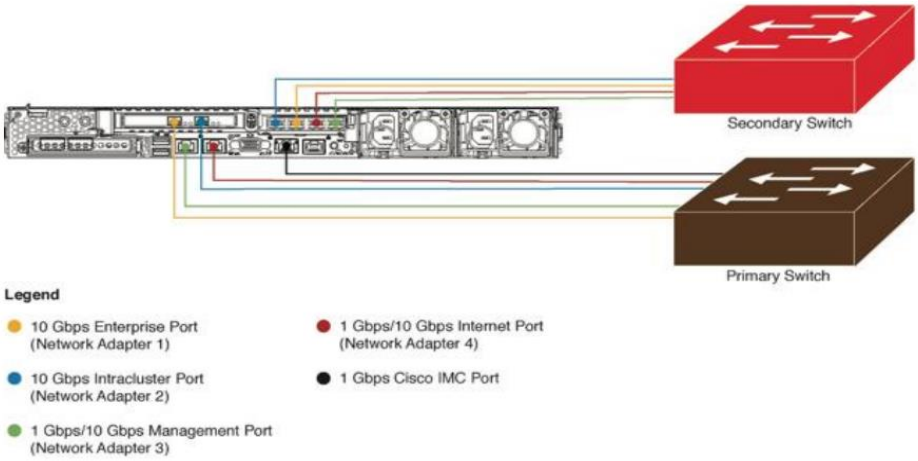

Imagen 33. DNA Center cluster deployment (dual NIC)

En nuestro proyecto desplegaremos un único DNAC. Sin embargo, en caso de que en algún momento sea necesario evolucionar a un cluster de 3 nodos, se deberán seguir las recomendaciones anteriores, y podríamos aplicar las siguientes configuraciones a los nuevos DNAC.

- Enterprise Port: 10.74.180.7 (node 2) and 10.74.180.8 (node 3)
- Intra-cluster Port: 10.74.180.39 (node 2) and 10.74.180.40 (node 3)
- Management Port: 10.76.49.33 (node 2) and 10.76.49.34 (node 3)
- CIMC Port: 10.76.49.36 (node 2) and 10.76.49.37 (node 3)

4.2 ISE

Como ya indicamos en el punto 3.8, nuestro NAC está formado por un deployment de máquinas virtuales, basadas en los modelos SNS-3655 ISE VM y SNS-3615 ISE VM.

El rendimiento, la estabilidad y la distribución de estos dispositivos en nuestra red, hace que sea uno de los servicios más resilientes y confiables de nuestra empresa.

Los requerimientos que debe cumplir la VM donde desplegamos la OVA del ISE se basan en el tamaño de la compañía.

OVA Template Type	Number of CPU Cores	CPU Reservation (in MHz)	Memory (in GB)	Memory Reservation (in GB)
SNS-3615 (Small)	16	16,000	32	32
SNS-3655 (Medium)	24	24,000	96	96
SNS-3695 (Large)	24	24,000	256	256

Imagen 34. Recursos de las VM para desplegar ISE

4.3 Wireless Lan Controller

El controlado inalámbrico (WLC) elegido es el modelo C9800-40-K9 que dispone de varios indicadores LED y puertos en el panel frontal.

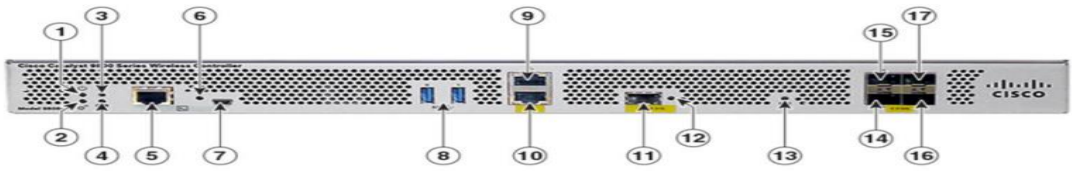

Imagen 35. Vista Frontal de C9800-40-K9

A continuación, vemos una pequeña descripción de cada uno de los puertos e indicadores de la imagen anterior:

Indicador	Descripción
1	PWR—Power LED
2	SYS—System LED
3	ALM—Alarm LED
4	HA—High-Availability LED
5	CON—RJ-45 compatible console port
6	EN—USB console-enabled LED
7	CON—Mini USB console port
8	USB ports 0 and 1
9	SP—RJ-45 10/100/1000 management Ethernet port
10	RP—RJ-45 10/100/1000 redundancy Ethernet port

11	RP—1-GE SFP port (The only supported SFPs on RP port are : GLC-SX-MMD and GLC-LH-SMD) LINK—RJ-45 connector LED
12	LINK—RJ-45 connector LED
13	SSD—SSD activity LED
14	TE0—1-GE SFP/ 10-GE SFP+ Port 0
15	TE1—1-GE SFP/ 10-GE SFP+ Port 1
16	TE2—1-GE SFP/ 10-GE SFP+ Port 2
17	TE3—1-GE SFP/ 10-GE SFP+ Port 3

Tabla 9. Puertos e Indicadores frontal C9800-40-K9

Imagen 36. Vista Trasera de C9800-40-K9

A continuación, vemos una pequeña descripción de cada uno de los puertos e indicadores de la imagen anterior:

Indicador	Descripción
1	Fans
2	Optional redundant Power supply (PEM 1)
3	Power supply (PEM 0)
4	Power/standby switch

Tabla 10. Puertos e Indicadores trasera C9800-40-K9

El chasis tiene un flujo de aire de adelante hacia atrás. Seis ventiladores internos introducen aire de refrigeración en el chasis y a través de componentes internos para mantener una temperatura de funcionamiento aceptable. Los ventiladores están numerados del 0 a 5, de derecha a izquierda.

Además de los puertos físicos, el Cisco 9800-40 WLC también tiene una interfaz lógica llamada Interfaz de Gestión Inalámbrica. Se utiliza para las comunicaciones del WLC con los puntos de acceso CAPWAP[(25)], para la gestión del WLC y para el descubrimiento y aprovisionamiento de Cisco DNA Center.

La denominación de los puertos del WLC es la siguiente:

- **Puerto de gestión WLC** - Interfaz de gestión inalámbrica (gestión de APs, reenvío de tráfico para conmutación central de SSIDs y gestión en banda).
- **Puerto de servicio WLC**: Gestión de dispositivos OOB de capa 3 (GUI, SSH)
- **Puerto de redundancia WLC**: Exclusivo para redundancia de conmutación por estados entre dos WLC.

Las conexiones que vamos a realizar en nuestro proyecto son las siguientes:

- Cada WLC conecta 2 puertos 10G a los switches Fusion en modo LAG.
- Los WLC se despliegan en modo HA-SSO
- No usaremos el puerto de servicio (dado que en Málaga no tenemos red de OOB, al menos de momento).
- El nivel 3 de los WLC son los equipos denominados Fusion
- El puerto RP se conectan directamente entre los WLC (aunque podrían conectarse a través de un switch intermedio)

Nota: *Los Fusion, aunque lo veremos en detalle en secciones posteriores, no es un componente del Fabric SDA.*

Los detalles de las conexiones son las siguientes:

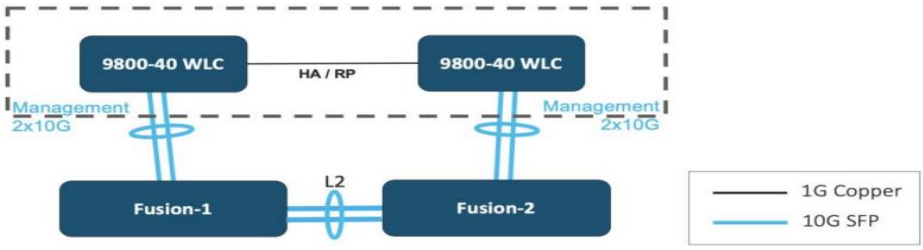

Imagen 37. Conexionado de los dos WLC (C9800-40-K9)

Cuando usamos LAG, es importante asegurarse de que todos los puertos del controlador tienen la misma configuración de Capa 2 y que coincide con la del switch al que conecta. Por ejemplo, evite filtrar algunas VLAN en un puerto y no en los demás.

Para un equilibrio de carga óptimo entre los puertos físicos del canal de puertos, utilice la opción src-dst-mixed-ip-port para equilibrar la carga.

```
¡
port-channel load-balance src-dst-mixed-ip-port
!
```

También es importante tener en cuenta que los WLC no soportan Jumbo Frames por lo que la MTU debe ser configurada a 1500.

4.4 Dispositivos de red

La nueva red SDA que vamos a desplegar también es una red de 3 capas en donde:

- Core = > Son los nodos de Border y Control Plane
- Distribución = > Son los nodos Intermedios
- Acceso = > Son los nodos Edge

La siguiente imagen muestra una topología a alto nivel del fabric SDA de nuestro proyecto:

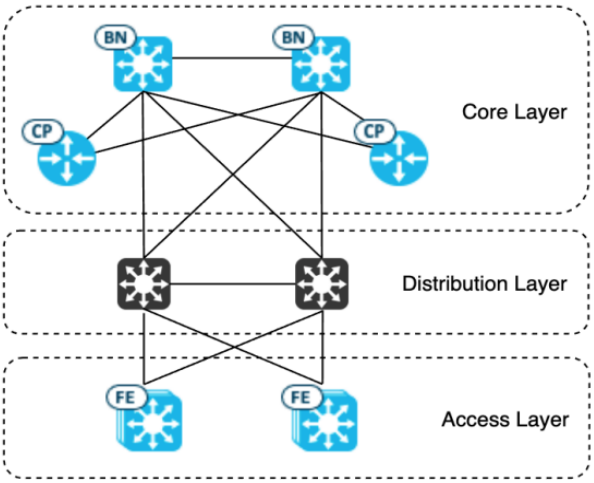

Imagen 38. Topología a alto nivel de SDA

Los nodos de Border se van a desplegar como switches standalone, estableciendo una conexión 10/25G entre ellos. Y una conexión 1G con los dos nodos del Plano de Control.

Los nodos intermedios también serán desplegados en modo standalone, estableciendo una conexión 10/25G entre ellos. Y se conectan a ambos Border con enlaces de 40G.

Los nodos Edge serán todos desplegados en modo stacking, y se conectan a los nodos intermedios mediante enlaces de 25G en el caso de los switches de acceso usuarios, activando un uplink en cada uno de los switches del stack (interfaces Twe1/1/1 & Twe2/1/1)

Existe un uplink activo Y mediante enlaces de 10G en el caso de los switches de acceso servidores ubicados en el Data Center.

Mostramos un HLD de estas conexiones:

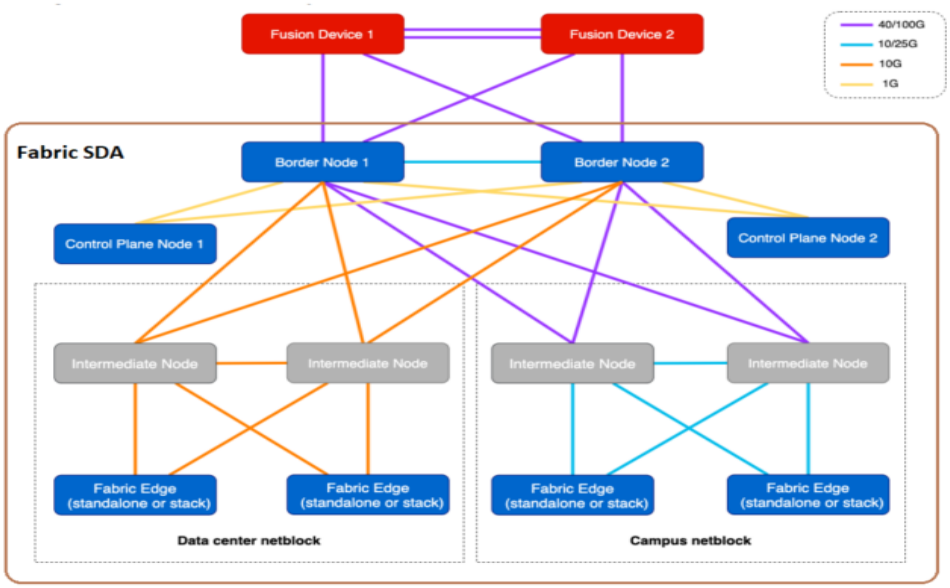

Imagen 39. HLD de Conexionado

En la imagen anterior mostramos las dos opciones en las que pueden desplegarse los Fabric Edge (standlone o stacking), sabiendo que en nuestro caso, tanto en los CT (acceso usuarios) como en el CPD (acceso servidores), se van a desplegar en modo stack.

Otro punto importante, es resaltar que el Fabric SDA va desde la capa de los Fabric Edge a la capa de los Border, siendo los elementos en rojo (Fusion) el equipamiento que va a permitir la comunicación entre los diferentes dominios (Virtual Network) del Fabric SDA en lo que conocemos como comunicación Este-Oeste, y entre el Fabric SDA y el resto de la red de la empresa, también conocido como comunicación Norte-Sur.

Aunque no lo hemos contemplado en el BoM del proyecto, al ser un equipamiento ya existente en nuestra empresa, los Fusion son una pareja de C9500 (mismo modelo que los Border Node).

En la siguiente imagen vemos una topología física completa del conexionado de todos los componentes del Fabric SDA, y del resto de dispositivos de red de la sede de Málaga.

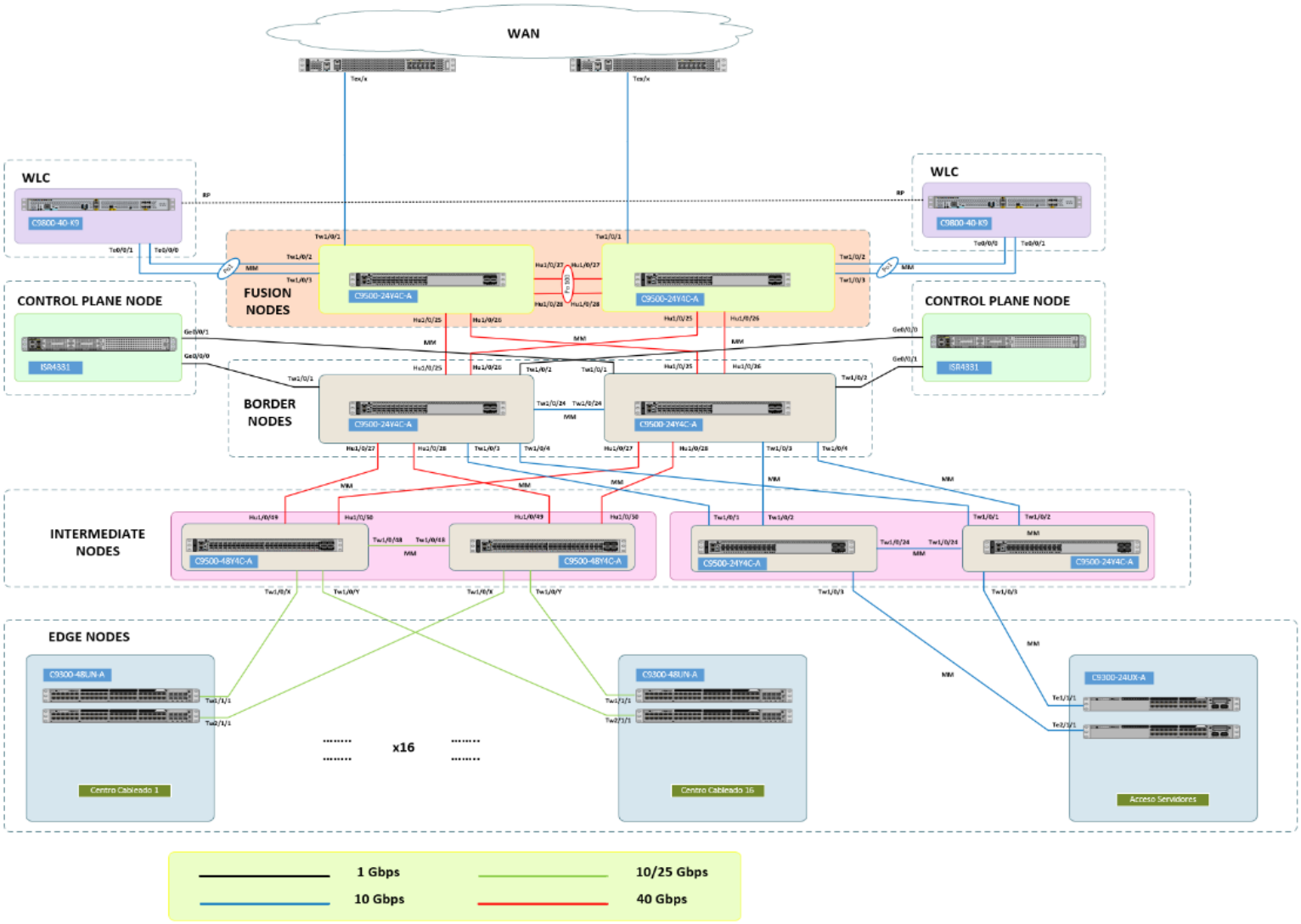

Imagen 40. LLD de Conexionado

5. Diseño y despliegue del Underlay

5.1 Visión general

La alta disponibilidad en la red de underlay se proporciona mediante enlaces duales de igual coste desde la capa de acceso hacia arriba. Esto permite una convergencia rápida y determinista en caso de fallo de un enlace o de un nodo monitorizado mediante BFD. Cuando disponemos de rutas redundantes, la conmutación por error depende principalmente de la detección de fallos de enlace, siendo este inferior al segundo. Hemos implementado un protocolo de enrutamiento de capa 3 punto-to-punto entre la capa de acceso y el resto de las capas.

