Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Diseño de una arquitectura SDN de datacenter distribuido en Organismo con varias sedes

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Enrique García Ramos

DIRECTORES: Felipe José Gil Castiñeira

CURSO ACADÉMICO: 2024-2025

Universidade Vigo

Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Diseño de una arquitectura SDN de datacenter distribuido en Organismo con varias sedes

Máster Universitario en Dirección TIC para la Defensa

Especialidad de Sistemas y Tecnologías de la Información /

Especialidad de Sistemas y Tecnologías de Telecomunicación

Universidad de Vigo

RESUMEN

Este trabajo aborda el diseño y despliegue de una solución SDN (*Software Defined Networking*) para la modernización de un *datacenter* con el objetivo de superar las limitaciones de las arquitecturas de red tradicionales, como la gestión descentralizada, la baja automatización y la falta de flexibilidad, proponiendo una solución que optimice la escalabilidad, la seguridad y la eficiencia operativa.

Se realiza un análisis detallado del marco teórico, contrastando las soluciones clásicas con las tecnologías actuales que aprovechan las ventajas de la virtualización, poniendo foco en la arquitectura SDN y los principales actores del mercado. A partir de esta revisión, se propone un diseño específico basado en Cisco ACI, que incluye tanto el plano físico como el lógico de la red, considerando un *fabric* extendido entre diferentes localizaciones geográficas. El proceso de creación de la solución cubre las fases de análisis, diseño, implementación y validación. Se abordan tareas desde la preparación inicial hasta la configuración avanzada de sus componentes clave, como el controlador y los nodos.

Las pruebas realizadas validan aspectos críticos como redundancia, rendimiento, escalabilidad y seguridad, demostrando que la solución cumple los requisitos planteados. Este enfoque no solo mejora la eficiencia y la gestión centralizada, sino que también facilita la integración con otros sistemas corporativos y garantiza la continuidad del servicio.

Finalmente, se concluye destacando las ventajas proporcionadas por SDN respecto a soluciones clásicas, como la automatización avanzada y la capacidad de respuesta a entornos dinámicos. Se presentan líneas futuras enfocadas en la incorporación de inteligencia artificial para optimizar aún más las operaciones de red, y en la expansión hacia entornos multinube.

PALABRAS CLAVE

Redes de centros de datos, SDN, virtualización, ACI, fabric *multisite*

AGRADECIMIENTOS

A mis padres y entorno más cercano, presentes y que nos miran desde arriba, porque ellos me han hecho como soy.

A mis tres niñas, que cada día me piden el último beso, esta vida es maravillosa gracias a ellas.

A mi trabajo y compañeros, por darme la oportunidad de mejorar cada día.

A mis compañeros de máster y director de proyecto, ha sido un placer retomar viejas amistades y ganar otras nuevas.

A todos, GRACIAS.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Introducción

En la actualidad, la transformación digital y el crecimiento exponencial en el uso de los datos han llevado a los centros de datos a afrontar desafíos importantes. La arquitectura de red tradicional, basada en modelos jerárquicos, se ha mostrado insuficiente para afrontar nuevas necesidades crecientes en cuanto a escalabilidad, flexibilidad y una gestión eficiente. Estas dificultades se ven acentuadas por la demanda de servicios más dinámicos, en un entorno empresarial globalizado y con la necesidad de garantizar una disponibilidad constante de los sistemas.

Las redes definidas por software (SDN, por sus siglas en inglés) han surgido como una respuesta innovadora a esta necesidad, que redefine la manera en que las redes son diseñadas, gestionadas y operadas. SDN separa el plano de control del plano de datos, permite centralizar la inteligencia de las redes y abre la puerta a una administración automatizada y más ágil. Este enfoque transforma las redes tradicionales en sistemas capaces de responder de una manera dinámica a las exigencias de los entornos tecnológicos más modernos.

Este proyecto se centra en la implementación de una solución SDN en un datacenter distribuido geográficamente, con el objetivo de modernizar una infraestructura previa de datacenter único. Esto permite no sólo modernizar una electrónica de red obsoleta, sino también aportar una inteligencia que integre herramientas de virtualización, segmentación avanzada y seguridad dinámica. Como resultado no solo se mejora la administración del sistema en su conjunto, sino que simplifica enormemente el despliegue de nuevos servicios, que pueden presentar una gran demanda en volumen de datos.

A través del uso de la solución del fabricante Cisco ACI, el proyecto se centra en diseñar y desplegar esta arquitectura SDN, garantizando la continuidad del servicio en un entorno distribuido, y estableciendo las bases para futuras implementaciones en escenarios más complejos.

1.2 Motivación para la realización de este trabajo

Este trabajo surge como respuesta a un caso real de un organismo que necesita una solución técnica que actualice la infraestructura de red de un *datacenter*, la electrónica de comunicaciones, y migre sus servicios en el momento en que este organismo planea expandirse a nueva sede.

La problemática es doble: se necesita proporcionar redundancia geográfica a la infraestructura de red del centro de datos de la empresa y solventar los inconvenientes de la arquitectura tradicional implantada, que además necesita ser renovada.

Este trabajo realiza una revisión de las características y condicionantes de una arquitectura jerárquica clásica de *datacenter*, como paso previo de un análisis más profundo de una solución SDN a partir de los equipos y soluciones disponibles por parte de los diferentes actores del mercado.

Para conocer el estado actual de la técnica se ha seguido una metodología consistente en recabar información disponible de fuentes abiertas, publicaciones y artículos académicos, que ha sido analizada, clasificada y seleccionada para la realización de esta memoria.

Una vez identificadas todas las alternativas para crear una solución, se realiza una propuesta concreta en base a las principales tendencias actuales, realizando un diseño de las capas física y lógica que permita su implantación solucionando todos los retos detectados por el organismo destinatario.

1.3 Objetivos

En primer lugar, se busca crear una infraestructura de red de un *datacenter* complejo garantizando la versatilidad y eficiencia. Para ello es necesario aprovechar las innovaciones más recientes vinculadas a las tecnologías de virtualización, que son un requisito imprescindible en cualquier *datacenter* actual. Se busca analizar y demostrar las enormes diferencias que hay entre una red tradicional de *datacenter* en comparación con una implementación automatizada y más "inteligente" de la infraestructura de red.

Se pretende mostrar como las redes tradicionales basadas en niveles son insuficientes para satisfacer los escenarios más complejos, siendo necesario disponer de las características de las más modernas redes definidas por software. Y la mejor manera, a criterio del alumno, es contrastar ambas opciones, hacer una revisión de los conceptos generales y de las principales características de estas redes inteligentes, e introducir diferentes opciones disponibles en el mercado. El objetivo final, desde esta **perspectiva general**, es mostrar los principales pasos y decisiones de diseño a seguir para implementar una solución comercial viable, de manera que se pueda validar el cumplimiento o no, de los beneficios de una red inteligente. Estos beneficios pasan por mejorar la automatización de la red, su administración, flexibilidad ante cambios, y opciones de escalabilidad ante nuevas necesidades.

Desde una **perspectiva más detallada**, el proyecto busca demostrar, con el despliegue realizado, que se cumplen una serie de características de bajo nivel que facilitarán no solo la gestión y mantenimiento de toda la infraestructura, sino un despliegue rápido de servicios ante una red cambiante, que responda rápidamente ante un fallo, y resulte en una disminución de costes operativos. Los objetivos más de bajo nivel son los siguientes:

- **Automatizar** la red, es decir, reducir la dependencia de configuraciones manuales en los equipos de red, mediante el uso de políticas centralizadas.
- Obtener una **vista centralizada** del rendimiento de toda la red, de sus equipos, así como de los distintas alarmas y avisos que puedan generarse.
- Mejorar la **seguridad** de la red mediante la configuración de políticas centralizadas, que puedan ser reutilizadas, y aplicadas de manera ágil a nuevos servicios, permitiendo la segmentación de redes cuando se requiera.
- Diseñar una red de fácil y rápida **actualización**, permitiendo hacer *upgrade* de versiones firmware de una manera sencilla, en toda la topología, que añadan funcionalidad o incrementen la seguridad.
- Mantener la **redundancia y alta disponibilidad** de equipos y enlaces, garantizando en todo momento la continuidad del servicio ante un mantenimiento programado, o simplemente un fallo hardware.
- Conseguir la **escalabilidad** suficiente, permitiendo al sistema crecer rápidamente si las aplicaciones o sistemas lo requieren (horizontalmente mediante la adición sencilla de hardware adicional, o verticalmente asignando más recursos).

- Permitir la rápida creación y configuración de **redes lógicas**, con independencia de la capa física que las soporta (por ejemplo, soportada por uno o **varios sites** geográficos diferentes). Además, debe permitir la **movilidad** de servidores o máquinas entre dependencias, sin impacto en el servicio de usuario, con una reconfiguración mínima.
- Aportar una solución **multisite** que sea segura, extensible a la nueva sede de la empresa.
- Soportar diferentes **dominios administrativos**, sobre la misma infraestructura física, de manera que esta pueda ser compartida por diferentes departamentos de la empresa, y cada uno de ellos mantenga su red lógica independiente. Una capa física compartida entre varios usuarios independientes, con aislamiento entre ellos.
- Debe ser una solución moderna, **interoperable** con otras tecnologías, y que **se integre** con el resto de los sistemas de todo tipo de la empresa (autenticación, *backup*, herramientas de monitorización, almacenamiento, virtualización, etc.).

Se ha consultado una bibliografía amplia en forma de artículos o documentos técnicos que resaltan las bondades y virtudes de SDN ([1] [2] [3] [4] [5] [6]), motivo por el cual se escoge esta tecnología para dar solución al dilema planteado.

1.4 Organización de la memoria

Esta memoria se organiza en capítulos que van desde los fundamentos teóricos de la tecnología hasta la validación de resultados y conclusiones.

En este primer capítulo se introducen los antecedentes, motivaciones y objetivos del proyecto. Estos objetivos se revisarán al final del trabajo para realizar una valoración de su grado de cumplimiento.

En el segundo capítulo, se presenta el marco teórico o estado del arte, donde se analizan los conceptos esenciales para poder comprender las redes definidas por software. Se explican las características de las arquitecturas tradicionales de datacenter y sus limitaciones frente a las crecientes demandas tecnológicas. Se introduce el concepto de SDN y se revisan las principales soluciones disponibles en el mercado, con un enfoque particular en las capacidades de Cisco ACI como solución SDN escogida. Este capítulo proporciona el contexto técnico necesario para comprender la solución que se plantea después.

El tercer capítulo está dedicado al diseño y despliegue de la solución SDN implementada con Cisco ACI. En él se describe el análisis de la situación inicial del datacenter y se establecen los requisitos necesarios para la implementación. Se presentan los diseños del plano físico y lógico de la red, así como los componentes esenciales como son el controlador y los nodos. También se describen aquellos elementos ajenos al ACI, como son la capa óptica o la red de nivel tres entre las sedes, necesarias para la solución SDN en su conjunto.

A continuación, el cuarto capítulo se centra en las pruebas realizadas y la validación de los resultados obtenidos. Se detalla el plan de pruebas desarrollado para evaluar aspectos como la facilidad de configuración del plano lógico, el rendimiento, la escalabilidad, la redundancia, la seguridad de la solución implementada o la integración con otros sistemas. Se analizan todos los objetivos planteados en el capítulo primero para valorar su grado de cumplimiento.

En el quinto capítulo se presentan las conclusiones del trabajo, demostrando si la solución SDN satisface los objetivos planteados y las necesidades del organismo. Se destacan los principales logros y beneficios de la solución implementada, que confirmen o no la eficacia de la arquitectura diseñada. Posteriormente se cierra el capítulo con la propuesta de unas líneas futuras.

Finalmente, la memoria incorpora las referencias bibliográficas empleadas, así como dos anexos que recogen el plan de pruebas seguido en el capítulo cuarto, y un glosario de términos técnicos utilizados.

2 ESTADO DEL ARTE (MARCO TEÓRICO)

El presente apartado comienza mostrando los conceptos clave que se consideran necesarios para poder entender la tecnología de las redes definidas por software. Posteriormente se dará una visión del porqué SDN, sus características, se verán diferentes opciones del mercado, y se cerrará el capítulo poniendo foco en una solución comercial concreta ampliamente utilizada en el entorno TI.

2.1 Conceptos tradicionales clave

Como paso previo a describir el estado del arte de una solución clásica de arquitectura de red en un *datacenter*, se revisan a continuación diversos aspectos que serán de utilidad para la comprensión de los sucesivos apartados.

2.1.1 Disponibilidad, redundancia, rendimiento y escalabilidad

La **alta disponibilidad** se refiere a la capacidad de un sistema para mantenerse accesible con la mínima interrupción posible, la mayor parte del tiempo, minimizando los tiempos de inactividad en caso de un fallo hardware o software. Se logra mediante la redundancia de los equipos y sistemas de respaldo, de manera que si un componente falla otro pueda ocupar su lugar, sin interrupción del servicio prestado.

La **redundancia** implica duplicar componentes críticos de un sistema o infraestructura (un enlace, servidor, fuente de alimentación de una máquina, etc.) para garantizar la continuidad del servicio en caso de un fallo. Aumenta la disponibilidad y fiabilidad del sistema, reduciendo el tiempo de interrupción.

La **escalabilidad** se refiere a la capacidad de un sistema para crecer, sin comprometer su rendimiento. Puede hacerlo principalmente de dos maneras. Una escalabilidad vertical consiste en aumentar los recursos del sistema existente (por ejemplo, añadiendo CPU, RAM o almacenamiento a un servidor). Una escalabilidad horizontal consiste sin embargo en añadir más recursos (en el mismo ejemplo, añadir más servidores para repartir la carga de trabajo).

La **latencia** es el tiempo que tarda un paquete de datos en viajar de un punto a otro de la red, de origen a destino. Puede ser más o menos importante según los requisitos de la aplicación o servicio. Por ejemplo, es muy importante en una aplicación que deba ejecutarse en tiempo real como una videollamada o una operación de trading financiero.

El RTT (*round trip time*) mide el tiempo de ida y vuelta, de manera que la latencia es la suma de ambos tiempos. Un RTT bajo es sinónimo de una comunicación rápida y eficiente, mientras que uno alto puede apuntar a largas distancias o a problemas de corte o congestión en una red.

La **calidad de servicio** (*QoS*) se refiere al conjunto de técnicas que se utilizan para gestionar y priorizar los diferentes tipos de tráficos en una red, asegurando que los servicios más críticos reciban un mayor ancho de banda. De esta manera se trata de garantizar que las aplicaciones más prioritarias cursen su tráfico sin interrupciones o degradación en la calidad del servicio que prestan, aún en casos de congestión de la red.

2.1.2 Redes y segmentación

Una LAN (***local Area Network***) es una red que conecta dispositivos dentro de un área geográfica limitada, como puede ser una oficina o edificio, permitiendo el intercambio de información a una u otra velocidad dependiendo de aspectos como el medio físico. El encaminamiento se realiza utilizando equipos de *switching* y *routing*.

Las topologías habituales para el despliegue de una LAN son en estrella, anillo o malla (*mesh*). Los medios de transmisión usados pueden ser cableados o inalámbricos, y los protocolos IEEE 802.3 (Ethernet) o IEEE 802.11a/b/g/n/ac (Wifi).

Una VLAN (***virtual LAN***) permite crear redes lógicas dentro de una misma LAN física. Las VLAN permiten segmentar el tráfico de la red para mejorar la seguridad. Cada VLAN se identifica con un único VLAN ID y se trata como una subred independiente, lo que permite que el tráfico de cada VLAN se mantenga aislado del tráfico de las demás. Esto se logra mediante el uso de etiquetas (802.1Q) en los paquetes de datos, que identifican a qué VLAN pertenece cada paquete. Las ventajas de una VLAN son, además de la segmentación y la seguridad (al reducir la propagación de amenazas entre segmentos de red), la flexibilidad pues equipos en diferentes ubicaciones físicas pueden pertenecer a la misma red lógica.

El protocolo ***Spanning Tree*** (STP) es un protocolo de red que garantiza una topología libre de bucles en una red Ethernet, que podrían causar tormentas de *broadcast* y degradar el rendimiento de la red. STP asegura que haya un único camino activo entre dos dispositivos en la red, al deshabilitar enlaces redundantes de manera lógica, mientras mantiene otros en estado de espera para ser activados en caso de fallo del enlace principal.

Ethernet VPN (**eVPN**, o *Ethernet Virtual Private Network*) es una tecnología de red que permite la extensión de redes ethernet a través de una infraestructura de red IP/MPLS. Es especialmente útil para interconectar diferentes centros de datos, pues permite extender la conectividad de capa 2 entre los sites geográficos, permitiendo que las VLAN se extiendan más allá de los límites físicos de una LAN. eVPN utiliza BGP (*Border Gateway Protocol*) como mecanismo para el intercambio de las rutas IP alcanzables en cada lado (nivel 3) y distribución de las direcciones MAC disponibles (nivel 2). Alguna de las características destacables de las eVPNs es que proporcionan aislamiento lógico entre diferentes redes al segmentar entre VRFs (V*irtual Routing and Forwarding*), soportan balanceo de carga *multi-homing* (varios enlaces activos), y son compatibles tanto con redes tradicionales como con redes definidas por software.

Para relacionar los conceptos previos, podemos decir que las redes LAN son la base de una red física, las VLAN nos permiten segmentar a nivel lógico esa red y organizar su tráfico, y STP asegura que estas topologías con múltiples switches estén libres de bucles y sean más estables. eVPN nos permitirá extender las redes LAN y VLAN a través de múltiples ubicaciones como puedan ser dos *datacenters*.

El siguiente concepto, VxLAN, se tratará en más detalle al ser un protocolo que se utilizará posteriormente en el despliegue de una solución definida por software.

VxLAN (Virtual Extensible LAN) es un protocolo de superposición de redes ideado para transportar tráfico de la capa de enlace de datos sobre la capa de red, concretamente tráfico ethernet sobre redes IP, empleando encapsulación MAC-in-UDP. VxLAN extiende la funcionalidad de las VLAN a través de redes de capa 3.

Inicialmente fue ideado para proveer los mismos servicios que una red VLAN convencional, aumentando la extensibilidad y la flexibilidad limitadas de este tipo de redes. Así, está diseñado para abordar muchos de los inconvenientes asociados con las VLAN tradicionales, específicamente:

- Mayor escalabilidad, en términos del número de segmentos de capa 2 soportados.
  Mientras que el estándar nos permite segmentar una red física en hasta 4096 VLAN, VxLAN puede escalar, mediante el uso de un ID de 24 bits, hasta 16 millones de segmentos individuales. Esto facilita la creación de redes virtuales en infraestructuras de gran escala y distribuidas.
- Permite la extensión de las fronteras de capa 2 a través de la capa 3 mediante el uso de encapsulación MAC-in-UDP.

VxLAN utiliza una cabecera de 8 bytes, consistente en un identificador VNID de 24 bits (*Virtual Network Identifier*) y un número de bits reservados.

En un entorno con VxLAN, los dispositivos que terminan los túneles VxLAN se denominan VxLAN *End Points* (VTEPs). Un VTEP es un dispositivo, virtual o físico, que mapea los *endpoints* a segmentos VxLAN, y realiza la encapsulación y desencapsulación.

Un VTEP consta de dos interfaces: una de capa 2 en el segmento LAN local (que se utiliza para conectarse directamente a los *endpoints*), y otra de capa 3 en la red de transporte IP (utilizada para encapsular las tramas de capa 2 en paquetes UDP, y enviarlos a la red de transporte).

En un entorno tradicional basado en IP, la dirección IP se utiliza para proporcionar información sobre la identidad de un dispositivo final, así como información acerca de dónde ese dispositivo final reside en la red. Una tecnología de superposición como VxLAN separa esencialmente estas funciones y crea dos espacios de nombres, uno para la identidad y otro para representar dónde reside ese dispositivo final.

En un entorno moderno, como el de redes definidas por software, VxLAN presenta ciertas ventajas que aportan cierta flexibilidad:

- Compatibilidad *multitenant*, donde múltiples clientes o usuarios pueden coexistir en la misma infraestructura de red física, sin interferencias entre ellos.
- Interoperabilidad con otros dispositivos o software de red, permitiendo integraciones con infraestructuras heterogéneas.
- En ciertas implementaciones puede utilizarse con protocolos de control como BGP-eVPN (Border Gateway Protocol - Ethernet VPN) para la distribución de información de reenvío de túneles, lo que mejora la escalabilidad y eficiencia de la red.

2.1.3 Seguridad

En este punto, y dado que será una funcionalidad importante en el caso de despliegue, se hará referencia al protocolo MACSEC (Media Access Control Security). Este protocolo se corresponde con el estándar 802.1AE del IEEE y define la forma de conectar dos equipos ("*hop-by-hop*") a nivel 2, garantizando la confidencialidad e integridad de los datos. MACSEC no incluye en su especificación el manejo de las claves y por tanto lo delega en otro protocolo, MKA (*MACsec Key Agreement*). MKA está incluido como parte del estándar 802.1xRev-2010 del IEEE y su propósito es proveer un método de descubrimiento de *peers* de MACSEC y negociar las claves para securizar el enlace. Es decir, gestionar de forma segura el intercambio de claves criptográficas entre dispositivos de red. Y lo hace autenticando los dispositivos y distribuyendo las claves de cifrado que protegerán los datos transmitidos en capa 2.

Se ha definido en el estándar tres formas para la generación de claves en su uso con MKA:

- Claves pre-compartidas (PSK).
- La clave maestra de sesión producto de una autenticación exitosa de EAP.

- Claves distribuidas por un servidor de claves de MKA.

MACSEC puede utilizarse en cualquier tipo de enlaces, es decir, sobre aquellos que conectan la electrónica de red como *switches* o *routers* (encripta el paquete entero salvo las MACs de origen y destino), o en aquellos enlaces que conectan a esta electrónica con dispositivos finales (un ordenador, teléfono, etc., donde se utilizaría un software como suplicante del propio protocolo).

Como se intuye por su nombre, MACSEC es encriptación de MAC sobre capa de enlace, y ofrece un cifrado en función de las velocidades de los puertos (1/10/40/100Gbps), de forma bidireccional y sin importar el tamaño del paquete, ejecutando la función de encriptación directamente sobre el puerto ethernet. Y no como otras opciones de encriptación, como IPsec, protocolo que típicamente está implementado sobre una plataforma centralizada ASIC optimizada para acelerar la encriptación, MACSEC está diseñado para no tener impacto en el rendimiento.

Por ejemplo, para un *router* con capacidad de mover terabits de tráfico, IPsec puede ser un cuello de botella y un factor limitante del ancho de banda máximo del dispositivo. Si ese *router* tiene una capacidad de tráfico multiterabit, y diez puertos 100 GEth requiriesen encriptación a capa 2, la solución con MACSEC ofrecerá 100 Gbps de encriptación AES-256 en cada puerto, bidireccional, sin importar el tamaño del paquete. De esta manera, el cifrado usando MACSEC será capaz de aprovechar todas las capacidades de ancho de banda del *router*, en cada uno de sus puertos.

Respecto a la aplicación de las políticas de MACSEC, estas son configuradas por interfaz o sub-interfaz, provocando que el link esté o no encriptado. Típicamente hay tres formas en cómo el interfaz participa en MKA / MACSEC:

- *Should-Not-Secure*: El switch no ejecuta MKA. Si otro dispositivo manda *frames* del protocolo MKA, estos son ignorados. El dispositivo de red envía y recibe solamente tráfico sin cifrar.
- *Should-Secure*: El switch intenta aplicar MKA, de manera que si el resultado es positivo el switch envía y recibe solamente tráfico cifrado. En caso de que MKA devuelva un *timeout* o falle, el dispositivo cursará el tráfico sin cifrar. Esta suele ser la opción por defecto.
- *Must-Secure*: El dispositivo de red intenta aplicar MKA. Si MKA da un resultado positivo, el switch envía y recibe solamente tráfico cifrado, pero en caso contrario, la conexión se marcará como insegura por fallo de autenticación y se cerrará la sesión, sin cursar tráfico. Tras un tiempo se reintentará el proceso.

2.2 Arquitectura de red clásica en un *datacenter*

2.2.1 Modelo de capas: Acceso, Agregación y Core

Llevamos más de veinticinco años con un modelo de arquitectura tradicional de *datacenter* que ha demostrado su eficacia, pero que ya no funciona con las necesidades actuales, puesto que los flujos de tráfico ya no son los mismos.

La arquitectura de red tradicional de un *datacenter* se organiza en tres niveles jerárquicos, que son las capas de acceso, agregación y *core.*

Es un modelo de separación por capas con funciones específicas, que permite simplificar el diseño y la gestión al tiempo que proporciona ciertas características de redundancia y escalabilidad. Lo primero por el uso de conexiones redundantes entre equipos para evitar puntos únicos de fallo. Lo segundo es posible desde el momento en que se pueden añadir nuevos switches en acceso o agregación para aumentar el número de servidores conectados, o la capacidad disponible.

Las tres capas, interconectadas, recogen el tráfico de los servicios, los agregan dentro del centro de datos, y una vez consolidados los cursan hacia el exterior, tal y como muestra la Figura 2-1.

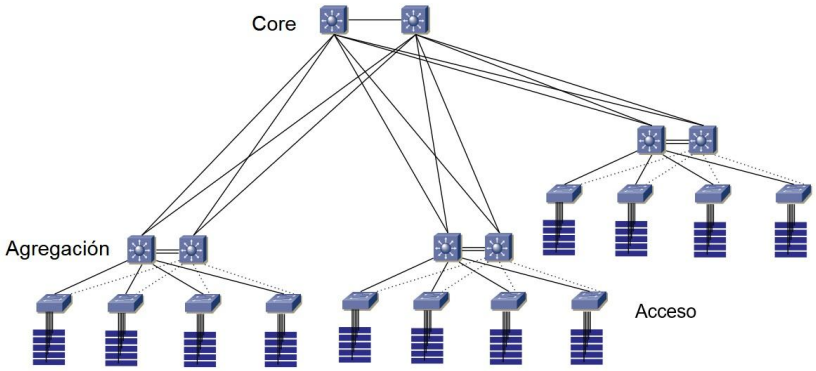

Figura 2-1 Arquitectura de *datacenter* tradicional en 3 niveles. Fuente: [7].

El nivel de **acceso** es el más próximo a las máquinas dentro del *datacenter*, y sirve para conectar los servidores a la infraestructura de red. Se realiza mediante la instalación switches de acceso que conectan directamente a los servidores, proporcionando un acceso de nivel 2 a la red, mediante la configuración de redes locales (LANs) o virtuales (VLAN).

Este nivel se caracteriza por ofrecer una gran cantidad de puertos de baja capacidad (habitualmente de gigabit ethernet), en interfaces eléctricas u ópticas, con distintos tipos de conector.

Esta electrónica de red, que conecta los servidores y cursa su tráfico hacia niveles superiores, permite una aplicación básica de políticas de seguridad.

La siguiente capa en la jerarquía, es la capa de **distribución o agregación,** entre la de acceso y la de núcleo. Este es el nivel en el que se consolida el tráfico desde los switches de acceso, y se enruta hacia el nivel superior. Aquí se encuentra habitualmente el nivel 3. Esta capa se caracteriza por:

- Una alta densidad de puertos de alta capacidad, para recoger los *uplink* de los switches de acceso.
- Utilizar conexiones redundantes hacia la capa superior.
- Alojar servicios de red como pueden ser *firewalls* o balanceadores de carga. Desde un punto de vista funcional suelen ejercer la función de frontera entre los servicios de nivel 2 y nivel 3 de la red.
- Consecuencia del punto anterior, suelen implementar políticas de enrutamiento, políticas de seguridad y de calidad de servicio (QoS).
- Facilitar por tanto la segmentación de la red (VLAN).

El siguiente nivel, superior en la jerarquía, es *backbone*, ***core* o núcleo**. Aquí se encuentran los equipos que proporcionan conectividad WAN al *datacenter*. Son los equipos responsables de interconectar el *datacenter* con las redes externas, de manera que esta capa hace de perímetro de acceso a la propia red interna del *datacenter*.

En esta capa el tráfico se transporta ya consolidado, por lo que equipos y enlaces presentan mayores anchos de banda, redundancia, y una baja latencia.

2.2.2 Problemática de las arquitecturas jerárquicas de DC

Si bien las arquitecturas tradicionales presentan una cierta modularidad, escalabilidad, o redundancia, ¿podemos tener un problema? Sea el caso en que conectamos hosts en la capa de acceso de tal forma que su tráfico agregado excede el que se puede cursar por sus enlaces externos, entonces tenemos un problema de sobresubscripción [7]. Altos ratios de sobresuscripción pueden ser razonables si tenemos mucho tráfico norte-sur (hacia una salida de Internet). No son razonables cuando hay mucho tráfico este-oeste, típicamente tráfico entre servidores en distinto rack, o aplicaciones distribuidas (tráfico SAN entre servidores y cabinas de almacenamiento, movimiento de máquinas virtuales que pasan de un servidor ESX a otro, *clustering*, etc.).

Las necesidades emergentes en el ámbito de las TIC evidenciaron además las carencias e **inconvenientes** de un *datacenter* tradicional:

- **Gestión descentralizada**, puesto que cada *switch* se configura individualmente, se vuelve compleja la gestión de los equipos y políticas, especialmente en *datacenters* grandes. Esto aumenta la probabilidad de errores humanos y complica la interoperabilidad entre equipos.
- La **baja automatización**, de manera que las tareas repetitivas, la configuración y el mantenimiento manual requieren un mayor tiempo, y genera un mayor coste operativo.
- Consecuencia del punto anterior, las políticas o el comportamiento de la red se ajustan de una manera **estática**. Esta **falta de flexibilidad** incrementa los tiempos de respuesta ante cambios en los requisitos de la red, o fallos, lo que supone un problema en entornos dinámicos y altamente escalables.
- Las políticas de seguridad se aplican de una manera más **rígida** en los diferentes elementos de red, en lugar de hacerlo de una manera más dinámica en función de los flujos de tráfico en tiempo real.
- Con grandes flujos de tráfico se pueden generar cuellos de botella, puesto que los **caminos están predefinidos** y pueden no ser siempre los más adecuados (por ejemplo, en flujos este-oeste entre servidores dentro del *datacenter*).
- La escalabilidad física no se traduce en una **escalabilidad lógica**, es decir, al añadir más switches en las capas de acceso o agregación, la red se vuelve más compleja y difícil de administrar, por el impacto en el *routing* y las políticas.

Otras desventajas de las redes tradicionales las descubriremos en el momento de afrontar la reconfiguración o migración de un servicio, ya que a la hora de **reconfigurar un servicio** nos enfrentaremos a un proceso más lento de lo deseado:

- Cualquier cambio como la implementación de una política de red, ajuste de enrutamiento, o activación de nuevo servicio, requiere configuración manual en múltiples dispositivos.
- A ser una gestión descentralizada no se dispone de una visión unificada de la red, lo que implica que esas reconfiguraciones a nivel de dispositivo deben coordinarse.

Al momento de realizar una **migración de servicios,** observaremos que esta:

- Es dependiente de la ubicación física del equipo: los servicios están vinculados directamente a la infraestructura física (servidores o switches específicos). Migrar un servicio a otros segmentos de red requiere reconfigurar manualmente direccionamiento IP, actualizar tablas de enrutamiento, y reconfigurar políticas de seguridad.
- Presenta una menor flexibilidad para tráficos este-oeste: La jerarquía tradicional está optimizada para tráficos norte-sur (cliente-servidor), y no tanto este-oeste (entre servidores), de manera que se pueden generar nuevos flujos horizontales y complicarse el proceso de migración.
- Exige un mayor tiempo y no permite reconfigurar y migrar servicios de manera dinámica, al no disponerse de una visión unificada de la red.

Y la situación no mejora en el caso de un ***datacenter* geográficamente distribuido**, entre varias localizaciones, pues encontraremos otras consideraciones adicionales o desventajas de las arquitecturas jerárquicas tradicionales:

- Las redes jerárquicas tradicionales no lidian bien con la **latencia** que se puede introducir entre servidores de ambas localizaciones (centros de datos), con la consiguiente degradación en el rendimiento de los servicios.
- La **sincronización de datos** entre localizaciones puede generar inconsistencias si las aplicaciones dependen de bases de datos replicadas o con almacenamiento distribuido. En una arquitectura tradicional, no existe un sistema centralizado que coordine estas operaciones de forma eficiente.

- Al mover servicios a otro *datacenter* lo habitual es que se generen nuevos flujos este-oeste entre servidores ubicados en ambos *datacenters*. Esto puede **saturar enlaces** de agregación o núcleo si no se dimensionan correctamente.
- Si se configuran diferentes redes de nivel 3 en ambos *datacenters*, será necesario enrutar entre ambos. Si los *datacenters* están conectados mediante redes de diferentes proveedores o tecnologías, puede ser más complejo **coordinar el enrutamiento** entre las regiones geográficas.
  En cualquier caso, pueden producirse nuevos flujos norte-sur, entre usuarios que se encuentren en una sede sobre un DC, que accedan a servidores ubicados en el DC remoto.

En conclusión, las arquitecturas jerárquicas tradicionales organizadas en los niveles de acceso, agregación y *core* han sido el estándar de la industria durante años. Sin embargo, estando diseñadas en base a caminos predefinidos y reglas estáticas, ven limitada su capacidad de adaptación por cambios dinámicos en el tráfico o la necesidad de nuevos servicios. Como se verá más adelante, las redes definidas por software han surgido como una respuesta a estas limitaciones.

2.3 Virtualización

2.3.1 Concepto y tipos de Virtualización

La virtualización es un proceso de abstracción lógica de una infraestructura física, para una mejor utilización de los recursos. Permite ocultar los recursos físicos reales de las aplicaciones, servicios o usuarios que los utilizan, proporcionando un entorno lógico o virtual que elimina la dependencia del sistema físico que subyace.

La virtualización se vale del software para crear una capa de abstracción sobre el hardware del sistema, lo que permite dividir sus componentes físicos (como procesadores, memoria y almacenamiento) en múltiples sistemas virtuales, conocidos comúnmente como máquinas virtuales (VM).

La virtualización permite:

- Mejorar la eficiencia de los recursos, al poder utilizar mejor la capacidad del hardware físico entre diferentes aplicaciones, que pueden correr cada una en su máquina virtual (VM) con su sistema operativo. Se reduce la infrautilización del hardware al compartir los recursos físicos.
- Realizar una gestión más sencilla. Al sustituir sistemas físicos por VMs definidas por software, se puede automatizar la configuración, definición y aplicación de políticas de seguridad.
- Reducir tiempos de inactividad. Es más sencillo configurar y/o ejecutar VMs redundantes en paralelo ante un error, que hacerlo con servidores físicos.
- Un aprovisionamiento más rápido que si hay que hacerlo con hardware.

Hoy en día la virtualización es una práctica habitual y extendida que no solo cubre escenarios presentes en un centro de datos, como la virtualización de servidores, sino que se extiende al ámbito de los usuarios finales. Otros muchos elementos de la infraestructura de TI se pueden virtualizar, los principales son los siguientes [8]:

- Virtualización de escritorio:
  - Permitiendo ejecutar en un mismo sistema varios sistemas operativos de escritorio, cada uno dentro de una máquina virtual.
  - Mediante la ejecución de un hipervisor en el sistema local.
  - Mediante una infraestructura de escritorio virtual (VDI), en que se ejecutan varios escritorios en máquinas virtuales que se encuentran en un servidor central, y se transmiten a los usuarios cuando inician sesión en un cliente ligero.

- Virtualización de red:
    - Esta es la que nos interesa en este trabajo, pues abstrae elementos y funciones hardware (por ejemplo, *switches*, *routers*, etc.) en un software que se ejecuta en un hipervisor.
    - El administrador utilizará la vista de red creada por software para gestionar la red desde una interfaz gráfica. Podrá modificar y controlar esos elementos de red sin manipular los componentes físicos subyacentes, lo que simplifica significativamente la gestión de la red.
    - La virtualización de red básicamente puede virtualizar los dispositivos hardware que realizan determinada función de red (NFV, como un *firewall*, un balanceador, etc.), o virtualizar el hardware mediante una capa software (plano de control) que la gestionará (SDN).
- Virtualización de almacenamiento:
    - Consolida los dispositivos de almacenamiento en una red, permitiendo gestionarlos como un único recurso. Mejora la asignación del almacenamiento a máquinas virtuales y optimiza el uso de los recursos.
- Virtualización de datos:
    - Ofrece un acceso unificado a los datos almacenados, a cualquier aplicación, independientemente del origen, el formato del archivo, o la ubicación donde se encuentre.
    - Se hace mediante una capa de software entre aplicaciones y almacenamiento, que traduce las solicitudes de datos, eliminando silos de información.
- Virtualización de aplicaciones:
    - Ejecuta un software de aplicación en el sistema operativo del usuario sin instalarla. Sólo la aplicación está virtualizada, no el sistema operativo del usuario (no todo el escritorio).
    - Básicamente puede ser de tipo local (la aplicación se ejecuta en el equipo del usuario), en modo *streaming* (la aplicación reside en un servidor que envía pequeños componentes software al equipo local para que se ejecuten), o basada en servidor (se ejecuta en el servidor y sólo envía la interfaz al cliente).
- Virtualización de centro de datos:
    - Abstrae el hardware de un *datacenter* en software, de manera que el administrador puede dividir el centro de datos físico, en varios centros de datos virtuales, y asignárselo a diferentes clientes.
    - Solución muy utilizada en entornos *cloud*. Es un modelo en el que el cliente accede a su propia infraestructura como un servicio (IaaS), habitualmente en modalidad de pago por uso.
- Virtualización de CPU:
    - Divide una CPU física en varias CPU virtuales para el uso por parte de las máquinas virtuales. En la actualidad no solamente está definida por software, sino que CPUs modernas incluyen un soporte hardware adicional.
- Virtualización de GPU:
    - Mismo concepto que el anterior, pero aplicado a la potencia de procesamiento gráfico de una GPU, para acelerar aplicaciones intensivas en gráficos como aplicaciones de vídeo, inteligencia artificial (IA), u otras.
    - Para uso de un único sistema operativo, o de diferentes máquinas virtuales.
- Virtualización del *cloud*:
    - Consiste en virtualizar los diferentes servicios del *datacenter* de manera que el proveedor de servicios puede ofrecer diferentes modelos de servicio *cloud* a un cliente. En función de hasta dónde llegue la parte gestionada por el

cliente/proveedor, tendremos un modelo que va desde un simple hosting, hasta un modelo de IaaS, PaaS o SaaS (servicio ofrecido por el proveedor más completo).

- IaaS, el proveedor es propietario de la infraestructura hardware y se la ofrece como servicio al cliente. El cliente controla los sistemas operativos, el almacenamiento y las aplicaciones desplegadas.
- PaaS, el cliente despliega las aplicaciones usando entornos de programación soportados por el proveedor, en la infraestructura *cloud* de este.
- SaaS, el cliente no controla ni la infraestructura *cloud* subyacente ni las aplicaciones, de manera que usa las aplicaciones del proveedor ejecutadas en el *cloud*.

2.3.2 Máquinas Virtuales e Hipervisor

Una **máquina virtual (VM)** es una emulación o representación de un equipo físico que utiliza software en lugar de hardware para ejecutar programas e implementar aplicaciones. Es una representación basada en software de un equipo físico.

Cada VM ejecuta su propio sistema operativo y se comporta como un equipo independiente, aunque se esté ejecutando en una parte del hardware del sistema subyacente real.

El sistema operativo que se ejecuta en una máquina virtual se denomina SO invitado. Cada máquina virtual incluye:

- Un archivo de configuración, que almacena los ajustes de la máquina virtual.
- Un archivo de disco virtual, que es una versión software de una unidad de disco duro.
- Un archivo de registro, que recoge las actividades de la máquina virtual, incluyendo su estoado, errores del sistema, cambios de hardware, migraciones de máquinas virtuales entre hosts, etc.

Un **hipervisor** es una capa software que interactúa con los recursos subyacentes de un *appliance* físico (llamado host) y asigna esos recursos a otros sistemas operativos (sistemas operativos huéspedes). En otras palabras, un hipervisor es la capa de software que gestiona las máquinas virtuales.

El hipervisor actúa como intermediario entre las máquinas virtuales y el hardware físico, asegurando que cada una tenga acceso a los recursos físicos que requiere. Además, separa los sistemas operativos invitados para evitar que las máquinas virtuales interfieran entre sí, afectando a su memoria o ciclos de procesamiento.

Existen principalmente dos tipos de hipervisores:

- Hipervisores de tipo 1, o "*bare-metal*", que interactúan directamente con los recursos físicos, reemplazando completamente al sistema operativo tradicional. Son comunes en entornos de servidores virtualizados.
- Hipervisores de tipo 2, que funcionan como aplicaciones sobre un sistema operativo existente. Su uso implica una mayor sobrecarga de rendimiento, ya que deben depender del sistema operativo del host para gestionar los recursos hardware asignados.

El hipervisor es, por tanto, un gestor de recursos virtuales, de manera que mediante una interfaz única se pueden configurar, administrar y supervisar los recursos virtualizados. Los recursos virtualizados pueden ser sistemas, redes, etc.

Típicos ejemplos hipervisores son VMware ESXi, Hiper-V de Microsoft, Citrix *hypervisor* (anteriormente conocido como *XenServer*) o KVM (solución de código abierto, parte del kernel de Linux). NSX de VMware, o ACI de Cisco son ejemplos de virtualización de redes.