Nota: *Todo el tráfico en SDA se enruta en la capa de acceso incluyendo las tramas de capa 2.*

En un diseño jerárquico, la capacidad, características y funcionalidad de un dispositivo específico se optimizan para su posición en la red y el papel que desempeña. Esto promueve la escalabilidad y la estabilidad. El número de flujos y sus requisitos de ancho de banda asociados aumentan a medida que atraviesan puntos de agregación y suben en la jerarquía desde el acceso a la distribución y al núcleo. Las funciones se distribuyen en cada capa. Un diseño jerárquico evita la necesidad de una red totalmente en malla en la que todos los nodos de la red están interconectados.

En una implementación de SDA, todos los enlaces del underlay se configuran con direcciones IP de capa 3. La red de underlay siempre funcionará en la Tabla de Enrutamiento Global (GRT) en todos los dispositivos. Sin embargo, la red del underlay también se extiende a través de los dispositivos Fusion y más allá para que haya conectividad entre los dispositivos de red (switches, enrutadores, puntos de acceso) y las redes externas (por ejemplo, DC, Internet, WAN).

La consideración clave para el Fabric SDA es que la red de underlay debe ser de alta velocidad, baja latencia (menos de 10 ms como guía general) y debe acomodar la configuración MTU utilizada para SDA en la red del campus (9100 bytes). El encabezado VXLAN agrega 50 bytes de sobrecarga de encapsulamiento. Los paquetes VXLAN se habilitan con el bit No Fragmentar (DF). Por lo tanto, si hay un dispositivo en el camino que ejecuta un MTU de 1500 bytes, descartará estos paquetes.

Algunos switches Ethernet admiten un MTU máximo de 9216 mientras que otros pueden tener un MTU de 9196 o menor. Dado que los MTU del servidor suelen ser de hasta 9000 bytes, habilitar un MTU de 9100 en toda la red garantiza que los marcos jumbo de Ethernet se puedan transportar sin fragmentación dentro y fuera del fabric.

Nota: *También se configurará un MTU jumbo (9100) en los switches Fusion, ya que a futuro transportarán SGT entre el Fabric SDA y los routers SDWAN, que serán el evolutivo de este proyecto y que se encuentra fuera del mismo*.

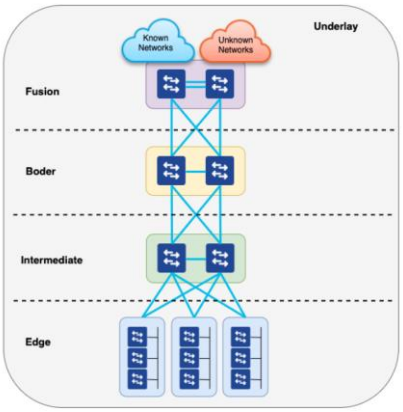

Imagen 41. Despliegue Underlay

El underlay está definido por los switches físicos que interconectan los dispositivos del fabric SDA. Todos los elementos de red que corran sobre el underlay deben establecer conectividad IP y ejecutar protocolos de enrutamiento dinámico.

- Una solución de acceso enrutado L3
- Eliminamos el uso de protocolos STP[26] y FHRP [27]
- Desplegamos múltiples rutas de igual coste (ECMP) [28] usando todos los enlaces disponibles.

5.2 Routing

Usaremos las siguientes características:

- IS-IS [29] como protocolo de enrutamiento dentro del Fabric SDA (Se habiloita enlaces point-to-point y interface Loopback 0)
- PIM ASM [30] permitirá usar L2 Flooding en el overlay si así se requiere.
- PIM SSM [31] permitirá usar Multicast de modo nativo en el overlay si así se requiere.
- BFD [32] como mecanismo de detección de fallo primario.
- Puertos trunk (802.1Q) desde los dispositivos de Border con los Fusion.

El protocolo de enrutamiento Integrated Intermediate System-to-Intermediate System (IS-IS) es un Protocolo de Gateway Interior (IGP) de estado de enlace. Los protocolos de estado de enlace se caracterizan por la propagación de la información necesaria para construir un mapa completo de conectividad de red en cada dispositivo participante. Ese mapa se utiliza luego para calcular la ruta más corta a los destinos. Los flujos de tráfico se pueden personalizar cambiando el costo métrico para una interfaz especificada.

La tecnología principal utilizada para el plano de control del Fabric SDA está basada en el Protocolo de Separación de Localizador/Identificación (LISP). LISP es un protocolo estándar del IETF [33] basado en un sistema de mapeo simple de Identificador de Extremo (EID) a Localizador de Enrutamiento (RLOC), para separar la "identidad" (dirección) de su "ubicación" actual (router adjunto). Esta tecnología proporciona muchas ventajas para SD-Access, como un menor uso de la CPU, tablas de enrutamiento más pequeñas (hardware y/o software), movilidad de host dinámica (con cable e inalámbrica), mapeo sin dirección (IPv4, IPv6 y/o MAC), segmentación de red integrada (VRF) y otras.

La siguiente figura muestra el enrutamiento ISIS en el Fabric SDA. Los nodos de Border y los Edge siempre deben anunciar sus interfaces Loopback0 en ISIS para cumplir con los requisitos de LISP. Los nodos intermedios realmente no necesitan anunciarlos a menos que también estén habilitados como nodos de borde. Sin embargo, estas interfaces Loopback0 también serán anunciadas por estos nodos para que DNAC pueda administrarlas utilizando esa Loopback0.

Los nodos de Border también anuncian dos rutas más:

- Una ruta predeterminada (default) para que el resto de switches puedan alcanzar cualquier servicio que se encuentre fuera del Fabric SDA (NTP [34], DNAC, ISE, DHCP, DNS, etc).
- La ruta por defecto anterior, no puede ser utilizada por los puntos de acceso para alcanzar a los WLC; por ello, se necesita una ruta especifica del WLC hacía el Fabric SDA.

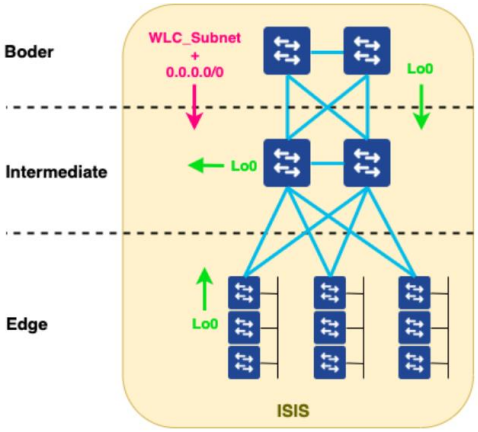

Imagen 42. Routing ISIS

Al ejecutar la automatización LAN de DNAC, la mayoría de las configuraciones de ISIS se empujarán automáticamente. Sin embargo, hay algunas configuraciones que deben hacerse manualmente en los BN (ya sea usando la CLI [35] del BN o el editor de plantillas de DNAC).

La automatización LAN siempre empuja la configuración para anunciar incondicionalmente una ruta predeterminada en los dispositivos semilla (por ejemplo, BN) en el proceso de ISIS. En este punto de la implementación, no hay configuraciones de tejido sino solo de underlay. Por lo tanto, no hay peering eBGP [19] entre BN y los dispositivos Fusion y la ruta predeterminada no es recibida por ningún dispositivo externo. Para evitar agujeros negros en ISIS, se debe configurar la publicación condicional de la ruta predeterminada como se muestra en el código a continuación.

```
! Border Nodes

ip prefix-list DEFAULT permit 0.0.0.0/0

ip access-list standard EBGP_NEXT_HOP
remark [FUSION_SWITCH_1]
permit [FUSION_SWITCH_1_UNDERLAY_IP] 0.0.0.0
remark [FUSION_SWITCH_2]
permit [FUSION_SWITCH_2_UNDERLAY_IP] 0.0.0.0

route-map DEFAULT permit 10
match ip address prefix-list DEFAULT
match ip next-hop EBGP_NEXT_HOP

router isis
default-information originate route-map DEFAULT
!
```

La publicación de la subred WLC en ISIS tampoco está configurada por la función de automatización LAN de DNAC. Por lo tanto, debe configurarse manualmente (ya sea mediante la CLI del BN o el editor de plantillas de DNAC), como se muestra en el siguiente código:

```
!Border Nodes

ip prefix-list WLC permit [WLC_SUBNET]/[MASK]

route-map BGP_TO_ISIS permit 10
match ip address prefix-list WLC

router isis
redistribute bgp [BGP_ASN] ip route-map BGP_TO_ISIS metric-type external
!
```

5.3 Lan Automation

La función de Automatización LAN de DNA Center es una alternativa a las implementaciones manuales de la capa de infraestructura (underlay) para nuevas redes.

Los switches de la LAN pueden ser desplegados sin configuraciones previas en la capa de infraestructura mediante el uso de las capacidades de Automatización LAN de DNA Center. El mecanismo que permite la conectividad y la configuración inicial de los switches compatibles es el Cisco Network Plug and Play (PnP). Para los despliegues de Automatización LAN, se pueden suministrar las credenciales de CLI y SNMP para acceder y preparar uno o más dispositivos semillas compatibles con PnP.

La Automatización LAN descubre los switches conectados directamente a las interfaces del dispositivo semilla elegido y sus switches vecinos inmediatos utilizando el Cisco Discovery Protocol (CDP), todos los cuales deben estar ejecutando el agente PnP y no tener una configuración previa hasta un máximo de dos saltos de distancia. Las credenciales suministradas permiten que DNA Center y los dispositivos semilla trabajen juntos para configurar los dispositivos descubiertos y agregarlos a un inventario administrado.

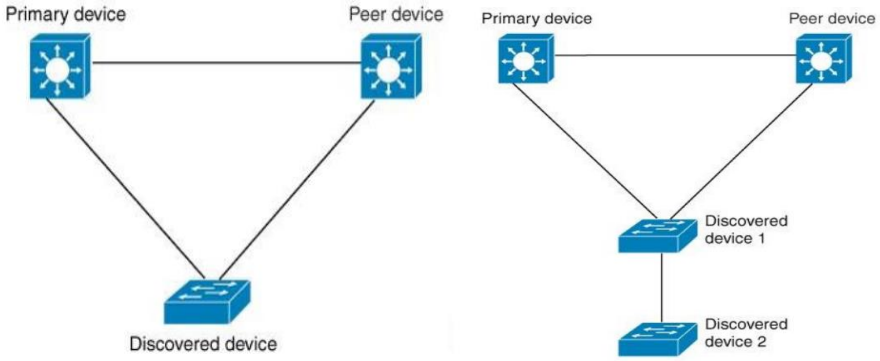

Imagen 43. Descubrimiento PnP

DNA Center configura un servidor DHCP en el dispositivo primario. Debido a que DNA Center entiende que el dispositivo descubierto está conectado tanto al dispositivo primario como al dispositivo secundario, configura dos conexiones punto a punto de capa 3 cuando se detiene la tarea de automatización de LAN. Se establece una conexión entre el dispositivo descubierto y el dispositivo primario; la otra conexión se establece entre el dispositivo descubierto y el dispositivo secundario.

Usando la automatización LAN, una vez que el dispositivo es descubierto por DNAC, se empujarán las siguientes configuraciones:

- Jumbo MTU (9100)
- Habilitar routing multicast (opción de habilitarlo o no)
- Se configura el direccionamiento IP de las Loopback 0
- Proceso de enrutamiento ISIS
- BFD en los enlaces del underlay
- Se habilita SSH, SNMP o SCP

Además, al final del proceso de automatización LAN, DNAC puede instalar la versión de software objetivo para el dispositivo descubierto, y seleccionada como favorita.

En la instalación inicial, se puede instalar una ruta estática en los switches Fusion para proporcionar conectividad entre DNAC y los dispositivos descubiertos por LAN Automation. Sin embargo, una vez que el Fabric SDA es desplegado y se ejecuta la transición de L3 en los Border Nodes, esa ruta estática debe ser reemplazada por enrutamiento dinámico (BGP). La siguiente plantilla debe ser aplicada en los Border Nodes una vez que se complete la transición de L3.

La automatización LAN descubre tanto switches en stack como independientes (standalone). Al descubrir switches apilados, se deben tomar en cuenta las siguientes consideraciones:

- La automatización LAN siempre se inicia en el switch activo. Iniciar LAN auto antes de que el stack esté completamente configurado puede causar problemas.
- Para formar un stack de switches antes del descubrimiento de la automatización LAN, se deben seguir los siguientes pasos:
    - Encienda el switch 1 y espere 120 segundos. Esto asegurará que se convierta en el switch activo dentro del stack.
    - Encienda el switch 2 y espere 120 segundos. Esto asegurará que se convierta en el switch en espera dentro del stack.
    - Una vez formado el stack de switches, iniciamos la automatización LAN y lo descubrimos.
    - Más tarde, durante el aprovisionamiento del switch, se empujará una plantilla personalizada (ver código a continuación) para establecer las prioridades del switch de manera que los switches siempre se inicien en las mismas prioridades (switch 1 siempre será el principal y el switch 2 el de reserva).

5.3.1 Dispositivo semilla

Los dispositivos semilla suelen ser los nodos de borde en una implementación SDA. Sin embargo, puede haber situaciones en las que sea necesario volver a ejecutar la automatización de LAN utilizando dispositivos semilla diferentes. Por ejemplo, cuando un nodo intermedio fue descubierto por primera vez por la automatización de LAN pero después de algún tiempo, se conectan nuevos switches Edge a ese nodo intermedio. En esta situación, puede ser necesario ejecutar la Automatización de LAN utilizando el nodo intermedio como dispositivo semilla en lugar de los nodos de borde.

En caso de ejecutar la automatización de LAN desde nodos intermedios (dispositivos semilla), tenga en cuenta que DNAC puede realizar un push de la ruta predeterminada/ default en ISIS. Si ese es el caso, esa ruta por defecto debe eliminarse. Como DNAC puede volver a enviar la misma configuración, se recomienda eliminar ese anuncio utilizando un mapa de ruta inexistente según el siguiente código. Incluso si DNAC vuelve a enviar "default-information originate", el route-map evitará que el switch anuncie la ruta predeterminada.

```
! Intermediate Nodes used as seed devices in LAN Automation
 ! DO_NOT_ADVERTISE_DEFAULT_ROUTE route-map does not exist in configuration

router isis
default-information originate route-map DO_NOT_ADVERTISE_DEFAULT_ROUTE
!
```

5.3.2 Descubrimiento de la red

Debemos utilizar la Automatización de LAN siempre que sea posible y configuraciones manuales del underlay cuando la automatización no sea posible (por ejemplo, un switch de borde que no se

puede conectar a su switch ascendente, o cuando hay plataformas de enrutamiento como nodos WLC, BN o CP, ya que no admiten la Automatización de LAN). El código a continuación enumera las configuraciones mínimas a instalar en los nodos de plano de control (routers) antes de que sean descubiertos por DNAC. Hay que tener en cuenta que algunas otras características (SNMP [(36)], Syslog, NTP, etc.) se configurarán automáticamente una vez que el switch sea descubierto y aprovisionado por DNAC.

```
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
!
service password-encryption
service sequence-numbers
!
hostname [HOSTNAME]
!
no ip domain lookup
ip domain name [DOMAIN]
!
 ip ssh version 2
ip scp server enable
!
 line vty 0 15
login local
transport input ssh
transport preferred none
!
interface loopback 0
description Fabric Node Router ID
ip address [Lo0_IP] 255.255.255.255
ip router isis
!
interface GigabitEthernet[UPLINK_1]
description Fabric Physical Link – TO BORDER1
ip address [IP_UPLINK_1] 255.255.255.254
ip router isis bfd interval 250 min_rx 250 multiplier 3
isis network point-to-point
no cts role-based enforcement
no shutdown
!
interface GigabitEthernet[UPLINK_2]
description Fabric Physical Link - TO BORDER2
ip address [IP_UPLINK_2] 255.255.255.254
ip router isis bfd interval 250 min_rx 250 multiplier 3
isis network point-to-point
no cts role-based enforcement
no shutdown
!
router isis net 49.0000.[Lo0_IP_ENCODED].00
domain-password [ISIS-PASSWORD]
ispf level-1-2 metric-style wide
nsf ietf
log-adjacency-changes
bfd all-interfaces ! username [LOCAL_USER] privilege 15 secret [PASSWORD]
!
enable password [PASSWORD]
ip domain name QUARTZ.com
!
crypto key generate rsa modulus 2048
!
netconf-yang
```

De manera similar, el código que se muestra a continuación enumera las configuraciones mínimas que se deben instalar en los controladores de LAN inalámbrica (WLC) antes de que sean descubiertos por DNAC. Tenga en cuenta que algunas otras funciones (SNMP, Syslog, NTP, ...) se configurarán automáticamente una vez que el WLC sea descubierto y aprovisionado por DNAC.

```
% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]: no
Would you like to terminate autoinstall? [yes]: yes
!
hostname [HOSTNAME]
!
interface GigabitEthernet0
ip address [SP_IP] [SP_MASK]
!
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 [SP_GW]
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
!
line vty 0 15
login local
transport input all
!
ip domain name [DOMAIN]
no ip domain lookup
!
vlan [VLAN_ID]
name [WLC_VLAN_NAME]
!
interface Vlan[VLAN_ID]
ip address [IP_MGMT] 255.255.255.240
no shutdown
!
ip route 0.0.0.0 0.0.0.0 [DEF_GW] name DEFAULT
!
interface TenGigabitEthernet0/0/0
switchport
channel-group 1 mode active
no shutdown
!
interface TenGigabitEthernet0/0/1
switchport
channel-group 1 mode active
no shutdown
!
port-channel load-balance src-dst-mixed-ip-port
!
interface Port-channel1
switchport
switchport mode trunk
switchport trunk allowed vlan [VLAN_ID]
!
ap dot11 5ghz shutdown
yes
!
ap dot11 24ghz shutdown
yes
!
ap country ES
```

```
wireless country ES
!
no ap dot11 5ghz shutdown
no ap dot11 24ghz shutdown
!
wireless management interface vlan [VLAN_ID]
!
ap dot11 24ghz cleanair
ap dot11 5ghz cleanair
no ap dot11 5ghz SI
i
ip http server
ip http authentication local
ip http secure-server
!
ip parameter-map type webauth global
 ip virtual-ip ipv4 [VIRTUAL_IP]
!
netconf-yang
!
username [LOCAL_USER] privilege 15 secret [PASSWORD]
enable secret [ENABLE_PASSWORD]
!
ip domain name RG.REPSOL.COM
!
crypto key generate rsa modulus 2048
ip ssh version 2
i
```

5.4 Multicast

Existen dos casos de uso para habilitar el uso de Multicast en el underlay:

1. **Habilitar la función L2 Flooding en cualquier pool IP del overlay**

El L2 flooding requiere la configuración del multicast PIM ASM en el underlay. Los RPs suelen ser los nodos Border del Fabric SDA. Si se usa la automatización LAN, entonces la configuración necesaria en el underlay se realiza automáticamente por DNAC. Si se usan configuraciones manuales en el underlay, entonces también se deben incluir las configuraciones de multicast.

2. **Habilitar routing multicast en el overlay**

Para entregar el multicast eficientemente en el overlay; el underlay debe estar habilitado para multicast.

6. Diseño y despliegue del Overlay

6.1 Jerarquía de red

La Jerarquía de Red usualmente representa las ubicaciones geográficas de la red, pero puede ser creada en base a los requerimientos del negocio. Una jerarquía de red puede contener áreas, edificios y pisos. Estas se utilizan para identificar dónde aplicar las configuraciones o ajustes de diseño más tarde. Por defecto, hay una área llamada Global.

Nota: *Nuestro modelo de DNAC tiene una limitación de 1000 campos dentro de toda la jerarquía*

La siguiente tabla muestra la jerarquía de red aplicada a nuestro proyecto (la sede de málaga formada por 4 edificios de dos plantas cada uno):

Name Object	Parent Object	Type Object
EMEA	Global	Area
ES_SPAIN	EMEA	Area
ESMAL	ES_SPAIN	Area
ED_1	ESMAL	Building
PLANTA_B	ED_1	Floor
PLANTA_1	ED_1	Floor
ED_2	ESMAL	Building
PLANTA_B	ED_2	Floor
PLANTA_1	ED_2	Floor
ED_3	ESMAL	Building
PLANTA_B	ED_3	Floor
PLANTA_1	ED_3	Floor
ED_4	ESMAL	Building
PLANTA_B	ED_4	Floor
PLANTA_1	ED_4	Floor

Tabla 11. Jerarquía en DNAC

Cada nivel en la tabla anterior cuenta en contra del máximo de elementos soportados en DNAC, en este caso, el número de elementos utilizados son: Global, EMEA, ES_Spain, ESMAL, la suma de todos los edificios y todos los pisos, lo que resulta en 16 (de un total de 1.000 para nuestro modelo de DNA).

6.2 Wireless

SD-Access Wireless se define como la integración de acceso inalámbrico en la arquitectura SD-Access para obtener todas las ventajas de la automatización de Fabric y DNA Center. Algunos de estos beneficios son:

- Plano de control inalámbrico centralizado: se aprovecharán las mismas características innovadoras de RF[37] que Cisco tiene hoy en las implementaciones de Cisco Unified Wireless Network (CUWN) en SD-Access Wireless.

- Plano de datos distribuido optimizado: el plano de datos se distribuye en los switches Edge para un rendimiento y escalabilidad óptimos sin los problemas asociados normalmente con la distribución de tráfico (subnetting [20], grandes dominios de difusión, etc.).

- Roaming L2 transparente en todas partes: Fabric de SD-Access permite que los clientes se muevan sin problemas por todo el campus mientras mantienen la misma dirección IP.

- Simplificación del túnel de invitados y de movilidad: ya no se necesita un controlador WLC con el role de anchor, y el tráfico de invitados puede ir directamente a la DMZ [38] [21] sin pasar por un controlador extranjero.

- Simplificación de políticas: SD-Access rompe las dependencias entre políticas y construcciones de red (direcciones IP y VLAN), lo que simplifica la forma en que podemos definir e implementar políticas para clientes cableados e inalámbricos.

- Segmentación fácil: la segmentación se lleva a cabo de extremo a extremo en la Fabric y es jerárquica, basada en redes virtuales (VNIs) y etiquetas de grupo escalables (SGT). La misma política de segmentación se aplica a usuarios cableados e inalámbricos.

Estos beneficios solo se aplican a las redes inalámbricas habilitadas para SD-Access Fabric (FEW[39] [22]). Las redes inalámbricas Over The Top (OTT) no son manejadas por el fabric y, por lo tanto, no recibirán estos beneficios.

La arquitectura inalámbrica de SD-Access es compatible con los siguientes controladores de LAN inalámbrica:

- AIR-CT8540/AIR-CT5520 con AireOS versión 8.5 o superior
- Catalyst 9800 que ejecuta IOS-XE 16.10 o superior

Existen 3 modos de despliegue:

1. **Fabric Edge Wireless**

La parte de control en el WLC y la parte de datos con VXLAN en los Fabric Edge. Trabajas con SGTs y dispones de las ventajas de SDA.

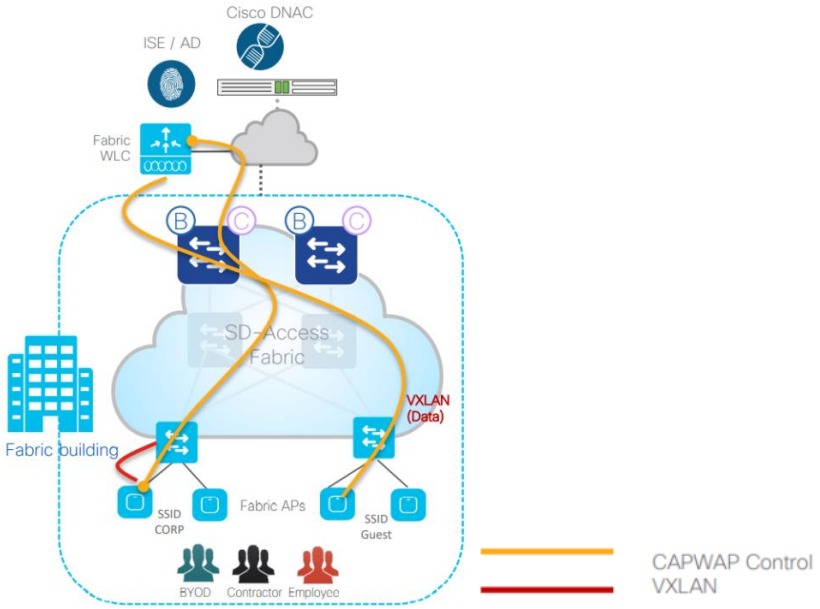

Imagen 44. Fabric Edge Wireless

El controlador inalámbrico en modo Fabric, gestiona y controla los AP en modo fabric del mismo modo que los controladores centralizados tradicionales en modo local, ofreciendo las mismas ventajas operativas. La diferencia clave entre el WLC tradicional y el de modo fabric es la forma en que se gestiona el tráfico inalámbrico de punto final.

En los despliegues en modo centralizado tradicional, tanto el tráfico de control como el de usuario se canalizan a través de Control and Provisioning of Wireless Access Points (CAPWAP) hasta el WLC. En el WLC, el tráfico de usuario se divide a través de una interfaz dinámica específica para un identificador de conjunto de servicios (SSID).

En los despliegues SDA, el tráfico de control sigue canalizándose al WLC a través de CAPWAP, pero el tráfico de usuario final se divide localmente en el AP y se reenvía al Fabric Edge a través de VXLAN.

El nodo fabric edge enruta el tráfico de extremo inalámbrico de la misma forma que se enruta el tráfico de extremo cableado.

Nota: *Este es el modo de despliegue de nuestro proyecto.*

2. OTT (WLC fuera del Fabric SDA)

Plano de control y de datos en el WLC. Sin SGTs y sin aprovechar las ventajas de SDA.
El Fabric sólo sirve como transporte para el tráfico de control y datos entre los APs y el WLC.

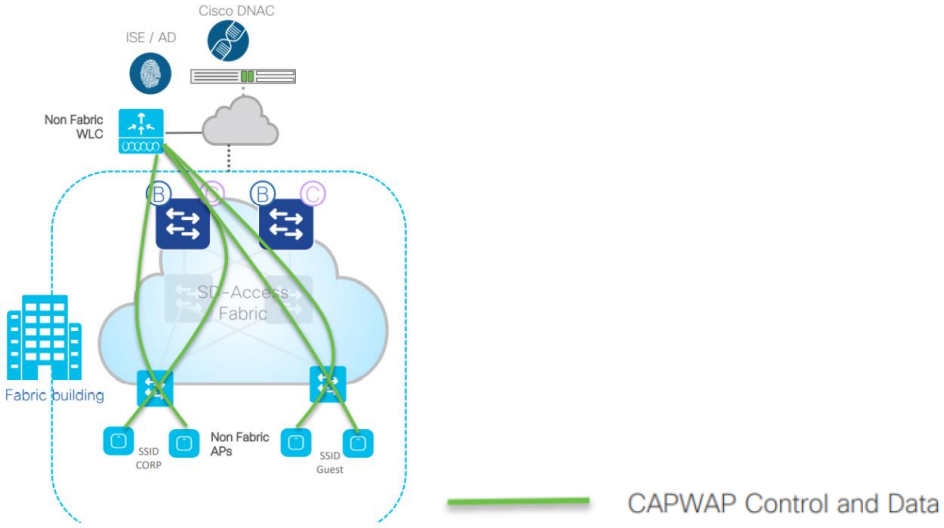

Imagen 45. Over The Top WLC

3. Modo mixto

Si tiene el hardware y software inalámbrico más reciente de Cisco, puede combinar redes inalámbricas con y sin fabric en la misma red administrada por Cisco DNA Center, habilitando o deshabilitando el modo de fabric por SSID [(40)] [41] . Para SSID sin fabric, el tráfico de datos del cliente se encapsula en CAPWAP y se envía al WLC sobre la fabric. Para SSID con fabric, el tráfico de datos del cliente se encapsula en VXLAN [42] y se reenvía en la fabric. La implementación actual de Cisco SD-Access incluso admite implementaciones inalámbricas de campo existentes (brownfield), donde Cisco DNA Center aprende y guarda la configuración existente después de descubrir el WLC en la red.

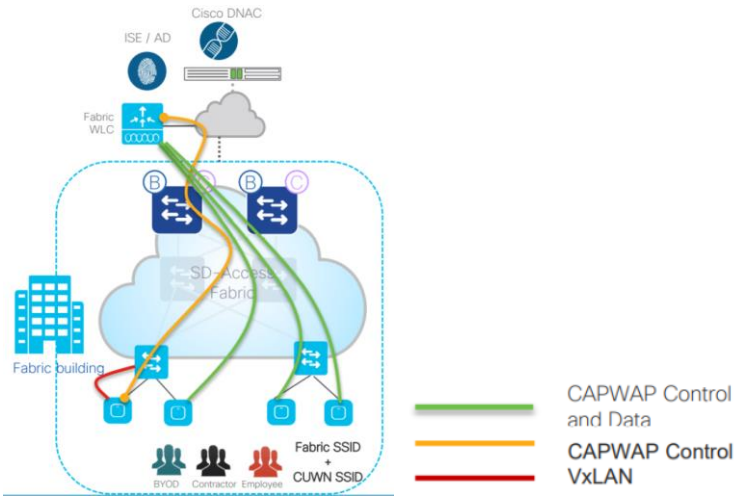

Imagen 46. Modo Mixto WLC

El WLC es descubierto y provisionado por Cisco DNA Center antes de ser agregado a la fabric. Después de la integración en la fabric, el WLC interactúa con la base de datos de seguimiento del host del plano de control (HTDB) para registrar la dirección MAC del cliente con la información de SGT y la red virtual (VN). Luego, la información de VN se asigna a una VLAN en los switches Edge del Fabric.

En caso de que un cliente realice una itinerancia, el WLC actualiza la HTDB (41) con la información de roaming específica del cliente.

Los WLC serán implementados en modo Standalone y descubiertos en DNA Center como WLC independientes. La configuración de HA-SSO (42) se automatiza desde DNAC. Una vez que se ejecutan como un par de nodos en HA (43), se verán en DNA Center como una única dirección IP. Esto significa que solo se verá un único WLC en DNA Center, pero en realidad, los WLC son dos nodos funcionando en HA.

Para la solución inalámbrica de SD-Access, los componentes más críticos son el WLC y el nodo del plano de control. En comparación con los clientes del Fabric cableados, el CP (Control Plane Node) desempeña un papel crítico para el roaming del cliente inalámbrico, ya que es responsable de mantener la información de ubicación del cliente dentro del Fabric.

Cuando tenemos Wireless Lan Controller en HA-SSO:

- Solo el WLC activo interactúa con el nodo CP
- La configuración del fabric y el estado CP se sincronizan entre el WLC activo y el de espera
- En caso de fallo, los AP y clientes permanecen conectados
- El nuevo WLC activo actualizará en bloque los clientes de la fabric en el nodo HTDB (actualización LISP)

Los Access Point estarán conectados a los switches Edge. Todos los puntos de acceso formarán parte del Fabric SDA y se configurarán en modo loca. Utilizando el Fabric como transporte, cada AP construye un túnel de control CAPWAP con el WLC para fines de control y gestión.

En nuestro modo de despliegue WiFi, en los WLANs que creemos en el Fabric, el plano de datos del usuario se distribuye con los APs aprovechando VXLAN como método de encapsulamiento. El AP convierte el tráfico 802.11 a 802.3, encapsulando el tráfico de datos del cliente en VXLAN, codificando la información VNID (44) y SGT del cliente en el encabezado VXLAN y lo envía al switch Edge al que está conectado.

Al igual que para los usuarios cableados, las políticas basadas en SGT y VRF (VNID o Virtual Network) para los usuarios inalámbricos en SSIDs del Fabric, se aplican en el switch Edge.

Aunque la energía eléctrica para cada AP de Cisco puede ser suministrada a través de cualquiera de las siguientes fuentes:

- Switches con 802.3at (PoE+) que proporcionan hasta 30W
- Switches con 802.3bt (uPoE) que proporcionan hasta 60W
- Switches con 802.3bt (uPoE+) que proporcionan hasta 90W
- Cisco Power Injector PWRINJ6

Los puntos de acceso inalámbricos se conectarán a los nodos Edge a través de puertos mGig[43] proporcionando la alimentación a través del estándar uPoE[44].

Durante la instalación y cableado de los APs, los APs deben ser conectados siempre que sea posible de tal manera que cuando ocurra una falla del switch, el impacto en la disponibilidad de RF se minimice o se elimine por completo. Por lo tanto, se recomienda encarecidamente conectar APs vecinos a diferentes switches de manera alternada, como se muestra en la siguiente figura.