2.3.3 NFV

Tradicionalmente, las funciones de red como *firewalls*, DNS, encriptación, NAT, etc. se han implementado utilizando hardware propietario en las instalaciones del cliente. Este enfoque es costoso por la variedad de hardware necesario, la necesidad de una instalación física en el site, y la dificultad ante las futuras y necesarias actualizaciones. Cada vez que se necesitaba agregar una función de red a un servicio era necesario desplazar a técnicos que instalasen ese hardware dedicado, con el consiguiente aumento de OPEX para la empresa.

Los proveedores de servicio comenzaron entonces a explorar formas de reducir estos costes y agilizar los despliegues de red. Así es como se llegó a la virtualización de las funciones de red (NFV).

NFV separa funciones como la de un *firewall* o un DNS del hardware dedicado y traslada esta función a servidores virtuales, como se muestra en la Figura 2-2. En lugar de instalar un hardware propietario más costoso, los proveedores de servicio pueden adquirir *switches*, almacenamiento y servidores, y ejecutar sobre estas máquinas virtuales (VMs) que realicen estas funciones de red. Al reunir diferentes funciones en un mismo servidor físico, se reduce el coste que inicialmente se tenía con el hardware dedicado. Además, en el caso de que se desee agregar una nueva función de red simplemente se levantará una nueva VM que realice esa función.

NFV se refiere por tanto a la estrategia de virtualizar funciones de red, cambiando diferentes elementos hardware de soluciones propietarias, por software que se ejecuta en servidores virtuales, corriendo sobre un hardware estándar (COT).

Un "virtual CPE" se refiere en general a cualquier función de red que se ejecuta en una VM.

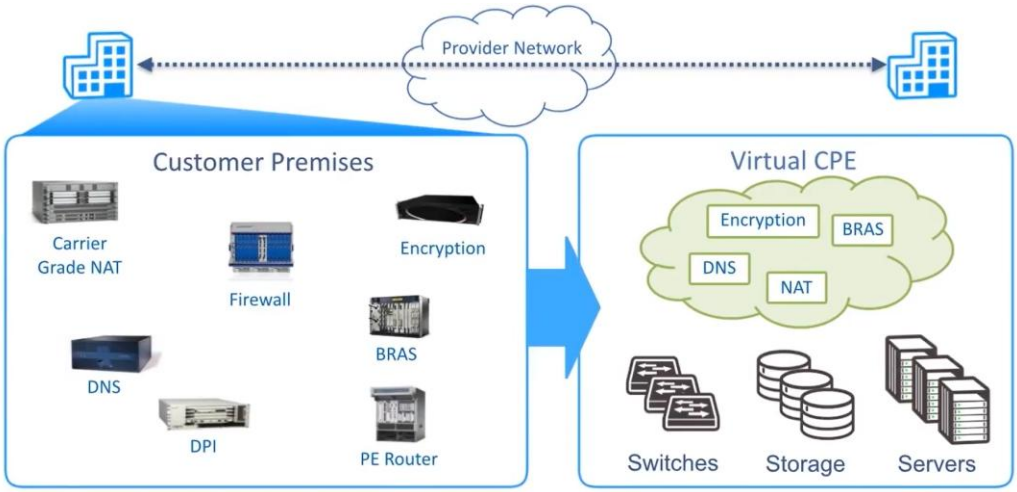

Figura 2-2 Concepto de NFV. Fuente: Ciena.

¿Y cómo se realiza el despliegue de estas funciones de red en el caso, por ejemplo, de una red con un par de ubicaciones geográficas (por ejemplo, con los elementos de red antes indicados en cada site, es decir, *firewall*, DNS y cifrado)? En lugar de instalar los dispositivos físicos en cada una de las dos ubicaciones, con NFV se puede instalar un servidor genérico en una de ellas y luego usar una plataforma estándar de virtualización de TI (como OpenStack o VMware) para configurar y levantar VMs con cada una de estas funciones de red. De esta manera el CPE físico es reemplazado por uno virtual, tal y como se aprecia en la Figura 2-3.

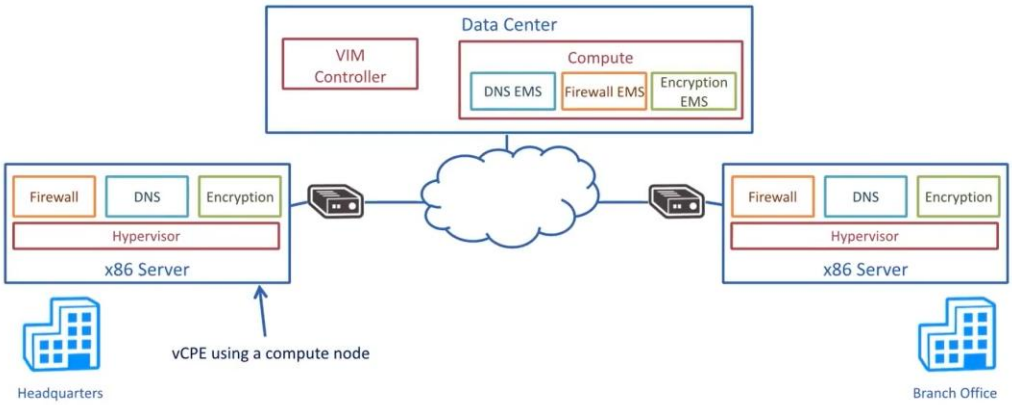

Figura 2-3 Despliegue de funciones de red. Fuente: Ciena.

El nodo de conmutación, o servidor que ejecuta las VMs, está compuesto por el software o hipervisor que administra las máquinas virtuales, y el resto de los recursos del nodo.

Un administrador de infraestructura virtualizada (VIM) administrará múltiples nodos de computación.

Para administrar las múltiples funciones de red se utiliza un software EMS, que a su vez también está virtualizado ejecutándose sobre un nodo del *datacenter*.

Un proveedor de servicios de red podrá disponer de múltiples centros de datos, sirviendo a múltiples clientes. Algunas funciones de red como el DNS tendrá sentido colocarlas en el centro de datos del proveedor, y otras como un *firewall* o el cifrado en las instalaciones del cliente.

También existe el concepto de NFV distribuida, lo que significa que se implementa en múltiples sites de una red del proveedor, ya sean sus centros de datos o instalaciones de clientes. Sea distribuida o centralizada (en el centro de datos), el orquestador es el elemento que crea y administra todas las instancias de recursos que se necesitan para desplegar un servicio. La orquestación permite a un proveedor de servicios crear flujos de trabajo que permiten gestionar de una manera automatizada los recursos necesarios para crear un servicio,

2.4 Tecnología SDN

2.4.1 Qué es SDN y cuál es su necesidad

En los últimos años, impulsado por la transformación digital, los usuarios han variado sus hábitos en el consumo de tecnologías digitales. Factores como el auge de los contenidos multimedia, el incremento en el uso de dispositivos móviles y la creciente necesidad de estar siempre conectados, han generado una demanda de redes más flexibles a nuevos servicios. Estas demandas han provocado patrones de tráfico a menudo impredecibles, con picos y variaciones en los recursos que necesitan. Esto ha dificultado que las arquitecturas de red tradicionales puedan adaptarse al ritmo requerido, haciendo evidente la necesidad de un enfoque de base que permita una escalabilidad más dinámica, y que no eleve el coste excesivamente.

Para abordar este desafío, se desarrollaron las redes definidas por software (SDN), que separan el plano de control del plano de datos. Esto permite que la red se configure automáticamente según los cambios en la demanda, optimizando su rendimiento y eficiencia.

La arquitectura SDN ofrece a los administradores la capacidad de gestionar y controlar el comportamiento de los elementos de la red mediante software, eliminando la necesidad de configuraciones manuales e individuales. Su principio clave es desacoplar la lógica de gestión de la red de la infraestructura física que la sustenta.

Dicho de otra manera, SDN es una nueva arquitectura de red, en la que de una gestión distribuida se pasa a una gestión centralizada. En el paradigma SDN tenemos separados ambos planos, control y datos, de manera que el primero se implementa de forma centralizada. El plano de datos consta de simples dispositivos de reenvío de datos y el plano de control incluye la figura del controlador [9].

Sin embargo, a menudo SDN se asocia con otra tecnología de virtualización de funciones de red (NFV) para flexibilizar la solución. Es necesario destacar la estrecha relación entre NFV (*Network Function Virtualization*) y SDN, e incluso con SDN-WAN en el caso de redes que incluyen varias ubicaciones, léase *datacenters*, conectados a cierta distancia.

No podemos hablar de un concepto sin mencionar al otro, motivo por el que en esta memoria se desarrollan ambos.

2.4.2 Conceptos de Overlay, Underlay, Fabric y APIs norte-sur

Para comprender SDN, y dado que se hará referencia al controlador, es útil familiarizarse con los conceptos de *Overlay*, *Underlay* y *Fabric* [10].

La capa ***overlay*** es una red virtual creada sobre la infraestructura física existente. Utiliza técnicas como túneles y encapsulaciones para establecer rutas lógicas entre dispositivos, lo que proporciona mayor flexibilidad y segmentación en la red. Entre los protocolos más utilizados en esta capa se encuentran VxLAN y GRE.

La capa ***underlay*** corresponde a la infraestructura física que ofrece conectividad básica entre dispositivos. Incluye elementos como *routers*, *switches* y enlaces físicos responsables de transportar el tráfico. Es fundamental que esta capa sea robusta y confiable.

El término ***fabric*** hace referencia a la arquitectura que integra las capas *overlay* y *underlay* en un solo sistema. Este enfoque permite una gestión centralizada y la orquestación de la red a través de un controlador SDN, ofreciendo un control detallado y una visibilidad completa de toda la red.

Para que la arquitectura SDN funcione de manera efectiva, es importante introducir los conceptos de interfaces norte-sur. Las APIs norte-sur son mecanismos que facilitan la comunicación entre las diferentes capas de la arquitectura SDN y los sistemas externos [10].

Las **APIs norte** conectan el controlador SDN con las aplicaciones de gestión y orquestación de red. Estas interfaces permiten la integración con herramientas de análisis, monitorización, seguridad y otros servicios. Por ejemplo, una API norte puede permitir que una aplicación de seguridad actualice en tiempo real las políticas de un *firewall*.

Por otro lado, las **APIs sur** permiten que el controlador SDN se comunique con los dispositivos de red situados en la capa inferior. Estas interfaces proporcionan un canal para enviar instrucciones y políticas a *routers* y *switches*. Un ejemplo de API sur es OpenFlow, que especifica como un controlador puede gestionar el tráfico interactuando con los dispositivos de red.

2.4.3 Arquitectura SDN

Una arquitectura SDN suele incluir tres capas principales, que son los planos de aplicación, control y datos (Figura 2-4).

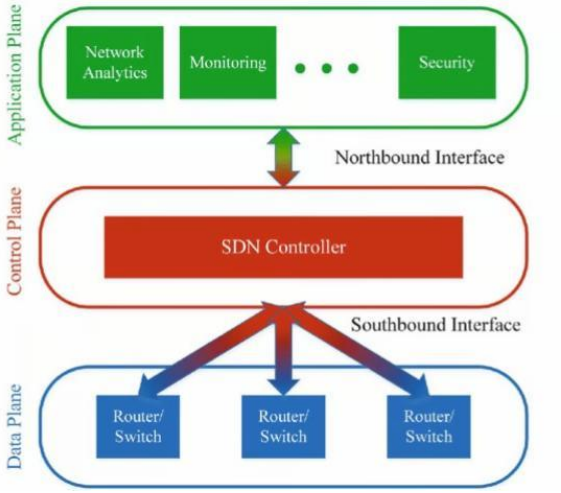

Figura 2-4 Planos en una arquitectura SDN. Fuente: [11].

El **plano de aplicación**, situado en lo alto de la arquitectura, es el que marca el comportamiento esperado de la red. En esta capa se incluyen aplicaciones, como las políticas de seguridad, herramientas para la gestión del tráfico, y la implementación de redes virtuales superpuestas.

El **plano de control** se encarga de decidir cómo se debe dirigir y gestionar el tráfico en la red, aplicando las políticas y reglas establecidas en el plano de aplicación. Su implementación se realiza a través de un controlador central que interactúa con los dispositivos de red situados en la capa inferior.

Las funciones del plano de control incluyen:

- Enrutamiento: determinar las rutas óptimas para el tráfico de red.
- Políticas de Seguridad: aplicar reglas de políticas de seguridad y acceso.
- Gestión de Tráfico: controlar la calidad del servicio (QoS) y la priorización del tráfico.

El **plano de datos**, también llamado de infraestructura, es donde se ubican los diferentes dispositivos o *appliances* físicos de la red, como pueden ser conmutadores y enrutadores. Son los dispositivos de esta capa los encargados de reenviar el tráfico a través de la red. Ejecutan las decisiones tomadas por el plano de control, realizando las siguientes acciones:

- Reenvío de los paquetes: transmiten los datos según las rutas establecidas por el controlador.
- Aplicar las políticas de seguridad y QoS determinadas por el plano de control.
- Monitorizar el tráfico, recogiendo estadísticas de rendimiento.

Para facilitar la comunicación entre los tres planos, de manera que la red funcione de manera coordinada, se definen las interfaces norte y sur.

Podemos diferenciar varios **modelos de arquitectura** en SDN, que encajan mejor o peor con los distintos tipos de infraestructura de red que podamos considerar. No es lo mismo la infraestructura de una pequeña empresa, con pocos dispositivos y una topología sencilla, que la de una gran empresa incluso con varias sedes. Para el primer caso puede funcionar bien una arquitectura SDN centralizada, y para el segundo caso mejor una que distribuya los recursos entre sus sedes.

En una arquitectura **SDN centralizada** las funciones de control y gestión, de todas las políticas y configuraciones, se reúnen en un único controlador central, que actúa como cerebro de la infraestructura en su conjunto. Este modelo permite a los administradores definir y gestionar la red de una manera sencilla, a pesar de que el controlador constituye un punto único de fallo, y presenta una escalabilidad limitada, entendida el número de equipos y flujos de red que puede gestionar.

En una arquitectura **SDN distribuida**, las funciones de control se reparten entre varios controladores, que trabajan en conjunto para gestionar la red, dividiendo esta responsabilidad. Cada

controlador gestiona una parte de la red, aumentando la flexibilidad, y se comunica con los otros para coordinar las decisiones de control. Necesitan por tanto una interfaz para compartir la información entre sí, que se denominan API en dirección este-oeste. Esta arquitectura mejora la escalabilidad, y elimina ese punto único de fallo mejorando por tanto la fiabilidad, pero a costa de añadir mayor complejidad a la gestión de la red. Los controladores tendrán que coordinarse, y en todo caso se introduce una latencia en la toma de decisiones, que dependerá en cierta medida del tamaño de la red.

Un modelo de arquitectura **SDN híbrida** combina elementos de las dos anteriores. En este caso se puede utilizar un controlador centralizado para realizar algunas funciones, mientras que otras se distribuyen en controladores distribuidos. Por ejemplo, el controlador centralizado puede gestionar las políticas globales, y los controladores distribuidos las políticas locales. El punto a favor es que presenta una buena escalabilidad y resiliencia, y se puede buscar un buen equilibrio entre centralización y distribución. Sin embargo, los controladores deberán coordinarse de manera eficiente, y en todo caso se añade complejidad a la implementación y gestión.

En una arquitectura **SDN superpuesta**, se emplean tecnologías de redes virtuales como VxLAN para construir una red lógica que opera sobre la infraestructura física ya existente. Esto permite a los administradores crear, ajustar o eliminar redes virtuales de forma sencilla.

En una arquitectura **SDN subyacente** (*underlay*), la infraestructura física de red sirve como base para soportar las redes virtuales superpuestas, conocidas como *overlays*. Estas redes pueden usar tecnologías como MPLS o el enrutamiento por segmentos para establecer enlaces virtuales entre los dispositivos de la red.

Ejemplo de soluciones SDN *underlay* son Cisco ACI (que proporciona conectividad física y soporte a las redes virtuales *overlay*), y Juniper Contrail (soporta las redes virtuales *overlay* y mejora la escalabilidad y fiabilidad de la red).

2.4.4 El controlador

En SDN el **controlador** es la aplicación software que se ejecuta en uno o varios servidores, y mantiene una visión global de la red. Es decir, desde un punto de vista lógico el controlador está centralizado, aunque a su vez pueda constar de múltiples controladores que puedan distribuirse físicamente.

Como se ha indicado, el plano de control toma las decisiones de enrutamiento del tráfico, y el plano de datos reenvía (Figura 2-5). Al centralizar la inteligencia de la red en el controlador, las SDN pueden adaptarse rápidamente a cambios en la demanda y optimizar el uso de los recursos de red. Esta arquitectura también facilita la automatización y la implementación de políticas de seguridad más robustas.

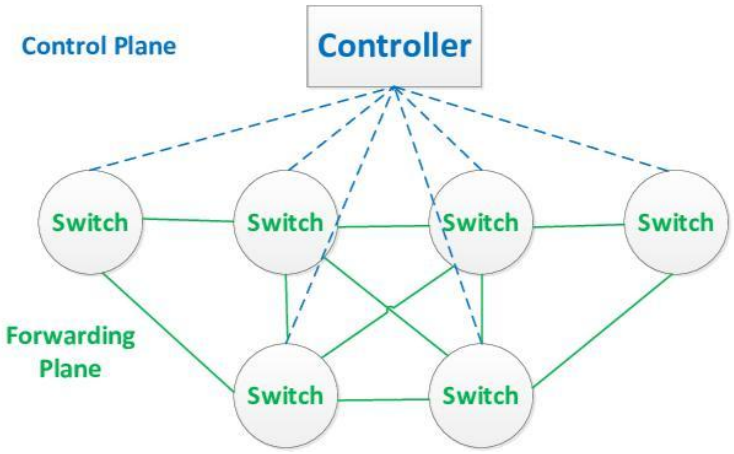

Figura 2-5 Planos de control y datos en SDN. Fuente: [11].

Este "cerebro" de la red interactúa con el "músculo", representado por los conmutadores, a través de una API de dirección sur. Esta API consiste en un conjunto de protocolos e interfaces que el controlador emplea para enviar órdenes a los conmutadores y recibir actualizaciones sobre su estado.

Asimismo, el controlador utiliza la API de dirección norte para conectarse con aplicaciones y sistemas de nivel superior que requieren acceder a la red.

2.4.5 Beneficios de SDN respecto a solución clásica

SDN se diferencia de las arquitecturas de red tradicionales en varias características clave:

- **Abstracción**: Se separa el plano de control del plano de datos, lo que permite modificar el comportamiento de la red de forma independiente a los switches y conmutadores.
- **Flexibilidad**: Es posible realizar cambios en la red sin necesidad de reconfigurar físicamente los dispositivos, lo que facilita a los administradores el poder adaptarse rápidamente a nuevas demandas.
- **Programabilidad**: La red puede gestionarse mediante API u otras herramientas de software, lo que simplifica la automatización de tareas y la integración con otros sistemas.
- **Virtualización**: SDN soporta la virtualización de recursos de red y la creación de redes virtuales, resultando especialmente útil en entornos con demandas dinámicas, como los entornos de nube.

En comparación con las redes tradicionales, la transición a una arquitectura SDN brinda varias ventajas:

- **Gestión centralizada**: Un controlador centralizado ofrece una perspectiva unificada de la red, lo que facilita tanto su administración como su mantenimiento.
- **Automatización**: La automatización de tareas repetitivas y complejas minimiza la probabilidad de errores y mejora la eficiencia operativa.
- **Visibilidad y control**: Las APIs norte-sur aseguran una gran visibilidad y un control detallado sobre los aspectos de la red.
- **Escalabilidad**: La red puede expandirse de forma dinámica sin que ello implique un incremento proporcional en la complejidad de su gestión.

Todo ello se traducirá en:

- Mejora de la eficiencia: Operaciones de red más rápidas.
- Reducción de costes: más rápido implica menos tiempo, y ahorro de costes.
- Mayor confiabilidad, la mejor visibilidad y automatización tienden a provocar una reducción en los errores humanos de gestión.

2.5 Principales actores SDN del mercado

En el contexto de transición tecnológica, desde la arquitectura tradicional de *datacenter* hacia SDN, diversos fabricantes han liderado la innovación en el mercado de SDN, desarrollando soluciones que abordan las necesidades emergentes de escalabilidad lógica, automatización y flexibilidad. Estos actores clave, como Cisco, VMware, Juniper Networks, Huawei, Nokia y Arista Networks, han adaptado sus soluciones a entornos empresariales y de *datacenter* distribuido, ofreciendo hardware especializado, software avanzado y enfoques diseñados para maximizar la eficiencia de las redes modernas.

A continuación, se presenta una descripción de las soluciones SDN que estos fabricantes han desarrollado, destacando sus principales características para transformar la infraestructura de *datacenter* hacia un modelo más ágil y dinámico.

2.5.1 Cisco ACI

Cisco es una empresa de origen estadounidense fundada en 1984, con sede en California, especializada en redes, telecomunicaciones y ciberseguridad. Con más de 80.000 empleados opera en más de 100 países, y tiene fuerte presencia en infraestructura de *datacenter* y entornos de nube.

Su solución recibe el nombre de Cisco *Application Centric Infrastructure* (ACI), y está enfocada a la simplificación de la operación del *datacenter* mediante políticas definidas por software y soporte multinube. Permite gestionar tanto entornos *on-premise* como híbridos, facilitando la automatización y el control de redes.

ACI utiliza un controlador centralizado llamado *Application Policy Infrastructure Controller* (APIC), con varias unidades en clúster, para crear y gestionar las políticas, y automatizar la configuración de la red.

Características clave de esta solución son:

- Políticas basadas en aplicaciones. Presenta un modelo en el que los flujos de tráfico se segmentan y configuran de manera centralizada, en base a políticas por tipo de aplicación, que denomina modelo *Application Centric*. Igualmente permite coexistir con un modelo tradicional denominado *Network Centric*, que facilita la migración desde arquitecturas tradicionales.
- Microsegmentación: Seguridad granular a nivel de grupos de aplicaciones. Cada grupo puede estar formado por diferentes *endpoints*, es decir, servidores físicos (corriendo en hardware específico) o máquinas virtuales, dentro de un grupo de aplicación.
- Políticas de seguridad centralizadas en base a lo que se denominarán contratos para permitir o denegar flujos de tráfico.
- *Multi-Site Orchestrator*: Gestión de múltiples *datacenters*, en base a diferentes topologías multi *site* que puedan darse en el entorno de empresa.
- Integración: Permite la integración con diversas aplicaciones y servicios, así como compatibilidad con servicios en la nube como AWS, Microsoft Azure o Google Cloud.

ACI utiliza un plano de control centralizado, y API RESTful, para integración con herramientas de automatización. El controlador se comunica con los switches conectados a los *endpoints* y les indica que creen los flujos de tráfico necesarios para permitir la comunicación.

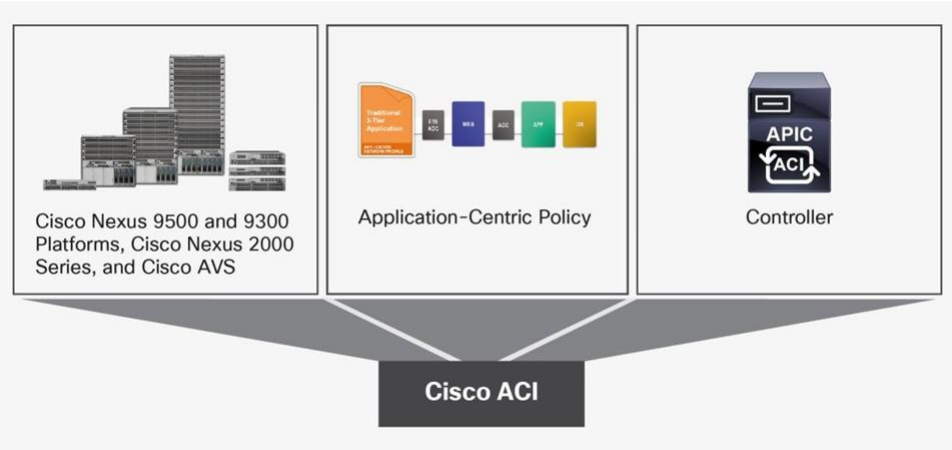

Figura 2-6 Elementos clave de Cisco ACI. Fuente: [12].

Los principales componentes hardware de Cisco ACI (Figura 2-6) son los switches Nexus de la serie 9000, y el controlador APIC. Los switches pueden formar parte de la estructura ACI, que llamaremos *fabric* ACI, a través de una variante del sistema operativo NX-OS que integran por defecto, llamada ACI OS. Están diseñados para soportar redes SDN mediante VxLAN y eVPN.

Modelos de la familia Nexus 9000 (Figura 2-7) como Nexus 93108TC-FX, 93180YC-FX y Nexus 9336C-FX2 son ejemplo de equipos ampliamente utilizados. Más detalle en la web del fabricante en [13].

Figura 2-7 Equipamiento Nexus 9000 Series de Cisco. Fuente: [13].

Los equipos se organizan en una estructura jerárquica que se denomina de tipo *Leaf and Spine* (Figura 2-8). Dos son por tanto los tipos de switches de la arquitectura. Los equipos *Leaf* de la base realizan la función de acceso. Estos son los que proporcionan la conectividad a los servidores del *datacenter*. También integran el clúster de controladores APIC, y realizan la función de Gateway con otros elementos externos al *fabric* ACI, como puede ser un *firewall* u otro equipo de interconexión a un sistema externo. En un nivel por encima se encuentran los equipos *Spine*, responsables de la conmutación del tráfico entre nodos *Leaf*. Son los que realizan la función de distribución del tráfico.

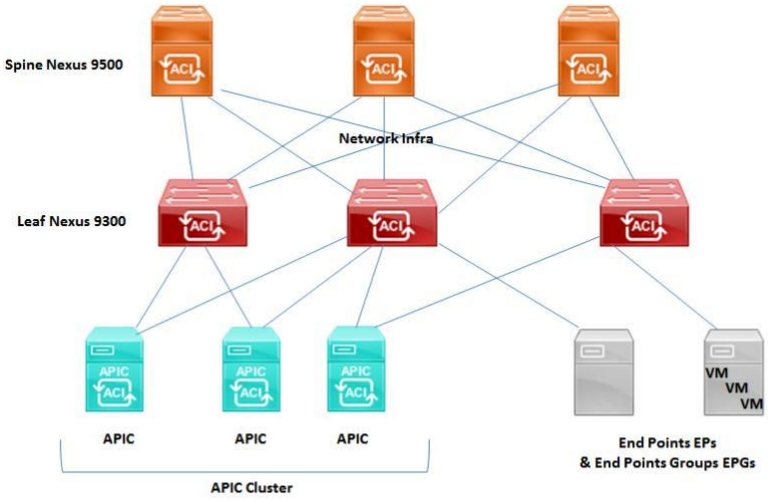

Figura 2-8 Infraestructura de Cisco ACI. Fuente: Cisco [14].

En el caso de una arquitectura con varias estructuras *Leaf* and *Spine*, que llamaremos Pods, algunos de los modelos Nexus 9K se configurarán con NX-OS en lugar de ACI-OS, para poder realizar una función de nivel 3 o *Inter Pod Network* (IPN). En este caso se tratará de una arquitectura más amplia, fabric extendido, entre diferentes sites o localizaciones geográficas. Se ampliará el detalle más adelante.

El controlador de la red (APIC) es el cerebro de la solución, se instala en un clúster de al menos tres unidades (recomendado), y es responsable de aprovisionar las políticas para los dispositivos físicos y virtuales, permitir flujos de datos, gestionar actualizaciones firmware de dispositivos, inventario, monitorización de alarmas y eventos, estadísticas de tráfico, etc. Entre otras características, el controlador APIC permite la integración con terceros, servicios de capa 4 a capa 7, e integración con VMware *VCenter*.

Para administrar la plataforma SDN, dos son las posibles interfaces de acceso: un CLI tradicional de estilo NX-OS y un acceso gráfico GUI basada en navegador, siendo este último el de uso recomendado. La GUI (Figura 2-9) está organizada para proporcionar navegación jerárquica a todos los componentes físicos y lógicos del sistema (descripción general de la GUI en la referencia [15]).

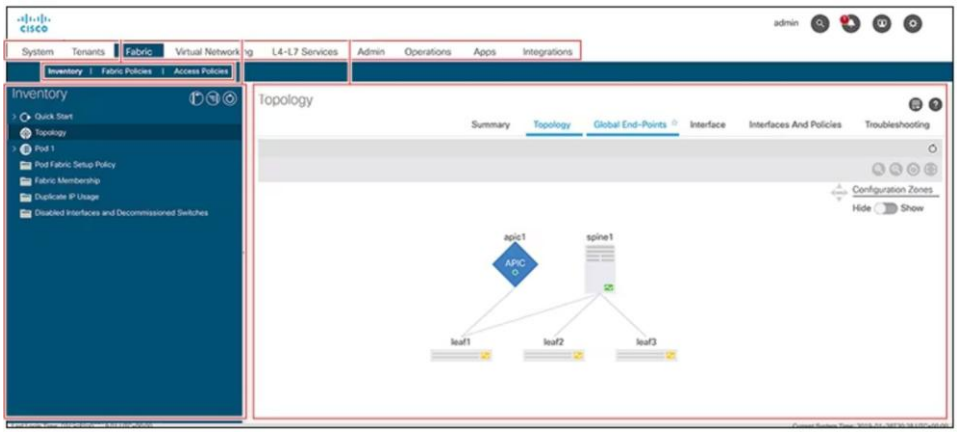

Figura 2-9 Interfaz GUI del APIC. Fuente: [15].

Cisco ofrece un simulador llamado "*Cisco Application Centric Infrastructure Simulator*" (disponible en [16]) que, sin necesidad de hardware físico, permite configurar una topología de red emulando los dispositivos, así como diseñar, configurar y probar políticas de conectividad y seguridad para diferentes escenarios. Igualmente facilita la integración con scripts y herramientas basadas en API REST.

2.5.2 VMware - NSX

VMware es una empresa estadounidense fundada en 1998, con sede en Palo Alto, California. En 2004 fue adquirida por EMC, que posteriormente sería absorbida por Dell Technologies en 2016. En diciembre de 2023 Broadcom completó la adquisición de VMware con objetivo de expandir su estrategia multinube, rebautizando la empresa como VMware by Broadcom.

La oferta de VMware en todo este tiempo ha sido muy variada. Vamos a realizar un breve recorrido hasta llegar a la solución de virtualización de red que más nos interesa.

Si inicialmente VMware Workstation 1.0 fue el primer producto comercial (que permitía a los usuarios ejecutar múltiples sistemas operativos como máquinas virtuales en un solo equipo), posteriormente se metió en el negocio de los servidores con los GSX y ESX servers. VMware ha sido tradicionalmente uno de los principales proveedores de servicios de virtualización con su plataforma de virtualización de servidores *vSphere*. Desde la última adquisición, Broadcom ha consolidado su oferta de producto en dos paquetes principales: *VMware Cloud Foundation* (VCF) y *VMware vSphere Foundation* (VVF).

Un componente importante de la solución VMware es el hipervisor ESXi, un *baremetal* centrado en la solución de *datacenter* (de tipo 1, es decir, reemplaza por completo el sistema operativo subyacente, y no se ejecuta simplemente como una aplicación). Es el sucesor del ampliamente utilizado ESX, servidor físico descontinuado de mayor tamaño.

Otro ámbito de negocio, en el que no profundizaremos, es la venta de software que virtualiza los sistemas operativos de escritorio (VMware Workstation Pro y VMware Fusion Pro), y la integración con escritorio virtual (VDI).

Como se ha indicado, tras la entrada de Broadcom la oferta comercial se concentró en el *Cloud Foundation* (VCF) y el *vSphere Foundation* (VVF). El primero es una plataforma de nube privada que proporciona una infraestructura hiperconvergente (HCI). Es el segundo es el orientado a la optimización de centros de datos en entornos *vSphere* tradicionales. A pesar de la simplificación la

plataforma, *vSphere* sigue estando disponible, siendo uno de sus componentes clave el VMware *vCenter*. *vCenter* es el componente de administración de *vSphere*, que permite asignar máquinas virtuales (VMs) a los hosts, les asigna recursos, monitoriza el rendimiento, automatiza el flujo de trabajo, y administra los privilegios de usuario en función de las políticas. Básicamente *vCenter* consta de:

- La interfaz de usuario, con un acceso por navegador para los administradores
- La Server *Database*, que almacena los datos para que los hosts de servidor ejecuten hipervisores y máquinas virtuales
- El *single sign-on*, que simplifica el acceso a toda la infraestructura de *vSphere*.

La mayoría de los usuarios empresariales necesitan más máquinas virtuales de las que puede albergar un único servidor físico. Para resolverlo VMware comparte recursos entre los hosts, agrupándolos en un clúster, que se tratará como una única máquina y, a continuación, utiliza la tecnología de agrupación en clústeres para agrupar los recursos hardware entre los hipervisores disponibles. Es decir:

- Un host es una máquina física que tiene VMware instalado y puede ejecutar máquinas virtuales.
- Un clúster es un conjunto de varios hosts interconectados entre sí. VMware agrupa estos hosts en un clúster para que, aunque haya varias máquinas físicas, se gestionen como una sola.
- De esta manera, los recursos de todos los hosts (CPU, memoria, almacenamiento, etc.) se combinan y gestionan de forma centralizada, lo que permite a VMware tratarlos como si fuera un solo sistema o servidor.
- En cada host del clúster se ejecuta un hipervisor, que es el software que gestiona las máquinas virtuales en ese host.
- Así, VMware puede compartir y distribuir los recursos hardware entre los diferentes hipervisores que están ejecutándose en los hosts del clúster.
- Esto significa que, si un host tiene más recursos disponibles, VMware podrá asignarlos a las máquinas virtuales que los necesiten, aunque se encuentren corriendo en otros hosts dentro del clúster.

De esta manera, se mejora el equilibrio entre las cargas de trabajo, se proporciona una alta disponibilidad, y mejora la tolerancia a errores (*vSphere* puede mover máquinas virtuales entre hosts físicos si detecta algún fallo hardware, facilitar el mantenimiento vaciando un host, etc.).

Como resultado de los años de experiencia en la virtualización de servidores, VMware decidió virtualizar y automatizar todo lo relativo al *datacenter*, mediante el concepto de SDDC, o centro de datos definido por software. Aquí es donde toma protagonismo NSX.

NSX es la solución SDN de VMware, plataforma de virtualización de red que proporciona una infraestructura SDN para y entornos de nube. Las principales características de esta solución son:

- Virtualización de la red: permite la creación de redes virtuales (VNs) de nivel 2 y 3, sobre la infraestructura física, desacopladas del hardware.
- Configuración y gestión automatizada de la red
- Microsegmentación, capacidad que permite aislar aplicaciones y cargas de trabajo a nivel de red.
- Escalado de soluciones multisite o entornos de nube.
- Integración con herramientas de automatización como *Terraform* y *Ansible*.

NSX no requiere hardware específico, puede ser suministrado por diferentes fabricantes. Opera sobre infraestructura ESXi o puede integrarse con switches físicos de otro fabricante compatible con VxLAN.

VMware NSX puede realizar funciones de red como la conmutación, enrutamiento, equilibrio de carga de tráfico, o *firewalls* en hipervisores que se ejecuten en equipos x86. Puede gestionar estas funciones conjuntamente desde una única interfaz, y aplicar políticas basadas en software para automatizar las funciones de red. La familia NSX ha evolucionado a lo largo del tiempo, tal y como se muestre en la Figura 2-10, para adaptarse a las necesidades de las redes definidas por software:

- En 2012, a raíz de la adquisición de la empresa de SDN Nicira, VMware lanza NSX, proporcionando una red SDN definida por software para centros de datos virtualizados.
- En 2013, enfocado en entornos *vSphere*, se lanza NSX-V.
  Esta versión ofrecía virtualización de red, microsegmentación y automatización de la red dentro de estos entornos. Sin embargo, estaba limitado a vSphere, lo que restringía su uso en otros hipervisores y plataformas.
- En 2017 se lanza NSX-T, como evolución del anterior, diseñado para soportar múltiples hipervisores y entornos de nube, con una arquitectura más flexible y escalable.
  Esta es la solución más reciente y avanzada de la familia NSX, que soporta múltiples hipervisores (*vSphere*, KVM, Microsoft *Hyper*-V), plataformas de contenedores (Kubernetes, Docker) y entornos de nube pública.

Figura 2-10 Evolución de la familia NSX. Fuente: [17].

Varios son los componentes clave de la arquitectura de NSX-T, distribuidos en las tres capas principales, que son los planos de administración, control y datos (Figura 2-11):

- Plano de Gestión:
  En el plano de gestión encontramos los *vCenter* y NSX manager en una relación de proporción.
  El NSX Manager es el controlador centralizado que gestiona la configuración y las políticas de la red. Proporciona una interfaz gráfica de usuario para la administración de la red. Instala agentes de usuario, VxLAN, genera certificados autofirmados para las capas de control y de datos, enrutamiento lógico distribuido, y módulos de *kernel* para *firewall* distribuido. Configura los hosts ESXi a través del agente de bus de mensajes.
- Plano de Control:
  El plano de control es la parte central de la arquitectura.
  El NSX *Controller* (en clúster) gestiona el plano de control, encargándose de la distribución de las políticas de red, y la gestión de la topología. Distribuye la información de *routing* a los ESXi, y mantiene tablas para direcciones VxLAN y MAC, así como las ARP.
  La máquina virtual NSX logical router participa de la implementación del routing dinámico (protocolos compatibles OSPF y BGP), de manera que recibe la información de enrutamiento necesaria a través de NSX Manager, y la reenvía al clúster de NSX controller, que la distribuye a los host ESXi.
- Plano de Datos:

El NSX Data Plane incluye los switches y enrutadores virtuales que implementan las políticas de red. Es donde se maneja el tráfico de datos, que seguirá cursándose incluso si las otras dos capas no funcionasen.
Los componentes de NSX se instalan directamente en el host ESXi a través del manager NSX, mediante el uso de unos paquetes de software VIB (*vSphere Installation Bundle*) utilizados en VMware para distribuir e instalar software, controladores, módulos o extensiones.
En el núcleo del hipervisor se instala de manera VIB el conmutador NSX o conmutador lógico, que es un conmutador distribuido estándar con funcionalidad adicional (VxLAN, DLR y *firewall*). VxLAN permite que el tráfico de red L2 pase a través de dispositivos de red L3, creando un túnel de red. El enrutador lógico distribuido (DLR) es parte de la red L3, que se instala en el ESXi para ser utilizado como Gateway por todas las VMs que aloja, mediante interfaces lógicas (LIF) con estas.
El único componente que no se instala como VIB sino como máquina virtual es la puerta de enlace Edge.
El NSX Edge proporciona servicios de enrutamiento (OSPF, BGP, estático), balanceador de carga, y seguridad en borde de la red (cortafuegos, VPN), permitiendo la conectividad entre diferentes segmentos de la red interna y hacia redes externas (funciones de retransmisión DHCP y DNS).

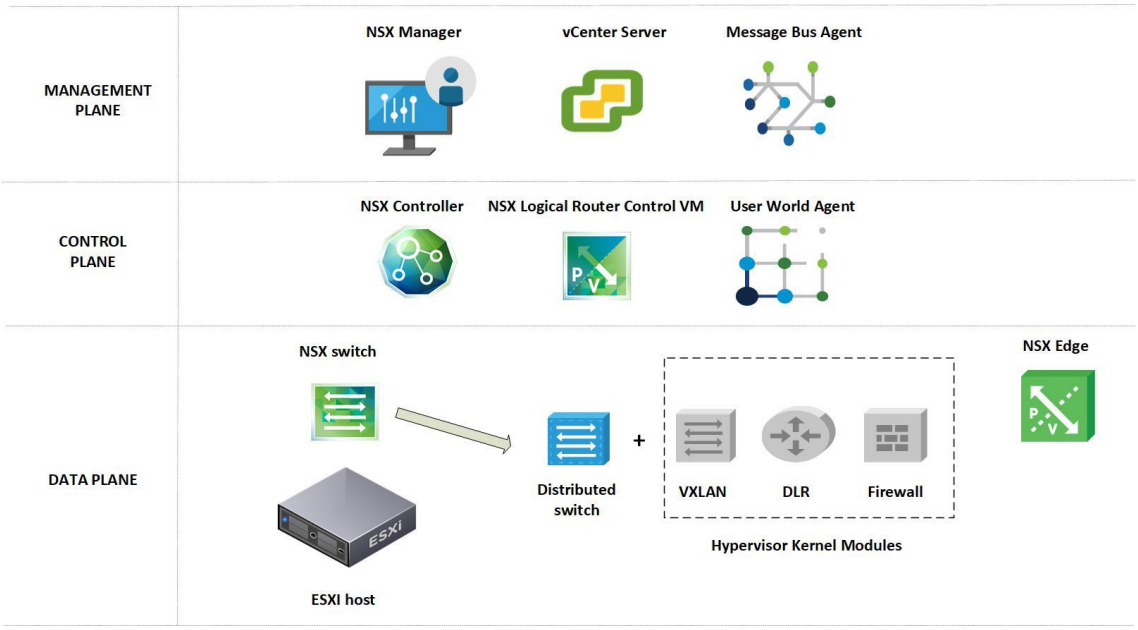

Figura 2-11 Arquitectura de VMware NSX. Fuente: [18].