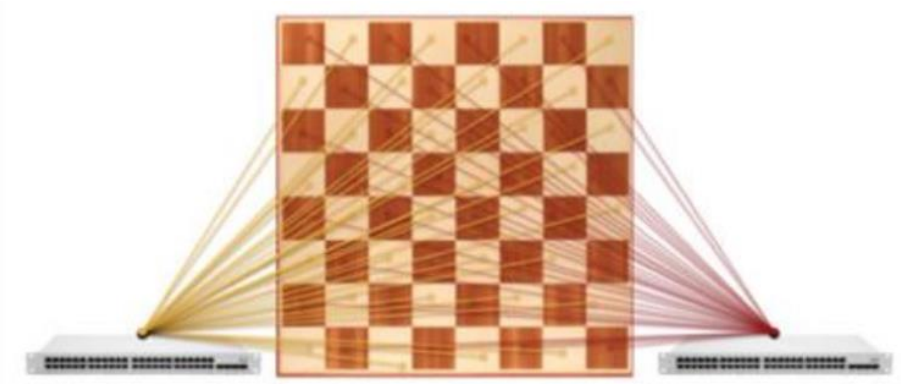

Imagen 47. Conectividad Salt-and-Pepper

Los puntos de acceso descubrirán el WLC usando la opción 43 de DHCP.

Queremos mejorar la experiencia de usuario y aumentar la eficiencia operativa de sus departamentos proporcionando acceso inalámbrico a los servicios de intranet e internet a los empleados. Todas los SSID/ WLANs estarán habilitados para SDA como ya hemos comentado y, dependiendo del caso de uso, formarán parte de diferentes VRF con acceso a todos los servicios de intranet y/o internet. Nuestra compañía admitirá dispositivos gestionados y no gestionados (que no están en el dominio) utilizando diferentes mecanismos de autenticación basados en la política de usuario.

Se explicará más información sobre los WLAN que vamos a desplegar y los detalles de autenticación más adelante dentro de esta misma sección. Para las SSID de 802.1x, cada tipo de dispositivo/usuario podrá acceder a recursos específicos según sus credenciales y grupo AD/base de datos interna de ISE. Se requerirá que los dispositivos realicen la autenticación 802.1x a través de ISE. ISE ya está integrado con los servicios de Active Directory (AD) para autenticar y autorizar dispositivos. Según la información del grupo de usuarios en Active Directory, ISE autenticará y colocará los dispositivos corporativos en el grupo IP y SGT de clientes correctos.

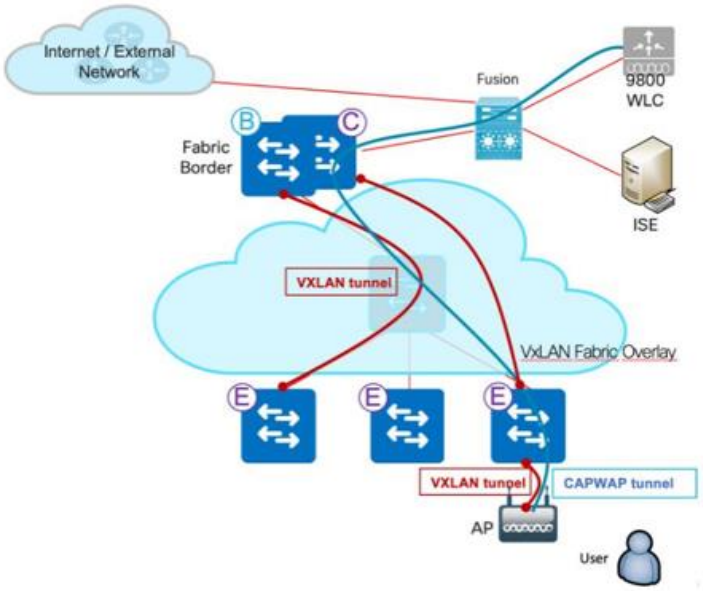

Imagen 48. Fabric WLAN with 802.1x

A continuación, mostramos el proceso paso a paso de cómo los usuarios y los endpoints se conectan a la LAN inalámbrica mediante 802.1x:

- El usuario se conecta al SSID.
- El SSID será un SSID habilitado en el Fabric SDA (fabric enabled SSID) y se formará un túnel CAPWAP para el plano de control entre el punto de acceso y el controlador de LAN inalámbrica, mientras que el túnel VxLAN para el plano de datos se extenderá hasta el Edge (fabric edge).
- El Suplicante nativo enviará una solicitud al Servidor de Autenticación (ISE) a través del controlador de LAN inalámbrica de Cisco utilizando la VLAN de gestión.
- ISE validará el acceso del usuario, autenticará al usuario utilizando la autenticación 802.1x y proporcionará una asignación dinámica de IP Pool y SGT.
- El endpoint obtendrá una dirección IP del servidor DHCP.
- Los datos del usuario fluirán utilizando VxLAN desde el punto de acceso hasta el nodo Edge (edge node).
- Si todos los pasos anteriores se realizan con éxito, los usuarios podrán acceder a la red satisfactoriamente.

Por otro lado, tenemos el acceso de invitados (no menos importante) dado que es fundamental en la mayoría de las arquitecturas empresariales, ya que sus entornos son altamente móviles y dinámicos hoy en día. El acceso para invitados proporciona a los usuarios como visitantes, contratistas y clientes, el acceso a los recursos necesarios.

En el WLC, el SSID de invitados se definire como una única WLAN utilizando solo filtrado MAC. La configuración requerida para lograr la autenticación y autorización para diferentes tipos de usuarios será gestionada por ISE, quién en base a las políticas y resultados de estas, concederá o denegará el acceso a la red.

El flujo de autenticación ocurre en dos fases. En la primera fase, ISE autenticará la dirección MAC del endpoint que se conecta al SSID de Invitados. Como la dirección MAC presentada pertenece a un dispositivo desconocido (huésped o corporativo), normalmente debería fallar la autenticación. El ISE debería permitir que la sesión continúe hasta la política de autenticación, la cual forzará la redirección al portal web.

A continuación, se muestra el flujo de tráfico para un usuario que se conecta al SSID de invitado:

1. El cliente se conecta a la SSID de invitado abierto en el WLC.
2. El WLC contacta al servidor ISE para MAB.
3. ISE envía un acceso-aceptar con la URL de redireccionamiento y la lista de control de acceso de redireccionamiento "ACL-REDIRECT" al WLC.
4. Ahora el cliente se coloca en una VLAN con una ACL donde obtiene una dirección IP y se coloca en CENTRAL_WEBAUTH_REQD.
5. El usuario se autentica en el portal de invitados.
6. Después de iniciar sesión correctamente, ISE envía una CoA[45] al WLC.
7. El usuario se vuelve a autenticar y aterriza en una Regla de Política diferente en ISE donde se otorga acceso completo, luego el WLC coloca al cliente en el estado RUN.
8. Todo el tráfico del cliente se reenvía en VXLAN en el VN DE INVITADO.
9. El usuario tendrá acceso a Internet y a los recursos que se consideren habilitar.

Los SSID/ WLANs que vamos a desplegar en nuestra empresa son los siguientes:

SSID	Security	Band	Traffic Type	Device Types	Description
Corporativo	802.1x (ISE)	2,4 & 5Ghz	Data + Voice	Dispositivos corporativos (laptops, iPADs, Tablets, IP Phones, etc).	Dispositivos con certificado corporativo. Dinámicamente se asigna a la VLAN a la que pertenece el equipo (AAA).
BYOD	802.1x (ISE)	2,4 & 5Ghz	Data	Dispositivos NO corporativos y de uso personal, por empleados de la compañía.	Dispositivos con certificado corporativo (enrolados previamente en MDM). Dinámicamente se asigna a la VLAN a la que pertenece el equipo (AAA).
Invitados	Mac-Filtering	2,4 & 5Ghz	Data	Externos a la compañía.	CWA

Tabla 12. Wlans desplegados

En cuanto a la WLAN de invitados, DNAC ofrece automatización para configurar el ACL de redirección y el portal cautivo en ISE. El portal puede personalizarse dentro de DNAC y enviarse automáticamente a ISE. En nuestra compañía, el SSID de invitados se configurará como MAB ya que hay una implementación existente de ISE con portales definidos.

```
! ACL-REDIRECT needed for Guest Auth.
ip access-list extended ACL-REDIRECT
deny udp host [DHCP_SERVER_1] eq bootps any eq bootpc
deny udp any eq bootpc host [DHCP_SERVER_1] eq bootps
deny udp host [DNS_SERVER_1] eq domain any range 0 65535
deny udp any range 0 65535 host [DNS_SERVER_1] eq domain
deny tcp host [DNS_SERVER_1] eq domain any range 0 65535
deny tcp any range 0 65535 host [DNS_SERVER_1] eq domain
deny udp host [DHCP_SERVER_2] eq bootps any eq bootpc
deny udp any eq bootpc host [DHCP_SERVER_2] eq bootps
deny udp host [DNS_SERVER_2] eq domain any range 0 65535
deny udp any range 0 65535 host [DNS_SERVER_2] eq domain
deny tcp host [DNS_SERVER_2] eq domain any range 0 65535
deny tcp any range 0 65535 host [DNS_SERVER_2] eq domain
deny ip host [ISE_PSN_VIP_1] any
deny ip any host [ISE_PSN_VIP_1]
deny ip host [ISE_PSN_VIP_2] any
deny ip any host [ISE_PSN_VIP_2]
deny ip host [ISE_PSN_VIP_3] any
deny ip any host [ISE_PSN_VIP_3]
permit tcp any range 0 65535 any eq www
exit
!
```

Vamos a ver un ejemplo de cómo el cliente inalámbrico A conectado al Fabric SDA mediante un punto de acceso conectado al Fabric Edge A, envía datos al cliente cableado B conectado al nodo Fabric Edge B.

Cuando el AP en modo Fabric recibe un paquete del cliente inalámbrico, elimina la cabecera 802.11 del paquete y la reemplaza con la cabecera 802.3. Cada SSID está asociado con un VNID de capa 2 y a cada usuario se le asigna un SGT, como resultado de la autorización del usuario en Cisco Identity Services Engine (ISE). Luego, el AP encapsula el paquete en VXLAN:

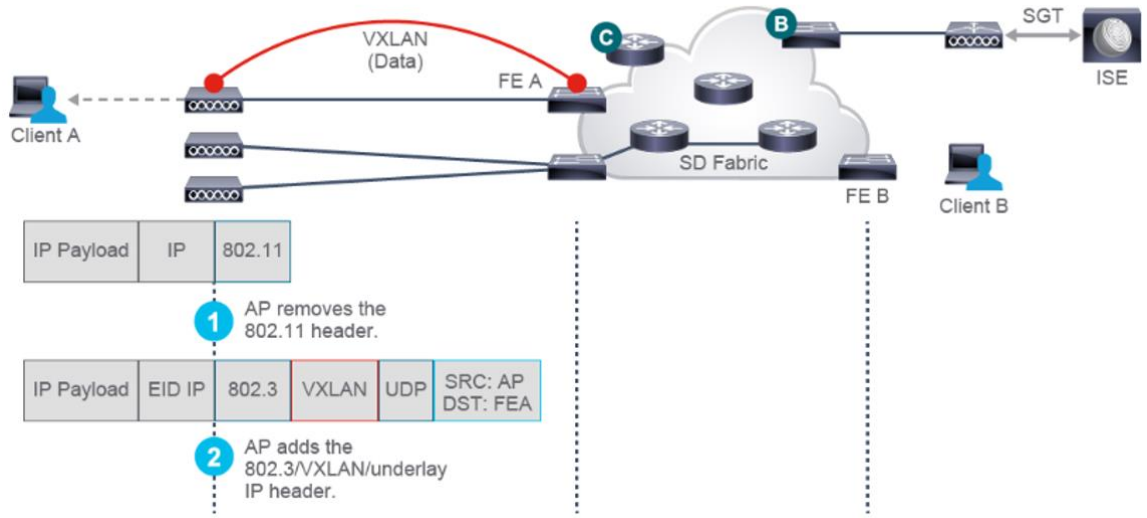

Imagen 49. VXLAN entre AP & FE

La cabecera VXLAN recién agregada al paquete contiene el SGT del cliente y la información de la red virtual. De esta manera, el AP incrusta la información de la política del cliente en el paquete y permite que la política siempre se mantenga con el cliente.

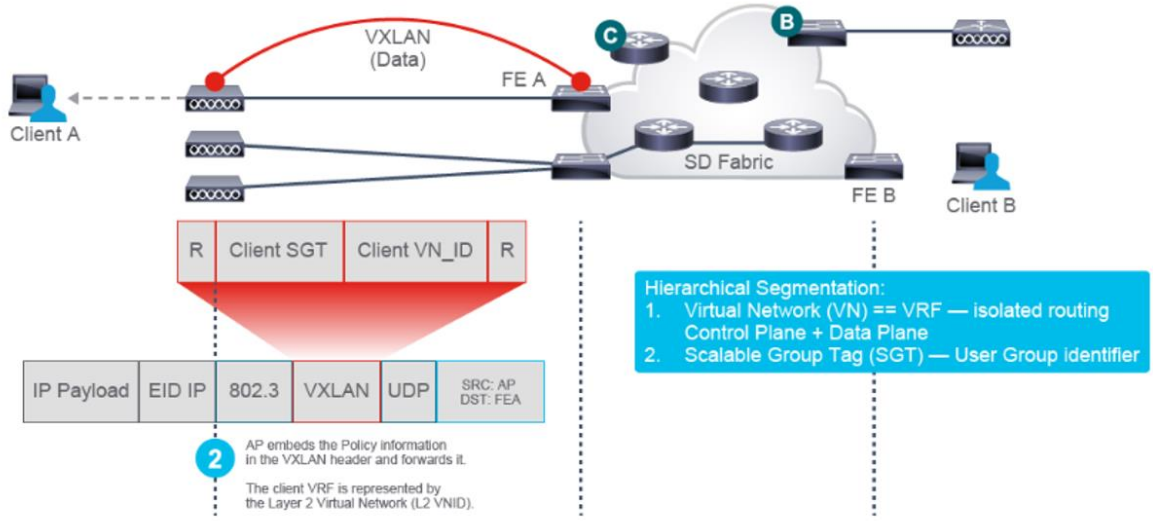

Imagen 50. Cabecera VXLAN

El AP reenvía el paquete a su primer switch de salto, que es el Fabric Edge A, al que el AP se conecta directamente. Debido a que la dirección IP de destino de VXLAN es la dirección IP del Fabric Edge A, el Fabric Edge A desen-capsula el paquete de VXLAN y maneja el tráfico del cliente en la instancia adecuada de enrutamiento y reenvío virtual (VRF).

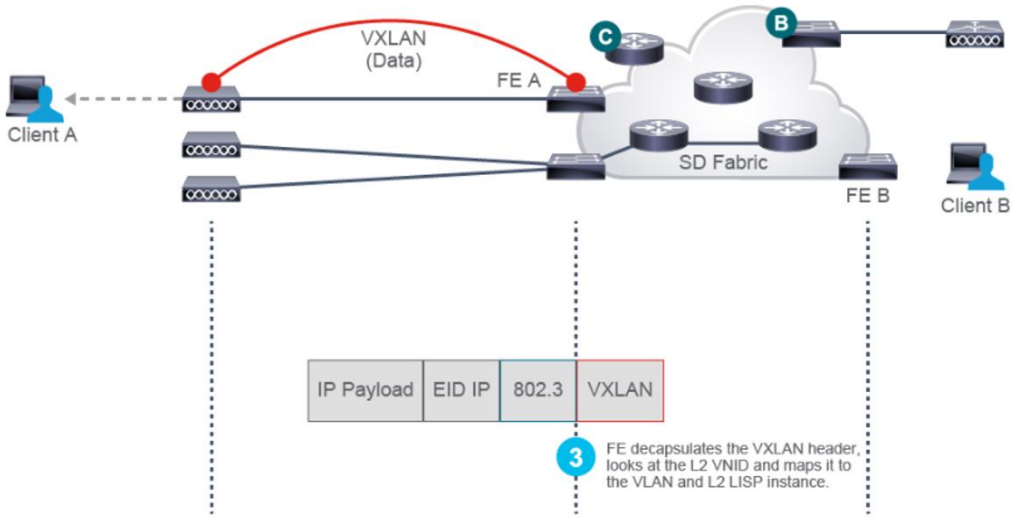

Imagen 51. Desencapsular Cabecera VXLAN

El Fabric Edge determina la VRF en el que colocar al cliente al examinar el VNID de capa 2 en la cabecera VXLAN recibida desde el AP. La instancia LISP de capa 2 en el switch asigna ese VNID al VLAN correspondiente.