2.5.3 Juniper Networks - Contrail

Juniper Networks es una multinacional estadounidense fundada en 1996, con sede en Sunnyvale, California. Especializada en soluciones de redes, ofrece equipos como *switches*, *routers* y soluciones SDN para centros de datos y telecomunicaciones. Cuenta con más de 11.000 empleados y tiene presencia global en más de 50 países y 120 localizaciones. Su enfoque principal está en la automatización, seguridad y rendimiento de redes avanzadas [19].

Contrail de Juniper Networks (Figura 2-12) es una solución de redes definidas por software (SDN) que automatiza la creación y administración de redes virtuales. Esta solución permite conectar, aislar y proteger cargas de trabajo en nubes privadas y públicas. *Contrail* está integrada con plataformas como *OpenStack*, *OpenShift* y Kubernetes, ofreciendo una orquestación híbrida de SDN. [20]

Es una buena opción para entornos multinube compartidos por múltiples usuarios, siendo esta una de sus dos principales aplicaciones:

- Entornos multinube (nubes privadas y públicas)
- Entornos de centros de datos, automatizando la configuración y gestión de su infraestructura.

Características principales de la solución Contrail con las siguientes:

- Redes Cloud-Native: está diseñado para integrarse de manera nativa en nubes privadas y públicas, con contenedores, donde integra cargas de trabajo virtualizadas. Soporta la integración de Kubernetes y *OpenStack*.
- Automatización basada en *NetOps*, ofrece la infraestructura como código.
- Seguridad, proporciona capacidades avanzadas de seguridad ofreciendo microsegmentación, encriptación y seguridad en las capas 4-7 para aplicaciones nativas en la nube. Permite la creación de cadenas de servicios que integran funciones de red virtualizadas y físicas.
- Ofrece la capacidad de gestionar múltiples clústeres y su federación, pudiendo escalar a miles de nodos.
- Monitorización en tiempo real, a través de una interfaz gráfica web que permite la visualización y gestión en tiempo real de la infraestructura de red.

Como solución SDN cuenta con un controlador e interfaz como principales componentes, con las siguientes características:

- Controlador *Contrail*: es un software que corre en máquinas virtuales (VMs) y se integra con plataformas de orquestación como Kubernetes, *OpenShift* y *OpenStack*, gestionando la creación y administración de redes virtuales.
- Proporciona una interfaz centralizada, que permite gestionar las políticas de red, y facilita la orquestación de conectividad virtual en diversos entornos. Permite monitorizar el rendimiento de las aplicaciones y los elementos de la infraestructura.

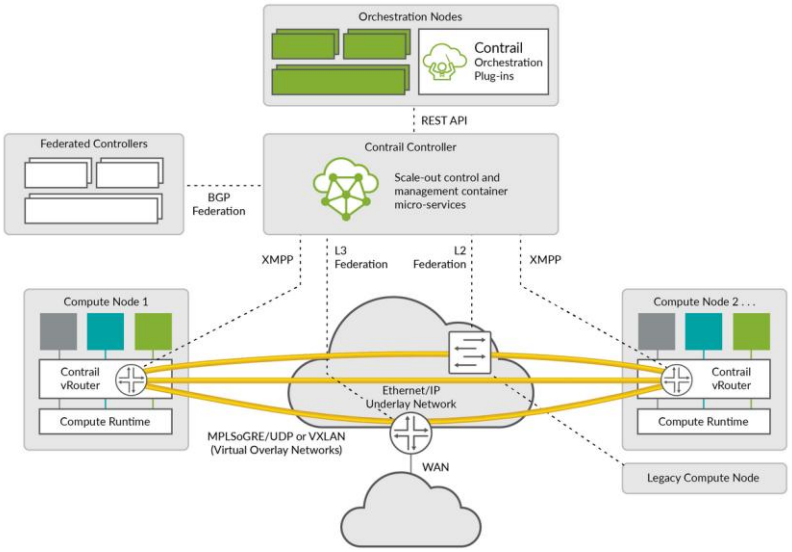

Figura 2-12 Arquitectura de Juniper Contrail Networking. Fuente: [21].

Entre los beneficios más obvios se encuentran la automatización (al eliminar la configuración manual de la infraestructura mediante la CLI de *JunosOS*), la escalabilidad (gestionando redes virtuales, políticas e instancias de computación sobre clústeres de hasta miles de nodos), seguridad (*multitenant* con cargas de trabajo aisladas) e integración (APIs) con sistemas de orquestación y herramientas de terceros.

La siguiente referencia ha sido utilizada y se puede consultar para ampliar la información en su extensa tabla de contenidos: [21].

2.5.4 Arista Networks - CloudVision

Arista Networks es una empresa estadounidense especializada en soluciones de redes para centros de datos y entornos de nube, que ofrece productos como switches y software de gestión de redes. Fundada en 2004, con sede en Santa Clara, California, Arista se destaca por su sistema operativo de red extensible (EOS) y su enfoque en la automatización y la visibilidad de la red. Es una empresa conocida en el campo de las redes definidas por software (SDN) y la virtualización de redes.

CloudVision es una plataforma de gestión de red multi-dominio orientada a servicios de red locales o en la nube, diseñada para ofrecer una gestión unificada de todo el ciclo de vida de la red, desde el diseño hasta las operaciones. A continuación, se detallan sus características y componentes principales, que también se muestran en la Figura 2-13:

Las principales características de esta solución son las siguientes:

- Arquitectura ofrecida tanto en implementaciones locales (físicas o virtuales), como nativa en la nube ofrecida como un servicio (SaaS).
- Automatización de las tareas, a través del módulo *CloudVision Studios*, para facilitar de una manera gráfica la provisión de los dispositivos, gestión de las configuraciones y control de cambios en la red, incluyendo actualizaciones y marchas atrás.
- Visibilidad centralizada mediante la supervisión del estado operativo de los switches físicos, que ejecutan EOS.
- Gestión de configuraciones, pudiendo organizar los dispositivos en jerarquías y realizar una categorización de los mismos por rol u otro parámetro.
- Mejora de la visibilidad del estado de la red mediante la transmisión de los estados de los dispositivos en tiempo real (telemetría y análisis de la red).

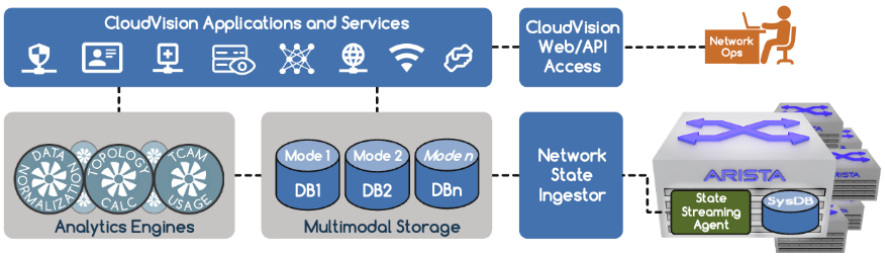

Figura 2-13 Arquitectura de Arista CloudVision. Fuente: [22].

Cloudvision está principalmente compuesta por:

- La arquitectura *NetDL* (Network Data Lake) que abstrae la red física, centraliza y consolida los datos de toda la red.
- El portal web de *CloudVision*, o interfaz gráfica que permite provisión, gestión y monitorización de la red y dispositivos (Figura 2-14).
- Una plataforma (CV UNO) que analiza y ofrece información sobre el rendimiento de aplicaciones y cargas de trabajo.
- APIs para integraciones tanto en dirección norte como sur.

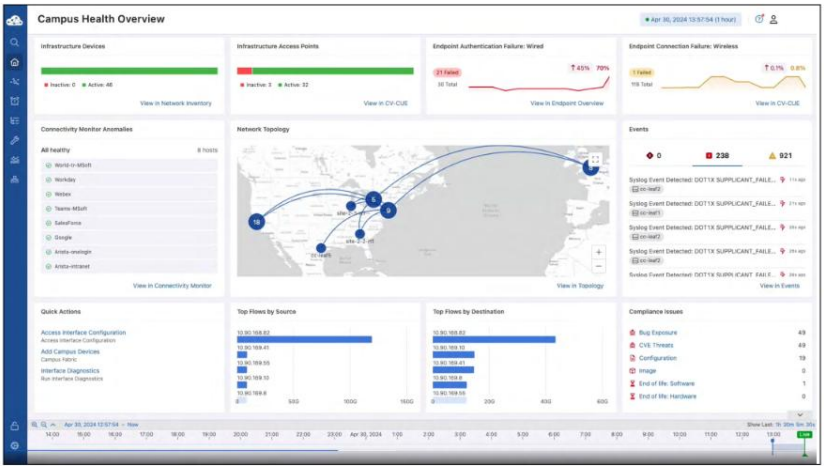

Figura 2-14 Portal Web CloudVision. Fuente: [22].

Las siguientes referencias han sido utilizadas para la redacción de este apartado, y le permitirán al lector ampliar la información sobre esta plataforma, con documentos originales del fabricante: [23], [24].

2.5.5 Huawei - CloudFabric

Huawei Technologies Co., Ltd. es una multinacional china de tecnología especializada en equipos de telecomunicaciones y electrónica de consumo. Fundada en 1987, con sede en Shenzhen, Guangdong, es uno de los principales proveedores globales de infraestructura de tecnologías TIC y dispositivos inteligentes. La empresa cuenta con más de 200,000 empleados y opera en más de 170 países. En la actualidad Huawei enfrenta restricciones en varios países del mundo debido a preocupaciones de seguridad, como Estados Unidos y algunos países de la Unión Europea, que han impuesto restricciones significativas o bloqueos a su participación en redes 5G. No así en el resto del mundo.

Huawei *CloudFabric* es una solución de red de centro de datos basada en redes definidas por software (DCN, Data Center Network), diseñada principalmente para entornos de nube pública y privada, así como servicios de hosting, orientado a facilitar el proceso de transformación digital de los clientes empresariales de los operadores.

Sus características principales son:

- Basada en las redes definidas por software, permite sinergias entre red y nube, pudiendo implementar servicios en este entorno.
- Ofrece conexiones de 100 Gbps de alta densidad, sobre una arquitectura de más de 5000 servidores.
- Presume de ser una arquitectura estándar y abierta, que facilita la integración con soluciones de código abierto.

Los componentes del *CloudFabric* (Figura 2-15) son [25]:

- El Controlador de red de centro de datos, *iMaster* NCE-Fabric, que gestiona los dispositivos de red.
- El orquestador Agile DCN, para centros de datos basados en SDN.
- Los switches *core* (*CloudEngine* 16800/12800)
- Los switches fijos (*CloudEngine* 9800/8800/7800/6800/5800) y virtuales (*CloudEngine* 1800V)
- La plataforma de análisis de red, *iMaster* NCE-*FabricInsight*, que detecta el estado de la red y el comportamiento de las aplicaciones en tiempo real.

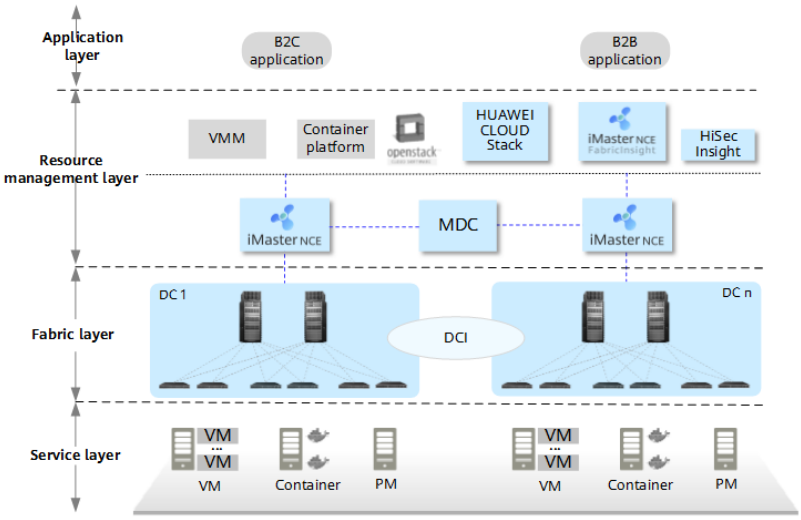

Figura 2-15 Arquitectura de Huawei CloudFabric DCN. Fuente: [25].

Como beneficios de esta solución, acorde a las características indicadas y por ser una solución SDN, destaca la automatización de los servicios, la orquestación de la red, la detección y análisis de fallos facilitada por la plataforma de análisis inteligente, y la posibilidad de ofrecer servicios de 100 Gbps.

Para ampliar la información se puede consultar el site del fabricante en la referencias: [25] y [26].

2.5.6 Nokia - Nuage Networks

Nokia es una multinacional finlandesa de telecomunicaciones y electrónica de consumo, fundada en 1865. Con sede en Espoo, Finlandia, siempre fue conocida por su innovación en redes móviles y soluciones de infraestructura. La compañía ha evolucionado desde la fabricación de teléfonos móviles hacia la tecnología de redes móviles y fijas, y servicios de telecomunicaciones, incluyendo 5G, Internet de las Cosas (IoT) y soluciones de nube.

Nuage Networks es una división de Nokia especializada en soluciones de redes definidas por software (SDN) y redes de área amplia definidas por software (SD-WAN). Ello le permite la automatización y orquestación de redes en entornos de centros de datos, nubes y WAN. Fundada en 2013 por Alcatel-Lucent fue adquirida en 2016 por Nokia.

Sus características más importantes son las siguientes:

- Automatización de toda la red, facilitando su gestión y operación.
- Ofrece tanto soluciones SDN como SDN-WAN, con diferentes grados de escalabilidad desde el centro de datos a nube privada y pública.
- Seguridad enfocada a las aplicaciones y los datos, basadas en el contexto y la identidad, de manera que las políticas de seguridad tienen en cuenta no solo la ubicación, hora o tipo de dispositivo que accede, sino también la identidad y rol de quien lo hace.
- Compatibilidad multinube, con la posibilidad de uso de distintas plataformas de manera unificada.
- Control centralizado de la red.

Los componentes principales (Figura 2-16) son los siguientes:

- La plataforma central de servicios virtualizados (VSP) que proporciona la automatización y orquestación de la red, red SDN o red SDN-WAN.
- Portal SD-WAN, para visualización y gestión de esta red
- El NSG, o dispositivo de acceso remoto con conectividad segura
- LA solución que integra SD-WAN con la seguridad en la nube (SASE)

La Plataforma VSP es la solución SDN que ofrece automatización basada en políticas a través de la red, desde el usuario hasta la carga de trabajo. A su vez sus componentes principales incluyen:

- un controlador de servicios (VSC) que es el cerebro de la red SDN (gestiona conectividad y políticas),
- un agente de servicios virtualizados (VSA) que aplica las políticas definidas por el VSC, y se encuentra implementado en los dispositivos

La parte de SDN-WAN se apoya en los servicios de red virtualizados (VSN)para conectar los centros de datos con las ubicaciones de las empresas cliente. La solución en su conjunto se muestra en la siguiente figura.

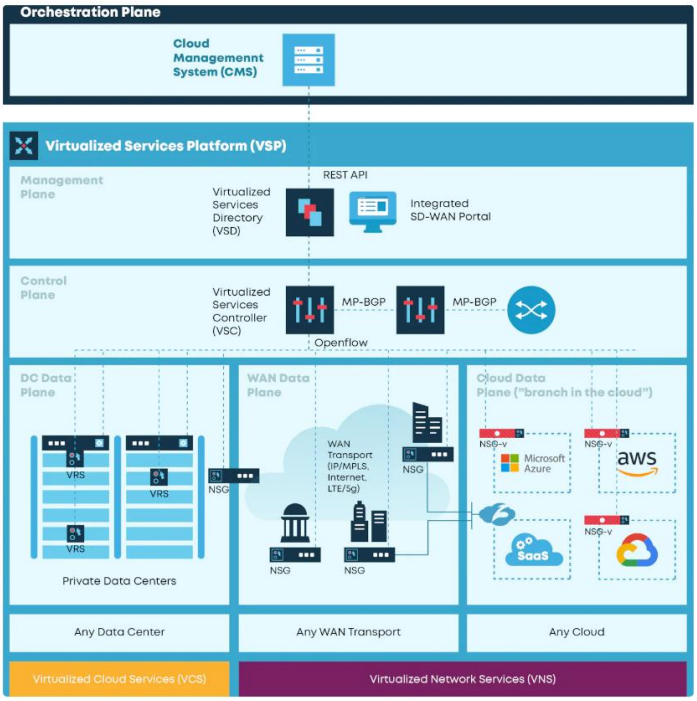

Figura 2-16 Arquitectura de Nokia - Nuage Networks. Fuente: [27]

Las siguientes referencias han sido utilizadas para la redacción de este apartado, y le permitirán al lector ampliar la información sobre esta solución: [27], [28].

2.5.7 Extreme Networks – Fabric Connect

Extreme Networks es otro fabricante de soluciones de redes definidas por software, cuya plataforma permite la gestión centralizada y programable de la infraestructura de red, separando el plano de control del plano de datos.

Extreme Networks, fundada en 1996, es una empresa estadounidense especializada en soluciones de redes para centros de datos y entornos de nube. En 2017 completó la adquisición del negocio de redes de centros de datos de Brocade, incorporando numerosos productos (como los switches VDX, MLX, SLX, CES, CER, Brocade *Workflow Composer y Automation Suites*), lo que fortaleció su posición en el mercado de las soluciones de centros de datos, enrutamiento y análisis.

La solución de Extreme está basada en SPB (*Shortest Path Bridging*), una implementación estandarizada del protocolo IEEE 802.1aq, diferente a la utilizada por las arquitecturas tradicionales. SPB utiliza el protocolo IS-IS para calcular rutas dinámicas en una red de capa 2 sin bucles, y con rápidos tiempos de convergencia. Permite la creación y configuración de redes Ethernet, incluyendo la virtualización y enrutamiento del tráfico.

Los principales componentes de la solución SDN son:

- Extreme Management Center (EMC), que es la plataforma software que permite la gestión centralizada y automatizada, así como la monitorización. Junto con el *ExtremeCloud* IQ (basada en la nube) se gestiona toda la red.
- *Extreme Fabric Connect*, o tecnología de red que permite la creación de una red virtualizada, facilitando la automatización y la segmentación. Sus principales características son las siguientes:
    - Un único protocolo (SPB) gestiona toda la infraestructura, sin necesidad de los habituales OSPF, STP, etc.
    - Automatización de los servicios y gestión centralizada. Se reducen las configuraciones manuales.
    - Aislamiento del tráfico mediante *Virtual Service Networks* (VSN), lo que aporta seguridad,
- *ExtremeAnalytics*, que proporciona información sobre el rendimiento y el uso de la red,
- Switches y *routers*, bien de la serie Extreme VSP o *Virtual Service Platform* (como los VSP 8600, VSP 7200, VSP 8400, con interfaces de 10/25/40/100 Gbps) o de series como la 5520 con soporte para *fabrics* -redes- extendidos (e interfaces a 1/10/25 Gbps).

Hay que tener en cuenta una debilidad de esta solución, relacionada con su particularidad SPB. Más allá de la dependencia del ecosistema de Extreme (aunque sea compatible con algunos estándares la compatibilidad completa requiere equipos específicos de Extreme), será necesario una curva de aprendizaje para implementar SPB.

Para más detalle pueden consultarse las referencias [29] y [30], que han sido utilizadas para la realización de este apartado.

2.5.8 Comparativa

Según se ha podido ver, diferentes fabricantes como Cisco, VMware, Juniper, Arista, Huawei, Nokia y Extreme Networks han desarrollado su solución SDN para infraestructura de red con enfoques diversos. Desde una plataforma basada en políticas y virtualización de una red en el entorno de un *datacenter*, hasta un entorno más amplio basado en nube, e incluso extendiendo su solución al ámbito de las redes WAN.

Se realiza a continuación un breve resumen para comparar sus principales características, fortalezas y debilidades, e identificar la mejor opción para el caso de despliegue que se realizará en un sucesivo capítulo.

- Cisco ACI: es adecuado para empresas con infraestructura previa de Cisco y que buscan un control de red basado en políticas. Destaca por su automatización avanzada y soporte global, pero depende de hardware propietario. Es una solución con gran presencia en el mercado, e interoperable.
- VMware NSX: está enfocada a la virtualización de redes, permite independencia del hardware y ofrece una gran seguridad. Como en el caso previo, de amplia implantación en la industria. Sin embargo, es costosa y puede ser compleja de integrar en entornos no VMware.
- Juniper *Contrail*: ofrece una solución abierta e interoperable que es apropiada para arquitecturas heterogéneas. Con menor presencia en el mercado, proporciona capacidades multinube y soporte para hypervisores.
- Arista *CloudVision*: recomendado para grandes centros de datos con un enfoque en escalabilidad y programabilidad. Sus APIs abiertas permiten flexibilidad, pero es más adecuado para entornos de gran escala.
- Huawei *CloudFabric*: competitiva en términos de coste-rendimiento, con capacidades avanzadas de analítica y automatización. Sin embargo, su integración con hardware no Huawei puede ser limitada. Hay que tener en cuenta los aspectos legales o normativos por

el país de origen de la compañía, en mercados como el europeo o americano. Esto puede condicionar un soporte técnico estable.

- Nokia Nuage Networks: es una solución completa que combina SD-WAN y SDN, ideal para redes distribuidas y multinube. Su implementación inicial puede ser compleja, pero destaca por su seguridad y flexibilidad.
- *Extreme Fabric Connect*: simplifica la gestión con un protocolo único (SPB), y es adecuada para empresas que priorizan la facilidad operativa y la seguridad. Sin embargo, depende del ecosistema de Extreme, y debe valorarse la necesaria curva de aprendizaje.

Fabricante	**Solución SDN**	**Características clave**	**Fortalezas**	**Debilidades**
Cisco	ACI	Controlador centralizado (APIC), integración con hardware propietario, enfoque en políticas.	Amplio soporte, automatización avanzada, integración con productos Cisco, altamente interoperable.	Dependencia del hardware Cisco.
VMware	NSX	Virtualización completa de red, compatible con entornos híbridos, aprovisionamiento rápido.	Permite independencia del hardware, fuerte integración con VMware *vSphere*, enfoque en seguridad granular.	Coste elevado, complejidad en la integración con terceros.
Juniper Networks	*Contrail*	Basado en *OpenContrail*, compatible con múltiples hypervisores, soporte multinube.	Integración sólida con arquitecturas existentes, interoperabilidad con estándares abiertos.	Menor presencia en el mercado, dependencia de configuración avanzada.
Arista Networks	*CloudVision*	Gestión centralizada basada en el estado, APIs abiertas, enfoque en redes abiertas.	Altamente programable, buena escalabilidad, integración en entornos heterogéneos.	Foco en centros de datos más grandes, requiere hardware compatible.
Huawei	*CloudFabric*	Enfoque en analítica de tráfico, switches de alta capacidad.	Escalabilidad alta, capacidades de automatización impulsadas por IA, buena relación coste-rendimiento.	Mayor complejidad en entornos no Huawei, restricciones políticas o regulatorias, soporte técnico regional variable.

Nokia	Nuage *Networks*	SDN para centros de datos y SD-WAN, soporte para conectividad multinube.	Integración fluida de red WAN y LAN, fuerte enfoque en seguridad, interoperabilidad en entornos diversos.	Implementación inicial compleja en redes pequeñas.
Extreme Networks	*Fabric Connect*	Basado en SPB, simplifica la gestión de red, soporta aprovisionamiento dinámico.	Reducción de la complejidad operativa, excelente aislamiento de tráfico, alto rendimiento.	Ecosistema dependiente del hardware Extreme, curva de aprendizaje para SPB.

Tabla 2-1 Comparativa de las soluciones SDN evaluadas Fuente: Propia.

Finalmente, para el caso de **despliegue concreto** que se desea implementar, se debe considerar que se prefiere una solución:

- Con amplia presencia y experiencia en el mercado.
- Que no requiere un soporte *cloud*.
- Que se desean evitar incertidumbres regulatorias.
- Que el coste aun no siendo condicionante sí es importante.
- Que necesita migrar sus servicios desde una arquitectura tradicional, implementada con equipos del fabricante Cisco.

Por lo anterior (Tabla 2-1 y consideraciones) la solución SDN de Cisco ACI es la escogida. Por este motivo se desarrolla a continuación en mayor detalle la tecnología SDN de este fabricante.

2.6 Solución SDN de Cisco ACI

2.6.1 Características

Cisco Application Centric Infrastructure, Cisco ACI, es la solución estrella de Cisco para los entornos de *switching* de *datacenter*.

Construido sobre la plataforma Cisco Nexus 9000, Cisco ACI utiliza un enfoque holístico basado en sistemas, con una estrecha integración entre hardware y software, entre elementos físicos y virtuales. Toma como base los principios de las redes definidas por software (SDN) para crear redes lógicas sobre una infraestructura o *fabric* físico.

Se basa en un modelo de abstracciones y presenta unas características que permiten una gestión robusta y más eficiente en los entornos de *datacenter*, de manera que permite:

- La separación física los planos de control y datos (*forwarding*).
- Gestión y supervisión centralizada del comportamiento de la red.
- Virtualización de la red para poder entregarla como un servicio, y su automatización para facilitar el despliegue de nuevos servicios.
- Programabilidad mediante API, permitiendo la interacción con otros proveedores, orquestadores, etc.
- Automatización de tareas, como la adición de nuevos equipos al fabric, que se autoconfiguran.

La solución de Cisco ACI para datacenter consta de los siguientes componentes:

- Cisco *Application Policy Infrastructure Controller* (APIC), que es el elemento que facilita la abstracción y permite independizar el plano lógico del físico.

- Switches Cisco serie Nexus 9000, con el rol que llamaremos de *Leaf* o *Spine*.
- Orquestador multi-site de Cisco ACI, que no será necesario en todas las implementaciones.

2.6.2 Arquitectura

La **arquitectura** SDN propuesta por Cisco para *datacenter* tiene como objetivo proporcionar una comunicación de baja latencia y alto ancho de banda entre cualquier punto de la topología (*fabric*), con independencia de la ubicación geográfica de sus componentes.

ACI organiza su arquitectura física en dos capas bien diferenciadas, la que provee la conectividad y la que realiza la conmutación. Permite la creación de un "*fabric* extendido" entre diferentes sites o *datacenters*, manteniendo un elevado ancho de banda y baja latencia, con independencia de la ubicación física de los equipos de red.

Esta arquitectura se denomina ***Leaf and Spine***, *fat-tree* o CLOS (Figura 2-17), y presenta las siguientes características:

- Topología "*fat-tree*" en dos niveles, que presenta menos saltos y baja latencia. Es una red CLOS de switches (*underlay*) que reduce el número de conexiones y cuyo número de saltos entre servidores es predecible (2 si están en el mismo *Leaf*, ó 4 en distintos: servidor-Leaf-Spine-Leaf-servidor).
- Se utiliza VxLAN para construir el *overlay*.
- La capa inferior de *Leafs*, es la que proporciona la conectividad a los servidores y resto de máquinas del DC, así como a los controladores de la solución SDN. Proporcionan los puertos.
- Los *Leaf* igualmente conectan los equipos externos al *fabric* ACI (como pueden ser *routers*, firewalls u otros dispositivos L4/L7), en cuyo caso de denominan Border Leaf. Constituyen los puntos de entrada y salida del *fabric* con el exterior.
- Se recomiendan equipos especialmente dedicados a la función de Border Leaf, aunque el despliegue no impide que un mismo *Leaf* realice las funciones de *Server* y *Border*.
- La capa superior de *Spines* realiza la conmutación, cursa el tráfico entre equipos *Leaf*.
- Tráfico con origen y destino en el mismo *Leaf* se maneja a nivel local, el resto del tráfico se reenvía desde el puerto de entrada en el *Leaf* origen hasta el puerto de salida en el *Leaf* destino, a través de la capa *Spine*.
- Cada equipo *Leaf* se conecta a los equipos *Spine*. No hay conectividad física directa entre equipos *Leaf*. De manera similar tampoco hay conectividad directa entre equipos *Spine*.
- Cisco recomienda un despliegue de la arquitectura basado en parejas. Es decir, tanto los *Leaf* como los *Spine* se instalan y cablean al resto de la arquitectura en pares. Esto permitirá grandes ventajas.
- Se recomienda que la conexión de un servidor o máquina del DC se realice contra una pareja de *Leaf* (si el servidor lo permite). La conexión en vPC (*virtual port channel*) a dos *Leaf* no solo permitirá balancear el tráfico o dar redundancia a la máquina (depende de su configuración), sino que, en caso de fallo de un *Leaf*, el tráfico podrá cursarse igualmente.
- De manera similar, los *Leaf* se conectarán a la pareja de equipos *Spine* del nivel superior, de manera que ante el fallo de un equipo *Spine* el tráfico se podrá cursar hasta destino.
- No solamente por fallo o incidencia, sino por operaciones de mantenimiento programadas, una conectividad en parejas permitirá estos trabajos programados (por ejemplo, actualización de firmware en los equipos del *fabric*), sin afección a los servicios (interrupción o corte del tráfico).

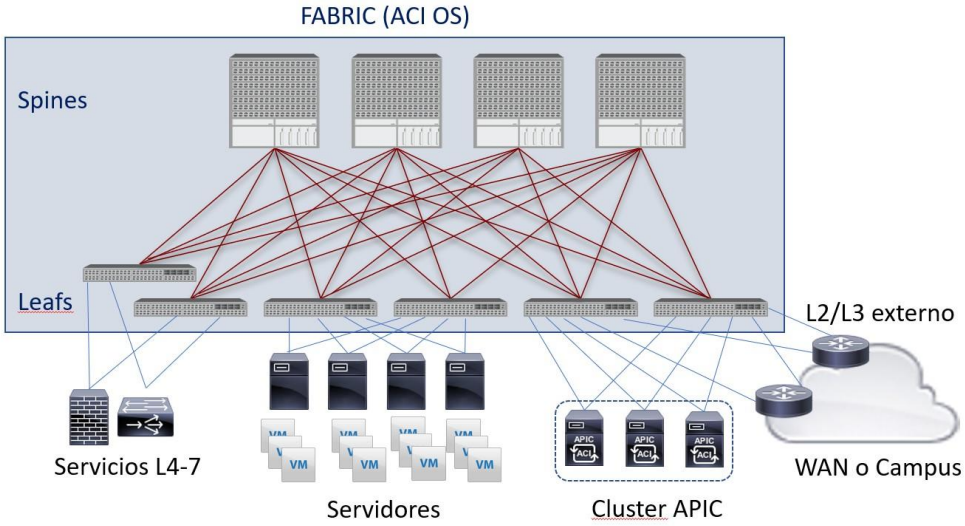

Figura 2-17 Arquitectura Leaf & Spine de Cisco ACI. Fuente: Propia.

La arquitectura permite la conexión de servidores físicos y virtualizados mediante conexión dual (vPC) a los switches *Leaf*. Los nodos Leaf con función de borde, que interconectan el ACI con servicios L4-7 o redes externas (intranets, WAN, etc.) utilizan OSPF como protocolo de enrutamiento para establecer las adyacencias con *routers* externos y aprender las rutas. Desde el punto de vista de la funcionalidad, los nodos *Spine* también son el punto de interconexión con otros *fabric*, realizando una función de *forwarding* de paquetes.

Esta arquitectura se puede extender a diferentes casos de uso, donde se tenga la necesidad de que toda la infraestructura se administre como una sola, por ejemplo:

- Un DC: sea el caso de una empresa que dispone de diferentes salas técnicas, que desea conectar, y se encuentran ubicadas en un mismo *datacenter* físico.
- Dos (o más) DC activo-activo: sea el caso en que la empresa u organismo dispone de varias sedes, geográficamente separadas, y desea conectarlas con esta solución SDN.

En la implementación de este "*fabric* extendido" son varias las opciones disponibles, que se tratarán más adelante, si bien en las más utilizadas hay un elemento común que es la "**interpod network**". La *interpod network,* o red IPN, es una red de nivel 3 externa al ACI que interconecta los diferentes *fabrics* físicos "Pods", dando lugar en su conjunto a un único *fabric* extendido. Cada Pod se comunica con la red IPN a través de los equipos *Spine* (Figura 2-18).

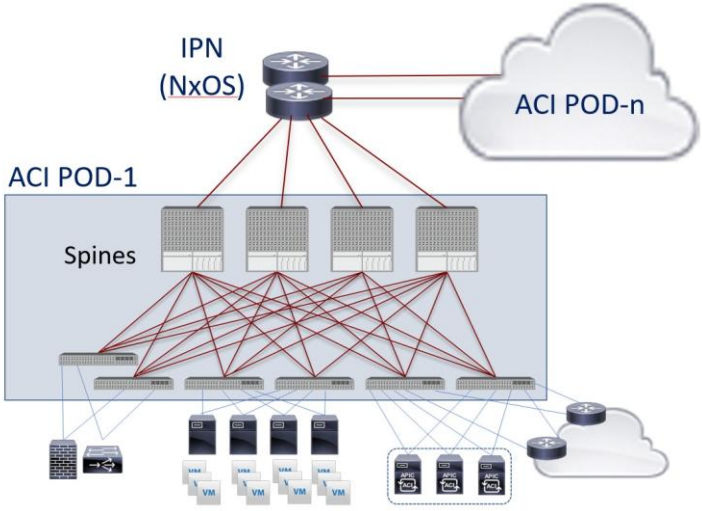

Figura 2-18 *Fabric* extendido mediante red IPN. Fuente: Propia.

Los IPN son, por tanto, dispositivos de nivel 3 que permiten la comunicación entre Pods, a través de túneles VxLAN. Estos dispositivos IPN trabajan en modo NxOS, y no ACI OS como los equipos del *fabric*, no pudiendo ser gestionados por el controlador APIC de la solución SDN.

Las características de los equipos IPN son los siguientes:

- No son gestionables vía APIC.
- No es obligatorio conectar los IPN a todos los Spines (recomendable a una pareja de *Spine*).
- Soporte *multicast* PIM BiDir.
- Soporte de OSPF.
- Aumento de MTU para soportar VxLAN (mínimo 1554 bytes para IPv4).
- DHCP-r*elay*.

Como se ha indicado, los IPN permiten la comunicación de los Pods mediante el establecimiento de túneles VxLAN. El protocolo de control que se utiliza para el transporte de tráfico entre los Pods, permitiendo la propagación de rutas y la conectividad entre los VxLAN virtual *end points* en ambos extremos, es BGP-eVPN (*Border Gateway Protocol* - Ethernet VPN).

En conclusión, respecto a las soluciones tradicionales de *datacenters*, ACI proporciona las siguientes ventajas:

- Arquitectura *Leaf and Spine* que, entre otras cosas garantiza la predictibilidad de la red, al haber siempre el mismo número de saltos entre el punto de entrada a la red y el de salida.
- Fabric VxLAN realizado en hardware, para garantizar un alto rendimiento, Gateway de salida distribuido por los equipos *Leaf*, con balanceo de tráfico en los enlaces del *fabric* por flujo, y priorización de paquetes de forma dinámica.
- Creación y modificación del *fabric* de nivel 3 y, por tanto, del plano de control MP-BGP eVPN, necesario para VxLAN.
- Provisión y gestión centralizada y automatizada de los equipos del *fabric*, aun estando ubicados en diferentes localizaciones geográficas.
- Creación de redes virtuales (denominadas *tenants*).
- Programabilidad vía API y otras herramientas de automatización del *datacenter*.
- ACI presenta un modelo de políticas basadas en aplicaciones, en el que los flujos de tráfico se segmentan y configuran de manera centralizada, en base a tipos de aplicación (modelo ***Application Centric*****,** mostrado en la Figura 2-19). Posteriormente el controlador transforma las políticas en configuraciones concretas que se aplican en los equipos.

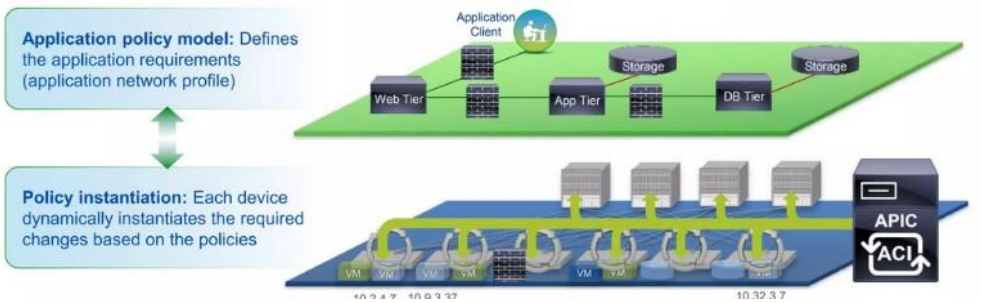

Figura 2-19 Modelo de políticas de aplicación (*Application Centric*). Fuente: [31].

2.6.3 Funcionamiento: VxLAN y Forwarding

Como se ha desarrollado previamente, VxLAN permite que el tráfico de red de nivel 2 pase a través de dispositivos de red de nivel 3, mediante la creación de un túnel. Esta es una característica especialmente útil en infraestructuras distribuidas de gran tamaño como las implementadas por Cisco ACI.

VxLAN es una tecnología clave dentro de ACI ya que todo el tráfico en el *fabric* está normalizado como paquetes de VxLAN. De hecho, ACI encapsula en paquetes VxLAN, no solo VLAN sino también paquetes NVGRE, según se muestra en la Figura 2-20.

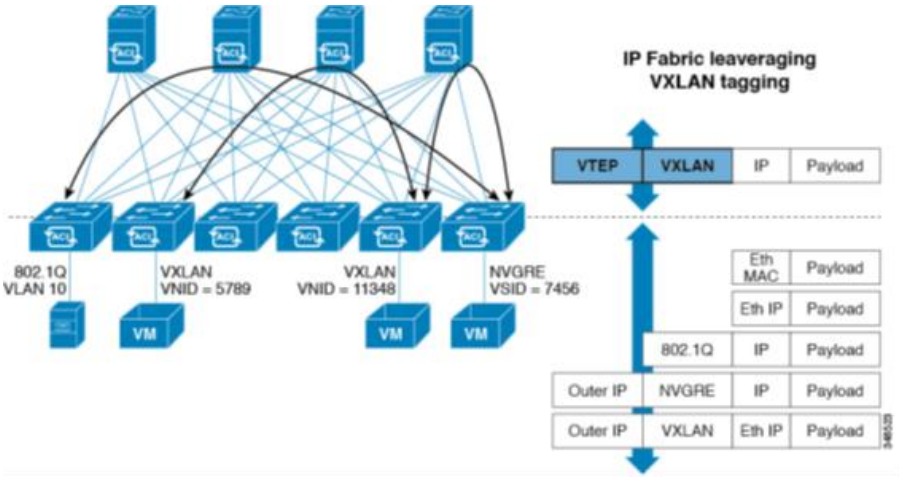

Figura 2-20 Encapsulación VxLAN. Fuente: Cisco.

Siendo el VTEP el elemento terminador del túnel VxLAN, en un entorno ACI el elemento que actúa como tal es el nodo *Leaf*. El *Leaf* mantiene una interfaz de capa 2 con el *endpoint*, y otra de capa 3 en la red de transporte IP (Figura 2-21). Es por tanto el dispositivo que encapsula y desencapsula las tramas VxLAN.

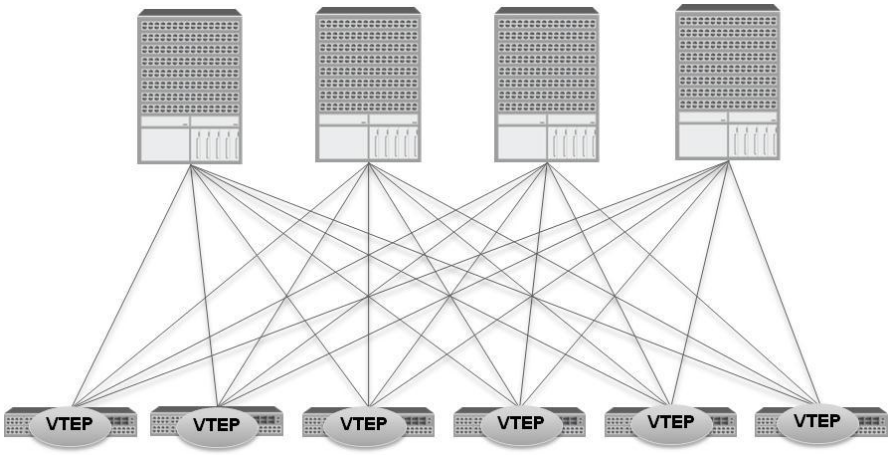

Figura 2-21 Leafs como VTEP en VxLAN. Fuente: Cisco.

En Cisco ACI, los *endpoints* se asignan a un ID de VLAN local, que luego se mapea a un VNID en la red VxLAN. Los *endpoints* no necesitan ser conscientes de la tecnología VxLAN, sino que simplemente se comunican como si estuvieran en una red de capa 2 tradicional. La dirección IP del *endpoint* sigue siendo utilizada como identificador del dispositivo, mientras que la dirección VTEP designa la posición de ese *endpoint* en la red.

En Cisco ACI, VxLAN se utiliza junto con protocolos de control como BGP-eVPN (*Border Gateway Protocol* - Ethernet VPN) para la distribución de información de reenvío de túneles, lo que mejora la escalabilidad y eficiencia de la red. Es decir, en una arquitectura extendida a varias ubicaciones (se verá más adelante), permite la propagación de rutas y la conectividad de extremo a extremo entre diferentes VTEPs, se encuentren o no en la misma ubicación.

Revisemos a continuación cómo se realiza el ***Forwarding*** en ACI.

En ACI el fabric se muestra como un único switch hacia fuera, capaz de hacer *bridging* y *routing*. Servicios como la movilidad de las máquinas virtuales y algunos softwares de *clustering* necesitan tener adyacencia a nivel 2 entre los servidores origen y destino. Mover el *routing* de nivel 3 fuera de ACI hacia la capa de acceso a priori impediría esta adyacencia, pues al enrutar en la capa de acceso sólo los servidores conectados al mismo switch, en la misma VLAN, tendrían visibilidad a nivel 2. En ACI, VxLAN resuelve ese dilema, desacoplando los dominios de nivel 2 de la infraestructura de nivel 3 subyacente.

Cisco ACI configura automáticamente todos los protocolos que participan en el *forwarding* y no es necesario un conocimiento profundo de los mismos para poner en marcha u operar el fabric ACI. El forwarding de Cisco ACI está basado en un overlay VxLAN. Los nodos *Leaf* son los VTEPs, de manera que ACI dispone de una base de datos de mapeos que contiene información sobre dónde (en qué TEP) residen los *endpoints* (direcciones MAC e IP). Cisco ACI puede llevar a cabo el *forwarding* de nivel 2 o nivel 3 en el *overlay*. El tráfico de nivel 2 lleva un VxLAN *network identifier* (VNID) para identificar bridge *domains*, mientras que el tráfico de nivel 3 (enrutado) lleva un VNID con un número que identifica el VRF.

Dependiendo de la configuración, el aprendizaje y *forwarding* en los nodos *Leaf* se puede basar en un "*flood and learn*" sobre un árbol *multicast* (similar a otras implementaciones VxLAN), o se puede usar la base de datos de mapeo de direcciones.

En un dominio de nivel 2, hay dos fuentes principales de *flooding*: el tráfico con destino MAC *unicast* desconocido, y el tráfico ARP. Para reducir la cantidad de *flooding* en el *fabric*, Cisco ACI realiza lo siguiente:

- Descubre la dirección IP o MAC (o ambas) de los *endpoints*.
- Reenvía las peticiones ARP al destino de la petición sin necesidad de hacer *flooding* en todo el *fabric*.
- Cada *Leaf* dispone de una tabla para el *forwarding* de los *endpoints* que tiene conectados llamada *local station table* (LST).
- Igualmente, cada *Leaf* dispone de una tabla con el mapeo de MAC o IP, a TEP, basándose en las sesiones activas (*global station tab*le, o GST).
- Los *Spine* disponen de la *proxy station table* (PST), tabla que contiene información sobre las direcciones MAC, IPv4 (/32) e IPv6 (/128) de todos los *endpoints*, y los VTEP en los que se encuentran.
- Cisco ACI mantiene actualizadas las entradas de todas las tablas realizando un seguimiento de los *endpoints* cuyas entradas puedan caducar.

2.6.4 Componentes: el controlador APIC y los nodos

Cisco ACI proporciona varias **interfaces de usuario**, que permiten acceder a la funcionalidad ofrecida por el controlador:

- CLI (*Command-Line Interface*), o Interfaz de línea de comandos.
- GUI (*Graphical User Interface*), o Interfaz gráfica de usuario, es el método de acceso al *dashboard* más utilizado, vía navegador, que permite acceder a la funcionalidad completa de administración del fabric ACI.
- Interface programable (API), permitiendo la automatización e integración con otras aplicaciones y sistemas (accesible por ejemplo mediante SDK en Python).

Nota: Adicionalmente ACI ofrece un *toolkit*, opción menos utilizada, que integra aplicaciones que permiten la reversión de configuraciones, seguimiento de *endpoints*, y otras funcionalidades.

El ***Application Policy Infrastructure Controller*** **(APIC)** es el componente principal de la arquitectura de Cisco ACI para *datacenter*. Es el cerebro de la solución SDN, punto unificado de automatización y gestión de la infraestructura ACI. Es donde se configuran las políticas que se

traducen en las estructuras de red necesarias para aprovisionar dinámicamente los servicios, se monitoriza el estado de salud de la red, y se administra el *fabric* en su conjunto.

El APIC es quien levanta el *fabric*, lo administra, se ocupa de la provisión y supervisión. Es accesible mediante las diferentes interfaces de usuario mencionadas, siendo la más utilizada por sencilla y completa, la interfaz gráfica (GUI).

Funciones de control realizadas por el APIC son las siguientes:

- *Policy Manager*: Repositorio de políticas distribuido responsable de la definición y despliegue de la configuración basada políticas de Cisco ACI.
- *Topology Manager*: muestra la topología de ACI.
- *Observer*: Subsistema de monitorización del APIC, que actúa como un repositorio de datos, su estado de funcionamiento, salud y rendimiento.
- *Boot Director*: Controla las actualizaciones de firmware de arranque de los switches *Leaf* y *Spine*, así como los elementos del controlador APIC.
- *Appliance Director*: controla el clúster de APIC.
- *Even Manager*: registra eventos y fallos del fabric (nodos o APIC).
- *Appliance Element*: Administra el inventario y el estado del APIC local.
- Integración de terceros: servicios de capa 4 a capa 7, VMware *vCenter* y *vShielf*, Microsoft *Hyper*-V, OVS y *OpenStack*, Kubernetes y Docker entre otros.

El controlador APIC se implementa como un clúster de varios *appliances* físicos (Figura 2-22). Cisco recomienda un mínimo de tres dispositivos, que se sincronizan y replican. El tamaño será directamente proporcional al tamaño de la infraestructura desplegada, hasta un máximo de 5 dispositivos.

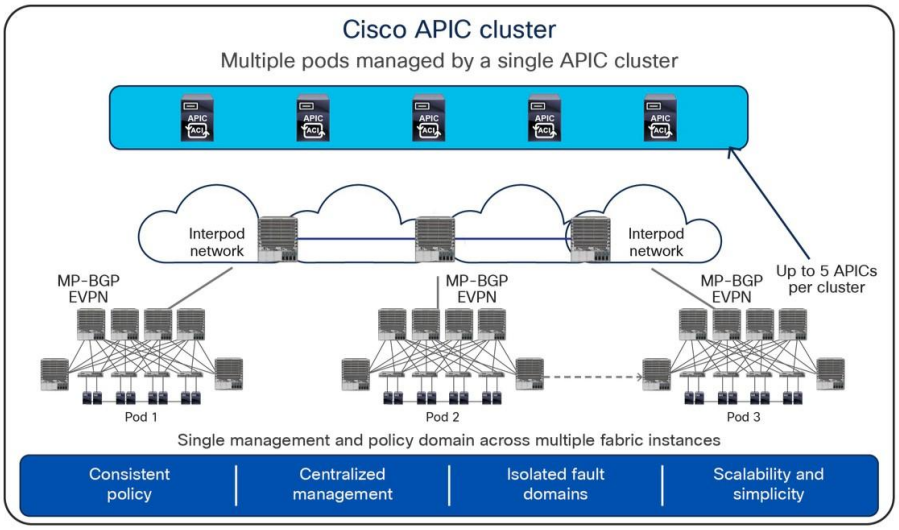

Figura 2-22 Clúster de controladores APIC. Fuente: [32].

Cualquier controlador en el clúster puede dar servicio a cualquier administrador, y se puede agregar o eliminar del clúster de forma transparente.

Con un clúster de 3 controladores el sistema garantiza que el administrador seguirá manteniendo acceso de lectura y escritura en el caso de pérdida de servicio en una unidad, con dos controladores activos. En el caso de pérdida de un segundo controlador (sólo uno activo) se mantienen permisos de lectura pudiendo monitorizar el sistema, aunque no crear o modificar políticas. En el caso de pérdida de los tres controladores, no se podrá monitorizar el sistema, pero este no deja de cursar tráfico.

Este es uno de los motivos, la alta disponibilidad, por la que Cisco recomienda separar geográficamente una de las tres unidades, en caso de una arquitectura extendida a varias ubicaciones.

En función de las necesidades de CPU, almacenamiento y memoria, básicamente hay dos tipos de controladores que se pueden desplegar, que llamaremos de tamaño medio (M) o largo (L). Actualmente las versiones más recientes lanzadas por el fabricante son las versiones M4 y L4. La elección de uno u otro dependerá del dimensionamiento de la arquitectura, del número "*edge ports*", y consecuentemente de switches (nodos), que se tenga y se necesite gestionar.

Por ejemplo, una solución con diez switches de 48 puertos cada uno, proporciona 480 *edge ports*. Un clúster APIC-M4 permite gestionar hasta 1200 *edge ports*. Por encima de esa cantidad es necesario un clúster APIC-L4.

Mas información sobre Cisco APIC en la referencia [33].

Los otros protagonistas del fabric son **los switches o nodos**, que forman la estructura *Leaf and Spine* comentada. Implementan las configuraciones y políticas generadas en el APIC, y son los elementos que proporcionan conectividad y redundancia. Los **nodos *Spine*** son los elementos centrales que actúan como conectores entre los diferentes nodos Leaf, y conmutan el tráfico entre ellos. Cuando se agrega un nodo *Spine* se crean caminos alternativos, caminos que permiten que los datos encuentren rutas alternativas a través del *fabric* en caso de que uno falle. Si esto sucede, el sistema no experimentará problemas porque la misma información de *forwarding* (reenvío de los datos) estará replicada en otro nodo *Spine*. Este es el motivo de desplegarlos por parejas. La pareja de ese *Spine* caído tiene copias de las tablas de rutas, necesarias para dirigir el tráfico a destino. Además, los *Spine* no solo proporcionan caminos redundantes, sino que también aumentan el ancho de banda disponible. Modelos de nodos *Spine* son los Cisco de la serie 9000 (como el Nexus 9332C, 9316D-GX, 9348D-GX2A, 93600, 9408 y 9500). Pueden ser de formato fijo o modular, con diferentes anchos de banda en los puertos, etc.

Los **equipos *Leaf*** por su parte se caracterizan por ofrecer una alta densidad de puertos, ópticos o eléctricos, lo que permite conectar una gran cantidad de dispositivos finales. Esto es crucial para entornos de centros de datos donde se requiere una conectividad masiva. Otra característica indispensable de los *Leaf* es que soportan VxLAN, lo que facilita la segmentación de la red y la creación de redes superpuestas. Además, están diseñados para integrarse con las capacidades de automatización de Cisco ACI, lo que incluye la configuración automática de las políticas de red, y su gestión centralizada a través de los controladores APIC. Al instalarse por parejas proporcionan redundancia y alta disponibilidad, en caso de fallo de uno de ellos, o del enlace con el servidor que conectan. Modelos típicos de nodos *Leaf* son los Cisco Nexus de la serie 9300 (muy utilizados por su alta densidad de puertos y capacidades), y de la serie 9200 (con un equilibrio más ajustado entre rendimiento y coste, para organizaciones más pequeñas).

2.6.5 Arquitecturas extendidas

Cuando el número de Pods es de dos o mayor, es necesario escalar la arquitectura *Leaf and Spine*, por el elevado número de fibras necesarias para cumplir con los requisitos de conectividad indicados, entre equipos *Leaf y Spine*. Y estas líneas, cuando conectan *datacenters* son enlaces WAN con un elevado coste. Este es el motivo por el que se han desarrollado diferentes arquitecturas para entornos de multi-DC que puedan funcionar en activo-activo (Figura 2-23), que se indican a continuación.

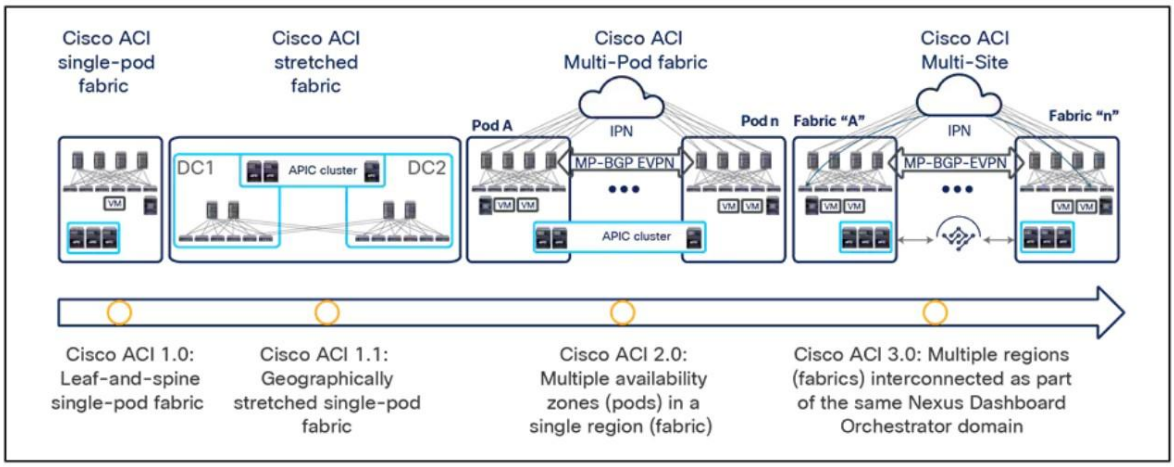

Figura 2-23 Evolución de arquitecturas extendidas ACI. Fuente: [34].

- Single Pod Fabric:
  - Disponible desde inicio con la reléase 1.0, esta fue la primera solución SDN soportada.
  - Consiste en una estructura clásica de *Leaf and Spine* (Pod único) como solución para un único *datacenter*.
  - Se ejecuta una única instancia de los protocolos del plano de control, entre todos los dispositivos de red en ese Pod. Todo el *fabric* está bajo la administración de un único clúster de controlador APIC, punto único de definición de las políticas.
  - Un único dominio de administración.
- *Streched Fabric*:
  - Esta fue la primera arquitectura distribuida soportada, extensible a varias localizaciones geográficas.
  - Ofrece un único *fabric* ACI extendido, es decir, funcionalmente esta arquitectura representa el despliegue de un único Pod. Solo se ejecuta una instancia de los protocolos del plano de control en todos los sites. El clúster APIC puede tener sus *appliances* repartidos en los diferentes *datacenters*.
  - Por contra, el número de enlaces entre DCs es alto.
  - Ciertos *Leafs* de "tránsito" asumen la labor de interconexión, entre los equipos *Spine* de ambas localizaciones.
  - En la actualidad no es una opción recomendada, salvo para despliegues muy sencillos con menor presupuesto, pues no proporciona mecanismos de aislamiento para evitar que los problemas de un site o *datacenter* impacten en el funcionamiento del otro (Pod único).
  - Más información en la referencia [35].
- MultiPod:
  - Esta es la arquitectura más común (y recomendada) para estos entornos de multi-DC en activo-activo. A cada ubicación física se le denomina Pod, y está formada por una arquitectura *Leaf and Spine.*
  - Ofrece un único *fabric* extendido a todos los Pods. Los Pods habitualmente son *datacenters* en diferentes ubicaciones geográficas (Figura 2-25), aunque también pueden responder a una organización de la infraestructura en un mismo *datacenter* (Figura 2-24).
  - Se dispone de un único clúster APIC, que gestiona las diferentes redes (Pods) y cuyos controladores se recomienda que estén repartidos en los Pods, para una solución más robusta.

- En un despliegue típico, el número de enlaces entre DCs queda reducido a dos. Se utiliza para ello la red IPN, que proporciona la conectividad entre Pods.
- Ofrece un aislamiento, reduciendo el impacto en el funcionamiento de unos Pods frente a problemas que pudieran darse en los otros. Esto se logra ejecutando instancias separadas de los planos de control (IS-IS, COOP, MP-BGP) en todos los Pods.
- Sin embargo, se deben cumplir ciertos requisitos. La red IPN debe cumplir no solo los criterios indicados anteriormente (soportar *multicast* PIM, MTU mínima de 1550, DHCP *relay*, QoS), sino que además la latencia máxima entre los Pods no puede exceder los 50 ms ida y vuelta (RTT, o round trip time).
- Más información en la referencia [36].

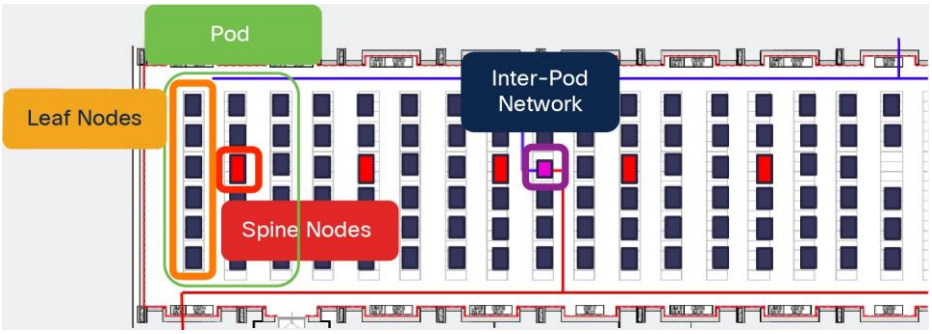

Figura 2-24 Arquitectura extendida MultiPod en un datacenter. Fuente: [36].

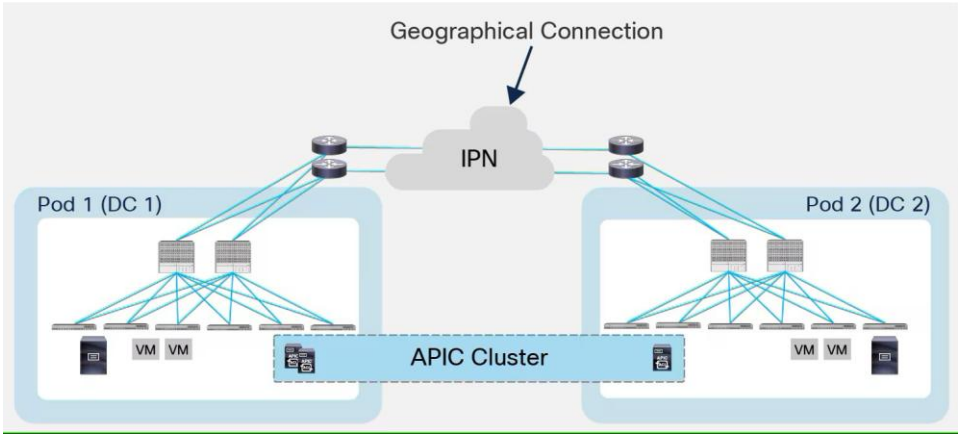

Figura 2-25 Arquitectura extendida MultiPod en dos *datacenters*. Fuente: [36].

- Multisite (Figura 2-26):
  - Esta arquitectura se soporta ya desde la versión ACI reléase 3.0.
  - En este caso tenemos entornos independientes de controladores. En cada DC se ubicará un clúster APIC independiente. Administración independiente.
  - La sincronización de las políticas en este caso se realiza mediante un ACI *Multi Site Policy Manager*, es decir, un orquestador multisite.
  - Esta arquitectura resulta por tanto más costosa que la multipod.
  - Está recomendada para entornos empresariales en los que el número de *datacenters* es elevado (por encima de tres), o bien cuando los *datacenters* están muy alejados y presentan una latencia elevada, o en entornos de *cloud* pública, o ante una combinación de estas situaciones.
  - Más información en la referencia [34].

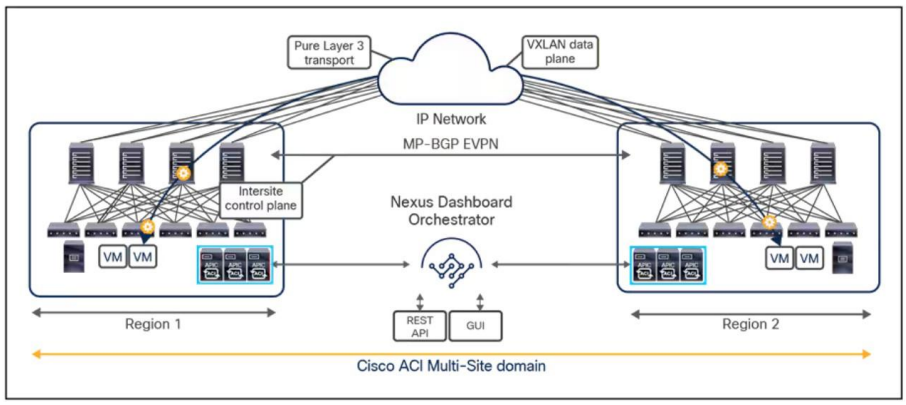

Figura 2-26 Arquitectura extendida MultSite. Fuente: [34].

- *Remote Leaf* (Figura 2-27):
  - En este caso se plantea una extensión de redes a centros de datos secundarios. Se caracteriza porque no es necesario la utilización de equipos *Spine* en el DC remoto.
  - El principal requisito es la ampliación de MTU, latencia máxima de 300 ms RTT, y un ancho de banda mínimo de 100 Mbps.
  - Se pueden disponer varias parejas de *Remote Leafs* en el mismo DC secundario.
  - Los equipos *Leaf* están totalmente gestionados por el clúster APIC del DC principal.
  - En este caso, se dispone de las mismas funcionalidades que en el DC principal, de manera que el tráfico local del DC secundario se cursa por un enlace de nivel tres a un *endpoint* externo (lo que llamaremos l3out, y que como se verá en la capa lógica conecta con un grupo de máquinas, o EPG externo al DC principal).
  - Esta arquitectura supone un ahorro importante de costes respecto a multipod (aun así, debe considerarse el coste del alquiler de la fibra oscura a operador), y está recomendada cuando el DC secundario es muy pequeño.
  - Hay que tener en cuenta las limitaciones en los flujos de tráfico. Si bien el tráfico local se conmuta directamente entre los *endpoints* (tanto virtuales como físicos) de ese mismo DC secundario, no ocurre así con el DC primario. Todo el tráfico que necesite el uso del "proxy" *Spine* se redirigirá hacia el DC primario, con las implicaciones correspondientes (latencia, etc.).
  - Más información en la referencia [37].

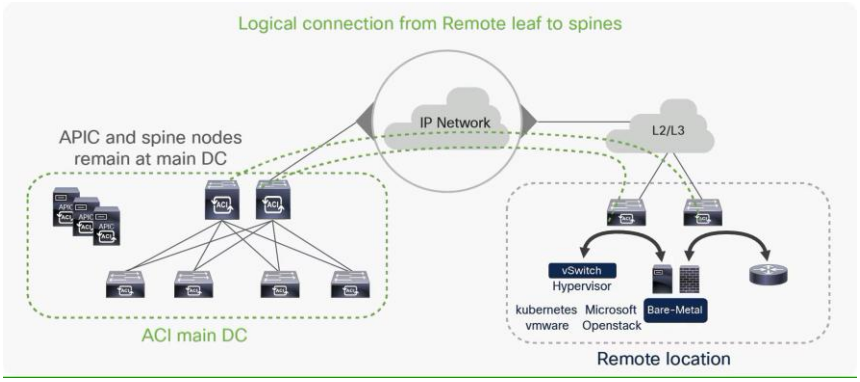

Figura 2-27 Arquitectura extendida Remote Leaf. Fuente: [37].

2.6.6 Plano lógico y contratos

Uno de los universos dentro de la estructura de ACI es el lógico, que define el plano de conectividad, el cual determina la comunicación dentro de ACI. Una configuración incorrecta de este plano inhabilitará el flujo de datos.

ACI trabaja con diferentes configuraciones lógicas que son contenedores anidados, pilares del plano de conectividad. Cada uno tiene una correspondencia o presenta unas equivalencias aproximadas con el modo *legacy* tradicional, que se representan en la Figura 2-28, y se explica a continuación.

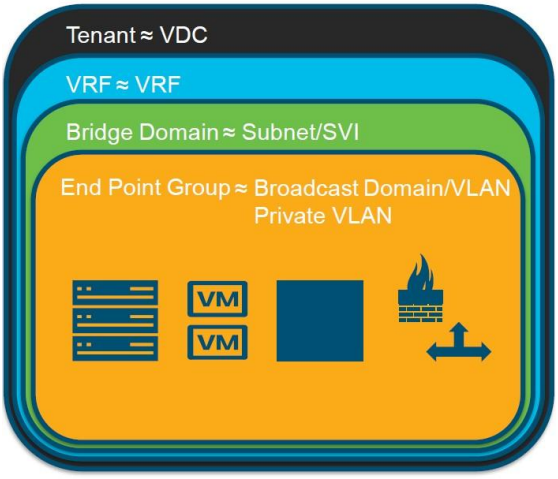

Figura 2-28 Modelo lógico de ACI. Fuente: [38].

- *Tenant*:

  El *Tenant* en ACI representa el objeto lógico de más alto nivel. Se trata de una construcción lógica empleada para separar las porciones de red, o entornos del cliente. En su interior se encuentran tanto los objetos que definen la red (VRF, BD, APP, EPG y *subnet*) como sus políticas de conectividad (contratos).

  Como contenedor lógico para políticas de aplicaciones permite al administrador ejercer un control de acceso basado en dominio. Diferentes *tenants* representan diferentes dominios administrativos. Un *tenant* constituye una unidad aislada desde un punto de vista de las políticas.

  El *fabric* puede albergar múltiples *tenants*. Todos los *tenants* se reparten y utilizan los recursos físicos (pensemos en los "Edge ports" de los switches). Por ejemplo, en una empresa se puede implementar un *tenant* de desarrollo, otro de preproducción, y un tercero de producción. Otro ejemplo pueden ser diferentes departamentos de la empresa que quieren un acceso independiente a unos recursos que se comunicarán o no con los de otro dominio.

  Los *tenants* pueden estar aislados unos de otros o compartir recursos.

  Estos recursos, u objetos que definen la red, son los filtros, contratos, redes externas, *bridge domains*, instancias de *Virtual Routing and Forwarding* (VRF), y perfiles de aplicaciones que contienen los *endpoint group* (EPG). Las entidades en los *tenants* heredan sus políticas.

  Se deberá configurar un *tenant* antes de poder desplegar cualquier servicio de capa 4 o capa 7. El *fabric* de ACI soporta Ipv4, IPv6 y configuraciones *dual-stack* para interconexiones de *tenants*.

- VRF (*Virtual Routing and Forwarding*):

  La VRF, también conocida como contexto, es una funcionalidad definida dentro del *tenant* que implementa una separación de tipo lógico en el *router*, virtualizando las tablas de enrutamiento. De esta forma existirán múltiples *routers* virtuales en un solo *router* físico, aislando entornos de capa 3.

Es decir, las VRFs son dominios independientes de nivel 3, redes lógicas que se definen dentro de un *tenant*. Un *tenant* contiene habitualmente más de una VRF.

- *Bridge Domain* (BD):

  Un *Bridge Domain* representa una construcción de *forwarding* en capa 2 dentro del *fabric*. Se define dentro de una VRF, y es equiparable al concepto de VLAN en redes *legacy*. Por tanto, opera a nivel 2 (tablas MAC).

  Sin embargo y a diferencia de las VLAN, cada BD permite la separación de entornos de difusión creando múltiples subredes contenidas en su interior. Al menos se debe contener una subred.

- *Subnet*:

  Las *subnets*, o subredes, se definen dentro del *Bridge Domain*, estando cada una asociada a un único BD. Son redes a nivel 3, es decir, con un direccionamiento IP asociado.

- *Application Profile* (AppP):

  El *Appication Profile* es el elemento lógico que describe todos los componentes de una aplicación, es decir, contiene todos los EPG que participan de una aplicación.

  Los AppP son por tanto los objetos lógicos que contienen las políticas de agrupación de EPG, dentro del *tenant*.

- *End Point Group* (EPG):

  Los EPG son agrupaciones de *endpoints* que se rigen por las mismas políticas (por ejemplo, de seguridad o de asociación a servicios de nivel 4 ó 7). Un EPG permite una administración conjunta de todos los EPs.

  Dentro de un EPG pueden coexistir elementos físicos y virtuales.

- End Point (EP):

  Los *endpoints* son los dispositivos conectados a la red de forma directa o indirecta. Son los equipos, físicos o virtuales, que se conectan al *fabric* ACI. La membresía de los *endpoints* en un EPG puede ser dinámica o estática.

  Se caracterizan por tener una dirección (*identity*), una ubicación, y un atributo (como la versión o el nivel de parche aplicado), Ejemplos de EPs son los servidores, máquinas virtuales, sistemas de almacenamiento en red, o elementos externos al ACI.

Mediante estos objetos lógicos ACI proporciona conectividad de capa 2, o funciones de puerta de enlace predeterminada a grupos de *endpoints*.

Si bien un BD/EPG de ACI permite que cada dispositivo IP conectado se aprenda como una dirección con máscara /32 (IPV4), esto no resulta factible en el caso de pretender conectar un dispositivo de red (router) que tenga una o más subredes detrás. Es decir, en caso de querer conectar un *Border Leaf* a un dominio de red externo de ACI, se puede utilizar una configuración que lo permite, y se denomina L3out.

El **L3out** (*Layer 3 Out*) es una configuración que proporciona conectividad de capa 3 entre el fabric de ACI y redes externas, mediante enrutamiento. Los L3Out permiten que los dispositivos y aplicaciones dentro del *fabric* de ACI puedan comunicarse con redes externas, como internet, intranets u otras redes.

Para utilizar un L3out básicamente se configuran interfaces de nivel 3 en los *Border Leaf* que conectan con el *router* externo, se establecen las adyacencias seleccionando un protocolo de

enrutamiento para el intercambio de rutas (OSFP / BGP), y se aplican las políticas de seguridad (contratos) deseadas.

Por otra parte, ACI está orientado a un modelo que se centra en la creación de grupos de máquinas (EPG) cuyos componentes (EPs) están orientados a un mismo tipo de aplicación. Un modelo de agrupación por tipo de aplicación, que se denomina modelo de ***Application Centric*.** Por ejemplo, mediante la implementación de un EPG que agrupe frontales web, otro que ubique las bases de datos, etc. El modelo de *Application Centric* permitirá aplicar políticas de fujo de tráfico de una manera común al EPG, a todos los servicios que contiene, de manera que se pueda simplificar la creación y gestión de estas políticas.

Cabe mencionar en este punto que, sin embargo, en las redes *legacy* tradicionales, dentro de una VLAN podemos encontrar casi de todo, desde un frontal web hasta la base de datos. Para facilitar la migración a Cisco ACI desde un esquema de red tradicional, Cisco desarrolló un modelo que se denomina de ***Network Centric*.** En este modelo, básicamente, 1 VLAN tradicional se traduce directamente en ACI en un EPG contenido en un BD con una única *subnet*, es decir:

1 *subnet* = 1 BD = 1 EPG = 1 VLAN.

Este modelo basado en una aproximación de red permite abordar en un primer paso la migración a ACI desde las redes tradicionales, y posteriormente, con los servicios activos dentro del fabric, ir planificando el movimiento de máquinas y servidores a EPG con la aproximación por aplicaciones.

A continuación, se hablará del elemento lógico de seguridad más importante de la solución Cisco ACI, el contrato.

Un **contrato** es una construcción lógica, una implementación de una política, que se utiliza para definir la comunicación entre grupos EPG. Es similar a la tradicional ACL, y actúa como elemento lógico que permite o deniega la comunicación entre los EPG.

El funcionamiento de los contratos presenta las siguientes características:

- Los contratos permiten definir la forma en que un EPG se comunica con otro.
- Un contrato básicamente permite tres acciones: permitir, denegar o redirigir.
- Por defecto, dentro de un EPG todos los EPs pueden comunicarse entre sí, no les afectan los contratos. Esta afirmación se puede evitar mediante la configuración expresa de una característica de aislamiento intra-EPG, o un contrato intra-EPG.
- El modelo de uso de los contratos es bajo una relación de cliente-proveedor. Uno o más EPG proveen un contrato, que otro u otros EPG consumen.
  Se está ofreciendo una protección cuando hay restricciones en la forma en la que unas partes de una aplicación deben interactuar con otras.
- Los contratos ofrecen sencillez al permitir que las políticas se definan una vez y se reutilicen muchas veces.
- Un contrato actúa a nivel de puerto, para todos los EPG que lo provean o consuman.
- Un contrato tiene sentido, es decir, si se quiere configurar una comunicación dúplex se deben configurar dos contratos.
- Por defecto, sin un contrato entre grupos EPG no puede haber comunicación *unicast* entre esos EPG. La excepción a esta afirmación es que los EPG se incluyan en lo que se denomina un "*Preferred Group*", o que la VRF se configure en un modo "*unenforced*" sobre el objeto *VzAny* (es decir, todos los EPG de la VRF). En este último caso, todos los EPG de la VRF podrían comunicarse entre sí.

Por ejemplo, en la Figura 2-29 se muestra la relación entre EPG y contrato. Sea el caso en que una aplicación que tiene por detrás una base de datos ofrece un servicio HTTPS de consulta mediante un frontal web. En este ejemplo, el EPG App provee (permitiendo) un contrato por el puerto 443 que el

frontal del EPG Web consume, al tiempo que consume un contrato por otro puerto que el EPG DB le provee. Los tráficos están permitidos solamente en el sentido indicado.

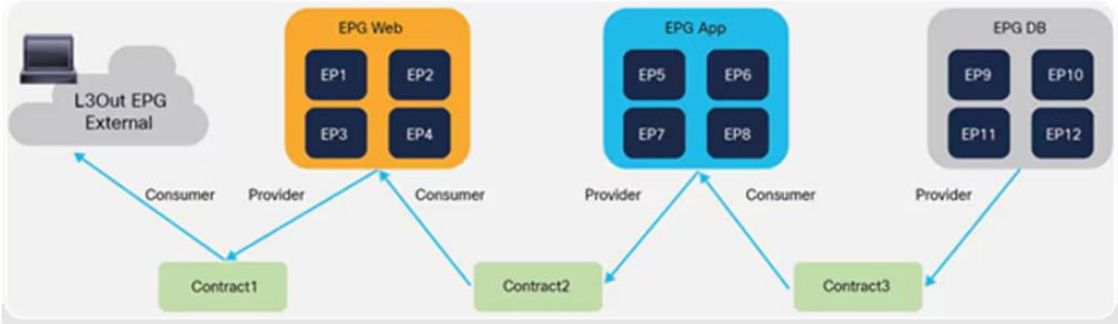

Figura 2-29 Relación entre EPG y contrato. Fuente: [18].

Como Cisco ACI recomienda un modelo basado en aplicaciones, es decir, en el que las máquinas de un EPG normalmente son todas del mismo tipo funcional, la mayor parte de las veces no será necesario definir más de un contrato entre una pareja de EPG. Sí puede ser necesario agregar más reglas de filtrado a un contrato, para lo es preciso aclarar los conceptos y la relación entre contrato, *subject*, filtro y entrada (Figura 2-30).

Un *subject* es una construcción lógica contenida dentro de un contrato, ejecutará una acción (permitir, denegar o redirigir). Un contrato puede contener uno o más *subjects*. Un *subject* hace referencia y puede contener uno o más filtros. Un filtro contiene una o más entradas, que son reglas de filtrado que especifican campos como el tipo de protocolo y puerto.

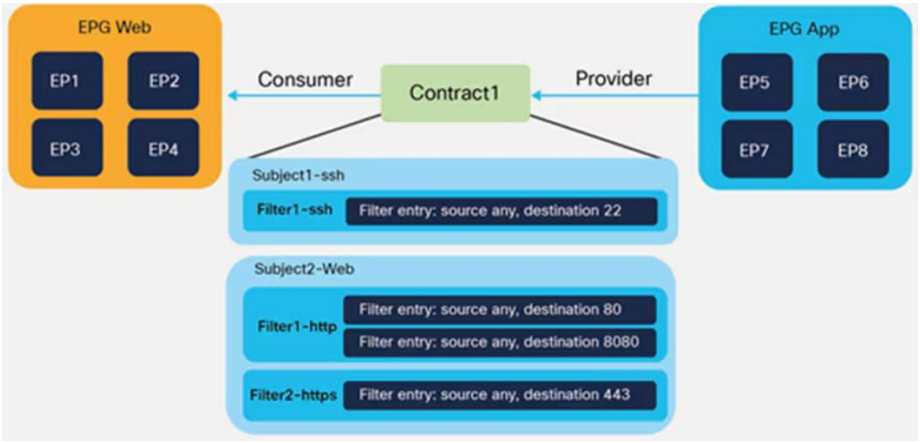

Figura 2-30 Conceptos de contrato, *subject*, filtro y entrada. Fuente: [18].

El hecho de que los contratos se configuran a nivel de puerto en la práctica implica que se deben identificar todos los flujos existentes, es decir, conocer exactamente todos los servicios (puertos) que se están ofreciendo y cuáles son los proveedores y clientes de esos servicios.

Cisco ACI presenta una limitación física en cuanto al número de contratos que se pueden configurar, sin un hardware específico adicional de alto coste. Esta limitación se produce a nivel de una tabla TCAM (*Ternary content-addressable memory*) que no es más que un buffer que se utiliza en los nodos, y tiene una capacidad limitada. Cuando esta memoria se llena no se pueden configurar más contratos.

El tamaño de la tabla es directamente proporcional al número de entradas en un contrato, el número de proveedores, consumidores que lo aplican, y el sentido de la comunicación, como se puede observar en la siguiente fórmula:

$$TCAM = (NEC) * (NCEPG) * (NPEPG) * 2$$

donde:

- NEC: Número de entradas en un contrato
- NCEPG: Numero de consumidores EPG
- NPEPG: Numero de proveedores EPG

Para más detalle sobre contratos en ACI se puede consultar el *whitepaper* de Cisco al respecto, en la referencia [39].

En la Figura 2-31 se muestra un resumen de los objetos lógicos a configurar durante la creación de la capa lógica, donde se resaltan algunas recomendaciones y ejemplos en cada caso.

Requirements	Notes	Example
Tenant	1 Tenant can be used company. Tenants can also separate functions of a business. NOTE: Shorter names are easier when using CLI	Prod/Dev
VRF	1 or more VRFs per Tenant	PROD-MAIN DEV-TEST,DEV-PROD
Bridge Domain	Recommended to have 1 BD per Legacy VLAN. For Network Centric Migrations, 1 BD should be used for each EPG.	VLAN_100,VLAN_101 BD_vMotion
Application Profile	Logical Container for EPGs. 1 AP is sufficient in most installations. NOTE: This is strictly a management entity. No policies are defined on this object.	Prod-AP
EndPoint Group	Ports/VLANs (static path bindings) are added to EPGs to define what Endpoints get defined in what EPGs. QOS/Contracts, etc are added to EPGs. For Network Centric Migrations, 1 EPG should be used for each Legacy VLAN.	VLAN_100 VLAN_101 vMotion
Contracts	Contracts can be re-used across multiple EPGs. If we compare this to an ACL, the Consumer is the Source, and the Provider is the Destination.	Web
Filters	Add Required Ports and Protocols to allow communication. Only what is specified in the filter → contract will be allowed between EPGs providing and consuming that contract.	SRC: Any, DST:80 SRC: Any, DST:443

Figura 2-31 Planificación de la capa lógica, resumen de objetos. Fuente: Cisco.

2.6.7 Modelos de Despliegue y Seguridad

Un aspecto relevante en la definición lógica de una arquitectura ACI, es decidir la conectividad que se mantendrá entre los elementos del *fabric*. Dos son las opciones que se plantean, consistentes en dejar el nivel 3 dentro o fuera del *fabric*.

En el caso de mantener el ***fabric* en capa 2**:

- Se configura como tal a nivel 2, de manera que no hay *routing* de capa 3 dentro del *fabric*.
- Se necesita un elemento externo al *fabric* donde se ubique el nivel 3.
  Los *gateways* de los *endpoints* conectados a los puertos de los nodos *Leaf* se encontrarán fuera del *fabric*, en elementos de red ajenos al ACI.
- Estos *gateways* habitualmente serán dispositivos de seguridad tipo firewall, que añaden funcionalidades adicionales de IPS, IDS o antivirus.
- Una importante limitación es que no estarían habilitados los contratos en el perfil del *fabric*. Las funciones de filtrado o seguridad deben confiarse a elementos externos al ACI.
- Se implementa por tanto de una manera parcial la funcionalidad que permite la solución SDN de Cisco ACI.

En el caso de configurar el ***fabric* en capa 3**:

- El nivel 3 y por tanto los *gateways* se encuentran dentro del *fabric*.
- Estarán habilitados los contratos. Se pueden implementar contratos entre grupos EPG. decidir no hacerlo, o implementarlos de una manera parcial.
- Facilita poder mantener dentro de ACI el nivel de seguridad vertical (flujos norte-sur) implementada en la solución tradicional previa a la migración a Cisco ACI.

Adicionalmente, se puede proporcionar una mayor seguridad en el plano horizontal (flujos este-oeste), es decir, entre servidores del *datacenter*.

- Se aprovecha mejor la tecnología ACI de Cisco, implementando una mayor funcionalidad.
- Mediante el uso de contratos en mayor o menor medida, se presentan varias opciones de implementación que aportan diferentes grados de seguridad horizontal.