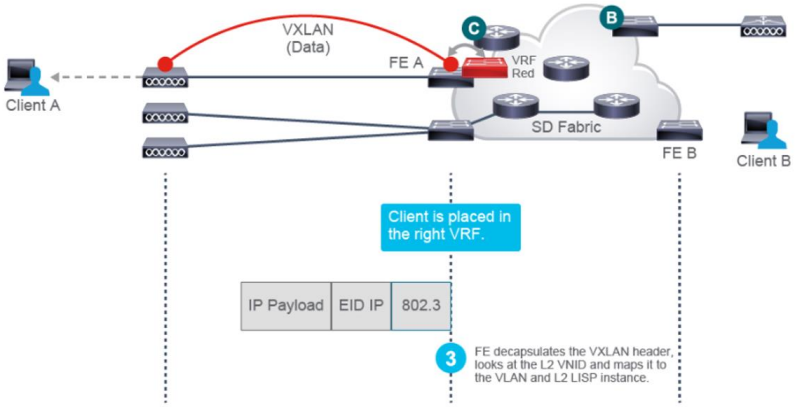

Imagen 52. VNID Process Wireless Client

Con la VRF del cliente, el Fabric Edge A busca la EID del cliente B y descubre que está detrás del Fabric Edge B. Luego, el Edge A reconstruye la cabecera VXLAN utilizando la dirección IP del locator de enrutamiento (RLOC) del Edge B como destino y envía el paquete encapsulado al Edge B.

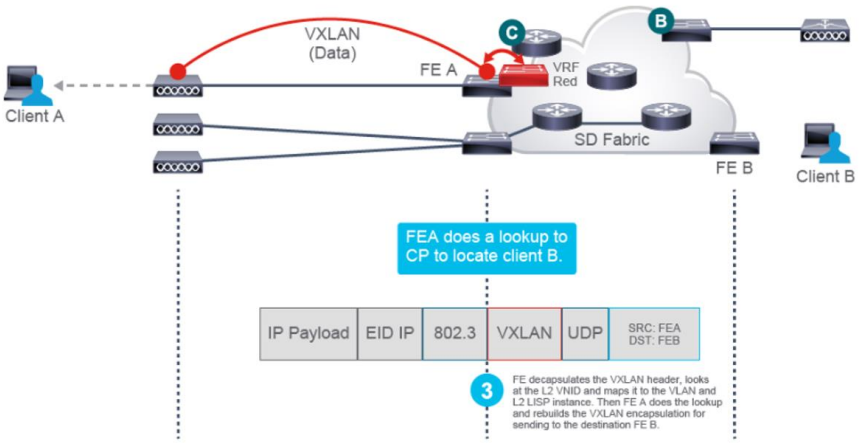

Imagen 53. Encapsulation VXLAN

Finalmente, el Edge B recibe el paquete y lo desen-capsula, busca la asignación de VLAN para el VNID de la cabecera VXLAN. También examina el valor de SGT y aplica la política correspondiente antes de reenviar el paquete decapsulado al cliente B.

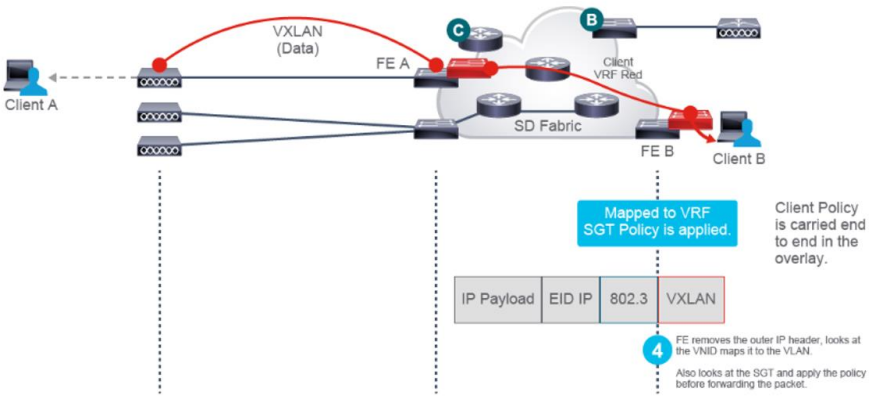

Imagen 54. Encapsulation VXLAN

Así es como la política del cliente se lleva de extremo a extremo en el overlay, de manera consistente tanto en los dominios cableado como inalámbricos.

6.3 Segmentación y Microsegmentación

La segmentación y micro-segmentación proporcionan aislamiento de tráfico dentro de la estructura SD-Access.

Segmentación (Macrosegmentación): Las Redes Virtuales (VNs) en la estructura SDA se utilizan para aislar la accesibilidad IP o la visibilidad de la tabla de enrutamiento entre dos segmentos o entidades. Son VRF en los dispositivos SDA.

Micro-segmentación: Las Etiquetas de Grupo Escalables (SGT) proporcionan micro-segmentación dentro de cada VN. Por defecto, la accesibilidad IP está disponible dentro de subredes o hosts dentro de la VN, sin embargo, en función del perfil de identidad, se puede controlar el flujo de tráfico entre grupos mediante SGACL de permitir/denegar.

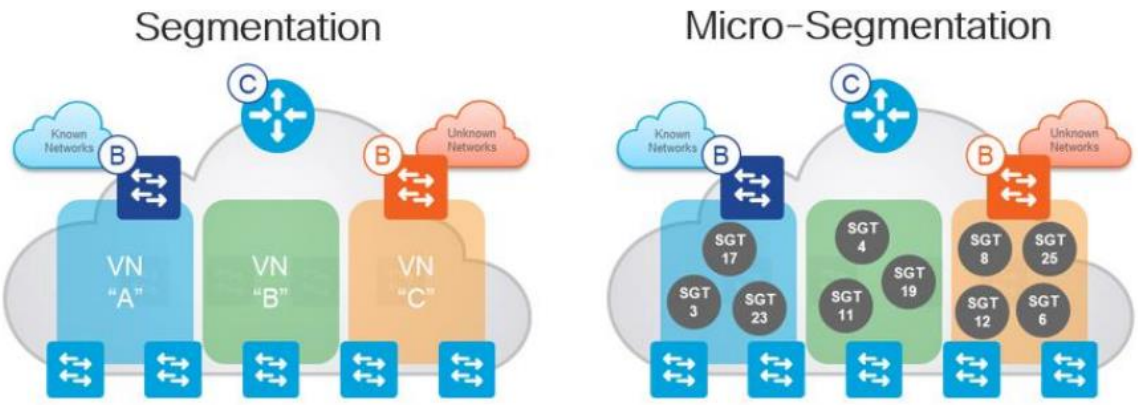

Imagen 55. Macro-Micro Segmentación en SDA

6.3.1 Virtual Networks

Las VNs están diseñadas para aislar completamente el tráfico entre ellas mediante diferentes instancias de enrutamiento. SDA no permite el tráfico entre VNs, por lo que se deben implementar dispositivos externos para hacer VRF leaking si es necesario.

En Quartz, hay un caso de uso en el que el tráfico en una VN debe filtrarse en otra VN. Por ejemplo, en la VN de invitados habrá paquetes DHCP que necesitan llegar a los servidores DHCP de Infoblox en los centros de datos. Como la VN de invitados no se extenderá a través de SDWAN, los endpoints en esa VN no podrán alcanzar la dirección IP de Infoblox. Otro ejemplo es permitir que el tráfico de invitados llegue a ISE para los portales cautivos. Para solucionarlo, se realizará VRF leaking en el enrutador SDWAN para permitir el tráfico entre el pool de direcciones IP de invitados en la VN de invitados y la subred de Infoblox en la VN de TI.

VN Name	Description
VN-1	Dispositivos corporativos con certificado de IT
VN-2	Dispositivos de la red OT
VN-3	Dispositivos de Sistema de Gestión de Edificios
VN-4	Dispositivos de Seguridad Corporativa
VN-5	Dispositivos de Invitados

Tabla 13. Virtual Networks

6.3.2 IP Pools

La siguiente tabla muestra los IP Pools creados para el desarrollo del proyecto:

Fabric Site	IP Pool Name	IPv4 Subnet / Mask	Gateway
ESMAL1	ESMAL1_COMMON_USERS	10.0.0.0/19	10.0.0.1
	ESMAL1_VOIP	10.0.32.0/22	10.0.32.1
	ESMAL1_PRINTERS	10.0.36.0/24	10.0.36.1
	ESMAL1_BMS	10.0.40.0/21	10.0.40.1
	ESMAL1_SEGCORP	10.0.48.0/21	10.0.48.1
	ESMAL1_GUEST	10.0.56.0/21	10.0.56.1
	ESMAL1_OT_CCTV	10.0.64.0/23	10.0.64.1

Tabla 14. IP Pools

Podríamos decir que los IP Pools son lo que conocemos en las redes tradicionales como concepto VLAN o Dominio de broadcast con salvedades/ mejoras.

6.3.3 SGTs

Son etiquetas de Grupo Escalables que se definen en función de los usuarios, endpoints o grupos de recursos de Quartz que requieren microsegmentación. La creación de un grupo escalable produce un valor SGT de 2 bytes. Con TrustSec, la clasificación de un endpoint ocurre en la interfaz de ingreso del Dispositivo de Acceso a la Red.

Dentro de ISE, se muestra tanto una representación decimal como hexadecimal para el SGT. DNAC muestra el valor de etiqueta (Tag Value) para cada SGT. Con fines de gestión, se proporciona un nombre significativo (un campo obligatorio) y una descripción.

La figura a continuación presenta la pestaña de Grupo de Seguridad en ISE (Centros de trabajo > Trustsec > Componentes en la GUI de ISE).

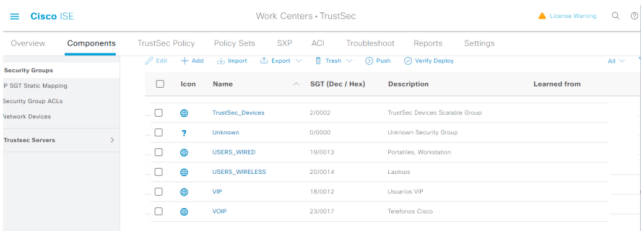

Imagen 56. SGTs en ISE

Los SGTs que se han creado son los siguientes:

SGT	Description	Virtual Network
USERS_WIRED	Laptop, Workstation	VN-1
USERS_WIRELESS	Laptops	VN-1
VOIP	Teléfonos Cisco	VN-1
GUEST	Dispositivos Invitados	VN-5
VIP	Dispositivos VIP de Invitados	VN-5
ILUMINACIÓN	Dispositivos BMS Iluminación	VN-4
MEGAFONIA	Dispositivos BMS megafonía	VN-4
CCTV	Cámaras de seguridad	VN-3
CONTROL_ACCESOS	Dispositivos de seguridad	VN-3
CCTV_OT	Cámaras de procesos	VN-2
INTRUMENTACIÓN	Dispositivos de OT	VN-2

Tabla 15. SGTs

Un **SGT** nada tiene que ver con una **VLAN/IP Pool**. En un IP Pool podemos tener 1 o muchos SGTs. De hecho, podríamos tener un mismo SGT presente en dos VLANs/IP pools. Por ejemplo: por el motivo que sea tenemos dos IP pools para telefonía, uno para teléfonos wired (10.0.32.0/22) y otro para teléfonos Wireless (10.0.90.0/22). Queremos tenerlos con direccionamiento diferente pero también queremos que todos lleven el mismo SGT: PHONE. Esta es una configuración válida en SDA. De hecho, esos IP Pools podrían incluso estar en VNs (VRFs) diferentes.

6.3.4 SGACLs

La microsegmentación se beneficia de políticas más específicas. En lugar de usar un enfoque de permiso explícito, es posible mejorar la seguridad con un SGACL que bloquea explícitamente los puertos comúnmente explotados por malware, manteniendo un permiso implícito.

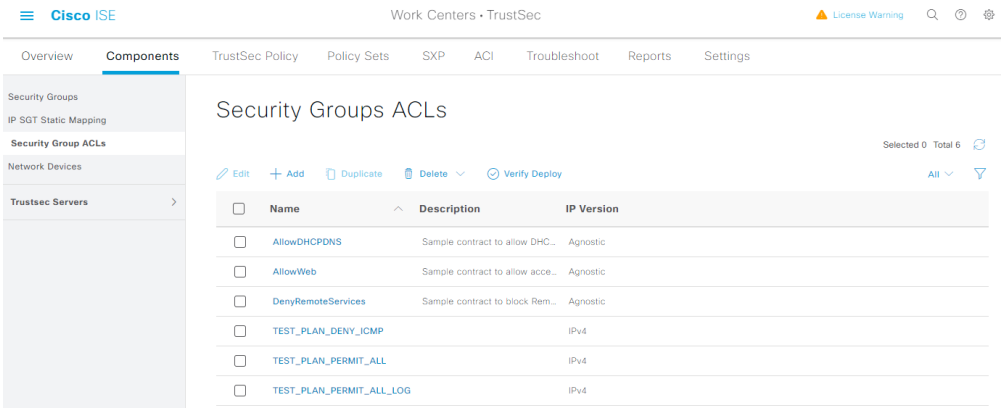

Imagen 57. SGACLs en ISE

Usando SGACLs, las políticas pueden definirse en función del SGT de origen y destino. La aplicación de políticas se representa como una matriz de permisos, con los miembros del grupo de seguridad de origen en un eje y los miembros del grupo de seguridad de destino en el otro eje.

Cada casilla en el cuerpo de la matriz contiene una SGACL que especifica el permiso entre origen y destino. Las SGACL no tienen información de origen y destino, sino que solo contienen lo que está permitido o denegado

6.4 Matriz de tráfico

Al asignar usuarios y dispositivos dentro de la red a Grupos Escalables (SGT) y aplicar control de acceso entre los Grupos Escalables (SGACL), TrustSec logra un control de acceso basado en roles y sin depender de la topología dentro de la red.

Las SGACL definen políticas de control de acceso basadas en identidades de dispositivos, en contraposición a las ACL tradicionales que usan direcciones IP. Por lo tanto, los dispositivos clientes pueden moverse libremente por la red y cambiar las direcciones IP. Siempre que los roles y permisos sigan siendo los mismos, los cambios en la topología de la red no afectan la política de seguridad.

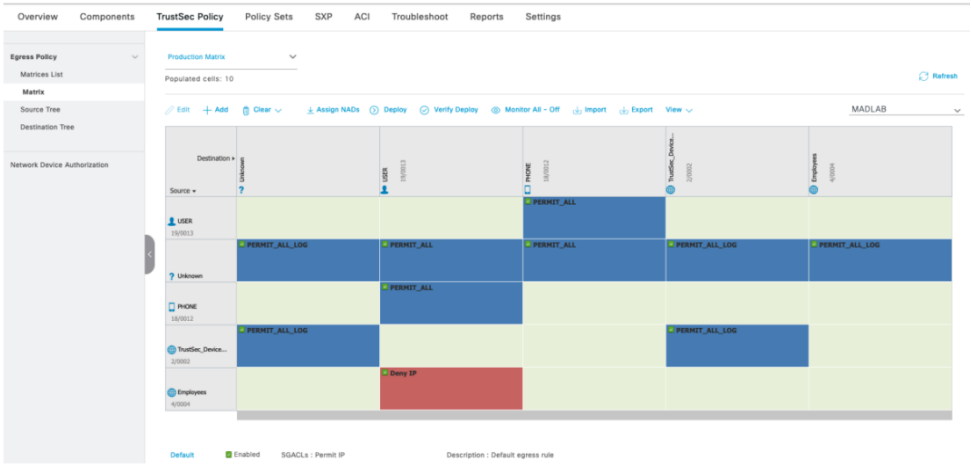

Imagen 58. Matriz TrustSec en SDA

6.5 Autenticación

En SDA, las plantillas de autenticación se configuran globalmente por sitio de la tela. Los modos admitidos son Closed, Low Impact y Open. En nuestro proyecto sólo vamos a implantar el modo Closed y Low Impact.

6.5.1 Closed

No permite ningún tráfico entrante antes de la autenticación, excepto para EAP[46], CDP[47] y LLDP[48], como se muestra en la imagen siguiente:

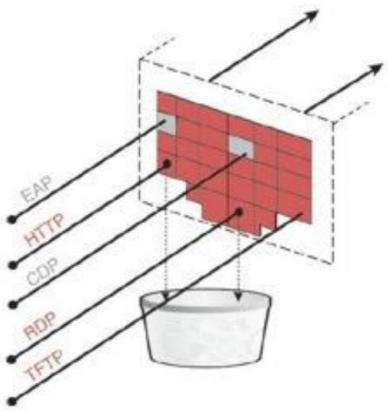

Imagen 59. Closed Authentication

Por defecto, el puerto no puede enviar ni recibir ningún paquete (solo EAP, CDP y LLDP). Sin embargo, si la casilla de verificación WoL[49] está habilitada en la plantilla de autenticación de DNAC, el puerto también podrá enviar paquetes al endpoint. Sin embargo, la casilla no estará habilitada ya que Wake on LAN[45] no es un requisito para Quartz.

6.5.2 Low Impact

En SDA, antes de que se produzca la autenticación, todos los puertos Edge funcionan operativamente en VLAN 1. Aunque VLAN 1 se crea en L2, no hay ninguna configuración en L3 (sin dirección IP), por lo que el tráfico en esta VLAN no puede ser enrutado.

Low Impact permite el tráfico de salida, pero restringe el tráfico de entrada solo a EAP, CDP, LLDP, DHCP y DNS (ver figura a continuación).

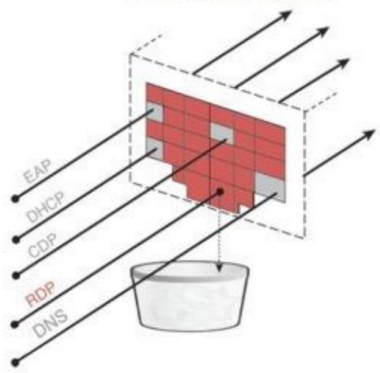

Imagen 60. Low Impact Authentication

6.6 Calidad de Servicio (QoS)

La Calidad de Servicio (QoS) se refiere a la capacidad de una red para proporcionar un servicio preferencial o diferencial a cierto tráfico de red seleccionado. Al configurar QoS, se puede asegurar que el tráfico de red sea manejado de modo más eficiente para los recursos de la red, mientras se cumplen los objetivos de la empresa, como garantizar que la calidad de voz cumpla con los estándares empresariales o garantizar una alta calidad de experiencia (QoE) para el video.

DNA Center permite la automatización de la implementación de QoS con políticas de aplicaciones, que incluyen los siguientes parámetros:

- Conjuntos de Aplicaciones: representan grupos de aplicaciones con necesidades similares de tráfico de red (por ejemplo: control-de-red, aplicaciones-saas o compartición de archivos). A cada conjunto de aplicaciones se le asigna un grupo de relevancia empresarial (relevante para el negocio, predeterminado o irrelevante para el negocio) que define la prioridad de su tráfico.

- Ámbito del Sitio: Sitios a los cuales se aplicará una política de aplicación.

- Tipo de Medio: Puedes definir si aplica al medio de acceso cableado o inalámbrico o ambos.

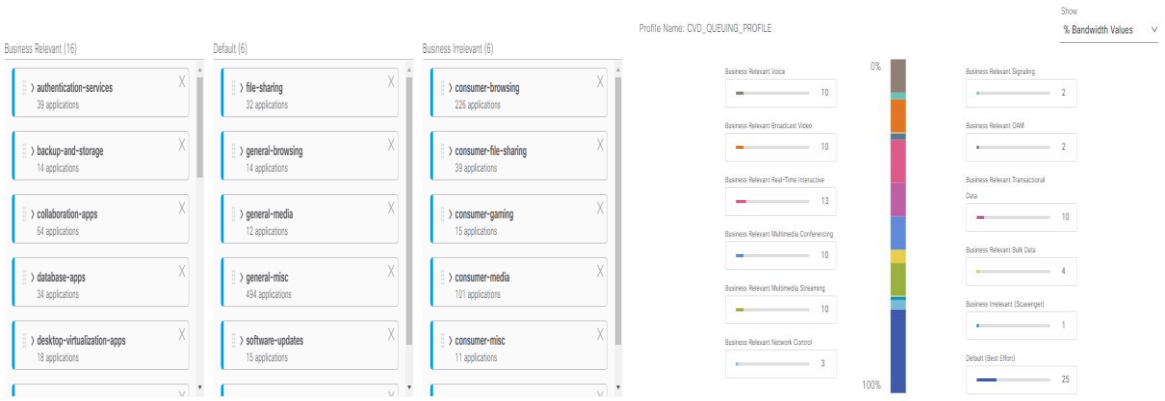

Imagen 61. QoS en DNA Center

6.6.1 Reconocimiento de aplicaciones (NBAR/CBAR)

El servicio de Visibilidad de Aplicaciones, alojado como una pila de aplicaciones dentro de Cisco DNA Center, te permite habilitar la función de Reconocimiento de Aplicaciones Basado en Controlador (CBAR) para clasificar miles de aplicaciones de red por defecto, personalizadas y tráfico de red.

Se debe instalar los siguientes paquetes en DNA Center:

- Política de Aplicaciones: te permite automatizar las políticas de QoS en LAN, WAN y inalámbricas dentro de tu campus y sucursal.

- Registro de Aplicaciones: te permite ver, administrar y crear aplicaciones y conjuntos de aplicaciones.

- Servicio de Visibilidad de Aplicaciones: proporciona clasificación de aplicaciones utilizando técnicas de Reconocimiento de Aplicaciones Basado en Red (NBAR) y CBAR[49].

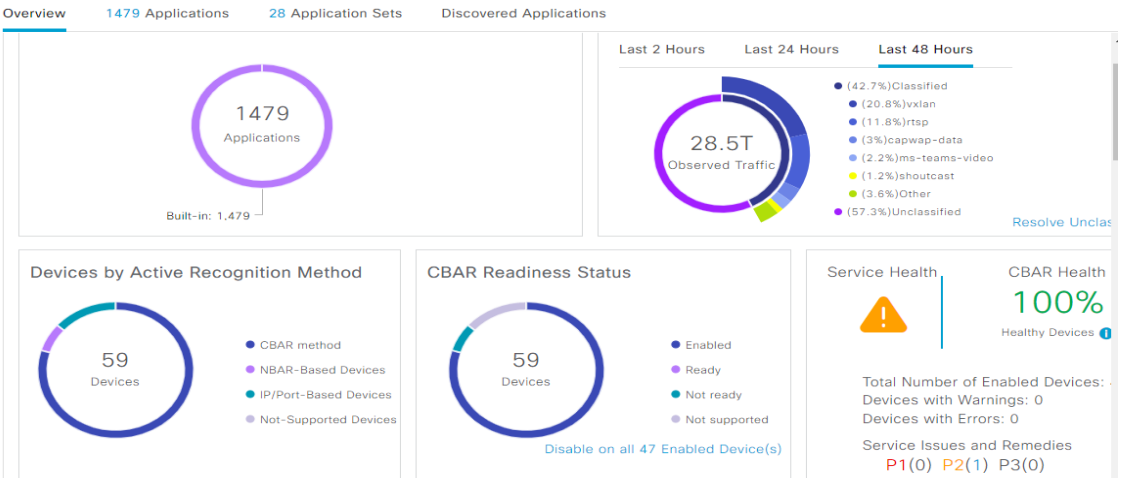

Imagen 62. Application Visibility

6.8 Creación de Templates

DNA Center proporciona un editor interactivo llamado Template Editor para crear plantillas por CLI. La herramienta permite crear plantillas personalizadas con o sin elementos o variables parametrizados. Las plantillas pueden ser escritas de tal manera que puedan ser reutilizadas en diferentes sitios o diferentes plataformas de hardware.

Template Editor ofrece las siguientes características:

- Crear, editar y eliminar una plantilla
- Agregar comandos interactivos
- Validar errores en la plantilla
- Controlar versiones de las plantillas para fines de seguimiento
- Simular plantillas
- Formularios
- Plantillas compuestas (una secuencia de plantillas regulares)

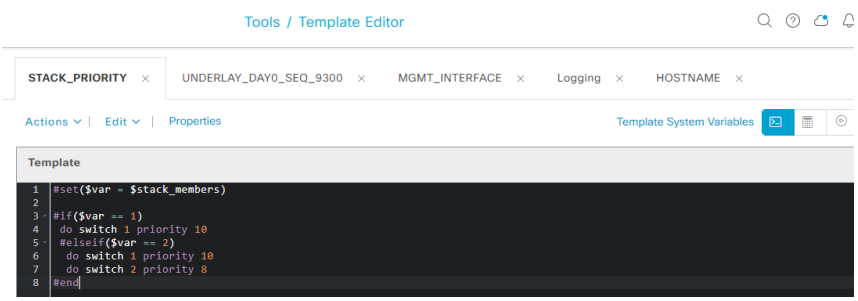

Imagen 63. Stack_Priority Template (Example)

7. Integración con Redes Externas

La conectividad desde el Fabric SDA con el exterior es crucial, ya que esto permite la comunicación Norte-Sur e Este-Oeste. Las redes externas son accesibles a través de los fusión.

7.1 Border Nodes

Los nodos de borde actúan como puerta de enlace entre el Fabric SD-Access y todas las redes y servicios externos. Cualquier VN que necesite acceder a cualquier servicio fuera del Fabric, como DNS, DHCP o Internet (tráfico Norte-Sur), deberá ser extendido fuera de los bordes hacia los dispositivos de fusión.

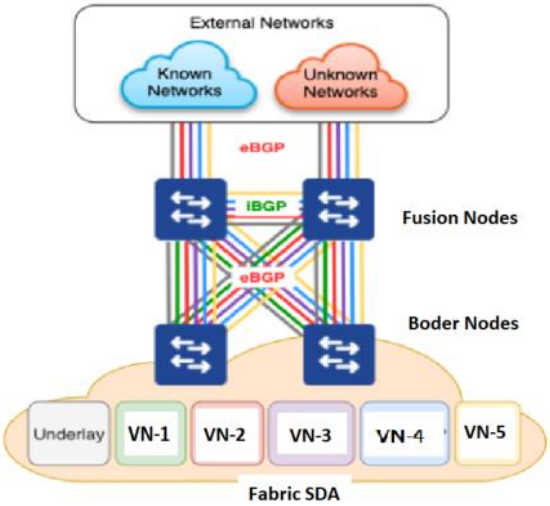

Imagen 64. External Routing

7.2 Fusion Nodes

Los switches Fusion tienen habilitan comunicaciones con los servidores NTP, DNAC o ISE, por la Tabla de Enrutamiento Global. Con el fin de reducir la complejidad, los switches Fusion fusionarán el Underlay y la VN IT en la Tabla de Enrutamiento Global y no en una VRF personalizada, ya que ambos representan el dominio de confianza en el sitio del Campus. La figura a continuación ilustra la segmentación en los switches Fusion en el sitio del Campus de Quartz.

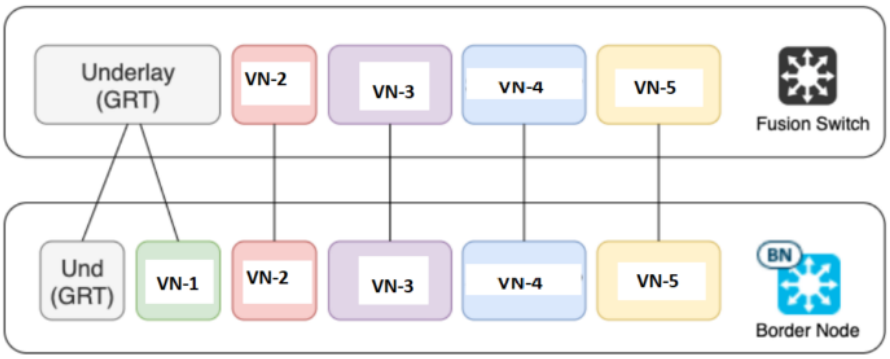

Imagen 65. Segmentación en Fusion Node

7.3 SD-WAN Node

Los routers SDWAN mantendrán la segmentación definida en la capa de fusión. Por lo tanto, se deben definir nuevas VPN de servicio en la implementación SDWAN existente. Todas las VPN se extenderán a través del SDWAN excepto la de invitados. En su lugar, la VPN de invitados proporcionará solo un acceso local a Internet.

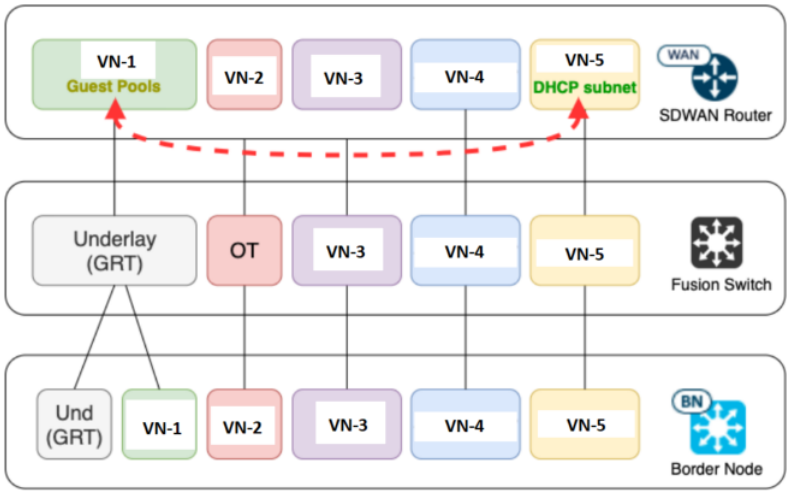

Imagen 66. VRF Leaking en Routers SD-WAN

8. ISE

8.1 Visión general

ISE provee los servicios de autenticación, gestión de identidad y el cumplimiento de las políticas de seguridad. Es un servidor de políticas que nos permite gestionar el acceso a una red corporativa. Centraliza y unifica el control de acceso seguro según el perfil del usuario y dispositivo que quiere acceder a la red. Trata temas de IDENTIDAD.

Identifica a un usuario con dispositivo corporativo, usuario con dispositivo no corporativo o invitados, proporcionando el nivel de acceso según el perfil, independientemente que se conecten a través de cable, red inalámbrica o con acceso remoto VPN.

ISE está disponible tanto como un dispositivo físico como una máquina virtual. Ambas formas, física y virtual, se pueden usar para crear clusters de ISE. Las máquinas virtuales de ISE son compatibles con VMware ESXi 5.x y 6.x o Kernel-based Virtual Machine (KVM) en Red Hat 7.x.

8.2 Roles

PAN (Nodo de administración de Políticas)

Proporciona funciones administrativas relacionadas con la gestión de la implementación y configuraciones de ISE.

MNT (Nodo de Monitorización)

Funciona como recolector de registros. Siempre debe haber al menos un nodo de monitorización en una implementación distribuida.

PSN (Nodo de Servicio de Políticas)

Controla el acceso a la red, el posture, el profiling, los servicios de invitados y el aprovisionamiento de clientes.

PxGRID (Es un servicio que se habilita en los nodos PSN)

Cisco pxGrid se utiliza para compartir información contextual de sesiones de Cisco ISE con otros sistemas como con DNAC en nuestro caso.

8.3 Autenticación

Los dispositivos en nuestro proyecto son autenticados (y posteriormente autorizados) por uno de estos métodos:

- 802.1x
- MAB

8.3.1 802.1X

IEEE 802.1X (comúnmente conocido como dot1x) se define como un estándar para "control de acceso a la red basado en puerto" para redes de área local. Los tres componentes principales de 802.1X son los siguientes:

1. Suplicante: es el software en el endpoint que se comunica con EAP en L2. Este software responde al autenticador y proporciona las credenciales de identidad con la comunicación EAP. En Quartz, los suplicantes 802.1x vienen nativamente con las distribuciones del sistema operativo.

2. Autenticador: es el dispositivo de red que controla el acceso físico a la red en función del estado de autenticación del endpoint. Toma paquetes L2 EAP del suplicante y los encapsula en paquetes RADIUS dirigidos al servidor de autenticación (ISE). Los autenticadores también se denominan NAD, y en nuestro caso serían los Fabric Edge y los WLC.

3. Servidor de autenticación: es el servidor que realiza la autenticación del cliente. Valida la identidad del endpoint y proporciona al autenticador (NAD) un resultado (permitir o denegar). En Quartz, ISE es el servidor de autenticación.

8.3.2 MAB

MAC Authentication Bypass (MAB) sólo debería usarse cuando no sea posible un método de autenticación más seguro (802.1X) debido a lo siguiente:

- MAB manual no es tan seguro como 802.1X porque la dirección MAC del dispositivo puede ser falsificada.
- MAB manual tiene un costo administrativo más alto porque requiere la creación manual, eliminación y auditoría de cuentas de direcciones MAC en ISE.
- MAB con perfilado es ligeramente más seguro porque utiliza atributos perfilados y la dirección MAC del punto final, pero aún puede ser falsificado.
- MAB con perfilado tiene un costo anual más alto porque requiere una licencia Plus (suscripción anual) para cada dispositivo que se autentique con este método.

Por defecto, una vez que expira el tiempo de espera de 802.1X, el switch envía al nodo ISE un marco RADIUS de acceso/solicitud con un nombre de usuario y una contraseña basados en la dirección MAC del dispositivo.

DNA Center provisiona políticas que permiten que se valide si el endpoint no admite 802.1X o falla la autenticación de 802.1X, se puede intentar MAB. En SDA, el valor de tiempo de espera que hemos configurado para 802.1X es de 7 segundos y los reintentos son 3. Esto significa que después de 21 segundos o tres tiempos de espera de 802.1X, el switch pasará a MAB, y los dispositivos que usan autenticación MAB deben esperar 21 segundos antes de poder ser autenticados.