Relacionado con los modelos de despliegue, se debe valorar el **nivel de securización de los flujos de tráfico**: los flujos verticales (norte-sur) entre usuarios y servicios alojados en el *datacenter*, y los flujos horizontales (este-oeste) entre máquinas o servidores del mismo o diferente *datacenter*.

Los **flujos norte-sur** deben ser gestionados de manera externa al ACI. Esta inspección puede ser realizada por un firewall norte-sur instalado en el acceso desde usuarios al Pod.

En el caso de un *fabric* extendido con varios Pods, si se configuran las VRF de manera que tengan presencia en ambos Pod, una pareja de firewalls norte-sur en activo-pasivo, instalada con redundancia geográfica entre los sites, puede realizar esta función. Incluso cada uno de los firewalls puede implementarse con una solución SDN de conocidos fabricantes, que permiten desplegar un orquestador y varias máquinas (firewalls) físicas o virtuales para añadir puertos y capacidad de procesamiento.

Para los **flujos este-oeste** entre servidores, a nivel de *datacenter*, son principalmente tres las opciones que se pueden implementar, en función del grado de seguridad que se desee proporcionar:

- Opción 1: Contrato *VzAny*:

  Esta es la situación en la que no se realiza control de las comunicaciones horizontales entre servidores del *datacenter*. Todo el tráfico horizontal está permitido, es decir, todos los servidores pueden hablar entre sí.

  Este escenario responde a una situación frecuente en las redes tradicionales de *datacenter* en que no se realiza un control de la seguridad horizontal. El hecho de que los sistemas estén configurados sobre VLAN tradicionales, que suelen contener todo tipo de máquinas que necesitan comunicarse, añade complejidad en el momento de realizar la migración a una solución SDN como Cisco ACI, basada en un modelo de aplicaciones (*Application Centric*).

  Para resolverlo, se puede definir en ACI una VRF "General" a la que se van migrando las VLAN tradicionales, de manera que se puede utilizar una aproximación de "*Network Centric*". Esta aproximación implica que los EPG en ACI se asimilan a las VLAN tradicionales, incorporando cada uno diferente tipología de máquinas. Y como siempre habrá recursos comunes, que necesitan comunicarse y ser accedidos por los diferentes EPG (VLAN tradicionales), una comunicación permitida entre todos los elementos es lo adecuado en ese momento tras la migración.

  Esto se puede conseguir configurando un "*alow*" sobre el objeto *VzAny*, que incluye a todos los EPG de la VRF (Figura 2-32), de manera que todo el tráfico horizontal quedará permitido entre todos ellos. Es realmente un contrato *any-any* con una política que permite la comunicación a nivel de VRF.

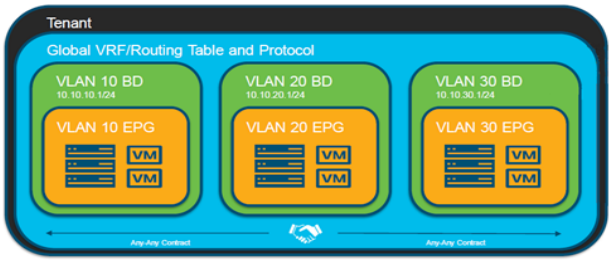

Figura 2-32 Contrato VzAny. Fuente: [38].

- Opción 2: Contratos entre EPG:

  A diferencia del caso anterior, esta opción permite añadir seguridad horizontal. Todos los flujos entre EPG estarán denegados por defecto, salvo que expresamente un contrato lo permita.

  El uso de contratos permite una granularidad del tráfico horizontal más específica que las tradicionales ACL, ya que los contratos especifican el flujo de datos entre equipos a nivel de puertos, es decir, servicios específicos capa 4.

  Sin embargo, será necesario identificar todos los flujos horizontales existentes, es decir, conocer exactamente todos los servicios (puertos) activos y cuáles son las relaciones entre esos servicios. A partir de ello, los contratos permitirán ciertas comunicaciones.

  En este caso es el ACI el que realiza todo el control de la seguridad horizontal, con las limitaciones indicadas sobre la tabla TCAM.

- Opción 3: PBR o *Service Graph*

  Esta es una opción intermedia entre las dos anteriores, que requiere un hardware adicional. Consiste en que el ACI asume parte de la carga, y otra parte se deriva hacia elementos externos. Esta política de redirección se denomina PBR (*Policy Based Redirect*) y se muestra en la Figura 2-33.

  Se configurarán contratos, pero de una manera más genérica, lo que implica que se necesita un menor detalle de los flujos existentes.

  Adicionalmente, se permite la implementación de políticas de seguridad mediante redirección a un elemento, firewall de nivel 3, externo al *fabric*. A este firewall se redirigirá únicamente aquel tráfico que se desee inspeccionar. Si además el firewall tiene capacidades avanzadas de IPS, IDS o antivirus, se tendrá la posibilidad de mejorar la securización del tráfico local entre *datacenters*. Véase en la siguiente figura el ejemplo en que el tráfico http se pasa por un firewall para transitar desde una máquina en un EPG cliente, hacia un frontal web.

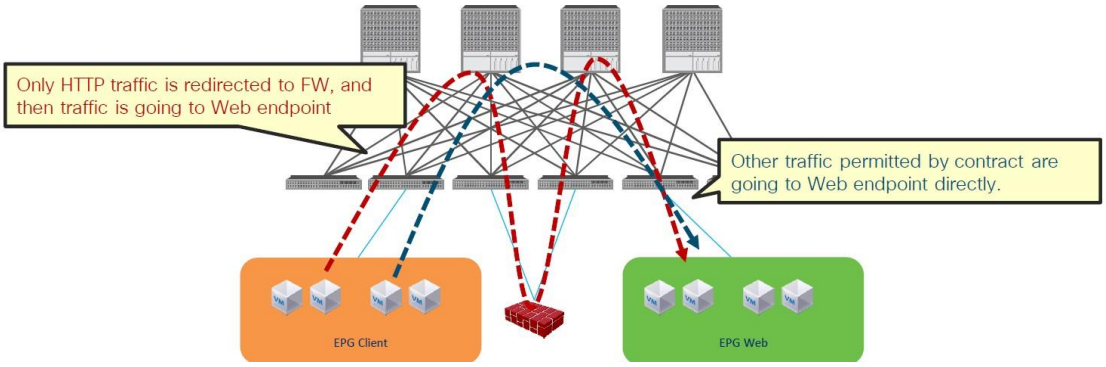

Figura 2-33 Ejemplo de PBR en ACI. Fuente: [38].

En el caso de una arquitectura de red que presente varios Pods, por ejemplo dos, se puede implementar una solución con doble firewall en activo-pasivo (uno en cada Pod), configurando el ACI para que la VRF extendida tenga presencia en ambos Pods. De esta manera los flujos que se quieran securizar horizontalmente pasarán por el firewall activo, incluso en el caso extremo en que origen y destino del flujo se encuentra en una misma sede, y el firewall activo en la sede remota. La alternativa, siguiendo con este ejemplo, sería el uso de los dos firewall en activo-activo, lo que obligaría a definir dos VRFs (una en cada sede) y añadir *routing* entre ambas. Ambas opciones son perfectamente factibles, y la decisión entre una y otra responderá a decisiones de diseño.

Con esta opción 3 se permite mejorar la seguridad horizontal sin las limitaciones de la opción 2 derivadas de los contratos, y la flexibilidad aumentando la granularidad de la inspección en ciertos flujos, a costa de la utilización de un equipamiento externo adicional.

En conclusión, desde el punto de vista de la seguridad, ACI permite implementar una o varias de las opciones indicadas, simultáneamente. Con todo lo desarrollado hasta el momento, se puede plantear el siguiente ejemplo.

Sea una típica situación en la que se plantea la actualización hacia una solución SDN de Cisco ACI desde una arquitectura tradicional:

- Puede ser interesante implementar una solución capa 3 con contrato *VzAny* sobre una VRF "general". Esta aproximación permitiría migrar tranquilamente las VLAN de la red *legacy* al ACI (aproximación de *Nertwork Centric*).
- Al mismo tiempo se configuraría otra VRF (basada en una aproximación de *Application Centric*) para nuevos servicios, con la opción PBR y una pareja de firewalls que filtrarían los flujos este-oeste que se desee inspeccionar.
- Una vez concluida la migración de la red *legacy*, se podría mover de manera planificada el equipamiento cada EPG (VLAN antigua) de la primera VRF hacia la segunda, que está orientada al modelo por aplicación y restringe los flujos por tipo de aplicación mediante el uso de contratos.

Al margen de la securización "lógica" indicada para los flujos verticales y horizontales dentro del *fabric*, otro aspecto a considerar es el de la seguridad "física" del enlace que une los Pods, en una arquitectura extendida con varias ubicaciones geográficas. Este aspecto será tratado en el siguiente capítulo, mediante la configuración de cifrado MACSEC en los enlaces entre sedes.

2.6.8 Plano físico y Static Path

El físico es el otro plano importante en la configuración del ACI, y tiene una sección relevante en el *dashboard* del APIC. Constituye la política de configuración que dará acceso al *fabric*, y maneja varios conceptos:

- *Interface Policy Group*:
  Se utiliza para configurar parámetros específicos en las interfaces de red. Es decir, cubre la configuración de los puertos en los nodos *Leaf*, a los que se conectarán servidores u otras máquinas. Por ejemplo, se puede:
  - Configurar la velocidad (*speed*) de un puerto
  - Habilitar protocolos de vecindad de equipos a nivel dos como LLDP (*Link Layer Discovery Protocol*) o CDP (*Cisco Discovery Protocol*)
  - Habilitar LACP (*Link Aggregation Control Protocol*) para poder agregar varios puertos físicos en un único enlace lógico
- AEP (*Access Entity Profile*):
  El AEP permite desplegar los EPG (*Endpoint Group*) en todos los puertos de la red. Contiene el *Physical Domain*, que es una agrupación de recursos físicos, y dentro de este dominio se encuentran los VLAN pools. Estos pools de VLAN automatizan la asignación de VLAN a los diferentes puertos, facilitando la gestión y configuración de la red

Es decir, el *Interface Policy Group* se encarga de configurar los parámetros específicos en las interfaces, mientras que el AEP gestiona la asignación de VLAN y la implementación de grupos EPG en los puertos de la red.

Finalmente, en el proceso de conectar un servidor físico al ACI mediante conexión a un nodo *Leaf*, se utiliza una técnica conocida como *Static Path*, mediante la cual se une la parte de configuración física con la lógica, habilitando la conectividad. Lo que se está haciendo es, básicamente, pasar una VLAN por el puerto (Figura 2-34).

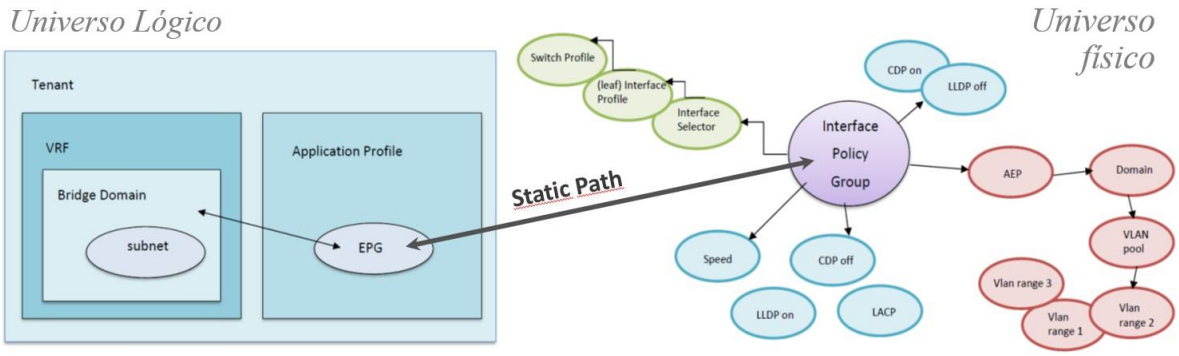

Figura 2-34 Asociación VLAN a puerto (*Static Path*). Fuente: Cisco.

3 DESPLIEGUE DE UNA SOLUCIÓN SDN

El presente capítulo muestra un despliegue que plantea la sustitución de los equipos que constituyen el núcleo de la red corporativa de una empresa, y el cambio de su arquitectura clásica por una solución SDN de *datacenter*, basada en la tecnología de Cisco ACI.

Se realiza en el contexto en el que la empresa amplía sus instalaciones a una nueva sede, añadiendo un nuevo centro de datos. La solución debe facilitar la migración de los servicios existentes a cualquiera de los centros de datos con que contará, permitiendo la movilidad de servidores físicos o virtualizados, y ser compatible con el despliegue en paralelo de nuevos servicios.

Se indicará a continuación el detalle de la solución aplicada, tareas y requisitos previos, componentes físicos a utilizar, topología de red planteada, la estructura lógica de objetos que permite implementar la solución, el procedimiento a seguir para su configuración, y la realización de un plan de pruebas y validación de la solución.

3.1 Análisis de la situación

3.1.1 Escenario Inicial

La empresa dispone de una única sede principal, y su equipamiento de red se encuentra distribuido en diferentes salas técnicas de un mismo *datacenter* (Figura 3-1). Es un equipamiento clásico, con equipos de conmutación del fabricante Cisco que se encuentran al final de su ciclo de vida, con una alta densidad de ocupación de puertos, y una topología en estrella y anillo con capacidades inferiores a 10 Gbps.

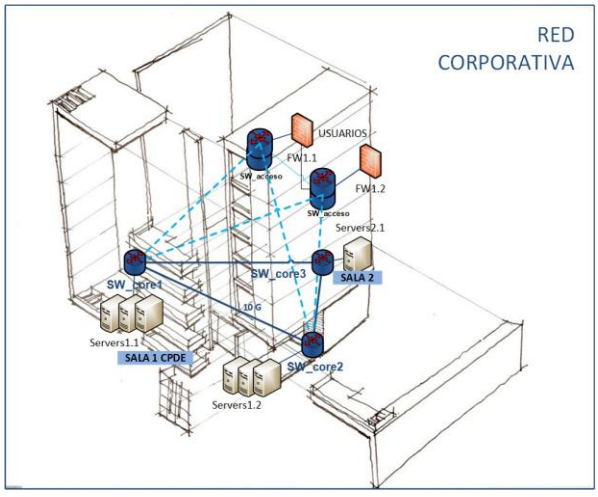

Figura 3-1 Escenario inicial – Red corporativa. Fuente: Propia.

Según se representa en la Figura 3-1, la red corporativa agrega las conexiones de acceso de los usuarios en las diferentes plantas de la sede, y entrega su tráfico a una pareja de equipos de agregación, switches *Catalyst* de Cisco a nivel 3, que se comportan de cara al resto de la red, como un único equipo mediante la tecnología VSS. En estos equipos se realiza una inserción en modo transparente de una pareja de firewalls del mismo fabricante (clúster en activo-pasivo), cuya función es proporcionar la seguridad en las conexiones norte-sur entre los usuarios y el *datacenter*.

Se utiliza EIGRP como como protocolo de enrutamiento dinámico con los equipos para el intercambio de rutas.

Desde el punto de vista de las instalaciones de *datacenter*, la electrónica a sustituir se distribuye en un total de dos salas técnicas repartidas en diferentes plantas del edificio. Ambas salas alojan un total de tres nodos de *core*, switches *Catalyst* configurados a nivel 3, a los que llegan agregadas todas las conexiones de los servidores instalados en su sala.

Estos tres switches de *core* forman un anillo físico de capacidad inferior a 10 Gbps, y se unen a los equipos de agregación de campus de manera redundante mediante un doble enlace.

3.1.2 Escenario Objetivo

El sistema desplegado debe proporcionar una solución al nuevo escenario, en el que la empresa amplía sus instalaciones con una nueva sede secundaria, separada más de 100 km de la principal.

Cada una de las sedes alojará un *datacenter*, y empleados que deberán poder acceder simultáneamente y de manera indistinta a los servicios alojados en cualquiera de los dos centros de datos.

Por tanto, la situación final esperada es la de una red definida por software capaz de distribuir información entre sus nodos, y comunicar los servicios prestados desde los DC de ambas sedes, a la electrónica de planta de la que cuelgan los usuarios.

Se desea además que toda la infraestructura pueda administrase desde un punto centralizado, y que la capacidad interna del sistema escale en todos sus puntos hasta 100 Gbps. La situación se representa en la siguiente Figura 3-2.

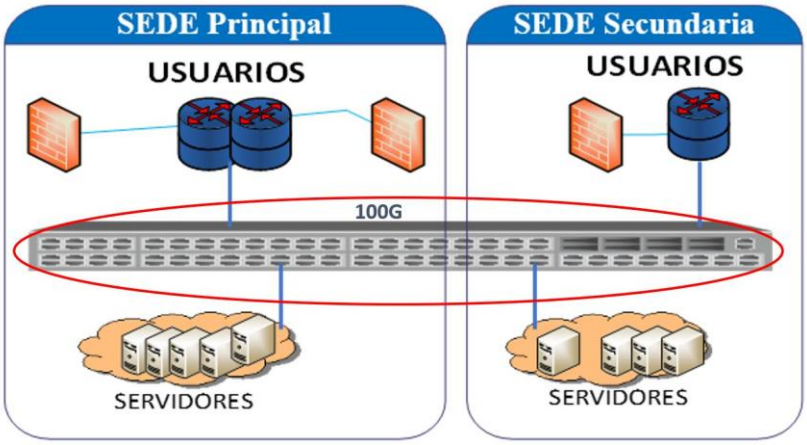

Figura 3-2 Escenario objetivo del *Fabric* extendido. Fuente: Propia.

Se debe ofrecer cierto aislamiento entre las sedes que reduzca el impacto en caso de indisponibilidad en una de ellas, garantizando la seguridad de las comunicaciones con un cifrado entre ambas a una tasa de 100 Gbps, y garantizando unos requisitos técnicos mínimos (latencia, multicast, DHCP *relay*, MTU, OSPF, QoS, etc.).

La tecnología que se empleará es la **solución SDN de Cisco ACI**, explicada ampliamente en el capítulo 2.6. Esta solución garantiza los requisitos planteados de este escenario objetivo. Los dispositivos que formen esta arquitectura, y que se indicarán más adelante, soportan conectividad de

nivel 2 y 3, implementan los principales algoritmos de enrutamiento, y ofrecen suficientes puertos ópticos y/o eléctricos que permiten la interconexión con la red actual y la migración de sus servicios.

Por tanto, la solución SDN de Cisco ACI que se plantea permite desplegar una red automatizada que se caracteriza por integrar en un mismo sistema los dos DC de las sedes principal y secundaria. Es una solución:

- Robusta, redundada, y escalable.
- Presenta un *fabric* extendido, clúster geográfico entre ambas sedes. Similar a un switch extendido en el que podríamos cambiar de puerto un equipo o servidor ubicado en cualquiera de los *datacenters*, sin impacto al servicio.
- Con un elevado ancho de banda (100 Gbps) en todos sus puntos.

Con ello, los objetivos que se persiguen son, entre otros:

- Simplificar la gestión y monitorización del sistema: gestión centralizada de ambas sedes en un mismo dominio.
- Reducir los tiempos de mantenimiento.
- Simplificar el despliegue de nuevos servicios.
- Mayor capacidad para servicios que demanden un gran volumen de datos.

3.1.3 Dimensionamiento y equipamiento necesario

Un paso inicial es evaluar la necesidad, dimensionar la solución, decidir el equipamiento que es necesario, las características y número de los equipos, así como otras necesidades asociadas.

Se necesitarán equipos *Leaf* que proporcionen puertos eléctricos y ópticos, en un número suficiente para conectar (migrar) los servidores existentes, y cierto margen que permita atender la demanda de nuevos servicios.

Realizando una inspección de los servicios activos en cada una de las dos salas técnicas, y su distribución por equipo, se categorizan estos por switch, tipo de conexión (óptica o eléctrica), y velocidad del servicio (*fastethernet*, *gigaethernet* o *ten-gigaethernet*), resultando la distribución que se indica en la Tabla 3-1.

Tipo de Conexión	Switch1	Switch2	Switch3	TOTAL
OPTICA				
1G	44	42	22	108
ELÉCTRICA				
10/100/1000 M	62	48	0	110
10G	6	6	4	16
TOTAL	112	96	26	234

Tabla 3-1 Dimensionamiento de los servicios previos (puertos). Fuente: Propia.

Una vez analizadas las redes configuradas en cada uno de los *Catalyst* que integran estos servicios, se identifican cerca de medio centenar de VLAN activas, estando todas ellas configuradas en los tres switches. Es decir, todas las VLAN configuradas tienen presencia en los tres switches de *core*, alojando el equipamiento que, por redundancia y robustez, se ha distribuido entre las salas.

Una cuestión a tener en cuenta es la conectividad de los servidores en servicio y la protección que puedan tener a nivel de equipo o tarjeta. La necesidad de puertos y el reparto de nuevos equipos por las

salas técnicas se verá condicionado por ello. Las posibilidades de conectividad que un servidor puede utilizar para conectarse a la electrónica de red son varias:

- Sin redundancia, utilizando una única interfaz de red.
- *Teaming* en activo-pasivo, configuración a nivel de tarjeta donde una de las interfaces se mantiene en espera.
- Con un *portchannel*, balanceando el tráfico entre un par de interfaces, mejorando rendimiento y redundancia.

Se asume que, siempre que el servidor o *appliance* a conectar lo permita, se hará mediante un enlace redundado, es decir, con doble puerto mediante un virtual *port channel* (vPC) hacia la pareja de switches *Leaf* (un puerto a cada switch). Se asume que esta es la situación habitual en la situación previa, y en cualquier caso la más conservadora para el nuevo despliegue, desde el punto de vista del dimensionamiento. Esto permitirá que el tráfico del servidor se curse sin corte de servicio ante un mantenimiento o incidencia de un nodo *Leaf*.

Acorde a estos números obtenidos, se utilizarán nodos *Leaf* que equipen puertos de cobre, y otros adicionales que permitan equipar transceptores ópticos. La instalación de los nodos se realizará en pares, como recomienda el fabricante. Se estima que con 48 puertos por *Leaf* (ópticos o eléctricos) para la conexión de los servidores, 96 puertos la pareja, se cubre la demanda de conectividad presente y futura.

Si bien el catálogo de Cisco es amplio, para cubrir las necesidades identificadas es suficiente el siguiente equipamiento:

- Nexus 93600CD-GX (Figura 3-3).
  Este es el elemento de red de la familia Cisco Nexus serie 9300, que adquirirá el rol de *Spine* dentro de la infraestructura ACI. Es un equipo no modular de un *rack unit* (1 RU), que permite flujos de 100 Gigabit Ethernet, con firmware ACI-OS. Ofrece 28 puertos a 10/40/100Gbps de tipo QSFP28 y 8 puertos a 10/40/100/400Gbps de tipo QSFP-DD.

Figura 3-3 Equipo con rol de *Spine*. Fuente: [40].

- Nexus 93108TC-FX3 (Figura 3-4).
  Elemento de red de la serie 9300 que adquirirá el rol de *Leaf* de conexionado de cobre dentro del propio *fabric*. No es modular y ocupa 1 RU. Dispone de 48 puertos a 100Mbps/1/10Gbps Base-T de tipo RJ45 y 6 puertos de *uplink* a 40/100Gbps de tipo QSFP28 (que también admiten una combinación de conectividad a 1/10/25/40/50/100 Gbps).

Figura 3-4 Equipo con rol de *Leaf* de cobre. Fuente: [41].

- Nexus 93180YC-FX3 (Figura 3-5).
  De la misma serie 9300, equipo de 1 RU, este elemento de red podrá adquirir diferentes roles dentro de la arquitectura. En caso de utilizar el firmware de ACI adquirirá el rol de *Leaf* de conexionado de fibra dentro del propio *fabric*. En el caso de utilizar el sistema operativo NX-OS adquirirá el rol de IPN.

Con ambos roles ofrece 48 puertos a 1/10/25Gbps de tipo SFP28 y 6 puertos de *uplink* a 40/100Gbps de tipo QSFP28.

Figura 3-5 Equipo con rol de *Leaf* de fibra, e IPN. Fuente: [41].

Los equipos con rol de IPN equiparán una licencia de seguridad adicional (ACI-SEC-XF), que les habilita para realizar el cifrado MACSEC en sus puertos, característica necesaria para el cifrado del tráfico entre los dos Pods.

- Controlador: APIC-CLUSTER-M4 (Figura 3-6).
  Se instalará **un clúster** compuesto por **tres APIC M4**, de configuración media (CPU, discos duros y memoria) y que permite gestionar hasta 1200 *edge ports* (es decir, utilizando *Leafs* de 48 puertos, puede gestionar hasta un máximo de 24 nodos *Leaf*).
  Admite hasta 10 unidades de almacenamiento de 2.5 pulgadas HDD SAS/SATA o SSD, así como NVMe SSD. Más información en la referencia [42].

Figura 3-6 Controlador Cisco APIC. Fuente: [32].

Para decidir qué ópticas (transceptores) utilizar en los puertos de red (NNI) de los nodos (*Leaf*, *Spine* o IPN), que interconectarán la electrónica red del fabric ACI, antes se debe decidir qué fibra óptica utilizar, si monomodo (SMF) o multimodo (MMF). La elección entre ambas depende principalmente de la distancia que se necesita cubrir y el ancho de banda requerido internamente en el *fabric*.

Para las tasas de 100 Gbps, una fibra óptica multimodo de tipo OM4 permite cubrir hasta una distancia aproximada de 150 m. Si la distancia entre los equipos de un mismo Pod va a ser inferior, como es el caso, se recomienda esta opción multimodo. No solo por resultar más económica que la monomodo, sino además porque con esta última aumenta la probabilidad de quemar las ópticas, probabilidad que aumenta a menor distancia. Máxime en situaciones habituales en que los equipos se encuentran instalados en un mismo rack, o racks contiguos.

Por tanto, debe calcularse la máxima distancia entre elementos de la arquitectura *Leaf* and *Spine* en cada Pod, que habitualmente es aquella necesaria para unir los *Leafs* de una sala técnica con el *Spine* que se encuentra (por robustez de la solución) en otra sala técnica. En el caso que nos ocupa, la mayor distancia es inferior al límite indicado, en ambos Pods, por lo que se usará **fibra óptica multimodo OM4** en ambos *datacenters*.

De esta manera, las ópticas Cisco recomendadas para las interfaces NNI son las QSFP-40/100-SRBD (100G and 40GBASE SR-BiDi QSFP *Transceiver*, 100m OM4 MMF, con conector LC). Más detalle en [43].

Aunque no es la situación implementada, en caso de optar por utilizar ópticas monomodo, se podrían utilizar módulos Cisco QSFP-100G-SM-SR, que soportan distancias de enlace de hasta 2 kilómetros sobre un par estándar de G.652 *Single-Mode Fiber* (SMF), con conectores LC dúplex. Funcionaría, pero por los motivos indicados no se utilizarán.

El resto de los elementos de la solución utilizaran interfaces a menor tasa, en eléctrico o con ópticas multimodo. Este es el caso de los controladores APIC (10 Gbps SFP+), los puertos de gestión fuera de banda de cada nodo (eléctrico RJ45), o las interfaces requeridas por los diferentes elementos que se conecten a los *Leaf* (servidores a 1/10G, en eléctrico u óptico) o *Border Leaf* (Firewalls a 40/100G habitualmente, etc.).

Se estima que la necesidad de puertos de la nueva sede secundaria se cubre con la instalación de una pareja de nodos de cada tipo, lo que ofrecerá a los sistemas del *datacenter*, 96 puertos ópticos y 96 eléctricos (hasta 48 máquinas o servidores con conexión redundada, de conectividad óptica, y otros tantos eléctrica).

Por otra parte, se tiene previsto crecer en servidores de conectividad óptica en la sala principal de la sede actual, motivo por el cual se añade una pareja adicional de nodos *Leaf* de fibra en la primera sala del Pod1.

Además, el *datacenter* de la sede secundaria alojará por robustez uno de los tres *appliances* que forman el clúster APIC.

Por todo lo indicado, y en base al análisis de los servicios activos, la distribución de los equipos para el nuevo escenario extendido a los dos sites, es la de la siguiente Tabla 3-2.

Tipo de Equipo	Modelo	DC 1	DC 2	TOTAL
Controlador	APIC M4	2	1	3
Spine	93600CD-GX	2	2	4
Leaf de cobre	93108TC-FX3	4	2	6
Leaf de fibra	93180YC-FX3	6	2	8
IPN	93180YC-FX3	2	2	4

Tabla 3-2 Distribución de equipos. Fuente: Propia.

3.2 Diseño del plano físico y Topología

El escenario contempla dos *datacenters* por lo que se considera una arquitectura multi-DC. Se utiliza una arquitectura extendida de tipo **Multipod**, formada por dos Pods que son las sedes principal y secundaria. Esto es posible porque se cumplen todos los requisitos técnicos necesarios (*multicast*, DHCP *relay*, MTU mínima de 1550, OSPF) así como un RTT máximo de 50 ms entre las sedes.

De esta manera se mantiene un aislamiento entre los Pods, reduciendo el impacto en el funcionamiento de uno de ellos frente a problemas que pudieran darse en el otro, y sin la complejidad o coste de una solución multisite.

El nuevo sistema despliega por tanto una arquitectura con un **único clúster APIC** de controladores, formado por tres *appliances*, distribuidos entre ambas sedes, garantizando una alta disponibilidad ante fallos, al tiempo que se proporciona un único punto para gestionar y controlar las políticas.

Cada Pod es una estructura *Leaf and Spine* de dos niveles, como puede observarse en la Figura 3-7, cuyos equipos físicos se instalan por parejas en la sala o salas técnicas que componen su *datacenter*, siguiendo criterios de redundancia y robustez.

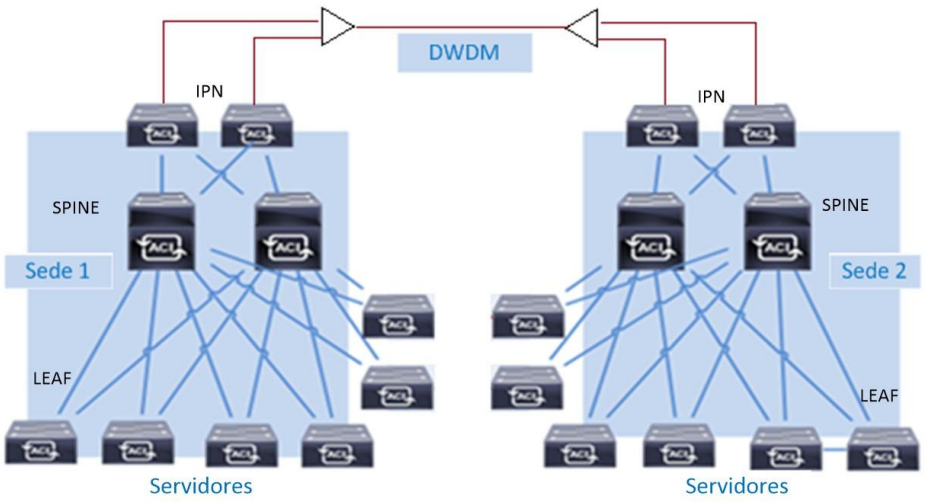

Figura 3-7 Topología de red propuesta. Fuente: Propia.

Aunque no es objeto de esta memoria, la conectividad entre las dos sedes puede realizarse mediante equipamiento óptico DWDM de fabricantes como Ciena. Este fabricante dispone de una solución técnica solvente (un portafolio con tarjetería de detección de cortes de fibra, amplificadores dinámicos, filtros pasivos, chasis modulares, tarjetas de tráfico con *throughputs* desde 100 Gbps a varios Tbps, con o sin cifrado, gestor centralizado, etc.), y garantiza los requisitos técnicos mínimos (como el de latencia RTT), impuesto por la arquitectura Multipod.

Al ser una solución en un entorno de multi *datacenter*, entre ambas sedes se requiere de elementos de interconexión adicionales (a la arquitectura *Leaf and Spine*), que forman la **red IPN** (*Inter Pod Network*) para proporcionar la conectividad sobre el enlace DWDM entre ambas sedes. Será la red IPN la que configure en los puertos de sus switches, sobre las interfaces ópticas de unión entre las sedes, la funcionalidad de cifrado MACSEC (requisito imprescindible en la solución), según se ha explicado en el apartado 2.1.3 previo.

De esta manera, según puede observarse en la Figura 3-8, en la topología final cada *switch Leaf* está conectado a los switches *Spine* de su sede. Estos *Spine* se conectan a una red IPN que provee el acceso a la sede remota mediante el equipamiento DWDM. Toda la conectividad entre switches *Leaf* de la misma o distinta sede (pasando por los switches *Spine*, la red IPN y el equipamiento DWDM) se realiza mediante enlaces de alta capacidad a 100 Gbps.

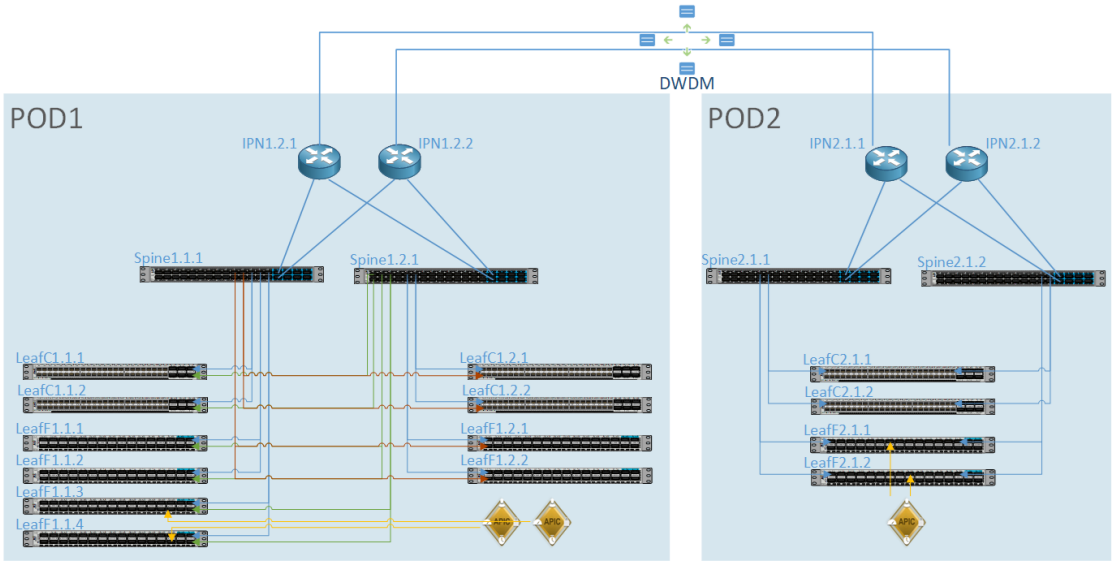

Figura 3-8 Esquema de red y equipos instalados. Fuente: Propia.

El Pod1 de la sede principal se caracteriza por estar repartido en dos salas técnicas. En cada sala se instala un nodo *Spine*, y uno de los tres controladores del clúster APIC (dos controladores en el Pod1). La instalación de los nodos Leaf se reparte entre las salas por parejas, con puertos de fibra o cobre, respondiendo al dimensionamiento previamente calculado en la Tabla 3-2.

El Pod2 de la sede secundaria consta de una única sala técnica, que aloja todos los nodos *Leaf y Spine* de este *datacenter*, así como el tercer controlador APIC del único clúster de la solución. En ambos extremos la pareja de IPN que conecta los Pods se ubica en la misma sala y rack (se instalan en *stack* a una distancia máxima de 5 m).

Siendo el esquema de red de la nueva arquitectura el indicado en la Figura 3-8, este tendrá que convivir con la red *legacy* un tiempo. Es por tanto necesario realizar la **interconexión de la red *legacy* con el *fabric* ACI**. La causa es que es necesario migrar los servicios que actualmente se encuentran en el *datacenter* tradicional.

Esta tarea no es inmediata, sino que se realiza moviendo máquinas de la red tradicional a un *Leaf* de ACI, mientras otras máquinas de esa misma VLAN permanecen conectadas a los switches *legacies* del *datacenter* original. Mientras dure esta situación intermedia la visibilidad entre las máquinas en ambas arquitecturas debe mantenerse.

Se debe, por tanto, extender cada una de las VLAN *legacy*, hasta el *fabric* ACI. La pasarela de unión entre la red *legacy* y el ACI se configura en modo troncal, dejando pasar todas las VLAN existentes en la infraestructura de origen (unas cincuenta como se ha indicado anteriormente). Una vez extendida la VLAN, esta se mantendrá hasta que todas las máquinas de esa VLAN se hayan migrado a los nodos *Leafs* del ACI. En ese momento se podrá borrar la VLAN de la red tradicional.

La situación se recoge en la Figura 3-9, donde se muestra un ejemplo en el que se migra una máquina de la VLAN 100.

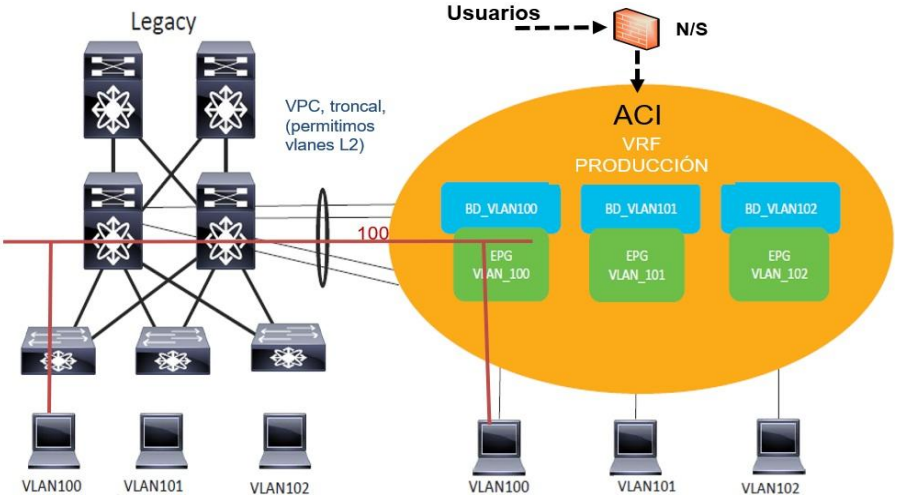

Figura 3-9 Interconexión red *legacy* - fabric ACI. Fuente: Propia.

3.3 Diseño del plano lógico

Debe tenerse en cuenta que en la arquitectura inicial tanto los switches de agregación de usuarios como los switches *core* a sustituir se encuentran a nivel 3.

Con el fin de determinar cómo se realizará la conectividad de los elementos del *fabric*, y teniendo igualmente en cuenta las consideraciones indicadas en el apartado 2.6.7 sobre modelos de despliegue, la solución recomendada a priori es la configuración del ACI a nivel 3. De esta manera, desde un punto de vista lógico, ambas sedes se comportarán como un mismo *fabric* extendido.

Sin embargo, hay que tener en cuenta como se ha indicado previamente, el proceso a seguir para la migración de los servidores a la nueva solución, y el tiempo previsto para su ejecución. De esta

manera, es fácil concluir que esta es una tarea que se alargará durante meses, en la cual la solución antigua o *legacy*, y la nueva arquitectura SDN deben coexistir.

En la arquitectura *legacy* los servidores y resto de máquinas activas prestando servicio se encuentran organizados en VLAN, redes de nivel 2, que encuentran su *gateway* o nodo de nivel 3 en el switch *core*. En estas VLAN pueden coexistir equipos muy dispares (como un *netscaler*, una base de datos, etc.), por lo que la migración de estos equipos debe estar muy planificada debido a las muchas dependencias.

Si se realizase directamente la configuración del ACI a nivel 3 para los servicios existentes, los servidores deberían cambiar su *gateway* al ACI en el momento de migrarlos a un *Leaf*. Ello implica el uso de nuevos rangos de direccionamiento en ese momento para las máquinas migradas. El hecho de que las máquinas de una misma VLAN *legacy* deban seguir comunicándose con las reubicadas mientras dure la migración, y la diferente naturaleza de las mismas, en la práctica imposibilita o al menos complica enormemente establecer el nivel 3 en ACI directamente.

Por tanto, la solución propuesta y que se implementa es configurar el **ACI a nivel 2 para los servicios *legacy***, hasta el momento en que se complete su migración, y al mismo tiempo establecer el **ACI a nivel 3 para los nuevos servicios** que se implanten.

Es preciso para ello, comunicar la red *legacy* al *fabric* ACI (apartado 3.2), y mantener esta comunicación hasta la efectiva migración de los servicios del *datacenter*, a la nueva arquitectura.

Pasando a definir el modelo lógico según se ha indicado en el apartado 2.6.6, sobre el plano de conectividad que condiciona la comunicación dentro de ACI, es necesario definir la capa lógica acorde a las necesidades del despliegue. Una configuración incorrecta inhabilitará el flujo de datos.

Se toman las siguientes **decisiones de diseño**:

- Se configuran **3 *tenants***, para separar en el *fabric* los tres entornos que se implantan: desarrollo, preproducción y producción.
- Los entornos de preproducción y producción no comparten recursos (no se unen por tanto a través de *firewall*).
- Los *tenant* de desarrollo y preproducción solamente disponen de una VRF cada uno.
- El *tenant* de producción configura en el momento del despliegue dos VRF:
    - Una **VRF "general"**, que sirve para ir recogiendo en sus EPG los servicios migrados de la red *legacy*. Como se ha indicado en el apartado 2.6.7, esta VRF sigue una aproximación de *Network Centric* y, por tanto, cada EPG incluye máquinas (físicas y/o virtuales) de distinta naturaleza.
    - Una **VRF "corporativa"** que sirve para ir integrando los nuevos servicios con una aproximación de *Application Centric*. También recogerá con el tiempo las máquinas de la VRF general previa, que se vayan desmontando o migrando.
- Dentro de la VRF general todos los EPG tienen visibilidad entre sí, al configurarse con un contrato genérico (***VzAny*)** a nivel de VRF y acción *permit*.
- En la VRF corporativa todos los flujos entre EPG están denegados por defecto. Solo se habilitan los flujos que permitan los **contratos** expresamente definidos, bien con una acción *permit*, o bien con una redirección a firewall externo (PBR).
- Se realiza por tanto un control de **flujos este-oeste** (horizontal) entre los servidores de un mismo o distinto Pod. Estos *firewalls* son independientes de los que pueda haber instalados para la inspección de los flujos norte-sur (de usuarios con el *datacenter*).
- Con el fin de realizar una inspección de los flujos horizontales se instala una solución SDN de otro fabricante (distinto a Cisco por seguridad) consistente en la instalación de un orquestador que coordina un clúster de firewalls, de manera que en cada sede (Pod) se instala una pareja en activo-pasivo, y ambas parejas funcionan en activo-activo mediante dicha orquestación.

Se pretende implantar, de esta manera, una solución sencilla y flexible que permite desplegar nuevos servicios utilizando toda la potencia de Cisco ACI, facilitando al tiempo la migración desde la red tradicional. Además, se incrementa la seguridad horizontal, mediante el uso de contratos, pudiendo realizar un ajuste más fino en los casos en los que se desee, mediante redirección a *firewalls* externos. La situación indicada es la que se refleja en la Figura 3-10.

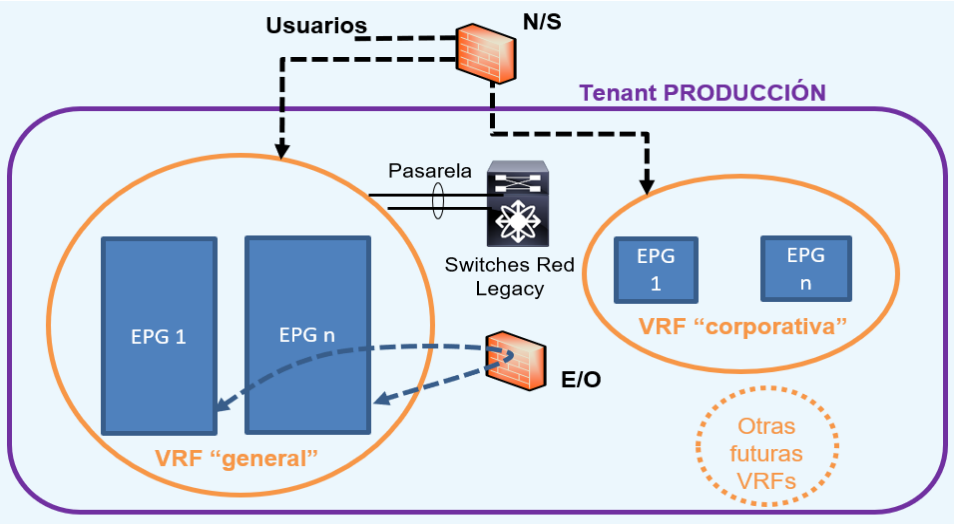

Figura 3-10 Diseño de VRFs en el *tenant* de Producción. Fuente: Propia.

Referente a los flujos se deben definir varios **contratos** para que la conectividad dentro y entre distintas VRF sea posible:

- Un contrato dentro de la VRF general, que es un *VzAny* a nivel de esta VRF, para permitir todos los flujos en su interior.
- Un contrato entre las VRF general y corporativa, para que los EPG de la corporativa puedan acceder a los recursos alojados (y migrados) de la red *legacy*.
- Un contrato para que los EPG dentro de la VRF corporativa puedan exportar sus rutas hacia fuera del ACI. Esto es necesario para la comunicación del ACI con redes externas (conectadas a los *Border Leaf*) sea posible, o simplemente para manejar los flujos norte-sur del ACI con la red de usuarios.
- Un número variable de contratos EPG a EPG, dentro de la VRF corporativa, que son los que habilitan los flujos concretos entre grupos EPG dentro de esta VRF (por defecto están todos denegados).

Además, se configura un **L3Out** (enlace de nivel 3) desde cada VRF hacia cada elemento externo al que el ACI desee acceder. Este puede ser el caso de una red externa que se encuentra detrás de un elemento de nivel 3, o el de un *firewall* (que es tratado por el ACI como un EPG externo más).

3.4 Tareas y requisitos previos

En este apartado se recopilan aquellas tareas y acciones previas, físicas o de configuración, que es necesario realizar de manera previa al levantamiento y configuración de la solución SDN multipod.

Inicialmente, previo a la configuración del sistema, es necesario completar una serie de tareas:

- Instalación física en las salas técnicas de los dos sites, del equipamiento ACI necesario:
  - Pod1: 2 controladores APIC, 2 *Spine*, 4 *Leaf* de cobre y 6 *Leaf* de fibra.
  - Pod2: 1 controlador APIC, 2 *Spine*, 2 *Leaf* de cobre y 2 *Leaf* de fibra.
- Instalación física en *stack* del par de nodos IPN en cada uno de los Pods (4 IPN en total). Incluyen las licencias necesarias para habilitar la función de cifrado MACSEC.

- Instalación del equipamiento DWDM, habilitando dos enlaces ópticos entre las sedes. En el extremo de cada enlace, conectado al DWDM, se encuentra el *uplink* de un equipo IPN. De esta manera cada IPN de un Pod tiene enfrentado un solo IPN del otro Pod.
- Cableado entre los componentes de toda la arquitectura ACI (ambos Pods) con fibra óptica multimodo OM4, y ópticas acordes a tasa de 100 Gbps con conector LC, según se justificó en el apartado 3.1.3.
- Cableado de todos los equipos físicos a switches de gestión externos al ACI, que permitan un acceso de gestión fuera de banda (OOB) a cada equipo.

3.4.1 Preparación de la capa óptica DWDM

Sin entrar a mayor detalle en este apartado, indicar que la solución DWDM del fabricante Ciena es muy apropiada para establecer un enlace óptico de 100 km entre las dos sedes. Esto es así debido a su capacidad para transportar grandes volúmenes de datos a unas tasas elevadas (100 Gbps y superior), de manera eficiente y con una baja latencia, cumpliendo sobradamente el requisito de 50 ms RTT, que impone la arquitectura de ACI Multipod.

A grandes rasgos los componentes involucrados en cada site, desde el exterior hacia el interior, son los siguientes:

- Tarjetas ESAM OTDR, utilizadas para la medición y monitorización de la fibra óptica, advirtiendo de posibles cortes en la integridad del enlace.
- Amplificadores adaptativos XLA, que mejoran la señal óptica a lo largo del enlace compensando de manera dinámica la atenuación.
- Filtros pasivos CMD4X, que permiten la separación y multiplexación de diferentes señales ópticas en el enlace DWDM. Estos filtros recogerán los enlaces *uplink* de las diferentes tarjetas de tráfico alojadas en los chasis.
- Chasis 6500, con un número variable de slots que proveen la infraestructura física para alojar la tarjetería de tráfico y gestión del enlace.
- Tarjetas de tráfico, que agregan los servicios y ofrecen protección por conmutación óptica en sus puertos de línea hacia los filtros. Facilitan una transmisión y recepción de datos estable y redundada a través del enlace óptico.

Ejemplo de servicio que recoge el DWDM es el del sistema ACI, entregado en uno de los puertos cliente 100G de sus tarjetas de tráfico, a través del *uplink* de un equipo IPN.

Es recomendable, y así se hace con este sistema, proporcionar una redundancia física de enlace óptico entre las sedes. Se realiza redundando los componentes desde la calle hasta los filtros en cada site, de manera que la tarjetería de tráfico se conecte a sus filtros pasivos. Ambos caminos ópticos pueden ser provisionados por diferentes operadores de red, para asegurar una alta disponibilidad en caso de corte de fibra en cualquiera de los caminos.

Esta configuración en doble enlace, mostrada en la Figura 3-11, será la que se aplique en este caso de despliegue SDN Cisco. Mas información sobre la capa óptica en la web del fabricante Ciena [44].

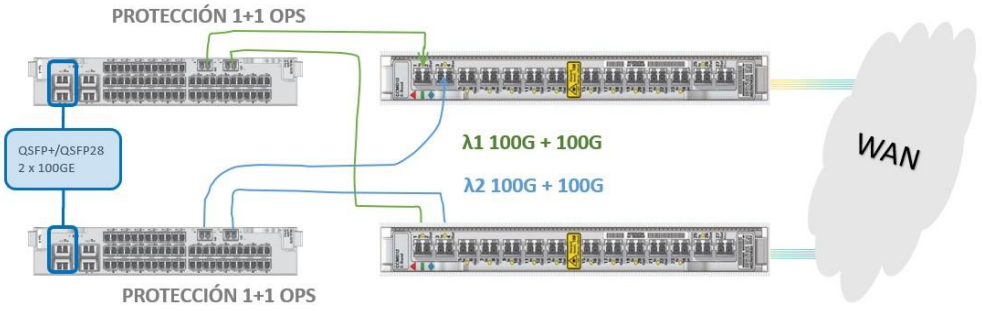

Figura 3-11 Configuración de los enlaces ópticos entre Pods. Fuente: Propia.

3.4.2 Red IPN

La configuración de la red IPN es una tarea externa al ACI (esta red no es gestionable por sus controladores APIC), pero necesaria para la solución SDN en su conjunto, pues esta red de nivel 3 es la encargada de proporcionar conectividad entre los dos Pods.

Esta tarea de configuración se realiza una vez que los enlaces ópticos están activos. Dependiendo de cómo se realice la configuración del ACI, la de los IPN podrá realizarse con anterioridad o en medio del proceso. Si se desea que la configuración de ACI levante todos los equipos de ambos Pods a la vez, la configuración de los equipos IPN debe realizarse antes. Este es el caso que se sigue en este despliegue.

Antes de configurar cada uno de los equipos de la red IPN es necesario recabar cierta información sobre el direccionamiento utilizado en cada una de sus interfaces, tanto en la conexión de cada uno contra el IPN remoto (Pod opuesto) como contra su pareja local de nodos *Spine*.

Debe definirse también la configuración MACSEC, aplicando la clave y definición tanto en origen como en destino.

```
key-chain macsec-psk no-show
key chain ACI_Pod2 macsec
  key 1001
    key-octet-string 7 ****** cryptographic-algorithm AES_256_CMAC
    send-lifetime 00:00:00 Oct 29 2024 duration 31536000
macsec policy ACI_Pod2
  cipher-suite GCM-AES-256
  key-server-priority 0
```

3.4.3 Software, direccionamiento y modelo de despliegue

Además de lo indicado, antes de poder comenzar a configurar el ACI, deberemos provisionar y recopilar cierta información:

- Elección de la versión software a instalar.
- Asignación de direccionamientos de gestión fuera de banda (OOB) para cada equipo (APIC, IPN, *Spine* o *Leaf*).
- Rangos de direccionamiento que ACI requiere para su funcionamiento interno (Tabla 3-4).
- Una información sobre cada uno de los equipos instalados, necesarios para la etapa de autodescubrimiento que se lanzará desde la interfaz gráfica del controlador (Tabla 3-5).

La versión software estable y más reciente recomendada por Cisco para el sistema es la de la Tabla 3-3.

Equipamiento	**Modelo**	**versión**
Controlador	APIC M4	5.3(2b)
Spine	93600CD-GX	n9000-15.3(2b)
Leaf de cobre	93108TC-FX3	n9000-15.3(2b)
Leaf de fibra	93180YC-FX3	n9000-15.3(2b)
IPN (NX OS)	93180YC-FX3	9.3.6

Tabla 3-3 Matriz de versiones software. Fuente: Propia.

En la Tabla 3-4 se pueden ver los rangos asignados al Fabric para que los asigne internamente a su criterio y de manera dinámica.

Descripción	Rango
TEP Pool Pod1	10.x.0.0/16
TEP Pool Pod2	10.y.0.0/16
BD Multicast Address pool	225.0.0.0/15
External TED pool Pod1	10.z.u.0/24
External TED pool Pod1	10.z.v.0/24

Tabla 3-4 External / TED pools asignados a ACI. Fuente: Propia.

A continuación, se muestra en la Tabla 3-5 un ejemplo del tipo de información que es necesario proporcionar en el proceso de autodescubrimiento del fabric. Se solicitará para todos los ítems, aunque por simplicidad se muestra solamente para alguno de los equipos instalados.

Equipo	Serial	Hostname	Pod	Node-ID	Rol	IP gest_oob
APIC1.1.1	xxx	Apic111	1	1	APIC	IP_Apic111
Spine1.1.1	xxx	Spine111	1	1001	*Spine*	IP_Spine111
LeafC1.2.2	xxx	Leafc122	1	1204	*Leaf*	IP_Leafc122
LeafF1.1.2	xxx	Leaff112	1	1210	*Leaf*	IP_Leaff112
IPN2.1.2	xxx	Ipn212	2	NA	NA	IP_Ipn212

Tabla 3-5 Datos necesarios para fase de autodescubrimiento. Fuente: Propia.

A la hora de asignar nombre a los equipos una recomendación práctica que se sigue en este tipo de despliegues es la utilización de una numeración que implícitamente nos de pistas de la ubicación física de cada equipo. Se suele seguir una nomenclatura en la elección de los *hostname* de cada equipo, del tipo: *Pod-Sala-Nºequipo*. Por ejemplo, un Spine123 es un *Spine* que se encuentra en el Pod1, sala 2, tercer equipo en esa sala.

3.5 Configuración del Sistema ACI

En este apartado se hace referencia a tareas previas, desarrolladas en el apartado 3.4.

Una vez completada la **instalación física** de todos los componentes del sistema en los dos Pods (controladores APIC, nodos *Leaf y Spine*, la red IPN, y el equipamiento DWDM), y realizados todos los cableados entre los mismos (servicio, pero también gestión fuera de banda), se procede a la puesta en marcha del sistema y su posterior configuración.

Se verifica que todos los componentes que conforman el sistema, previamente citados, se encuentran correctamente conectados a nivel de datos, y alimentados (doble fuente de alimentación a circuitos independientes, siendo recomendable de 32 A).

Se procede al **encendido** de los mismos, en ambos sites, siguiendo el siguiente orden recomendado:

- Equipos DWDM (verificando los correctos niveles de potencia, protección de enlaces, etc.).
- Equipos IPN. No es necesario habilitar de inicio el MACSEC en los puertos, aunque puede hacerse.
- Equipos *Spine.*
- Equipos *Leaf*, indistintamente de cobre y/o de fibra.
- Verificado la ausencia de alarmas o *warnigns* en los equipos (es decir, resueltos los problemas que puedan darse como carga de *firmware*, etc.) es recomendable habilitar en todos ellos un acceso de gestión fuera de banda (OOB) mediante conexión UTP a switches de gestión, asignando el correspondiente direccionamiento IP.
- Se enciende el primer APIC, comenzando por uno de los dos ubicados en el Pod1 principal desde donde se realiza la configuración del sistema. El encendido de los otros dos APIC esperará a que el primero se haya configurado.

Se verifica en este momento que ambas sedes se ven correctamente, con los **enlaces DWDM** funcionando sin problema y las licencias cargadas correctamente.

A continuación, se procede a configurar cada uno de los equipos de la **red IPN**. Para ello se realiza una conexión local a la consola del equipo, y tras introducir las credenciales y ganar privilegios (*Enable / conf terminal*) procederemos a configurar los puertos y servicios. Es opcional definir la configuración de MACSEC en este momento.

Una vez comprobada la correcta conectividad entre todos los IPN, y con el resto de la arquitectura ACI levantada, procedemos con la configuración del ACI propiamente dicha.

3.5.1 Configuración inicial y Autodescubrimiento

La **configuración inicial** de ACI comienza mediante un acceso por consola, en la que se nos solicita una serie de valores globales para el funcionamiento interno del *fabric*.

Se debe realizar una conexión serie al APIC del Pod1 que configuremos, para conectar un pc de forma local al controlador. En ese momento aparecerá un *setup* de bienvenida, según se puede observar en la Figura 3-12, que solicitará unos valores para la definición global del sistema:

- *Number of controllers*: “3” que son los que tendrá el clúster.
- *Controller name/id*: por ejemplo “apic1”.
- POD *id*: “1” pues este controlador se encuentra en Pod1.
- VTEP *pool*: “0.0.0.0/16”.
  (Como se explicó en el apartado 2.6.3, este es el rango IP que utilizará internamente ACI para permitir la comunicación entre dispositivos dentro de la red ACI, mediante VxLAN).
- *Infra VLAN id*: por ejemplo “4093”.
- OoB *config*: la IP de gestión OOB que le demos a este APIC, por ejemplo “192.168.70.161/24”.
- *Username/password*.

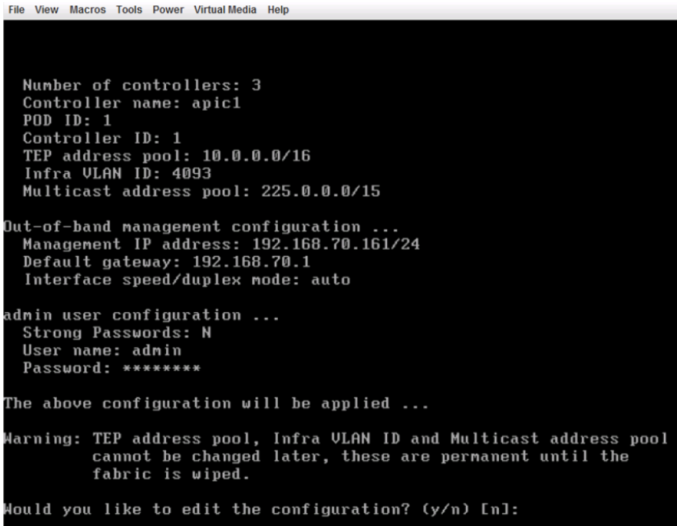

Figura 3-12 Configuración inicial del ACI (CLI). Fuente: [45].

En este momento, se puede repetir el proceso en los otros dos APICs, actualizando los datos correspondientes solicitados por el *wizard*.

Se debe indicar que, si el siguiente paso da problemas, puede ser necesario conectarse al puerto CIMC del APIC para habilitar el protocolo LLDP, fundamental para realizar el descubrimiento de los equipos del ecosistema SDN (en el caso real de despliegue fue necesario).

A partir de este punto procedemos a lanzar la interfaz gráfica web, e iniciar el **autodescubrimient**o de los componentes de ACI. El técnico podrá conectarse directamente a un puerto de gestión del APIC metiendo su IP en el mismo rango OOB del APIC, para lanzar la interfaz GUI mediante el navegador (Figura 3-13).

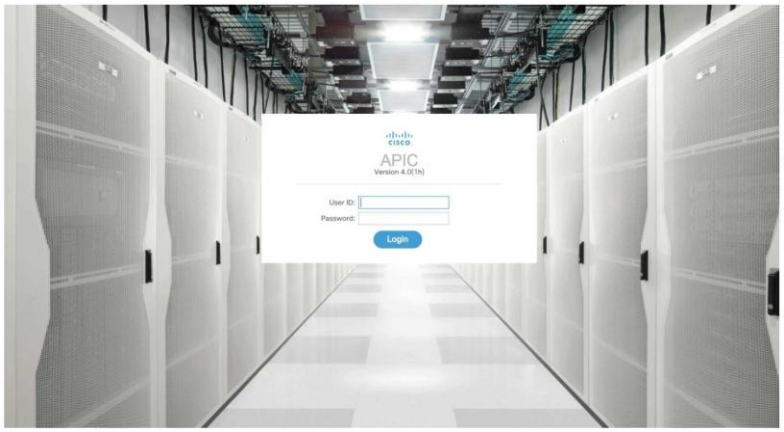

Figura 3-13 Acceso GUI al APIC. Fuente: [38]

Al ingresar con las credenciales previamente configuradas por consola, aparece la vista de la Figura 3-14, *dashboard* ofrecido por el controlador. En la misma se puede ver que el sistema tiene ya conocimiento de los tres controladores, y muestra el estado de salud general del sistema.

No se explicará la distribución del *dashboard* (que se puede consultar en la referencia [15]) aunque se llama la atención del lector sobre las pestañas "*System*" para monitorización general del estado del sistema, "*Tenant*" donde se puede configurar la parte lógica, "*Fabric*" para la parte física, y "*Admin*" para labores de mantenimiento, entre otras.

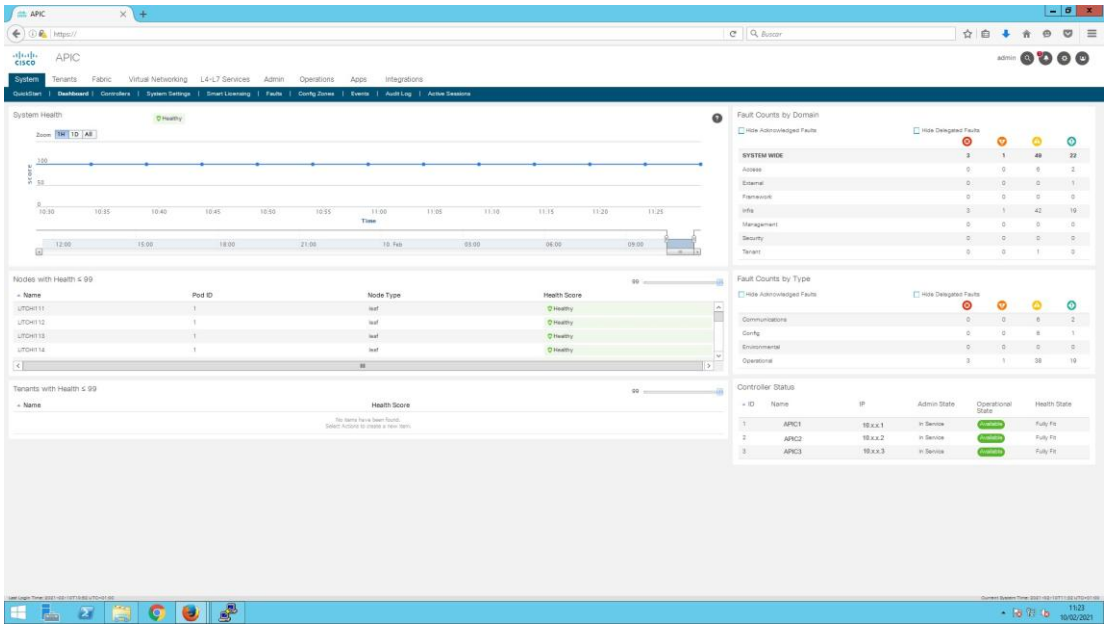

Figura 3-14 Dashboard APIC de Cisco ACI. Fuente: Propia.

En este punto es necesario recopilar información básica que utilizará el ACI internamente para el descubrimiento de la topología, como son los números de serie de los equipos, *hostnames* asignados (así lo mostrará el *dashboard*), número de Pod en el que se han instalado, y *host-ID* de cada equipo (ver Tabla 3-5).

El proceso para añadir un nodo se realiza desde la pestaña *Fabric -> Inventory -> Fabric Membership y Nodes Pending Registration*.

Ahí encontraremos la lista de dispositivos que ACI reconoce, pero no sabe qué rol desempeñan, hasta que se lo indiquemos. El descubrimiento de equipos, lo que ACI muestra en esa lista, irá aumentando secuencialmente:

- Primero se descubrirán los 2 *Leaf* a los que el APIC está directamente conectado.
- Posteriormente los *Spine* que se conectan a los anteriores *Leaf*, un nivel por encima.
- A continuación, se mostrará el resto de nodos *Leaf y Spine* de la arquitectura.
- Si la configuración de los equipos IPN entre ambos Pods está correctamente realizada, aparecerá el resto de la arquitectura del Pod remoto al APIC desde el que estamos configurando. Evidentemente, si entramos en cualquiera de los otros dos APIC del clúster, la vista es la misma, pues el clúster se mantiene sincronizado.

Para completar el descubrimiento de cada uno de los elementos listados en la lista de *"pending nodes"*, se selecciona cada una de las entradas y se va aportando la información que se solicite de la Tabla 3-5. Podremos observar cómo los nodos van pasando a un estado de "*registering*" y posteriormente "*discovering*".

Al cabo de unos minutos podremos encontrar todos los nodos bajo la pestaña de "*registered nodes*", habiendo quedado integrados en el *fabric* a todos los efectos. En las siguientes figuras (Figura 3-15, Figura 3-16 y Figura 3-17) se muestra la situación final.

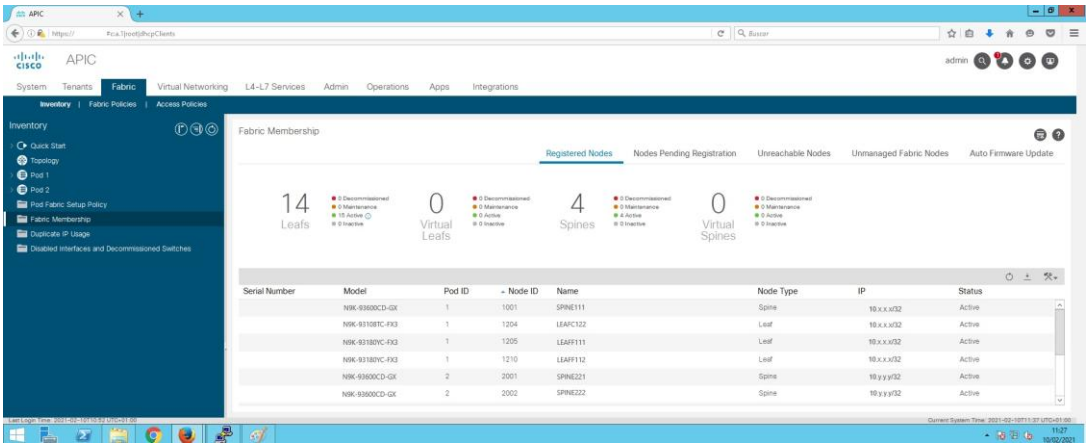

Figura 3-15 Relación de nodos registrados en el *fabric* ACI. Fuente: Propia.

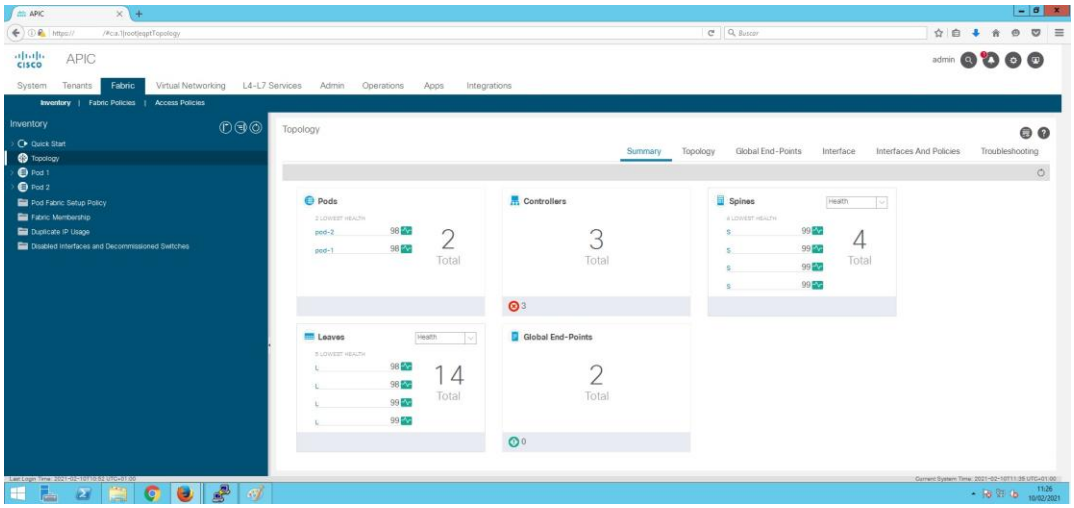

Figura 3-16 Estado final del *fabric* ACI (vista APIC). Fuente: Propia.

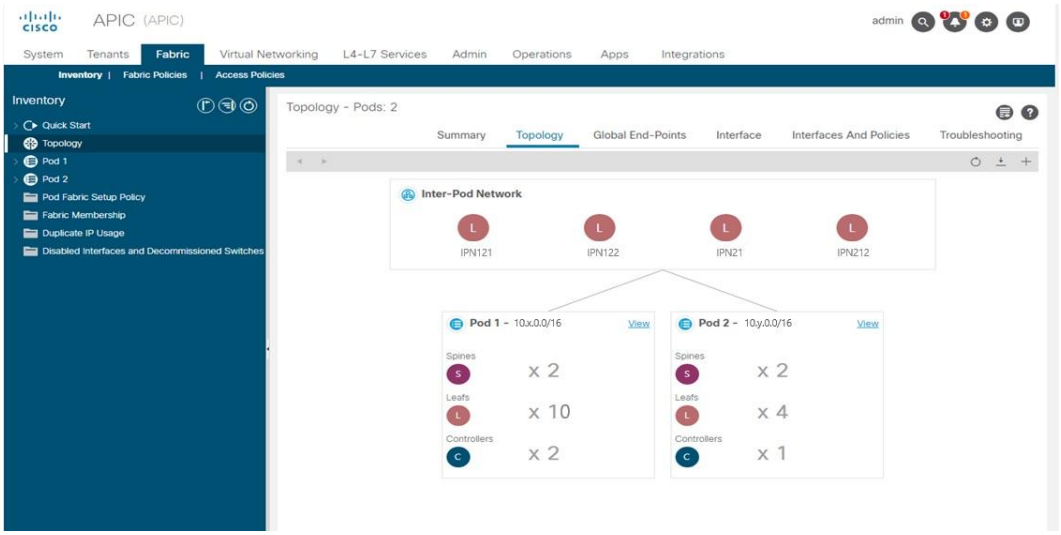

Figura 3-17 *Dashboard* – Topología final del *fabric* ACI. Fuente: Propia.

3.5.2 Alta de Tenant, VRF y AEP

Una vez desplegada la arquitectura con todos los nodos del *fabric* operativos, y visibles desde los controladores APIC, es necesario configurar la capa lógica, como paso previo a conectar servidores físicos y comenzar a dar servicio.

Como se ha comentado en el apartado 2.6.6 el plano de conectividad queda definido por los contenedores lógicos, por lo que iremos configurándolos de fuera hacia dentro (Tenant, VRF, Bridge Domain, EPG).

Se hace notar que el APIC crea automáticamente tres *tenants*, al margen de los que como administradores vayamos a definir en función de las redes lógicas que queramos configurar. Los tres *tenants* creados por defecto son:

- *Infra*: contiene las políticas que gobiernan el *fabric* (i.e. *Overlay* de VxLAN).
- *Common*: contiene los recursos accesibles para todos los *tenants* (i.e. firewalls).
- *Mgmt*: contiene las políticas referentes a la administración del *Fabric* (i.e. OOB).

El APIC los muestra en el apartado *Tenants* > *All Tenants.*

Estos *tenants* son usados internamente por el *fabric*. Aunque el *tenant* de infraestructura permite compartir recursos entre los *tenants* que defina el usuario, esta es una opción altamente desaconsejada, pues normalmente los *tenants* son dominios administrativos que no deben comunicarse.

Por ejemplo, en el despliegue actual hemos creado los *tenants* de desarrollo, producción y preproducción. La idea es poder utilizar el mismo *fabric* físico que subyace manteniendo la independencia de los tres entornos (pudiendo por ejemplo conectar físicamente servidores de los tres entornos a un mismo *Leaf*), Comunicar el entorno de preproducción con el de producción, así como el de desarrollo con el de producción, supone un riesgo demasiado alto.

Para configurar un *tenant* (Figura 3-18) acudiremos al apartado del *dashboard*: *Tenant* > *Add tenant* > *Tenant Name*.

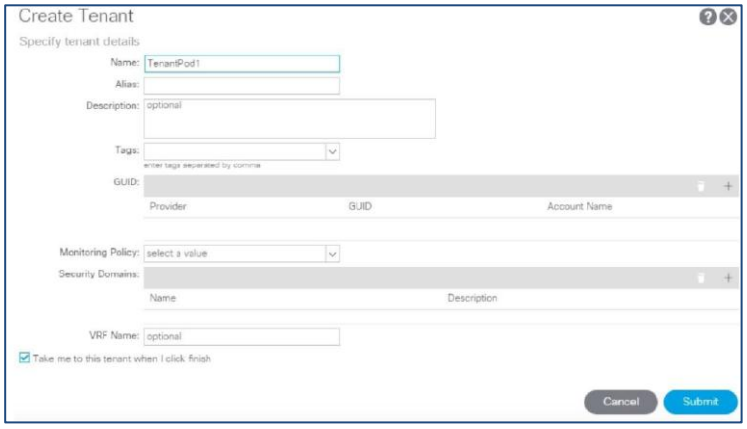

Figura 3-18 Dashboard – Alta de Tenant. Fuente: [45].

Una vez creado el *tenant* (por ejemplo, de nombre "test1") el *dashboard* nos da la ocasión de ir creando el resto de los contenedores lógicos dentro de este dominio administrativo (Figura 3-19).

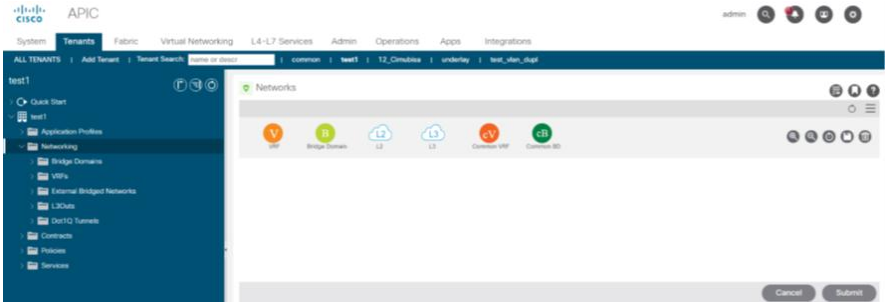

Figura 3-19 *Dashboard* – Contenedores lógicos dentro de *Tenant*. Fuente: [45].

Para completar el esquema de conectividad dentro del *tenant* es necesario realizar las siguientes configuraciones:

- Crear una red privada dentro del *tenant* (VRF).
- Crear un AP (Application Profile).
- Añadir EPG a dominios VMM. Es la parte de añadir los servicios, conectando físicamente los servidores a los *Leaf*, y realizando las configuraciones.

Procedemos por tanto a crear la primera red lógica de nivel 3 dentro del *tenant*, la VRF, pues como se ha comentado es necesario crear los dominios de nivel 3, que alojaran los diferentes subredes ligadas a los *bridge domains* (capa 2), y resto de grupos EPG.

Para crear una VRF dentro del *tenant* "test1" accederemos a esta ruta: *Tenants* > *test1* > *Networking* > *VRFs* > *Create VRF* (Figura 3-20).

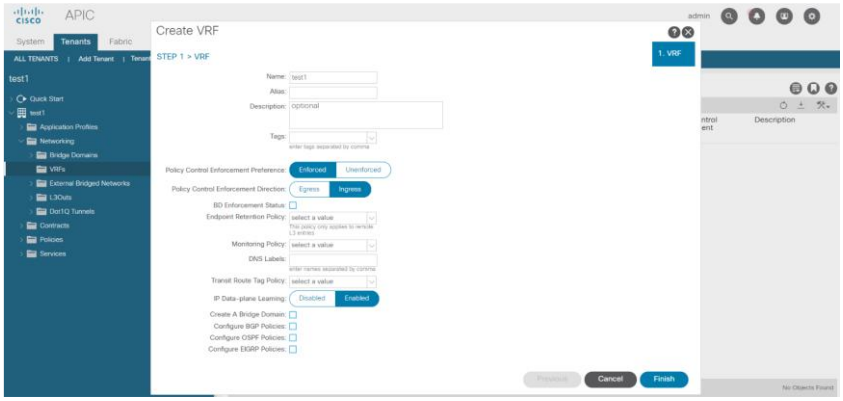

Figura 3-20 Dashboard – Creación de VRF. Fuente: Cisco

Daremos ahora de alta el AEP (*Attachable Access Entity Profile*), y crearemos a continuación un *Phiysical Domain* (dentro de Domain Profile): *Fabric* > *Access Policies* > *Policies* > *Global* > *Attachable Access Entity Profiles*.

En este momento debe definirse el rango de VLAN que ACI puede asignar, el VLAN *Pool*. En la valoración del estado inicial (apartado 3.2) vimos que había unas cincuenta VLAN en la red *legacy*. Aun así, indicamos un rango lo suficientemente amplio, por ejemplo, de 1 a 2999 (Figura 3-21).

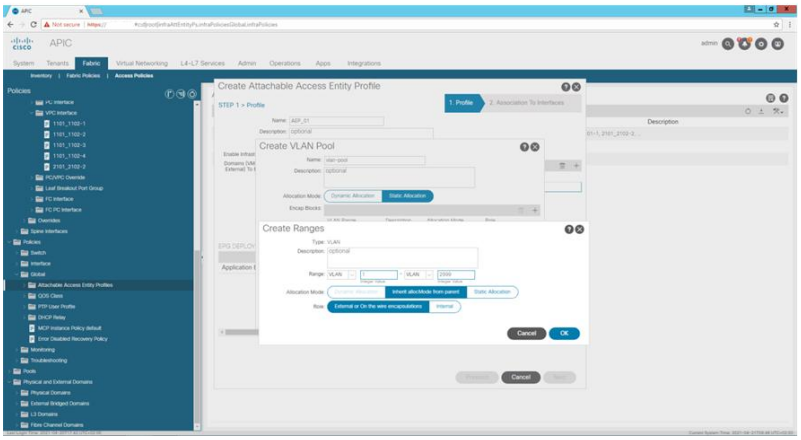

Figura 3-21 Dashboard – Creación de AEP -VLAN pool. Fuente: Propia.

Finalmente, sólo falta crear el *Application Profile* (AP) que es el contenedor lógico de los EPG, o grupos de máquinas que alojan los servidores. Podremos hacerlo dentro de la pestaña *Tenants* > *Application Profiles* del APIC.

Llegados a este punto, el APIC tiene una configuración básica, suficiente para proceder a añadir un servicio.

En el siguiente apartado se muestra un ejemplo en el cual se creará un servicio de nivel dos. Es decir, se conectará físicamente un servidor a un puerto de una pareja de nodos *Leaf*, se realizará la configuración del plano físico (puertos físicos de esos *Leaf*), que se asociará a los objetos lógicos (*bridge domain* y VLAN). Posteriormente con la técnica del *static path* se ligarán ambos universos, físico y lógico (como se ha indicado en el apartado 2.6.8). De esta manera, el ACI cursará el tráfico de ese servidor.

3.5.3 Creación de un servicio de nivel 2

Para integrar un servicio en capa 2, es necesario disponer de una serie de datos y realizar el procedimiento que se indicará a continuación.

Los datos necesarios son: Puertos requeridos en los nodos *Leaf* (dónde conectamos el servidor), ubicación física del servicio, VLAN a utilizar y descripción del servicio.

Los pasos a realizar serán cuatro:

- Alta de los puertos en el/los nodos *Leaf* seleccionados,
- Creación del *Bridge Domain* (BD),
- Creación de EPG,
- Creación de *Static Path* para enlazar los puertos con el EPG.

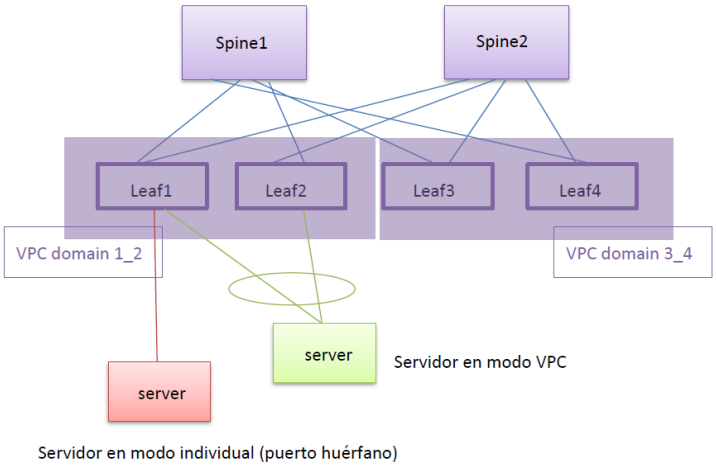

Figura 3-22 Creación de un servicio de nivel 2 en ACI. Fuente: Cisco.

Para dar de alta un puerto físico en el sistema, hay dos formas, en función de la conectividad del servidor a uno o a dos nodos *Leaf* (Figura 3-22). Se puede dar de alta un puerto de manera individual (*orphan port*) o dos puertos formando un VPC (virtual port channel) entre una pareja de nodos *Leaf* (como un *port channel* pero entre puertos de diferentes equipos). Dependerá de la disponibilidad de puertos en el servidor que se conecta, y cómo se quiera hacer.