8.4 Autenticación y Autorización

8.4.1 Políticas de Autenticación

Estas son las principales características de una política de autenticación de ISE:

- La política de autenticación puede garantizar que no se acepten protocolos inseguros. Es importante destacar que esto no solo mejora la seguridad de la red, sino que también garantiza que los recursos de ISE no se sobrecarguen analizando paquetes que ni siquiera son compatibles con la organización.

- Facilita la selección del método y almacén de identidad correctos para la autenticación. ISE puede configurarse para utilizar identidades internas y externas. Ejemplos de almacenes de identidad externos son AD, LDAP y repositorio de certificados. La política de autenticación puede ayudar a garantizar que se seleccione el almacén de identidad correcto para la autenticación del usuario. Lo hace examinando atributos clave en la información enviada desde el autenticador sobre el cliente.

- La política de autenticación también garantiza la validación adecuada de las credenciales. Por ejemplo, si se utiliza un certificado para la autenticación, ISE debe asegurarse de que el certificado esté correctamente formado y que contenga la información correcta requerida para fines de autenticación. También debe asegurarse de que el certificado no haya expirado ni haya sido revocado. La política de autenticación activará todas estas importantes comprobaciones.

- Por último, la política de autenticación envía solicitudes al motor de autorización de ISE.

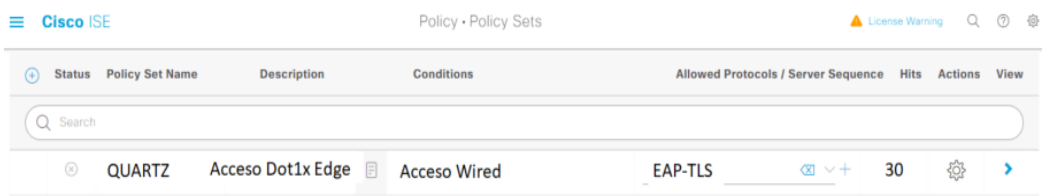

Imagen 67. Quartz Policy Example

8.4.2 Políticas de Autorización

Las políticas de autorización proporcionan la capacidad de definir y configurar perfiles de autorización para dispositivos específicos y grupos de dispositivos que accederán a recursos de red. Las políticas de autorización de red asocian reglas con identidades de dispositivos y grupos específicos para crear los perfiles correspondientes. Cuando las reglas coinciden con los atributos configurados, la política devuelve el perfil de autorización correspondiente y se autoriza el acceso a la red en consecuencia.

Las políticas de autorización pueden contener requisitos condicionales que combinan uno o más grupos de identidades utilizando una condición compuesta que incluye comprobaciones de autorización que pueden devolver uno o más perfiles de autorización. Además, los requisitos condicionales pueden existir aparte del uso de un grupo de identidades específico (por ejemplo, utilizando "Any" predeterminado).

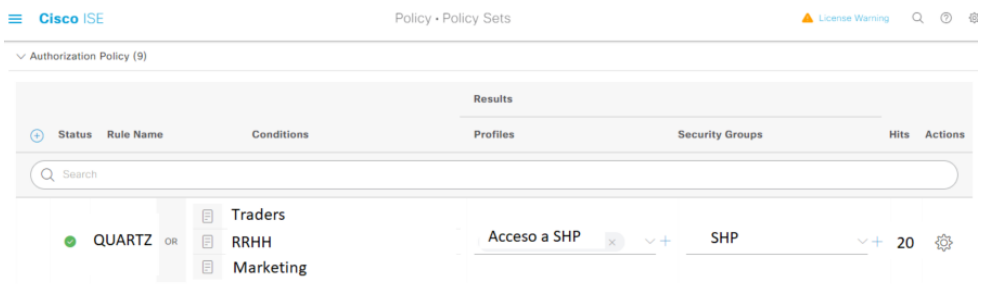

Imagen 68. Quartz Authorization Policy Example

9. DNA Center

DNA Center es la única herramienta para controlar y gestionar la solución SD-Access. Su gestión centralizada e intuitiva hace que sea rápido y fácil diseñar, aprovisionar y aplicar políticas en toda la red. Además, proporciona mayor visibilidad en la red para optimizar el rendimiento de ésta y las aplicaciones. Con un único panel de control, nos permite ahorrar tiempo al automatizar la gestión de la red. Podemos diseñar nuestra red empresarial por ubicaciones geográficas, crear sitios y agregar dispositivos de red. Con su capacidad para configurar y aprovisionar miles de dispositivos de red en minutos, no en horas, podemos optimizar el tiempo y recursos de la empresa.

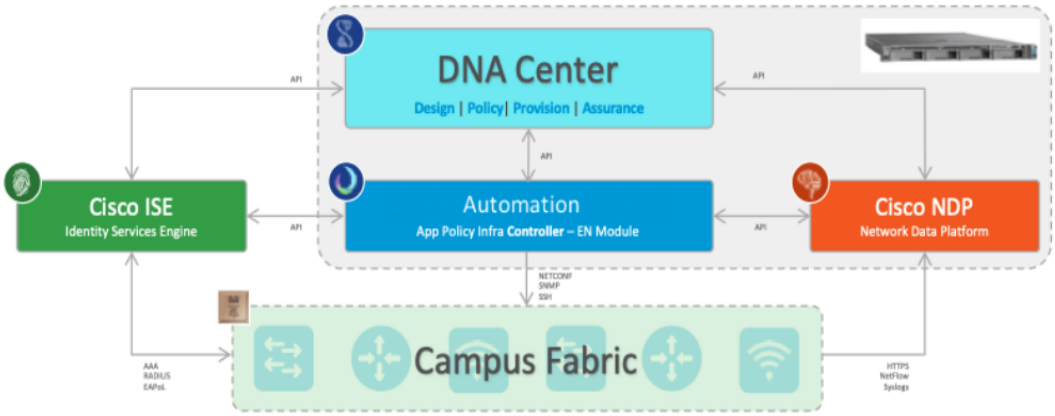

Imagen 69. Componentes de DNA Center

La Plataforma de Datos de Red (NDP) y DNAC de Cisco están integradas para el aprovisionamiento automatizado de telemetría y el enriquecimiento de datos. La funcionalidad de NDP está integrada en la herramienta de Asistencia de DNA Center, lo que proporciona una solución completa para garantizar niveles de servicio más altos y consistentes, capaces de satisfacer las crecientes demandas empresariales. La siguiente figura muestra una visión general de las características y funcionalidades de la integración de NDP y DNAC.

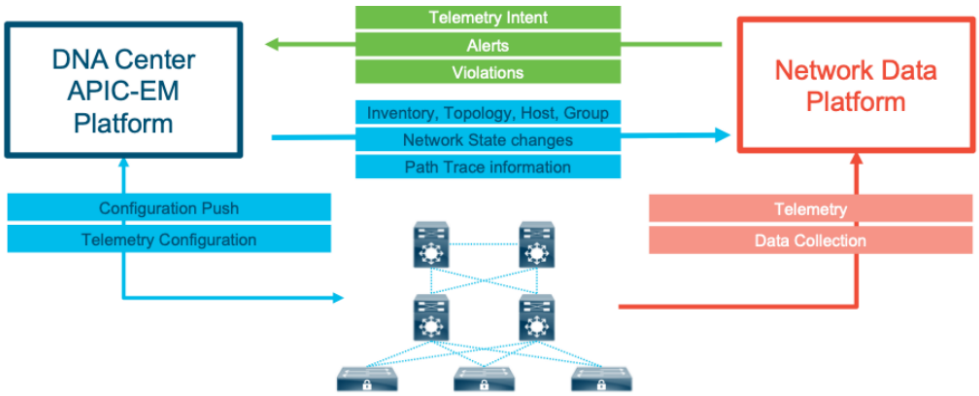

Imagen 70. Integración NDP y DNAC

9.1 Fundamentos

Al automatizar tareas diarias como la configuración, el aprovisionamiento y el troubleshooting en SD-Access con DNA Center, se logran los siguientes resultados: reducción del tiempo que lleva adaptar la red, mejora en el tiempo de resolución de problemas y reducción del impacto ante ataques de seguridad. Esto se traduce en importantes ahorros de CapEx y OpEx para la empresa.

DNA Center tiene los siguientes cuatro flujos de trabajo intuitivos para lograr los resultados mencionados:

1. Diseño/ Design: Este paso implica la creación de un diseño de red empresarial desde cero o la optimización de uno existente, utilizando una interfaz gráfica intuitiva y herramientas de simulación de red.

2. Política/ Policy: En este paso, se definen y aplican políticas de red, lo que permite un control centralizado y coherente del acceso a la red y la seguridad en todos los dispositivos.

3. Aprovisionamiento/ Provision: Este paso implica la configuración automatizada y el aprovisionamiento de miles de dispositivos de red, lo que permite una implementación rápida y eficiente de cambios y actualizaciones.

4. Asistencia/ Assurance: En este paso, se utiliza la telemetría para monitorear y solucionar problemas en tiempo real, lo que permite una solución rápida y proactiva de los problemas de red antes de que afecten a los usuarios. También se utilizan herramientas de análisis de datos para mejorar continuamente el rendimiento y la eficiencia de la red.

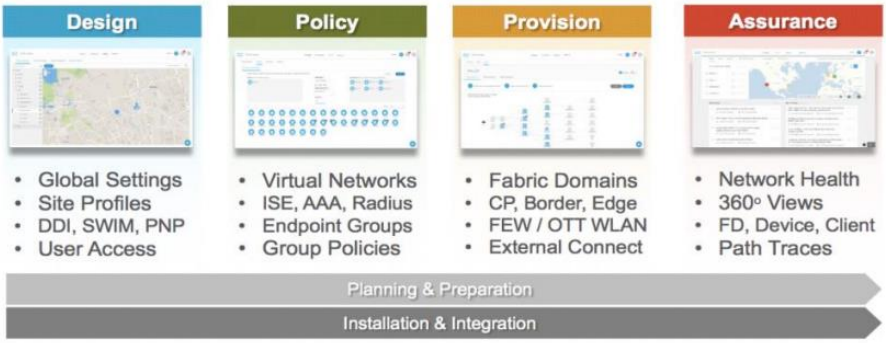

Imagen 71. Flujos de trabajo de SD-Access

9.1.1 Diseño

El área de diseño es donde se crea la estructura y el marco de la red, incluyendo la topología física, la configuración de la red y los perfiles de tipo de dispositivo que se pueden aplicar a los dispositivos en toda la red. La siguiente figura es un ejemplo del panel de diseño de DNAC:

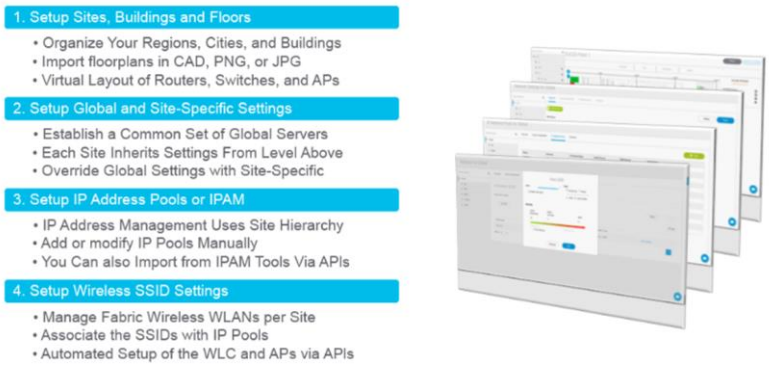

Imagen 72. DNAC Diseño

9.1.2 Políticas

DNA Center ayuda a lograr los objetivos empresariales al permitir la creación de políticas que reflejan la intención comercial de la organización para un aspecto particular de la red, como el acceso a la red. DNA Center toma la información recopilada en una política y la traduce en configuraciones específicas de red y dispositivo requeridas por los diferentes tipos, fabricantes, modelos, sistemas operativos, roles y limitaciones de recursos de los dispositivos de red. Usando la pestaña de políticas de DNA Center, se pueden crear redes virtuales, políticas de control de acceso, políticas de copia de tráfico y políticas de aplicación. La siguiente figura es un ejemplo del panel de políticas de DNAC:

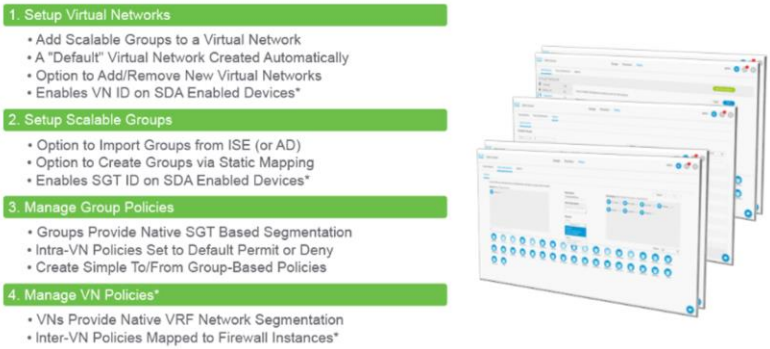

Imagen 73. DNAC Políticas

9.1.3 Provisión

Después de configurar las políticas en la red, los dispositivos deben ser aprovisionados. En esta etapa, las políticas se despliegan en los dispositivos de red. Hay 3 aspectos del aprovisionamiento de los dispositivos:

- Agregar los dispositivos a los sitios
- Desplegar las políticas requeridas (provisionamiento)
- Crear dominios de tejido y agregar dispositivos al tejido

La siguiente figura es un ejemplo del panel de aprovisionamiento de DNAC:

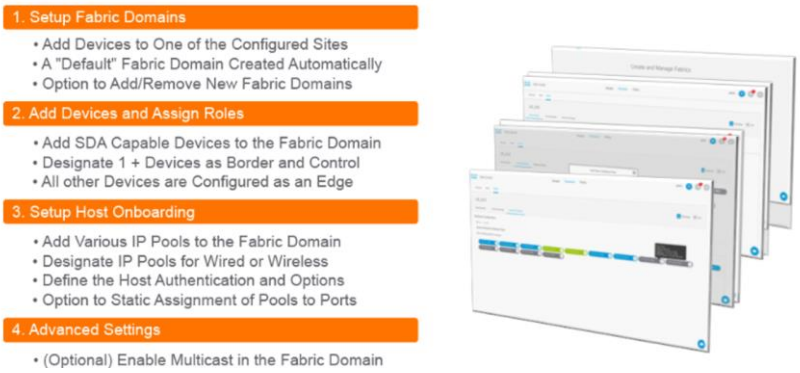

Imagen 74. DNAC Provisionamiento

9.1.4 Assurance

Cisco DNA Assurance ofrece una solución integral para asegurar mejores y consistentes niveles de servicio que satisfagan las crecientes demandas del negocio. Assurance aborda no solo la monitorización y resolución reactiva de problemas en la red, sino también los aspectos proactivos y predictivos de la gestión de la red, garantizando el rendimiento del cliente, la aplicación y el servicio.

Assurance proporciona los siguientes beneficios:

- Proporciona información práctica sobre problemas relacionados con la red, el cliente y la aplicación. Estos problemas consisten en la correlación básica y avanzada de múltiples piezas de información, eliminando así el ruido blanco y las falsas alarmas.

- Proporciona tanto el enfoque guiado por el sistema como el auto-guiado para la resolución de problemas. Para una gran cantidad de problemas, Assurance proporciona un enfoque guiado por el sistema, donde se correlacionan múltiples Indicadores Clave de Rendimiento (KPI), y se utilizan los resultados de pruebas y sensores para determinar la causa raíz del problema, y luego se proporcionan posibles acciones para resolver el problema.
  El enfoque se centra en resaltar el problema en lugar de monitorear los datos. Con frecuencia, Assurance realiza el trabajo de un ingeniero de soporte de nivel 3.

- Proporciona puntuaciones detalladas de salud para la red y sus dispositivos, clientes, aplicaciones y servicios. Se asegura de la experiencia del cliente tanto para el acceso (puesta en marcha) como para la conectividad.