Si la conexión es con un puerto ("huérfano"), necesitamos conocer algunos datos (Leaf id, port id, y las políticas LLDP / CDP / AEP). La configuración la realizaremos desde: *Fabric > Access Policies > Switches > Leaf Switches > Profiles > Leaves Leaf id:*

- Seleccionaremos el *Leaf*, o lo crearemos (*Create Leaf Profile*)
- Crearemos el *Interface Profile*, dando nombre al puerto
- En *Interface Selectors > Create Access Port Selector* indicaremos el Puerto y le asignaremos un *Policy Group*, o lo crearemos si es la primera vez.
  Para crear un *Policy Group* seleccionaremos un *Attached Entity profile*, marcamos los protocolos que necesitamos (por ejemplo, *CDP_Enable*, *LLDP_Enable*) y aceptamos.

Si la conexión es con doble puerto en el servidor, a dos nodos *Leaf* (vPC), el proceso es similar, pero indicando los puertos por duplicado (son dos, a un *Leaf* distinto).

Para proceder a dar de alta un Bridge Domain (BD), necesitaremos unos datos (nombre del BD, VRF asociada, *tenant*) y seleccionaremos el apartado *Tenants* > *producción* > *Networking* > *Bridge Domain* > *Create BD*:

- Seleccionamos el nombre del BD, tipo "regular", y seleccionamos la VRF en la que estará contenido. Para garantizar la compatibilidad con entornos *legacy*, se recomienda habilitar el *check* de "ARP flooding"
- No se configura el apartado de "L3 *configurations*" pues estamos configurando un servicio de nivel 2.

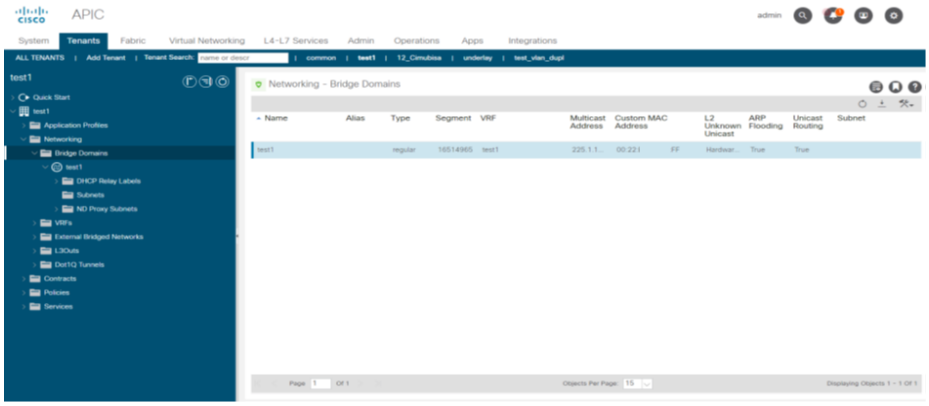

Figura 3-23 Alta de un Bridge Domain. Fuente: [45].

Una vez creado el BD (Figura 3-23), ya se puede proceder a dar de alta el EPG (en este punto debemos tener creado el *Application Profile*, como se ha indicado previamente).

Para crear el EPG necesitaremos algunos datos (APP *name*, EPG *name*, tenant, BD) y seleccionaremos la opción: *Tenants* > *producción* > *Application Profile* > *APP* >*Application EPG* > *Create Application EPG*. El asistente solicitará los datos indicados, tras lo cual se creará el EPG.

Llegados a este punto es necesario ligar ambas partes recién creadas (tenemos creado el interfaz y el EPG que vamos a conectar mediante el *Static Path*).

Con los datos requeridos (tenant, APP, EPG, *node name*, *path*, VLAN *id*, *mode trunk/Access*) seguiremos el proceso indicado por el APIC en la siguiente ruta: *Tenants* > *producción* >*Application Profile* >*APP* >*Application EPG*.

El asistente básicamente nos pedirá que seleccionemos el EPG en cuestión (*EPG_vlan x* >*Static Ports* y seguiremos con *Deploy Static EPG on PC, VPC, or interface*), el tipo de puerto (*port* o vPC), el nodo y puerto concreto, la VLAN que queremos dejar pasar (esto es importante), y el modo 802.1P de la interfaz, es decir, si va en modo *Access* (una VLAN) o en modo *trunk*.

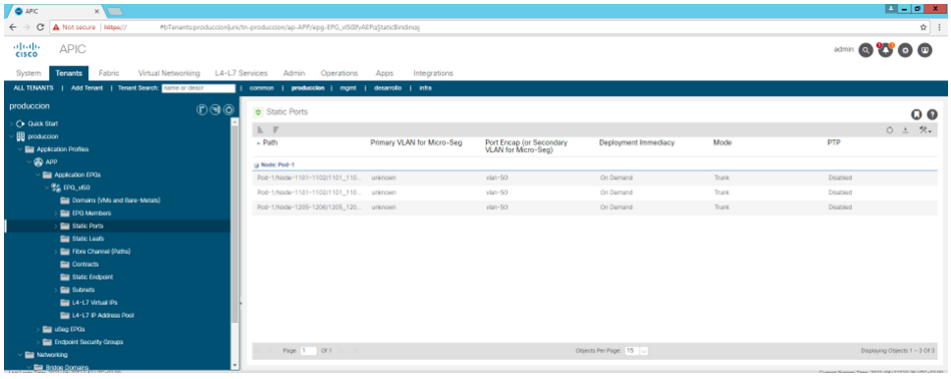

Figura 3-24 Creación de un servicio de nivel 2. Fuente: Propia.

Una vez creado el EPG y tras conectarlo con el *Static Path* se debe asociar (la primera vez) el Domain, para que este coincida en las configuraciones de la parte física y lógica realizadas previamente: *Tenants > producción > Application Profile > APP > Application EPG* (Figura 3-24).

3.5.4 Integración con otros sistemas

ACI permite la integración con distintos sistemas y aplicaciones, que se comentarán brevemente a continuación, implementándose en este despliegue algunas de ellas.

Respecto a la **AAA** (Autenticación, Autorización y Auditoría), al margen de los usuarios locales gestionados por el APIC, ACI se integra con servidores externos como *Radius* y *Tacacs+*, así como con la solución propietaria Cisco ISE. Hay que indicar que esta integración no se ha realizado hasta la finalización del despliegue, para evitar contratiempos e incomodidades durante las configuraciones.

Aunque no se ha integrado ACI con **VMware vCenter**, ACI permite esta integración realizando a alto nivel los siguientes pasos:

- Preparar el clúster de *vCenter* asegurando la compatibilidad de hardware y versiones, con la de ACI OS.
- Proporcionar al APIC las credenciales de *vCenter*.
- Definir en ACI un VMM *(Virtual Machine Manager*) Domain, asociándolo a *vCenter*.
- Configurar los DVS (*Distributed Virtual Switches*), de manera que ACI los crea en *vCenter* y los asocia con los EPG.
- Configurar en ACI los EPG y asociarlos a las VLAN correspondientes en los hosts ESXi.
- Asignar las políticas.
- Asignar los puertos de los nodos *Leaf* con los de los hosts ESXi.
- ACI sincronizará los DVS, DPG (*Distributed Port Groups*) y la nomenclatura de los servicios generados con vCenter.
- Podremos entonces verificar en el *vCenter* que los DVS y *port-groups* reflejen la configuración definida en ACI.

Sin embargo, se le ha encontrado un inconveniente. En el caso de disponer previamente de una amplia infraestructura en VMware con muchos DVS (*Distributed Virtual Switches*) configurados, sucede que cuando se integra con el *fabric*, es ACI quien manda la nomenclatura de los servicios, de manera que la misma entra en conflicto con la ya definida previamente en el vCenter.

El formato en el que ACI manda estas cadenas está basado en la estructura del VMM Domain y EPG, y es de la siguiente forma: *TenantName|ApplicationProfile|EPGName.* En cualquier caso, esto no supone un problema con la implementación de nuevos servicios.

Referente a la monitorización, ACI provee extenso soporte para **SNMP** v1, v2 y v3, incluyendo *Management Information Bases* (MIB) y notificaciones (*traps*). El estándar SNMP permite que aplicaciones de terceras partes que soportan los distintos MIB gestionen y monitoricen el *fabric* ACI.

ACI también puede integrarse con sistemas de registro de eventos. Tiene la capacidad de enviar mensajes de System Log (**syslog**) bien a consola, a un archivo local, o a un servidor remoto de *logging*. Un mensaje de *syslog* típicamente contiene un conjunto de información acerca del fallo o evento, y puede también contener logs de auditoria o registros de inicio/fin de sesión.

En el APIC es accesible a través de *Admin > External Data Collectors > SNMP y SYSLOG.*

Si se desea realizar copias de seguridad de las políticas, a pesar de que los APICs del clúster están distribuidos geográficamente y se mantienen sincronizados, se puede hacer, vía SCP, FTP o SFTP.

Indicar sobre las posibilidades de **almacenamiento**, que Cisco ACI soporta conexiones Fibre Channel (FC) sobre un switch *Leaf* usando el modo *N-Port Virtualization* (NPV). NPV permite al

switch agregar tráfico FC desde hosts conectados en local (N ports) a un nodo *proxy* (NP *port*) de un switch de *core* (Figura 3-25).

Hay que tener en cuenta que en la aplicación de FC NPV, el rol de los *Leaf* de ACI es, simplemente, proveer una ruta para el tráfico FC entre las SAN y un switch *core*, todos conectados localmente. El nodo *Leaf* no realiza *switching* entre los distintos hosts SAN, y el tráfico FC no es reenviado a los nodos *Spine*.

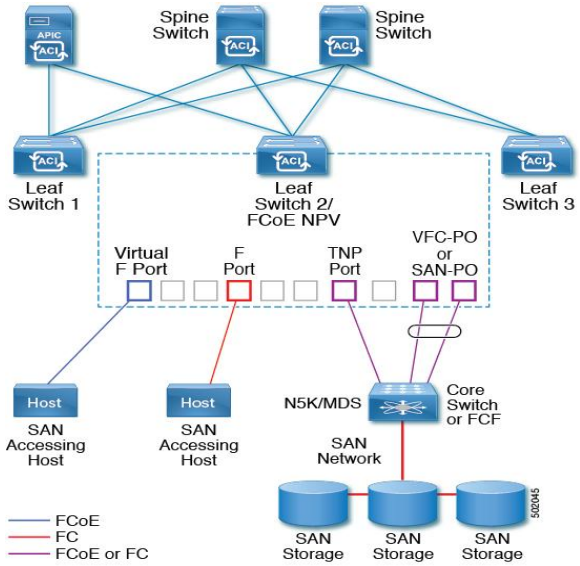

Figura 3-25 Manejo de tráfico FC (almacenamiento) por ACI. Fuente: [45].

Por último, tal y como se ha indicado en apartados previos, es conveniente integrar los elementos del ACI y de la *interpod network* en una red de gestión fuera de banda (Figura 3-26). En la figura que se muestra a continuación se indica la topología implementada, con switches de gestión en cada una de las tres salas técnicas (de los dos Pods) que se agregan, y son accesibles mediante unas consolas de gestión.

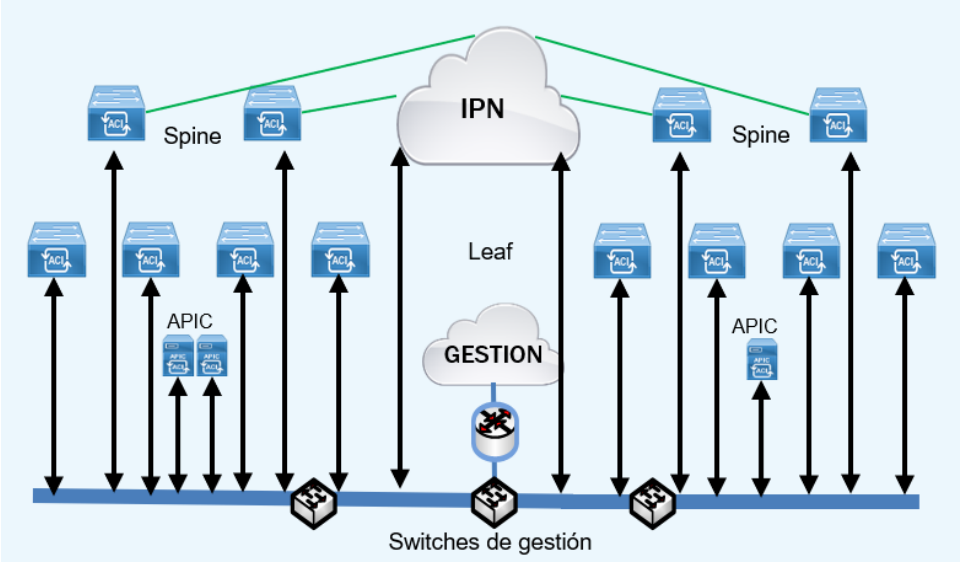

Figura 3-26 Gestión fuera de banda equipos ACI e IPN. Fuente: Propia.

4 PRUEBAS, VALIDACIÓN Y RESULTADOS

4.1.1 Plan de pruebas

Para una correcta validación de la solución SDN de Cisco desplegada, se ha planificado y ejecutado un amplio plan de pruebas (a nivel de arquitectura, funcionales, etc.), que permita verificar el correcto funcionamiento del sistema, y el grado de cumplimiento de los objetivos inicialmente planteados en esta memoria.

Como **entorno** de pruebas se ha creado un *Tenant* diferente denominado NRFU (*Network Ready For Use*) con los siguientes objetos lógicos:

- una VRF (*vrf_NRFU*)
- dos Bridge domains (BD_10 y BD_11). A los *Bridge Domains* se ha asignado el siguiente direccionamiento IP:
  - BD_10: 192.168.10.1/24
  - BD_11: 192.168.11.1/24

El **equipamiento** utilizado han sido los propios nodos *Leaf* de la solución implantada, que dan la conectividad (14 unidades, con configuraciones de las interfaces en modo acceso y *trunk*), así como los tres controladores APIC del clúster M4 instalado.

En algunas pruebas, cuando ha sido necesario verificar conectividad contra elementos externos al ACI, se han utilizado dos switches Cisco C3560X, así como portátiles con SO Windows 10.

Los **prerrequisitos** para el inicio de las pruebas han sido que toda la infraestructura en ambos Pods estuviese en servicio, alimentada por doble fuente, con sus flujos de conectividad habilitados a nivel de *firewall*, y el software actualizado a la última versión estable recomendada.

En la siguiente tabla se muestra la **relación de 34 pruebas** que se ha realizado y su resultado.

Número de prueba	**Descripción**	**Resultado (A)probado / (N)o aprobado**
1 - Pruebas básicas de la infraestructura		
1.1	Salud de los equipos	A
1.2	Clúster de APIC	A

1.3	Actualización de versiones de software	A
1.4	Versiones de Software	A
1.5	Dominios Físicos	A
2 - Pruebas de Capa 1		
2.1	Topología Física	A
2.2	Perfiles y políticas en interfaces	A
2.3	Selectores de Switches y asociaciones	A
3 - Pruebas de Capa 2		
3.1	VPC	A
3.2	VLAN Pools	A
3.3	Perfiles y políticas de Capa 2	A
3.4	APs y EPGs	A
3.5	VRFs, BDs y asociaciones	A
3.6	Vlanes Duplicadas	A
4 - Pruebas de Capa 3		
4.1	BGP Interno	A
4.2	Nivel 3 en ACI	A
5 - Pruebas de Redundancia		
5.1	Fallo de Power Supply	A
5.2	Fallo de Power Grid	N
5.3	Fallo de APIC	A
5.4	Fallo de Nexus	A
6 - Pruebas de administración OOB (fuera de banda)		
6.1	Redes de administración out-of-band	A
6.2	SSH via out-of-band	N
6.3	HTTPS via out-of-band	A
6.4	Syslog	N
6.5	SNMP	N
6.6	NTP	N
7 - Pruebas de la red IPN		
7.1	Topología IPN	A

7.2	Adyacencias OSPF	A
7.3	External TEP interfaces en switches Spine	A
7.4	MP-BGP eVPN	A
7.5	Verificar base de datos COOP	A
7.6	Comprobar túneles dinámicos	A
7.7	Comprobar redundancia de circuitos de interconexión	A
7.8	Comprobar seguridad de circuitos de interconexión MACSEC	A

Tabla 4-1 Casos de prueba realizados. Fuente: Propia.

En el **Anexo I: Plan de Pruebas,** se detallan los 34 casos de prueba ejecutados, que respaldan la valoración del sistema. Cada uno se ha realizado en base a una **plantilla** en la que se han recogido:

- Título, propósito de la prueba y requisitos de preparación previos para poder realizarla.
- Procedimiento de actuación a alto nivel.
- Objetivos concretos a verificar.
- Resultado esperado.
- Resultado de la prueba (aprobada, o no).
- Observaciones.

A modo de ejemplo, se muestra a continuación la plantilla de la prueba 1.3 (Tabla 4-2), en la que se ha verificado que se puede actualizar el firmware de los nodos de la topología, de una manera sencilla, durante la operación normal del sistema, y sin impacto en el tráfico de los servicios activos en ese momento.

Núm.	1.3	Revisión	1.0	Autor:		Fecha:	
Categoría		Versiones de Software					
Equipo		Nexus 93XX, APIC-CLUSTER					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**Actualización de versiones de software**					
Propósito:		Verificar que al actualizar los nodos pares/impares de un Pod, el impacto en el tráfico es mínimo o nulo.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Acceder a uno de los controladores por HTTPS 2. Realizar las revisiones necesarias descritas abajo.					
Verificar:							
1. Crear grupos de mantenimiento: 2 grupos por cada Pod repartidos en nodos pares e impares (Pod1_par, Pod1_impar, Pod2_par y Pod2_impar). En cada grupo se meterán los switches (*Leaf* y *Spine*) con *hostname* par o impar, de cada Pod.						Aprobado [X]	No Aprobado [ ]
2. Lanzar una actualización de software sobre un grupo de mantenimiento.						Aprobado [X]	No Aprobado [ ]
3. Con un PC/VM en cada Pod conectado a los *Leaf* comprobar que la conectividad se mantiene (excepto cuando se actualiza el switch al que está						Aprobado [X]	No Aprobado [ ]

conectado el PC/VM).	
Resultados Esperados:	Sin impacto en el tráfico.
Paso: (Inicial)	
Fallo: (Inicial)	
Razón de la No Aprobación:	
Observaciones:	Se han creado dos grupos de actualización de nodos par e impar por cada datacenter (Pod1 y Pod2). El impacto sobre la red ha sido nulo, y siempre se ha cursado el tráfico sin cortes.

Tabla 4-2 Plantilla tipo de un caso de prueba realizado. Fuente: Propia.

4.1.2 Validación y Resultados

El motivo de la agenda con 34 casos de prueba ha sido poder validar el sistema implantado, y el grado de cumplimiento de los objetivos de bajo nivel planteados en el apartado 1.3. Se ha organizado conforme a la Tabla 4-1, cubriendo diferentes casuísticas y cuestiones como son la administración de la plataforma (salud de los equipos, disponibilidad de la topología multisite, actualizaciones, alarmas), para poder ver el comportamiento del sistema ante distintos tipos de fallos, la posibilidad y complejidad de realizar diferentes configuraciones en capas 1/2/3, o aspectos de seguridad como el cifrado.

A continuación se hace una revisión del grado de cumplimiento de estos objetivos, que son:

- Vista centralizada de los equipos y su rendimiento:
  - Como puede observarse en la Figura 4-1, se dispone de una vista centralizada de la topología, que muestra todos los equipos del *fabric* en las dos sedes, y su rendimiento.

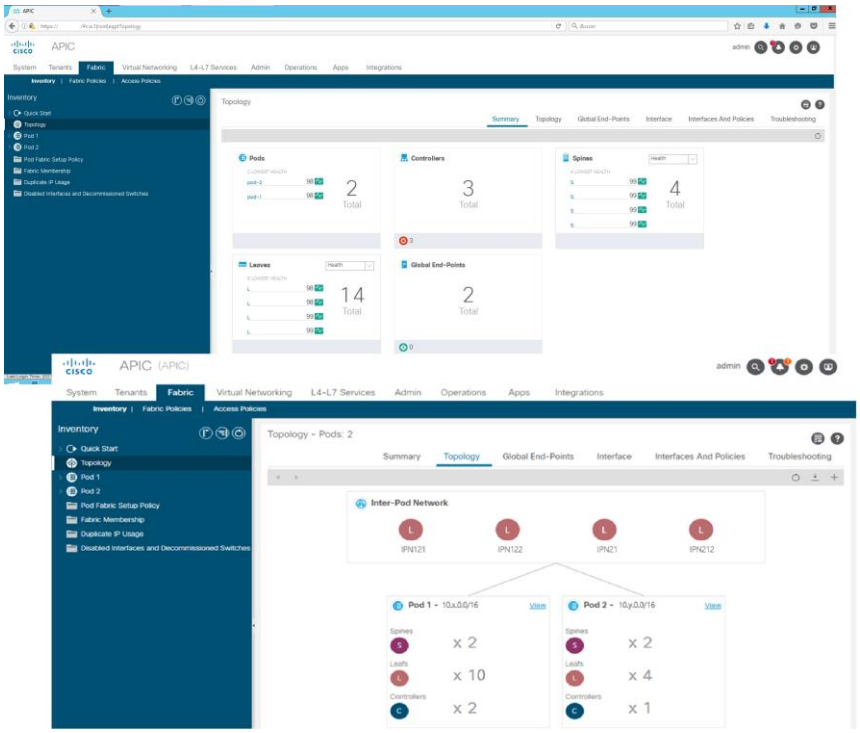

Figura 4-1 Vista de la topología extendida (2 Pods) en APIC. Fuente: Propia.

  - Por otra parte, la prueba 1.1 de "Salud de los Equipos" validó el correcto funcionamiento de todos los nodos y controladores de la red, mostrando que en el

APIC (apartado *System>Dashboard)* se pueden verificar las alarmas y salud de los equipos.

- La interfaz (Figura 4-2) permite acceder a uno de los Pods y seleccionar un equipo para inspeccionar el estado de sus puertos (Figura 4-3).

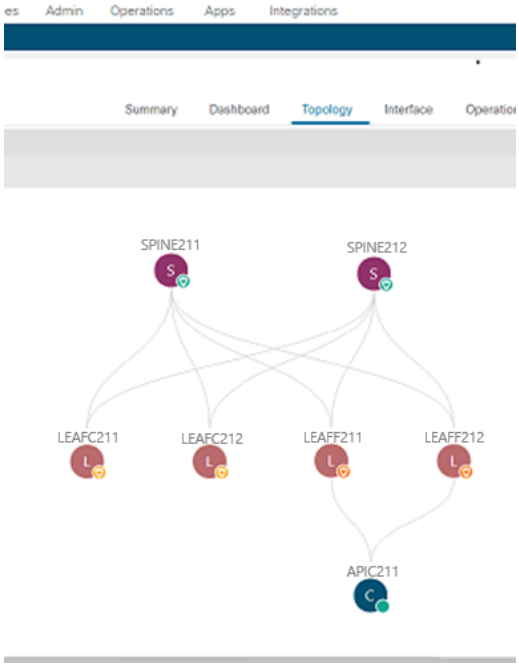

Figura 4-2 Vista de la topología del Pod2 en APIC. Fuente: Propia.

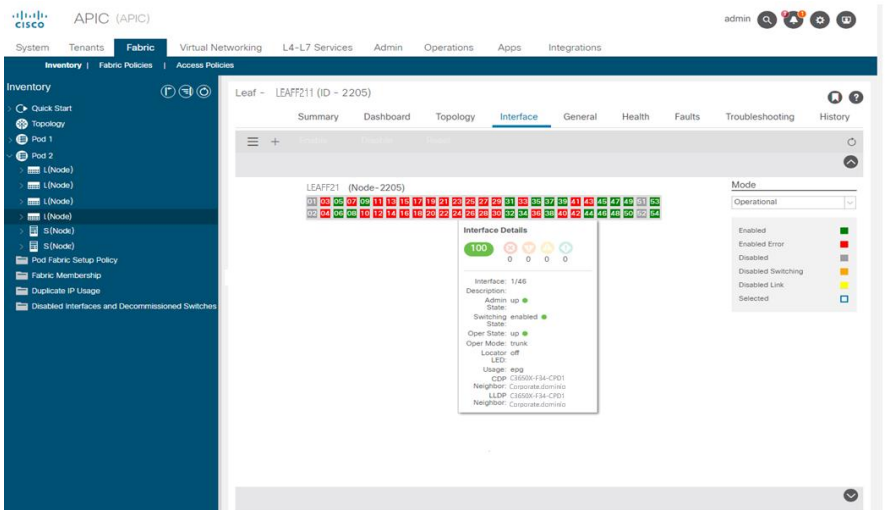

Figura 4-3 Vista de las interfaces de un Leaf en APIC. Fuente: Propia.

- Automatización de la red:
  - Este objetivo persigue reducir la dependencia de las configuraciones manuales. El objetivo se cumple desde el momento en que el APIC permite crear y reutilizar la capa lógica de objetos que proporciona la conectividad, y los contratos que implementan la seguridad.
    Los procesos automatizados para la creación de redes lógicas, implementación de políticas de seguridad y configuración de puertos se verificaron exitosamente en gran cantidad de pruebas en las capas 1, 2 y 3, como las pruebas 2.2 (de creación de políticas y perfiles para conexiones contra interfaces a otros dispositivos fuera del fabric) o prueba 3.3 (perfiles y políticas de capa 2, como Storm-control, LLDP, CDP y Port-channel).

- Seguridad mediante la automatización de las políticas, que puedan ser reutilizadas permitiendo la segmentación de redes:
    - La introducción de segmentación mediante la creación de grupos EPG y políticas de acceso dinámicas fue probada con éxito en "APs y EPGs", donde se evidenció además que estas configuraciones de seguridad pueden gestionarse de una forma centralizada (prueba 3.4).
- Facilidad de actualización:
  Se configuraron políticas de actualización del software de nodos, creando grupos de actualización par e impar en los Pod, Cada grupo contenía el nodo *Leaf* y *Spine* par o impar de la estructura *fat tree* de ese Pod. Se actualizó el firmware de estos grupos par/impar con éxito y sin corte de servicio.
- Redundancia y alta disponibilidad:
    - Pruebas de redundancia como "Fallo de APIC" y "Fallo de Nexus" confirmaron que el sistema mantiene su funcionamiento normal sin impacto en el servicio incluso ante fallos hardware o un mantenimiento programado.
      La prueba 5.3 verificó que al perder un APIC no hay impacto en el tráfico de la red, funcionando sin problema las otras dos unidades del clúster, que mostraron una alarma.
      La prueba 5.4 verificó que al perder una mitad de los Nexus que conforman la infraestructura de ACI el tráfico sigue funcionando por la otra mitad.
      Pruebas como la 5.1 mostraron la disponibilidad ante fallos hardware de componentes, como una fuente de alimentación.
- Escalabilidad:
    - La adición de nuevos equipos quedó demostrada durante la incorporación de nuevos nodos *Leaf* a la arquitectura, durante el proceso de configuración. El clúster de controladores APIC M4 instalado soporta hasta 1200 *edge ports*, y en la actualidad solo hay instalados 672 (14 switches de 48 puertos), por lo que hay margen para introducir otros 11 nodos de similares características.
    - La validación de la adición de nuevos nodos sin interrupción se confirmó mediante pruebas de topología física y túneles dinámicos (pruebas 2.1 y 7.6).
    - Además, la adición de funcionalidad mediante actualizaciones no son un problema, como se demostró con el caso de prueba 1.3.
- Configuración de redes lógicas:
    - La implementación de VRFs y BDs demostró que la solución permite la creación rápida y flexible de redes (prueba 3.5), con independencia de la capa física. Se creó con éxito una VRF nueva a la que se asociaron sin problemas BDs y grupos EPG.
    - La movilidad de servidores entre ubicaciones del fabric no es un problema, como demostró la migración de equipamiento de la red *legacy* al fabric.
- Solución multisite, dada la expansión de la empresa a una segunda sede:
    - La conectividad entre Pods se verificó con la prueba "Seguridad de conexión Inter-CPDs MACSEC", garantizando comunicación segura entre sedes (prueba 7.8).
    - El funcionamiento de la solución multisite se probó también testeando el funcionamiento correcto del sistema ante la caída de uno de los dos enlaces entre los Pods (prueba 7.7).
- Diferentes dominios administrativos:
    - La definición de diferentes *tenants*, como se ha indicado en el capítulo de despliegue, demuestra la definición de dominios administrativos diferenciados.
    - La funcionalidad de administración OOB desde un acceso a Pod remoto, que se validó en las pruebas de acceso mediante HTTPS, así como la recepción de los *traps* SNMP, confirman dicha separación de los dominios administrativos (pruebas 6.1, 6.2 y 6.5).

- Integración con otros sistemas:
    - Se logró la interoperabilidad verificada con herramientas como Syslog, SNMP (Zabixx) y Cisco ISE, así como la compatibilidad con sistemas de registro, monitorización y autenticación externas a ACI (pruebas 6.4, 6.5 y 6.6). En las pruebas se verificó que ACI genera mensajes SYSLOG, envía los *traps* SNMP ante una caída de equipo o interfaz, y sincroniza con NTP.
    - Además, aunque finalmente no se realizó la integración con VMware se comprobó que el vCenter recibe correctamente los grupos (*TenantName*| *ApplicationProfile*| *EPGName*) creados por ACI.
    - La integración con firewalls de un segundo fabricante ha funcionado correctamente, permitiendo el filtrado de los flujos norte-sur, así como los este-oeste.

En consecuencia, las pruebas realizadas han permitido validar el cumplimiento satisfactorio de todos los objetivos de bajo nivel que se habían planteado.

5 CONCLUSIONES Y LÍNEAS FUTURAS

5.1 Conclusiones

Este proyecto tenía objetivos que podemos analizar desde una doble perspectiva: una más general que perseguía mostrar los pasos y decisiones de diseño a tomar para poder implantar una solución SDN comercial, y otra más detallada que contaba con unos objetivos de bajo nivel que perseguían implantar una solución flexible para dotar a un organismo de una nueva arquitectura versátil para su *datacenter*.

Desde la perspectiva más general, con el desarrollo de este trabajo se ha podido mostrar la gran diferencia entre una red tradicional de *datacenter* y una red definida por software. Tras introducir los conceptos de un *datacenter* tradicional, virtualización y tecnología SDN, se analizaron diferentes opciones comerciales, para inclinarnos (según la comparativa realizada en el apartado 2.5.8) por la tecnología SDN de Cisco ACI. Posteriormente se desarrollaron los principales pasos a seguir desde el análisis de la arquitectura previa hasta la implantación de Cisco ACI, pasando por el dimensionamiento de la arquitectura, y decisiones de diseño en los planos físico y lógico, hasta la efectiva configuración de la solución.

Tras la batería de pruebas aplicada y con los resultados de la validación efectuada en el apartado 4.1.2, donde se han revisado uno a uno todos los objetivos de bajo nivel planteados inicialmente, se ha podido constatar en primera persona la enorme satisfacción del cliente, que ha transmitido como una felicitación explícita, pues la nueva arquitectura cumple ampliamente y excede todos los objetivos marcados inicialmente. Esto se justifica si se considera el *feedback* de los diferentes involucrados: usuarios, administradores y resto de departamentos TIC de la empresa.

Los usuarios, empleados, pueden acceder a los servicios alojados en el *datacenter*, con independencia de la sede donde se encuentren, ellos mismos o los servicios. Esto facilita la movilidad en el trabajo, según las necesidades organizativas de la empresa, o simplemente ante necesidades puntuales de los proyectos en los que participan.

Además, el acceso a servicios proporcionados por el *fabric* es de alta velocidad, a 100 Gbps, multiplicando en más de un por diez la capacidad inicial.

La solución ha permitido la coexistencia de las dos redes, la *legacy* y la SDN. Esto ha permitido que el departamento de operaciones y sistemas pueda planificar y afrontar mejor los complicados trabajos de migración de los servicios previos.

Desde el punto de vista del departamento de ingeniería, se dispone de una red bien dimensionada de acuerdo a las necesidades actuales y previstas de la empresa, con una gran capacidad de crecimiento en puertos físicos libres, y unos parámetros (latencias, ancho de banda, etc.) que permitirán lanzar

nuevos proyectos y servicios con altas exigencias. Las comunicaciones entre las sedes son seguras, al cifrarse el tráfico que se transporta sobre la nueva red óptica, redundada.

Los administradores han visto totalmente facilitado su trabajo:

- Disponen de una interfaz centralizada que les permite monitorizar el estado de toda la arquitectura extendida (Figura 3-15, Figura 3-16 y Figura 3-17).
- Pueden dar de alta servicios rápidamente añadiendo servidores físicos o virtualizados en caso de ser necesario, y configurando los objetos lógicos (como se ha visto en el apartado 3.5.3).
- Pueden hacer un *troubleshooting* o resolver una incidencia de manera más ágil basándose en un amplio conocimiento del estado de toda la red, lo que reduce los tiempos de respuesta a incidencias.
- Pueden mover servicios sin interrupciones.
- Pueden configurar y automatizar las políticas de seguridad, permitiendo, denegando o inspeccionando flujos, de una manera centralizada. También pueden elegir redireccionarlos a un *firewall* externo para una inspección más granular.
- Pueden actualizar *firmwares* o aplicar parches en horarios laborales, con la seguridad de que la infraestructura está redundada y no habrá afección al servicio.
- Pueden tener la tranquilidad de que, si falla una fuente de alimentación, un equipo completo, o se daña una fibra interna de conexión entre equipos, el sistema les avisará y seguirá funcionando.
- Pueden generar entornos de prueba configurando un *tenant* de desarrollo, sobre la misma capa física en la que corren los servicios en producción, con la tranquilidad de que no habrá intromisión o contacto entre los entornos.
- Pueden integrar el nuevo sistema SDN con el resto de los sistemas de la empresa, como AAA, monitorización de eventos, *backups*, sistemas de almacenamiento, etc.

En conclusión, se consideran logrados todos los objetivos que se plantearon desde ambas perspectivas, general y más detallada, con un *feedback* muy positivo por parte del cliente. En consecuencia, la implementación de una solución SDN basada en Cisco ACI ha demostrado ser efectiva para superar los desafíos de las arquitecturas de red tradicionales.

5.2 Líneas futuras

Como líneas futuras de trabajo, que amplíen el trabajo fin de máster aquí desarrollado, se sugieren las siguientes:

- **Integración con Inteligencia Artificial (IA):**
  Se propone investigar cómo los modelos de IA pueden optimizar aún más la gestión de la red, prediciendo fallos, identificando patrones de tráfico anómalos, y ajustando automáticamente las configuraciones para maximizar el rendimiento y disponibilidad de la red SDN.
- **Expansión hacia entornos multinube**:
  Dado el crecimiento de las soluciones en la nube, resulta relevante explorar cómo integrar de manera eficiente la infraestructura SDN con múltiples proveedores de servicios en la nube, garantizando interoperabilidad y continuidad del servicio.
- **Mejoras en la seguridad**:
  Implementar técnicas de análisis en tiempo real para la detección y mitigación proactiva de amenazas mediante la integración o uso de dispositivos y herramientas avanzadas de monitorización, así como adoptar enfoques Zero Trust (no confiar en ningún dispositivo de la red) para una mayor protección de los datos y los sistemas.

- **Analizar la posibilidad de integración** con otros servicios, como aquellos entornos donde la baja latencia y/o el ancho de banda sean críticos (como IoT, o redes móviles).
- **Automatización basada en políticas**: Seguir desarrollando herramientas que permitan definir políticas dinámicas adaptativas, que mejoren la respuesta automática a las necesidades de la red en tiempo real.

6 BIBLIOGRAFÍA

[1] C. O. V. D. Peterson, Software-Defined Networks: A Systems Approach, Systems Approach LLC (Publisher), 2021-01-14, p. 192.

[2] Open Networking Foundation (ONF), "Software-Defined Networking (SDN) Definition," 20 10 2024. [Online]. Available: https://opennetworking.org/sdn-definition/. [Accessed 12 2024].

[3] E. R. Moraguez, «Redes Definidas por Software (SDN): El Futuro de las Redes,» 01 2024. [En línea]. Available: https://lovtechnology.com/redes-definidas-por-software-sdn-el-futuro-de-las-redes/. [Último acceso: 12 2024].

[4] CiberSafety, «Todo lo que necesitas saber sobre las Redes SDN: Tipos y ventajas,» 14 06 2024. [En línea]. Available: https://cibersafety.com/redes-sdn-que-son/. [Último acceso: 12 2024].

[5] Geeksforgeeks.org, "Difference between Software Defined Network and Traditional Network," 14 10 2024. [Online]. Available: https://www.geeksforgeeks.org/difference-between-software-defined-network-and-traditional-network/. [Accessed 12 2024].

[6] FS.COM, «Redes Definidas por Software (SDN): Tipos, Ventajas y Aplicaciones,» 24 06 2022. [En línea]. Available: https://www.fs.com/es/blog/software-defined-networking-sdn-types-advantages-and-applications-4870.html. [Último acceso: 12 2024].

[7] Universidad Pública de Navarra, «Redes de Nueva Generación (Área Ing. Telemática),» 10 2022. [En línea]. Available: https://www.tlm.unavarra.es/~daniel/docencia/rng/rng15_16/slides/Tema1-19-ArquitecturaEnDCs.pdf. [Último acceso: 12 2024].

[8] IBM, «¿Qué es la virtualización?,» 12 2024. [En línea]. Available: https://www.ibm.com/es-es/topics/virtualization. [Último acceso: 12 2024].

[9] E. a. A. E. a. R. K. Amiri, "An Efficient Hierarchical Distributed SDN Controller Model," in *2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI)*, 2019, pp. 553-557.

[10] «Cisco CCNA – Arquitectura Definida por Software Basada en Controladores,» CCNA 200-301, [En línea]. Available: https://eclassvirtual.com/cisco-ccna-arquitectura-definida-por-

software-basada-en-controladores/. [Último acceso: 12 2024].

[11] "Trusted Business Resources for Growth," [Online]. Available: https://geekflare.com/. [Accessed 12 2024].

[12] Cisco, "ACI simulator datasheet," [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/application-centric-infrastructure-simulator/datasheet-c78-733252.pdf. [Accessed 12 2024].

[13] Cisco Support, "Cisco Nexus 9000 Series Switches," 05 11 2013. [Online]. Available: https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/series.html. [Accessed 12 2024].

[14] "What is Cisco ACI?," 13 02 2020. [Online]. Available: https://learningnetwork.cisco.com/s/article/what-is-cisco-aci-x. [Accessed 12 2024].

[15] Cisco, "Cisco APIC GUI Overview," [Online]. Available: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/getting-started/b-Cisco-APIC-Getting-Started-Guide-411/b-Cisco-APIC-Getting-Started-Guide-411_chapter_011.html. [Accessed 12 2024].

[16] Cisco, "Cisco Application Centric Infrastructure Simulator," [Online]. Available: https://www.cisco.com/c/en/us/support/cloud-systems-management/application-centric-infrastructure-simulator/series.html#~tab-documents. [Accessed 12 2024].

[17] JMG Virtual Consulting, «La Solución definitiva para SDN se llama VMware NSX-T,» 26 01 2021. [En línea]. Available: https://jmgvirtualconsulting.com/vmware-vsphere/la-solucion-definitiva-para-sdn-se-llama-vmware-nsx-t-3-0/. [Último acceso: 11 2024].

[18] J. Mestrovic, "VMware NSX architecture," [Online]. Available: https://binarymaps.com/nsx/vmware-nsx-architecture/. [Accessed 12 2024].

[19] Juniper, "Company Profile," 01 2025. [Online]. Available: https://www.juniper.net/us/en/company/profile.html.

[20] Juniper Networks, «Contrail Networking,» 01 2025. [En línea]. Available: https://www.juniper.net/mx/es/products/sdn-and-orchestration/contrail/contrail-networking.html#:~:text=Contrail%20Networking%20es%20una%20soluci%C3%B3n%20nativa%20de%20la,cargas%20de%20trabajo%20en%20nubes%20privadas%20y%20p%C3%BAblicas..

[21] Juniper Networks, "Contrail Networking Installation and Upgrade Guide," 28 08 2023. [Online]. Available: https://www.juniper.net/documentation/mx/es/software/contrail-networking19/contrail-install-and-upgrade-guide/topics/concept/understanding-contrail-networking.html. [Accessed 12 2024].

[22] Arista Networks, Inc, "Arista CloudVision Whitepaper," Santa Clara, CA, 2024.09.

[23] Arista Networks, Inc., "CloudVision Configuration Guide," 12 2024. [Online]. Available: https://www.arista.com/en/cg-cv/cv-cloudvision-portal-cvp-overview. [Accessed 12 2024].

[24] Arista cloudvision Inc., "CloudVision," 12 2024. [Online]. Available: https://www.arista.com/en/products/eos/eos-cloudvision. [Accessed 12 2024].