La siguiente imagen es un ejemplo del panel de assurance de DNAC:

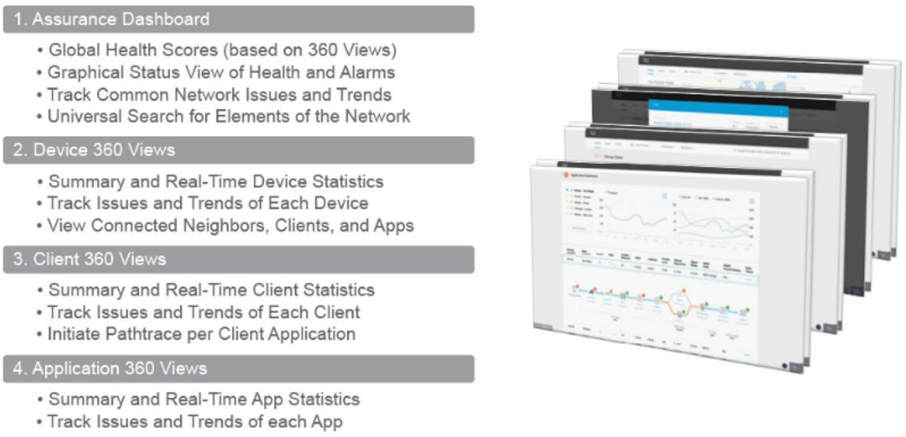

Imagen 75. DNAC Assurance

9.2 Integración con ISE

ISE y DNAC están integrados para la Automatización de Identidad y Políticas. Cisco PxGrid se utiliza para la integración entre ISE y DNAC. Los grupos de usuarios y las políticas se pueden gestionar desde DNAC y la información se envía a ISE a través de la conexión PxGrid. La siguiente figura muestra una descripción general de las características y funcionalidades de la integración entre ISE y DNAC.

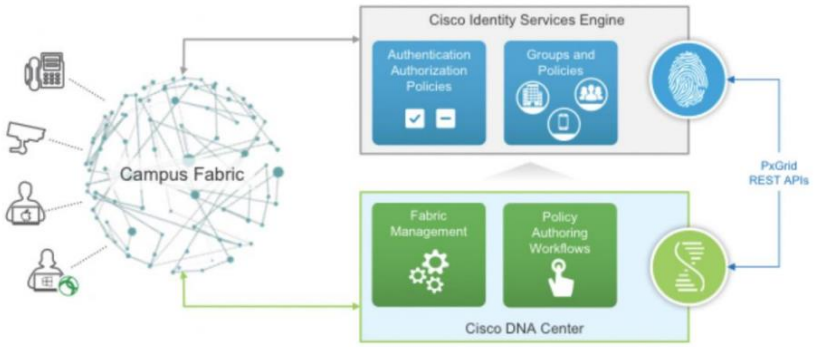

Imagen 76. Integración ISE & DNA

En Quartz, la persona pxGrid de DNAC e ISE instalarán certificados firmados por la CA interna de Quartz; por lo tanto, la integración DNAC - ISE se realizará en función de estos certificados. Tanto RADIUS como TACACS+ se habilitarán como protocolos AAA.

10. Conclusiones

10.1 Conclusiones

SD-Access permite la transformación de TI mejorando la visibilidad, definiendo y aplicando políticas de acceso basadas en grupos, segmentando la red para aislar el tráfico, reducir el riesgo y contener las amenazas, logrando coherencia en las políticas de toda la empresa, desde los usuarios hasta las aplicaciones. La construcción de esta solución de próxima generación implica algunos elementos fundamentales clave, que incluyen:

- Arquitectura basada en controladores
- Motor de aplicación de políticas
- Estructura de red
- Infraestructura programable

Arquitectura basada en controladores: En las redes tradicionales, los administradores suelen centrarse en la gestión de cada dispositivo por separado, lo que requiere mucho tiempo y puede generar errores. En cambio, SD-Access se basa en un enfoque basado en intenciones que utiliza DNA Center como centro de control y comando para orquestar y operar la red. Con este enfoque, se puede configurar rápidamente toda la red, desde la configuración inicial de los dispositivos hasta las políticas asociadas con usuarios, dispositivos y endpoints. La gestión centralizada reduce la complejidad y aumenta la eficiencia en la gestión de la red, lo que permite a los administradores concentrarse en impulsar la intención empresarial en lugar de la gestión de dispositivos individuales.

Motor de aplicación de políticas:

Las políticas de acceso se definen en el DNA-C y se almacenan en el ISE. El ISE se encarga de autenticar y autorizar los endpoints según las políticas de seguridad establecidas, otorgando un nivel de acceso adecuado a la red basado en las necesidades de cada usuario. Todo esto se logra mediante la configuración automática y dinámica de los dispositivos de red cuando los endpoints se conectan a la red, sin que los usuarios finales tengan que hacer nada. De esta manera, se asegura un acceso seguro y controlado a la red, lo que reduce el riesgo de amenazas y aumenta la eficiencia en la gestión de la red.

Estructura de red:

Con un controlador y políticas en su lugar, se puede construir una nueva red basada en Fabric que aprovecha superposiciones de redes virtuales (overlays) para facilitar la movilidad, segmentación y programabilidad a gran escala. El overlay utiliza el plano de control para mantener actualizado el mapeo de los endpoints a su ubicación de red, lo que mejora la escala y la convergencia. Esta solución permite la transformación de TI a través de la mejora de la visibilidad, la definición y aplicación de políticas basadas en grupos, la segmentación de red y la coherencia en las políticas de toda la empresa, desde los usuarios hasta las aplicaciones.

Infraestructura programable:

Implica dotar a los dispositivos existentes con capacidades avanzadas para permitir la gestión del ciclo de vida completo basado en estándares abiertos. Esto significa que se deben utilizar herramientas y tecnologías que permitan la automatización y la orquestación de las diferentes fases del ciclo de vida de los dispositivos, desde la configuración inicial hasta la monitorización y el mantenimiento continuo. Esto asegura que la infraestructura pueda adaptarse rápidamente a las necesidades cambiantes de la empresa, lo que permite una mayor flexibilidad y agilidad en la gestión de la red.

10.2 Lecciones Aprendidas

La realización de este Trabajo de Fin de Grado ha supuesto una gran cantidad de esfuerzo y dedicación. Es una tarea compleja que me ha obligado a adquirir conocimiento de los conceptos y tecnologías asociadas a esta solución de red.

He tenido que montar un mini-laboratorio para poder desplegar y experimentar con diferentes aspectos de SD-Access, incluyendo la configuración de políticas, la provisión de dispositivos y la resolución de problemas con la asistencia de Cisco DNA Assurance.

En el despliegue del laboratorio también se ha contemplado las herramientas que se utilizan en SD-Access, como Cisco Identity Services Engine (ISE) y Cisco PxGrid. La integración de estas herramientas es esencial para el correcto funcionamiento de SD-Access y para asegurar la identidad y la política de automatización.

La documentación de esta solución por parte del fabricante Cisco es bastante conocida y de fácil acceso, por lo que no ha sido complicado documentarse y poder desarrollar este TFG.

11. Anexos

11.1 Acrónimos

SDN	Software Defined Network
DNA	Digital Network Architecture
ISE	Identity Services Engine
CT	Cuarto Técnico
QoS	Quality of Service
WLC	Wireless Lan Controller
NAC	Network Access Control
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
BoM	Bill of Materials
VN	Virtual Network
SGT	Scalable Group Tag
API	Application Programming Interface
MAB	MAC Authentication Bypass
VLAN	Virtual Local Area Network
VTEP	VXLAN Tunnel End Point
LISP	Location Identifier Separation Protocol
EID	Endpoint ID
RLOC	Routing Locator
SGACL	Security Group Access Control List
LACP	Link Aggregation Control Protocol
OOB	Out of Band
CIMC	Cisco Integrated Management Controller
NIC	Network Interface Card
CAPWAP	Control and Provisioning of Wireless Access Point
STP	Spanning Tree Protocol
FHRP	First Hop Redundancy Protocol
ECMP	Equal Cost Multi-Path
IS-IS	Intermediate System to Intermediate System
PIM-ASM	Protocol Independent Multicast – Any Source Multicast
PIM-SSM	Protocol Independent Multicast – Source Specific Multicast
BFD	Bidirectional Forwarding Detection
IETF	Internet Engineering Task Force
NTP	Network Time Protocol
CLI	Command Line Interface
SNMP	Simple Network Management Protocol
RF	Radiofrecuencia
DMZ	Demilitarized Zone
FEW	Fabric Edge Wireless
SSID	Service Set Identifier
HTDB	Host Tracking Database
HA-SSO	High Availability – Stateful Switchover)
HA	High Availability
VNID	Virtual Network Identifier
CoA	Change of Authorization
EAP	Extensible Authentication Protocol
CDP	Cisco Discovery Protocol
LLDP	Link Layer Discovery Protocol

WoL	Wake-on-Lan
CBAR	Controller based application recognition

11.2 Glosario

LAN+WLAN. La LAN es una red de área local que se encuentra en una zona limitada como una oficina, edificio, escuela, etc. Una WLAN es una red de área local inalmámbrica.

Endpoint. Dispositivo o nodo final que se conecta a una red para enviar o recibir datos. Un endpoint puede ser un ordenador, un portátil, un servidor, un dispositivo móvil, una impresora, un escáner, un sensor, un dispositivo IoT (Internet de las cosas), o cualquier otro dispositivo conectado a la red.

Onboarding. Proceso de añadir dispositivos a la red existente para que puedan acceder a los recursos de la red de forma segura y eficiente.

Profiling. Proceso mediante el cual se trata de identificar y clasificar el tipo de dispositivo que se añade a la red, mediante atributos propios como el fabricante de la tarjeta de red (OUI) o el sistema operativo entre otros.

Posture. Proceso mediante el cual se verifica si el dispositivo que solicita acceso a la red o uno ya existente, cumple con los requerimientos de seguridad configurados (antivirus instalado, versión de firmware actualizado, BBDD del antivirus actualizado, etc)

Underlay. Infraestructura de red física.

Overlay. Es la capa lógica que trabaja sobre el underlay.

Border Node. Es la puerta de entrada/salida entre el Fabric de SDA y las redes externas. Es el responsable de encapsular y entregar el tráfico entre el Fabric y el resto de la red. Y también, tiene la función de traducir el contexto (mapeo e identidad de usuario / dispositivo) dentro del propio Fabric.

Control Plane Node. Sirve como una base de datos central, rastreando a todos los usuarios y dispositivos a medida que se conectan a la red del Fabric y mientras se desplazan. El Fabric control plane permite que los componentes de la red (switches, enrutadores, WLC, etc.) consulten esta base de datos para determinar la ubicación de cualquier usuario o dispositivo conectado al fabric

Intermediate Node. Son los dispositivos más simples en la arquitectura de fabric de SD-Access. Ayudan a completar la capa del underlay, aglutinando todos los uplinks de los Fabric Edge hacia los Border Nodes.

Edge Node. Son responsables de conectar los endpoints al fabric y de encapsular / desencapsular y reenviar el tráfico desde estos endpoints hacia y desde el Fabric. Los Fabric Edge Nodes operan en el perímetro de Fabric y son los primeros puntos de conexión de los usuarios y la implementación de la política.

InfoBlox. En el contexto de nuestro trabajo, la solución de la que hablamos es InfoBlox DDI, que es una Solución integrada de gestión de DNS, DHCP y dirección IP que proporciona una gestión centralizada de todos los aspectos de la asignación de direcciones IP y nombres de dominio.

Uplink. Conexión física (cable o fibra) de red, que se utiliza para enviar datos desde un dispositivo de una capa inferior hacia la capa superior (acceso, distribución,core)

Transceiver. Módulos o adaptadores que se emplean para añadir compatibilidad entre los diferentes tipos de conectores de cobre o de fibra.

Cisco Platform Exchange Grid (pxGrid). Es un marco de trabajo de seguridad para la integración de sistemas de seguridad en una red. Permite compartir información entre

diferentes plataformas con el objetivo de mejorar la visibilidad y la capacidad de respuesta ante las posibles amenazas.

Spanning Tree. Protocolo que funciona en el nivel de la capa 2 del modelo OSI y su principal objetivo es controlar los enlaces redundantes, asegurando el rendimiento de una red

TrustSec. es un mecanismo diseñado por Cisco que permite segmentar dinámicamente el tráfico de la red organizando los dispositivos terminales en diferentes grupos lógicos

Datasheet. es un documento en forma de sumario que contiene la descripción de las características de un objeto, material, proceso o programa de manera detallada

Peering BGP. Intercambio de tráfico entre dos dispositivos de red mediante el protocolo de routing BGP.

Subnetting. Es un proceso utilizado en redes de computadoras para dividir una red IP en subredes más pequeñas. Esto se realiza mediante el uso de máscaras de subred para definir el tamaño y el rango de direcciones IP asignadas a cada subred

DMZ. Es una zona o área desmilitarizadas en una red informática. En el contexto de redes, una DMZ es una subred separada y aislada que se encuentra entre la red interna (generalmente la red local) y la red externa (generalmente Internet). La DMZ actúa como una capa adicional de seguridad al proporcionar un espacio separado y controlado donde se ubican los servidores y servicios públicos.

Fabric Edge Wireless. Fabric Edge Wireless en Cisco SDA permite la integración de redes inalámbricas en la arquitectura de SDA, lo que proporciona una solución unificada para la conectividad tanto cableada como inalámbrica.

SSID. Un SSID es un nombre único que identifica una red inalámbrica. Cada red inalámbrica tiene un SSID asociado, que permite a los dispositivos móviles y otros dispositivos encontrar y conectarse a esa red específica.

VXLAN. Es un protocolo de red que se utiliza para crear redes virtuales overlay en entornos de centros de datos

mGig. Los puertos Multigigabit son compatibles con versiones anteriores de dispositivos de 100 Mbps y Gigabit estándares, y admiten conexiones de 2,5 Gbps y 5 Gbps y con cables anteriores de categoría 5E (CAT5e) y categoría 6 (CAT6).

uPoE. Acrónimo de Universal Power Over Ethernet, ha sido creado por Cisco. Este estándar es una versión actualizada del estándar IEEE 802.3at con el que se pueden utilizar los cuatro pares de cables para suministrar hasta 60 vatios de potencia, aumentando así el número de dispositivos compatibles.

Wake-on-Lan. Es una función y protocolo de red que permite encender o despertar de manera remota un dispositivo de red, como un ordenador, que se encuentra en estado de suspensión o apagado.

11.3 Listado de Imágenes

11.4 Listado de Tablas

11.5 Bibliografía

- http://librosnetworking.blogspot.com/2020/08/diseno-de-redes-corporativas.html
  [consultado el 03 de marzo de 2023]

- https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-data-sheet-cte-en.pdf
  [consultado el 03 de marzo de 2023]

- https://jesuseduardoespinoza.medium.com/introducci%C3%B3n-a-la-arquitectura-de-red-sda-de-cisco-sdn-3-34750db93186
  [consultado el 05 de marzo de 2023]

- https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/install_guide/2ndgen/b_cisco_dna_center_install_guide_2_2_3_2ndGen.html
  [consultado el 05 de marzo de 2023]

- https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/dna-center/214471-cisco-dna-center-3-node-cluster-high-ava.html
  [consultado el 05 de marzo de 2023]

- https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/tech_notes/b_dnac_sda_lan_automation_deployment.html
  [consultado el 06 de marzo de 2023]

- https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/EE/DG/ee-dg/ee-dg.html
  [consultado el 06 de marzo de 2023]

- https://www.lookingpoint.com/blog/sd-access
  [consultado el 07 de marzo de 2023]

- https://docs.netscaler.com/es-es/citrix-adc/current-release/networking/vxlans.html
  [consultado el 10 de marzo de 2023]

- https://www.cisco.com/c/dam/global/da_dk/assets/training/seminaria-materials/Software_Defined_Access_2017.pdf
  [consultado el 11 de marzo de 2023]

- https://es.scribd.com/document/390858793/REDES-VXLAN#
  [consultado el 11 de marzo de 2023]

- https://es.linkedin.com/pulse/protocolo-lisp-miguel-cejudo-lafuente
  [consultado el 11 de marzo de 2023]

- https://www.ciscopress.com/articles/article.asp?p=2992605
  [consultado el 12 de marzo de 2023]

- https://www.xerox.es/oficina/latest/SECFS-06S.PDF
  [consultado el 13 de marzo de 2023]

- http://librosnetworking.blogspot.com/2021/07/introduccion-cisco-trustsec.html
  [consultado el 13 de marzo de 2023]

- https://ccnadesdecero.es/spanning-tree-protocol-stp-como-funciona/
  [consultado el 13 de marzo de 2023]

- https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user_guide/b_cisco_dna_center_ug_2_2_3/b_cisco_dna_center_ug_2_2_3_chapter_01111.html#id_114499
  [consultado el 24 de abril de 2023]

- https://www.solutel.com/cisco-ise/#:~:text=CISCO%20ISE%20es%20un%20servidor,quiere%20acceder%20a%20la%20red
  [consultado el 24 de abril de 2023]

- https://www.cisco.com/c/es_mx/support/docs/cloud-systems-management/dna-center/215516-trustsec-whitelist-model-with-sda.pdf
  [consultado el 25 de abril de 2023]

- https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/index.html#~benefits
  [consultado el 25 de abril de 2023]

- https://www.cisco.com/site/us/en/products/networking/dna-center-platform/index.html#tabs-9e2187ae1d-item-8d800bd1e7-tab
  [consultado el 26 de abril de 2023]

- https://blogs.cisco.com/tag/software-defined-access
  [consultado el 27 de abril de 2023]