[25] Zhang Fan - Huawei Technical Support, "What Is CloudFabric?," 01 12 2023. [Online]. Available: https://info.support.huawei.com/info-finder/encyclopedia/en/CloudFabric.html.

[Accessed 12 2024].

[26] Huawei Support, "Huawei CloudFabric Support Guide, Manuls & PDF," 12 2024. [Online]. Available: https://support.huawei.com/enterprise/en/network-solution/cloudfabric-pid-22604572. [Accessed 12 2024].

[27] Nokia, "Virtualized network services," 12 2024. [Online]. Available: https://www.nokia.com/networks/ip-networks/virtualized-network-services/. [Accessed 12 2024].

[28] NuageNetworks from Nokia, "Virtualized Cloud Services – SDN for Today's Modern Telco Cloud Data Center," 12 2023. [Online]. Available: https://www.nuagenetworks.net/solutions/telco-cloud/. [Accessed 12 2024].

[29] Exterme Networks, "What is a SDN Network?," 12 2024. [Online]. Available: https://www.extremenetworks.com/resources/faq/s/sdn-network. [Accessed 12 2024].

[30] Exterme Networks, "Network Fabric," 12 2024. [Online]. Available: https://www.extremenetworks.com/solutions/network-fabric. [Accessed 12 2024].

[31] Canada, Cisco, "ACI Hands-on Lab," 30 05 2016. [Online]. Available: https://es.slideshare.net/slideshow/aci-handson-lab/62547117#34. [Accessed 12 2024].

[32] Cisco, "Cisco Application Policy Infrastructure Controller Data Sheet," 29 08 2023. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/application-policy-infrastructure-controller-apic/datasheet-c78-739715.html. [Accessed 12 2024].

[33] Cisco, "Cisco Application Policy Infrastructure Controller (APIC)," [Online]. Available: https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html. [Accessed 12 2024].

[34] Cisco, "Cisco ACI Multi-Site Architecture White Paper," 10 08 2024. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739609.html. [Accessed 12 2024].

[35] Cisco, "Cisco ACI Stretched Fabric Design," 21 07 2017. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b_kb-aci-stretched-fabric.html. [Accessed 12 2024].

[36] Cisco, "ACI Multi-Pod White Paper," 09 05 2022. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-737855.html. [Accessed 12 2024].

[37] Cisco, "Cisco ACI Remote Leaf Architecture White Paper," 21 08 2024. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-740861.html. [Accessed 12 2024].

[38] Matthias Wessendorf, "Cisco Live! (BRKACI-2210)," in *The missing ACI Pilot's Operating Handbook*, Barcelona, 2019.

[39] Cisco, "Cisco ACI Contract Guide White Pape," 02 12 2024. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-743951.html?dtid=osscdc000283. [Accessed 12 2024].

[40] Cisco, "Cisco Nexus 9300-GX Series Switches Data Sheet," 19 01 2024. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/nexus-9300-gx-series-switches-ds.html?dtid=osscdc000283. [Accessed 12 2024].

[41] Cisco, "Cisco Nexus 9300-FX3 Series Switches Data Sheet," 06 12 2024. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-744052.html?dtid=osscdc000283. [Accessed 12 2024].

[42] Cisco, "Cisco APIC M4/L4 Server Installation and Service Guide," 06 09 2024. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/server/m4-l4-server/APIC-M4-L4-Server/m_overview.html?dtid=osscdc000283. [Accessed 12 2024].

[43] Cisco, "Cisco 100GBASE QSFP-100G Modules Data Sheet," 20 09 2024. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/datasheet-c78-736282.html. [Accessed 12 2024].

[44] Ciena Corporation, "6500 Family of Packet-Optical Platforms," 2024. [Online]. Available: https://www.ciena.com/products/6500. [Accessed 12 2024].

[45] Telecomunicaciones, Mira, Cisco ACI 4.x Bootcamp, 3 ed., Madrid: DCAC9K, 2020, p. 392.

[46] Cisco, «Implementación de ACI centrada en aplicaciones,» 15 10 2024. [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/cx/cx-cloud/cx222468-deploying-aci-as-application-centric.html?dtid=osscdc000283. [Último acceso: 12 2024].

ANEXO I: PLAN DE PRUEBAS

En el presente anexo se incluye la plantilla de cada uno de los casos de pruebas realizados sobre la infraestructura SDN de Cisco ACI desplegada.

Se hace de acuerdo al escenario, equipamiento y agenda de pruebas, indicados en el apartado 4.1.1 del Plan de Pruebas llevado a cabo.

Los casos de prueba se clasifican en cada una de las siete categorías indicadas.

1. Pruebas básicas de la infraestructura

Núm.	1.1	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas Básicas					
Equipo		Nexus 93XX, APIC-CLUSTER					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**Salud de Equipos**					
Propósito:		Verificar que los equipos se iniciaron de manera correcta y que fueron descubiertos e integrados a los controladores.					
Preparación:		Supone que todo el hardware incluido se ha instalado correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Acceder a uno de los controladores por HTTPS 2. Realizar las revisiones necesarias descritas abajo.					
Verificar:							
1. Confirmar que los dispositivos están encendidos. Revisar los LEDs de los equipos y confirmar que todos los módulos están habilitados y que no hay errores / alarmas presentes.					Aprobado X	No Aprobado ☐	
2. En la interfaz del navegador vaya a Fabric> Inventory> Fabric Membership verificar los equipos asociados a su correspondiente pod.					Aprobado X	No Aprobado ☐	
3. En la interfaz del navegador ir a System>Dashboard y verificar las alarmas y la salud de los equipos.					Aprobado X	No Aprobado ☐	
4. En la interfaz del navegador ir a Fabric> Inventory> Fabric Membership> Unreachable Nodes y verificar si se muestra algún nodo.					Aprobado X	No Aprobado ☐	
Resultados Esperados:		1. LEDs en verde y/o no hay LED de alarma. 2. Están todos los equipos con hostnames, son soportados y tienen dirección IP. 3. No hay alarmas y/o la salud es superior a 99%. 4. No deben existir nodos inalcanzables.					
Paso: (Inicial)							
Fallo: (Inicial)							
Razón de la No Aprobación:							
Observaciones:							
Núm.	1.2	Revisión	1.0	Autor:		Fecha:	

Categoría	Pruebas Básicas		
Equipo	Nexus 93XX, APIC-CLUSTER		
Tecnología:	Centros de datos	**Prueba de Conformidad**	Estándar
Nombre del Fabric ACI:	FABRIC_ACI		
Titulo:	**Clúster de APIC**		
Propósito:	Verificar que se formó el clúster de controladores (APIC) de manera correcta.		
Preparación:	Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.		
Procedimiento:	1. Acceder a uno de los controladores por HTTPS 2. Realizar las revisiones necesarias descritas abajo.		
Verificar:			
En la interfaz del navegador vaya a System> Controllers> Controllers y verificar la salud del clúster.		Aprobado [X]	No Aprobado [ ]
Resultados Esperados:	En el Dashboard, se muestran los tres controladores en servicio y en el estado Fully-Fit.		
Paso: (Inicial)			
Fallo: (Inicial)			
Razón de la No Aprobación:			
Observaciones:			

Núm.	1.3	Revisión	1.0	Autor:		Fecha:	
Categoría		Versiones de Software					
Equipo		Nexus 93XX, APIC-CLUSTER					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**Actualización de versiones de software**					
Propósito:		Verificar que al actualizar los nodos pares/impares de un Pod, el impacto en el tráfico es mínimo o nulo.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Acceder a uno de los controladores por HTTPS 2. Realizar las revisiones necesarias descritas abajo.					
Verificar:							
1. Crear grupos de mantenimiento: 2 grupos por cada Pod repartidos en nodos pares e impares (Pod1_par, Pod1_impar, Pod2_par y Pod2_impar). En cada grupo se meterán los switches (*Leaf* y *Spine*) con *hostname* par o impar, de cada Pod.						Aprobado [X]	No Aprobado [ ]
2. Lanzar una actualización de software sobre un grupo de mantenimiento.						Aprobado [X]	No Aprobado [ ]
3. Con un PC/VM en cada Pod conectado a los *Leaf* comprobar que la conectividad se mantiene (excepto cuando se actualiza el switch al que está conectado el PC/VM).						Aprobado [X]	No Aprobado [ ]
Resultados Esperados:		Sin impacto en el tráfico.					

Paso: (Inicial)	
Fallo: (Inicial)	
Razón de la No Aprobación:	
Observaciones:	Se han creado dos grupos de actualización de nodos par e impar por cada datacenter (Pod1 y Pod2). El impacto sobre la red ha sido nulo, y siempre se ha cursado el tráfico sin cortes.

Núm.	1.4	Revisión	1.0	Autor:		Fecha:	
Categoría		Versiones de Software					
Equipo		Nexus 93XX, APIC-CLUSTER					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**Versiones de Software**					
Propósito:		Verificar que los equipos fueron actualizados a las versiones de software correctas.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Acceder a uno de los controladores por HTTPS 2. Realizar las revisiones necesarias descritas abajo.					
Verificar:							
1. En la interfaz del navegador ir a Admin> Firmware> Nodes, verificar las versiones de software de los nodos de red.					Aprobado [X]		No Aprobado [ ]
2. En la interfaz del navegador ir a Admin> Firmware> Controllers verificar las versiones de software de los APIC.					Aprobado [X]		No Aprobado [ ]
3. En la interfaz del navegador ir a Admin> Firmware> Nodes verificar que existen grupos con Nexus asociados.					Aprobado [X]		No Aprobado [ ]
Resultados Esperados:		1. La versión de software debe ser **aci-n9000-dk9.15.3(2b).bin** en todos los switches Nexus. 2. La versión de software debe ser **aci-apic-dk9.5.3(2b).iso** en todos los servidores APIC. 3. Debe haber 4 grupos, separando nodos pares e impares tanto de leafs como de spines.					
Paso: (Inicial)							
Fallo: (Inicial)							
Razón de la No Aprobación:							
Observaciones							

Núm.	1.5	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas Básicas					
Equipo		Nexus 93XX, APIC-CLUSTER					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**Dominios Físicos**					
Propósito:		Verificar que se han creado los AAEP y dominios físicos correspondientes.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					

Procedimiento:	1. Acceder a uno de los controladores por HTTPS 2. Realizar las revisiones necesarias descritas abajo.
Verificar:	
1. En la interfaz del navegador vaya a Fabric> Access Policies> Physical and External Domains> Physical Domains y verificar que se han creado los dominios necesarios.	Aprobado ☒ No Aprobado ☐
2. En la interfaz del navegador vaya a Fabric> Access Policies> Policies> Global> Attachable Access Entity Profiles y verificar que se han creado las políticas necesarias.	Aprobado ☒ No Aprobado ☐
Resultados Esperados:	Se muestra un dominio físico. Se muestran el AAEP asociado.
Paso: (Inicial)	
Fallo: (Inicial)	
Razón de la No Aprobación:	
Observaciones:	

2. Pruebas de Capa 1

Núm.	2.1	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas de Capa 1					
Equipo		Nexus 93XX, APIC-CLUSTER					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**Topología Física**					
Propósito:		Verificar que los equipos están interconectados de manera correcta y los enlaces se encuentran funcionando					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Acceder a uno de los controladores por HTTPS 2. Realizar las revisiones necesarias descritas abajo.					
Verificar:							
1. En la interfaz del navegador vaya a Fabric> Inventory> Topology y verificar que la topología es correcta.						Aprobado ☒ No Aprobado ☐	
2. En la línea de comandos de cada Leaf teclear el comando **show lldp neighbors**						Aprobado ☒ No Aprobado ☐	
Resultados Esperados:		1. Los equipos se ven conectados de la misma manera a la mostrada en el diagrama de este documento. 2. Se muestran los vecinos conectados en los puertos correspondientes.					
Paso: (Inicial)							
Fallo: (Inicial)							
Razón de la No Aprobación:							
Observaciones:							

Núm.	2.2	Revisión	1.0	Autor:		Fecha:	

Categoría	Pruebas de Capa 1		
Equipo	Nexus 93XX, APIC-CLUSTER		
Tecnología:	Centros de datos	**Prueba de Conformidad**	Estándar
Nombre del Fabric ACI:	FABRIC_ACI		
Titulo:	**Perfiles y políticas de interfaces**		
Propósito:	Verificar que se han podido crear políticas y perfiles para las conexiones a las interfaces a otros dispositivos fuera del fabric.		
Preparación:	Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.		
Procedimiento:	1. Acceder a uno de los controladores por HTTPS 2. Realizar las revisiones necesarias descritas abajo.		
Verificar:			
1. En la interfaz del navegador ir a Fabric> Access Policies > Policies > Interface y verificar que se han podido crear políticas de Link-level.	Aprobado [X] No Aprobado [ ]		
2. En la interfaz del navegador ir a Fabric> Access Policies> Interfaces > Leaf Interfaces > Policy Groups> y verificar que se han podido crear Grupos de políticas.	Aprobado [X] No Aprobado [ ]		
3. En la interfaz del navegador ir a Fabric> Access Policies> Interfaces > Leaf Interfaces > Profiles y verificar que se han podido crear los perfiles.	Aprobado [X] No Aprobado [ ]		
Resultados Esperados:	1. Se observan políticas en la tabla de la derecha. 2. Se observan grupos de políticas en la tabla de la derecha y estos se encuentran asociados a un AAEP y a una o más políticas. 3. Se observan perfiles en la tabla de la derecha y se encuentran asociados a 1 o más interfaces.		
Paso: (Inicial)			
Fallo: (Inicial)			
Razón de la No Aprobación:			
Observaciones:			

Núm.	2.3	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas de Capa 1					
Equipo		Nexus 93XX, APIC-CLUSTER					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**Selectores de Switches y asociaciones**					
Propósito:		Verificar que se han podido crear políticas y perfiles para las conexiones a las interfaces a otros dispositivos fuera del fabric.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Acceder a uno de los controladores por HTTPS 2. Realizar las revisiones necesarias descritas abajo.					

Verificar:	
1. En la interfaz del navegador ir a Fabric> Access Policies> Switches > Leaf Switches > Profiles Se han creado Perfiles para los Leafs	Aprobado [X] No Aprobado [ ]
2. En la interfaz del navegador ir a Fabric> Access Policies> Switches > Leaf Switches > Profiles, hacer clic en Profile y verificar que hay un selector de Switch asociado (repetir el proceso para cada perfil).	Aprobado [X] No Aprobado [ ]
3.. En la interfaz del navegador ir a Fabric> Access Policies> Switches > Leaf Switches > Profiles, se puede asociar un perfil solo para esta prueba y borrarlo al terminar (utilice los botones de '+' y 'x').	Aprobado [X] No Aprobado [ ]

Resultados Esperados:	1. Se ha creado un perfil por cada switch. 2. Se ha asociado el(los) nodo(s) correspondiente al perfil. 3. Se ha podido asociar una switch al perfil. • Selector de switch asociado • Si no existe, probar si puede asociar uno para esta prueba y borrarlo al terminar (utilice los botones de '+' y 'x').
Paso: (Inicial)	
Fallo: (Inicial)	
Razón de la No Aprobación:	
Observaciones:	

3. Pruebas de Capa 2

Núm.	3.1	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas de Capa 2					
Equipo		Nexus 93XX, APIC-CLUSTER					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**VPC**					
Propósito:		Verificar que se han creado los dominios de vPC en las parejas de switches correspondientes y que se ha creado algún perfil de vPC.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Acceder a uno de los controladores por HTTPS 2. Realizar las revisiones necesarias descritas abajo.					

Verificar:	
1. Ejecutar el comando show vpc brief en cada leaf y verificar el estado. Repetir la prueba en cada leaf.	Aprobado [X] No Aprobado [ ]

Resultados Esperados:	El vPC correspondiente en cada pareja de leafs se encuentra formado y todos los vPCs se encuentran levantados y sin inconsistencias. Ir a Fabric > Access Policies > Configure an interface, PC, and VPC y verificar que en la parte inferior izquierda aparecen 8 dominios de VPC en el apartado VPC Switch Pairs.
Paso: (Inicial)	
Fallo: (Inicial)	
Razón de la No Aprobación:	

Observaciones:	

Núm.	3.2	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas de Capa 2					
Equipo		Nexus 93XX, APIC-CLUSTER					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**Vlan Pools**					
Propósito:		Verificar que se han creado los VLAN pools correspondientes y se han asociado al dominio físico apropiado.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Acceder a uno de los controladores por HTTPS 2. Realizar las revisiones necesarias descritas abajo.					
Verificar:							
1. En la interfaz del navegador ir a Fabric> Access Policies> Pools> VLAN y verificar que se ha podido crear al menos un VLAN pool.					Aprobado [X]		No Aprobado [ ]
2. En la interfaz del navegador ir a Fabric> Access Policies> Physical and External Domains> Physical Domains y verificar que cada dominio tiene asociado un VLAN pool.					Aprobado [X]		No Aprobado [ ]
Resultados Esperados:		Verificar que se han creado los VLAN Pools deseados.					
Paso: (Inicial)							
Fallo: (Inicial)							
Razón de la No Aprobación:							
Observaciones:							

Núm.	3.3	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas de Capa 2					
Equipo		Nexus 93XX, APIC-CLUSTER					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**Perfiles y políticas de capa 2**					
Propósito:		Verificar que se han podido crear políticas y perfiles relacionados a protocolos de Capa 2.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Acceder a uno de los controladores por HTTPS 2. Realizar las revisiones necesarias descritas abajo.					
Verificar:							
1. En la interfaz del navegador ir a Fabric> Access Policies> Policies> Interface y verificar que se han podido crear políticas de nivel 2: Storm-control, LLDP, CDP y Port-channel.					Aprobado [X]		No Aprobado [ ]
Resultados		Se observan políticas en la tabla.					

Esperados:	• Storm Control • LLDP • CDP • Port-Channel
Paso: (Inicial)	
Fallo: (Inicial)	
Razón de la No Aprobación:	
Observaciones:	

Núm.	3.4	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas de Capa 2					
Equipo		Nexus 93XX, APIC-CLUSTER					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**APs y EPGs**					
Propósito:		Verificar que se han creado Application Profiles y End Point Groups y que los EPG se han podido asociar a alguna interfaz con una Vlan existente en el pool, asimismo se han relacionado todos los objetos previamente verificados para dar conectividad a un host y/o aplicación dentro del mismo.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Acceder a uno de los controladores por HTTPS. 2. Desde una máquina virtual o un PC conectado a los Leafs genere tráfico. 3. Identifique correctamente la Vlan y direccionamiento de dicha máquina o PC. 4. Realizar las revisiones necesarias descritas abajo.					
Verificar:							
1. En la interfaz del navegador ir a Tenants> (nombre del tenant)> Application Profiles> seleccione un AP y ver que contiene uno o más EPG.					Aprobado [X]	No Aprobado [ ]	
2. En la interfaz del navegador ir a Tenants> (nombre del tenant)> Application Profiles> seleccionar un EPG dentro de un AP, ir a Operational> Client Endpoint en el panel de trabajo, verificar que se han descubierto dispositivos.					Aprobado [X]	No Aprobado [ ]	
Resultados Esperados:		1. Existen tanto APs como grupos EPG creados, esto demuestra que se pueden desplegar configuraciones sin problemas. 2. Al menos un EPG ya muestra dispositivos conectados y descubiertos en las Vlanes correspondientes.					
Paso: (Inicial)							
Fallo: (Inicial)							
Razón de la No Aprobación:							
Observaciones:							

Núm.	3.5	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas de Capa 2					
Equipo		Nexus 93XX, APIC-CLUSTER					

Tecnología:	Centros de datos	**Prueba de Conformidad**	Estándar
Nombre del Fabric ACI:	FABRIC_ACI		
Titulo:	**VRFs, BDs y asociaciones**		
Propósito:	Verificar que se han creado las VRF y los BD necesarios correctamente, y que éstos se han asociado para dar conectividad a través de la infraestructura de ACI.		
Preparación:	Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.		
Procedimiento:	1. Acceder a uno de los controladores por HTTPS. 2. Desde una máquina virtual o una PC conectada a los Leafs genere tráfico.		
Verificar:			
1. En la interfaz del navegador ir a Tenants>Nombre del tenant>Networking> VRFs y verificar que se ha creado una VRF.		Aprobado [X]	No Aprobado [ ]
2. Ir a cada una de las VRF, y en Panel de Trabajo> Operational > Asociated EPG y verificar que se han asociado los EPG correspondientes a dicha VRF.		Aprobado [X]	No Aprobado [ ]
3. En la interfaz del navegador ir a Tenants>Nombre del tenant > Networking> Bridge Domains. Verificar que los BDs correspondientes están asociados a una VRF.		Aprobado [X]	No Aprobado [ ]
Resultados Esperados:	1. La VRF se ha configurado. 2. A cada VRF se han asociado los EPG correspondientes. 3. A cada VRF se han asociado los BDs correspondientes		
Paso: (Inicial)			
Fallo: (Inicial)			
Razón de la No Aprobación:			
Observaciones:			

Núm.	3.6	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas de Capa 2					
Equipo		Nexus 93XX, APIC-CLUSTER					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**Vlans duplicadas**					
Propósito:		Verificar que, con el uso de VLAN duplicadas en diferentes leafs, el servicio de ambas VLAN es procesado correctamente en el fabric.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Acceder a uno de los controladores por HTTPS. 2. Desde dos orígenes diferentes, enviar tráfico utilizando el mismo ID de VLAN y segmentos de red diferentes.					
Verificar:							
1. En el origen, enviar tráfico hacia el destino y viceversa.					Aprobado [X]		No Aprobado [ ]
Resultados Esperados:		1. Hay conectividad correcta entre el origen y el destino.					
Paso: (Inicial)							

Fallo: (Inicial)	
Razón de la No Aprobación:	
Observaciones:	Pruebas realizadas con ping entre portátil en Pod1 y switch de Pod2 en ambas VLANes.

4. Pruebas de Capa 3

Núm.	4.1	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas de Capa 3					
Equipo		APIC-CLUSTER					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**Route reflector de BGP interno**					
Propósito:		Verificar que se ha configurado full mesh de iBGP entre los Spine.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Acceder a uno de los controladores por HTTPS. 2. Desde una máquina virtual o una PC conectada a los Leafs genere tráfico.					
Verificar:							
1. En la interfaz del navegador ir a System> System Settings> BGP Route Reflector y en el panel de trabajo verifique que se tienen 4 Spines asociados.						Aprobado [X]	No Aprobado [ ]
2.En la interfaz del navegador ir a Fabric> Fabric Policies> Pods > Policy Groups y verificar que existe alguna política que tiene asociada a su vez la política default en la columna BGP Route Reflector Policy.						Aprobado [X]	No Aprobado [ ]
3. En la interfaz del navegador ir a Fabric> Fabric Policies> Pods > Profiles y verificar que las polticias del punto anterior esten asociadas a su perfil correspondiente.						Aprobado [X]	No Aprobado [ ]
4.Conectarse a los 4 nodos Spine y comprobar que el protocolo BGP está corriendo con el AS 65001 ejecutando el comando **show bgp process vrf overlay-1**.						Aprobado [X]	No Aprobado [ ]
5.Desde los mismos nodos Spine, comprobar las adyacencias bgp ejecutando el comando: **show bgp vpnv4 unicast summary vrf overlay-1**.						Aprobado [X]	No Aprobado [ ]
6.Conectarse a los nodos Leaf y verficar que el proceso bgp está corriendo y verificar las adyacencias.						Aprobado [X]	No Aprobado [ ]
Resultados Esperados:	1.Se tienen 4 nodos Spine asociados y se configuró el AS 65001 correctamente. 2.La políticas están creadas y asociadas. 3.Los distintos Pod_profiles tienen asociada las políticas. 4.Cada nodo Spine tiene activado el protocolo BGP en el AS 65001. 5.Cada nodo Spine tiene adyacencias BGP con los Leafs de su pod local y con los nodos Spine del pod remoto. 6. Cada nodo Leaf tiene activado el protocolo BGP en el AS 65001 y tiene adyacencias con los nodos Spine del pod al que pertenece.						
Paso: (Inicial)							
Fallo: (Inicial)							
Razón de la No Aprobación:							
Observaciones:	Pruebas realizadas con ping entre portátil en Pod1 y switch de Pod2.						

Núm.	4.2	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas de Capa 3					
Equipo		Nexus 93XX, APIC-CLUSTER					
Tecnología:		Centros de datos		**Prueba de Conformidad**		Estándar	
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**Nivel 3 en ACI**					
Propósito:		Verificar que hay conectividad correcta con el nivel 3 configurado en ACI					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Acceder a uno de los controladores por HTTPS. 2. Desde una máquina virtual o una PC conectada a los Leafs genere tráfico.					
Verificar:							
Enviar tráfico, desde una maquina conectada a los Leafs mediante VPC, a la IP configurada en ACI, simulando su default gateway en ACI.					Aprobado [X]	No Aprobado [ ]	
Resultados Esperados:		1. La comunicación es correcta.					
Paso: (Inicial)							
Fallo: (Inicial)							
Razón de la No Aprobación:							
Observaciones:		Pruebas realizadas con ping entre portátil en Pod1 y switch de Pod2.					

5. Pruebas de Redundancia

Núm.	5.1	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas de Redundancia					
Equipo		Nexus 93XX					
Tecnología:		Centros de datos		**Prueba de Conformidad**		Estándar	
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**Fallo de power-supply**					
Propósito:		Verificar que al tener problemas en una fuente de alimentación en los dispositivos dónde se tienen de manera redundante no hay impacto en el tráfico de la red. Comprobar también que al perder una fuente, una alarma se muestra en la interfaz del controlador.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Acceder a uno de los controladores por HTTPS. 2. Desde una máquina virtual o una PC conectada a los Leafs genere tráfico. 3. Realizar las revisiones necesarias descritas abajo.					
Verificar:							
1. Desde un PC, VM o switch auxiliar lanzar un ping al gateway y mantener durante toda la prueba.					Aprobado [X]	No Aprobado [ ]	
2. En la interfaz del navegador vaya a System> Faults, verificar que no hay alarmas, sacar una fuente de los dispositivos que cuentan con redundancia y					Aprobado [X]	No Aprobado [ ]	

verificar que aparece la alarma. Repetir el proceso para cada fuente, una a la vez.	
3. Al terminar la revisión anterior en la interfaz del navegador ir a System> Faults y verificar que las alarmas han desaparecido.	Aprobado ☒ No Aprobado ☐
Resultados Esperados:	1. El ping debe responder y no debe interrumpirse. 2. Las alarmas se deben de mostrar de manera adecuada y desaparecer al restaurar la fuente. 3. Al terminar la prueba el impacto en la red debe haber sido nulo y las alarmas deben hacer desaparecido.
Paso: (Inicial)	
Fallo: (Inicial)	
Razón de la No Aprobación:	
Observaciones:	Pruebas realizadas con ping entre portátil en Pod1 y switch de Pod2.

Núm.	5.2	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas de Redundancia					
Equipo		Nexus 93XX					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**Fallo de power grid**					
Propósito:		Verificar que al tener problemas de electricidad con una fase no hay impacto en el tráfico de la red. También comprobar que una alarma se muestra en la interfaz del controlador.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Acceder a uno de los controladores por HTTPS. 2. Desde una máquina virtual o una PC conectada a los Leafs genere tráfico. 3. Realizar las revisiones necesarias descritas abajo.					
Verificar:							
1. Desde un PC, VM o switch auxiliar realizar ping al gateway y mantener durante toda la prueba.					Aprobado ☐ No Aprobado ☐		
2. En la interfaz del navegador ir a System> Faults Verificar que no hay alarmas, apagar una fase y verificar que aparece la alarma. Repetir el proceso para cada fase, una a la vez.					Aprobado ☐ No Aprobado ☐		
3. Al terminar la revisión anterior en la interfaz del navegador ir a Systems> Faults y verificar que las alarmas han desaparecido.					Aprobado ☐ No Aprobado ☐		
Resultados Esperados:		1. El ping debe responder y no debe interrumpirse 2. Las alarmas se deben de mostrar de manera adecuada y desaparecer al recuperar la fase. 3. Al terminar la prueba el impacto a la red debe haber sido nulo y las alarmas deben haber desaparecido.					
Paso: (Inicial)							
Fallo: (Inicial)							
Razón de la No Aprobación:							
Observaciones:		No realizada por necesidad de coordinación con el Técnico electricista para que corte una fase.					

Núm.	5.3	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas de Redundancia					
Equipo		Nexus 93XX					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**Fallo de Apic**					
Propósito:		Verificar que al perder un APIC no hay impacto en el tráfico de la red. Comprobar también que se muestra una alarma en la interfaz de los otros controladores.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Acceder a uno de los controladores por HTTPS. 2. Desde una máquina virtual, un PC o un switch auxiliar conectado a los Leafs generar tráfico. 3. Realizar las revisiones necesarias descritas abajo.					
Verificar:							
1. Desde un PC, VM o switch auxiliar lanzar un ping al gateway y mantener durante toda la prueba.					Aprobado [X]	No Aprobado [ ]	
2.En la interfaz del navegador ir a System> Faults y verificar que no hay alarmas, apagar un servidor APIC y verificar que aparece la alarma. Repetir el proceso para cada APIC, uno a la vez. Apagar los dos APICs de los Pod 1. Apagar los tres APICs.					Aprobado [X]	No Aprobado [ ]	
3. Al terminar la revisión anterior en la interfaz del navegador ir a Systems> Faults y verificar que las alarmas han desaparecido. Ir también a System> Controller> Controllers y verificar que el clúster está formado de nuevo.					Aprobado [X]	No Aprobado [ ]	
Resultados Esperados:		1. El ping debe responder y no debe interrumpirse. 2. Las alarmas se deben mostrar de manera adecuada y desaparecer al recuperar el APIC. Al apagar los dos APICs del Pod 1, el sistema no permite realizar cambios de configuración en el APIC restante. Al apagar los tres APICs, no se pueden realizar cambios de configuración, pero el fabric sigue prestando servicio. 3. El clúster debe estar formado de vuelta con los 3 dispositivos y no debe existir impacto alguno.					
Paso: (Inicial)							
Fallo: (Inicial)							
Razón de la No Aprobación:							
Observaciones:		Pruebas realizadas con ping continuo entre portátil en Pod1 y switch de Pod2.					

Núm.	5.4	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas de Redundancia					
Equipo		Nexus 93XX					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**Fallo de Nexus**					

Propósito:	Verificar que al perder una mitad de los Nexus que conforman la infraestructura de ACI el tráfico sigue funcionando por la otra mitad.
Preparación:	Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.
Procedimiento:	1. Acceder a uno de los controladores por HTTPS. 2. Desde una máquina virtual o una PC conectada a los Leafs genere tráfico. 3. Realizar las revisiones necesarias descritas abajo.
Verificar:	
1. Desde un PC, VM o switch auxiliar lanzar un ping al gateway y mantener durante toda la prueba.	Aprobado ☒ No Aprobado ☐
2. En la interfaz del navegador ir a Systems> Faults y verificar que no hay alarmas, desconectar o apagar todos los Nexus impares (Leafs y Spines) uno por uno hasta que todos estén apagados. En Fabric> Inventory> Fabric Membership verifique que los Nexus desaparecen y vuelven a aparecer al encenderlos. Repetir el proceso para los Nexus pares.	Aprobado ☒ No Aprobado ☐
3. Al terminar la revisión anterior en la interfaz del navegador ir a Systems> Faults y verificar que las alarmas han desaparecido. Verificar los LEDs de los Nexus físicamente. En Fabric> Inventory> Fabric Membership verificar que todos los equipos aparecen de nuevo.	Aprobado ☒ No Aprobado ☐
Resultados Esperados:	1. El ping debe responder y no debe interrumpirse. 2. Las alarmas se deben de mostrar de manera adecuada y desaparecer al recuperar los equipos. 3. Todas los Nexus están funcionando. El impacto a la red fue prácticamente imperceptible. Los equipos fueron descubiertos de nuevo sin alarmas.
Paso: (Inicial)	
Fallo: (Inicial)	
Razón de la No Aprobación:	
Observaciones:	Pruebas realizadas con ping entre portátil en Pod1 y switch de Pod2.

6. Pruebas de administración OOB (fuera de banda)

Las pruebas que se indican a continuación se realizan desde la perspectiva en la que ACI entiende por *fuera de banda*. Esta es toda gestión realizada por fuera del clúster de controladores APIC, de los elementos de aquella red cuyo tráfico transcurre de manera paralela, aunque esa red no cumpla estrictamente con los criterios de fuera de banda (switches Nexus de la red IPN, switches catalyst de gestión, etc.).

Núm.	6.1	Revisión	1.0	Autor:		Fecha:	
Categoría		Redes de Administración					
Equipo		Nexus 93XX, APIC CLUSTER					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**Redes de administración OOB**					
Propósito:		Verificar que todos los equipos tienen asignada una dirección de red de fuera de banda.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					

Procedimiento:	1. Acceder a uno de los controladores por HTTPS.	
Verificar:		
1. Ir a Tenants> mgmt> Node Management Address >Panel de Trabajo> Static Node Management Address y verificar que los nodos cuentan con direccionamiento en la red fuera de banda.		Aprobado ☒ No Aprobado ☐
1.Ir a Tenants> mgmt> Node Management EPG y verificar que la red fuera de banda cuenta con su respectivo EPG		Aprobado ☒ No Aprobado ☐
Resultados Esperados:	1. Todos los nodos tienen una IP configurada asignada para la red 'Out-of-Band'. 2. Existe un EPG para la red 'Out-of-Band'.	
Paso: (Inicial)		
Fallo: (Inicial)		
Razón de la No Aprobación:		
Observaciones:		

Núm.	6.2	Revisión	1.0	Autor:		Fecha:	
Categoría		Redes de Administración					
Equipo		Nexus 93XX, APIC CLUSTER					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**SSH via OOB**					
Propósito:		Verificar que el servicio de SSH se configuró correctamente.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Conectar un PC, que cuente con un navegador web, a una red que pueda alcanzar las redes de administración de ACI. 2. Realizar las revisiones necesarias descritas abajo.					
Verificar:							
1.Conectarse mediante SSH a cada una de las direcciones IP de los equipos en la red 'Out-of-Band'.						Aprobado ☐ No Aprobado ☒	
Resultados Esperados:		1. Se muestra la pantalla de login y se puede acceder a los equipos.					
Paso: (Inicial)							
Fallo: (Inicial)		LEAFC111 no tiene ssh en mgmt, no se alcanza gateway de gestión.					
Razón de la No Aprobación:							
Observaciones:		Los demás equipos se conectan vía SSH sin ningún problema.					

Núm.	6.3	Revisión	1.0	Autor:		Fecha:	
Categoría		Redes de administración					
Equipo		APIC CLUSTER					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar

Nombre del Fabric ACI:	FABRIC_ACI
Titulo:	**HTTPS**
Propósito:	Verificar el servicio de HTTPS funciona correctamente en los APIC.
Preparación:	Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.
Procedimiento:	1. Conectar un PC, que cuente con un navegador web, a una red que pueda alcanzar las redes de administración de ACI. 2. Realizar las revisiones necesarias descritas abajo.
Verificar:	
1.Conectarse mediante HTTPS a cada una de las direcciones IP de los dispositivos en la red 'Out-of-Band'	Aprobado ☒ No Aprobado ☐
Resultados Esperados:	1. Se muestra la pantalla de login y se puede acceder a los equipos.
Paso: (Inicial)	
Fallo: (Inicial)	
Razón de la No Aprobación:	
Observaciones:	Prueba realizada desde los equipos Consolas.

Núm.	6.4	Revisión	1.0	Autor:		Fecha:	
Categoría		Redes de Administración					
Equipo		APIC CLUSTER					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**Syslog**					
Propósito:		Verificar que el APIC es capaz de generar mensajes de syslog.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Disponer de un servidor de syslog. 2. Realizar las revisiones necesarias descritas abajo.					
Verificar:							
1. Realizar alguna configuración en el APIC que genere un mensaje de syslog.					Aprobado ☐ No Aprobado ☐		
Resultados Esperados:		1. Se muestra el mensaje correspondiente en el servidor de syslog.					
Paso: (Inicial)							
Fallo: (Inicial)							
Razón de la No Aprobación:							
Observaciones:		Se está pendiente de actualizar la versión del sistema de monitorización del cliente.					

Núm.	6.5	Revisión	1.0	Autor:		Fecha:	
Categoría		Redes de Administración					

Equipo	APIC CLUSTER		
Tecnología:	Centros de datos	**Prueba de Conformidad**	Estándar
Nombre del Fabric ACI:	FABRIC_ACI		
Titulo:	**SNMP**		
Propósito:	Verificar que el APIC es capaz de generar mensajes SNMP ante una caída de equipo/interfaz.		
Preparación:	Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.		
Procedimiento:	1. Disponer de un servidor que permita la recepción de traps SNMP. 2. Realizar las revisiones necesarias descritas abajo.		
Verificar:			
1. En el navegador Ir a Fabric > Fabric Policies > Policies 2. Desconectar el interfaz de uno de los equipos del fabric. 3. Comprobar que se recibe el trap correspondiente en el servidor SNMP.	Aprobado ☐ No Aprobado ☒		
Resultados Esperados:	1. Se muestra el trap correspondiente en el servidor SNMP.		
Paso: (Inicial)			
Fallo: (Inicial)			
Razón de la No Aprobación:			
Observaciones:	Se verifica la recepción de los traps, pero coincide con una actualización del sistema de monitorización y queda pendiente repetir prueba hasta dicha actualización. Con Zabixx vía SNMP funciona correctamente. No se aprueba hasta repetición del caso de prueba.		

Núm.	6.6	Revisión	1.0	Autor:		Fecha:	
Categoría		Redes de Administración					
Equipo		APIC CLUSTER					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**NTP**					
Propósito:		Verificar que el APIC se sincroniza correctamente con los servidores de tiempo indicados.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Disponer de un servidor que permita la sincronización de la hora y del día del APIC. 2. Realizar las revisiones necesarias descritas abajo.					
Verificar:							
1. Comprobar que la fecha y la hora están sincronizados con los servidores NTP configurados: - En los APIC, ejecutar el comando **show ntpq.** - En los switches del CPD de XXX, ejecutar los comandos **show ntp peer-status** y **show ntp statistics peer ipaddr 10.m.n.250 o 10.p.q.254** (pod 2)		Aprobado ☐ No Aprobado ☒					

- En los switches del CPD de sede1, ejecutar los comandos **show ntp peer-status** y **show ntp statistics peer ipaddr 10.m.n.250** - En los switches del CPD de sede2, ejecutar los comandos **show ntp peer-status** y **show ntp statistics peer ipaddr 10.p.q.254** 2. La correcta sincronización se puede verificar en el APIC, en Fabric > Fabric Policies > Policies > Pod > Date and Time > Policy NTP > NTP Server **10.m.n.250** haciendo click en Operational.	
Resultados Esperados:	1. Existe sincronización de la fecha y la hora en el clúster de APIC.
Paso: (Inicial)	
Fallo: (Inicial)	LEAFC111 no sync ntp ya que no ve el gateway de gestión.
Razón de la No Aprobación:	
Observaciones:	Los demás equipos sincronizan NTP sin ningún problema.

7. Pruebas de la red IPN

Núm.	7.1	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas red IPN					
Equipo		Nexus 93XX					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**Topología IPN**					
Propósito:		Verificar que los equipos están interconectados de manera correcta y los enlaces se encuentran funcionando					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Acceder a uno de los controladores por HTTPS 2. Realizar las revisiones necesarias descritas abajo.					
Verificar:							
1. En la interfaz del navegador vaya a Fabric> Inventory> Topology y verificar que la topología es correcta y que cada nodo está asociado a su Pod correspondiente.						Aprobado ☒	No Aprobado ☐
2. En la línea de comando de cada nodo IPN teclear el comando show lldp neighbors						Aprobado ☒	No Aprobado ☐
Resultados Esperados:		Se muestran los vecinos conectados a los puertos correctos.					
Paso: (Inicial)							
Fallo: (Inicial)							
Razón de la No Aprobación:							
Observaciones:							

Núm.	7.2	Revisión	1.0	Autor:		Fecha:	

Categoría	Pruebas red IPN		
Equipo	Nexus 93XX		
Tecnología:	Centros de datos	**Prueba de Conformidad**	Estándar
Nombre del Fabric ACI:	FABRIC_ACI		
Titulo:	**Adyacencias OSPF**		
Propósito:	Verificar que las adyacencias OSPF entre los equipos de la red IPN son correctas.		
Preparación:	Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.		
Procedimiento:	1. Acceder a los equipos de la red IPN vía SSH 2. Realizar las revisiones necesarias descritas abajo.		
Verificar:			
1. Acceder a los cuatro equipos de la red IPN por línea de comando	Aprobado [X] No Aprobado [ ]		
2. En la línea de comando de cada IPN teclear el comando **show ip ospf neighbors vrf fabric-mpod**	Aprobado [X] No Aprobado [ ]		
Resultados Esperados:	Cada equipo de la red IPN muestra adyacencia OSPF: Con el otro equipo de su mismo CPD a través del port-channel configurado. Con los dos switches Spine de su mismo CPD. Con el equipo IPN del CPD remoto a través del enlace WAN establecido.		
Paso: (Inicial)			
Fallo: (Inicial)			
Razón de la No Aprobación:			
Observaciones:			

Núm.	7.3	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas red IPN					
Equipo		Nexus 93600GD-CX; APIC-CLUSTER					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**External TEP interfaces en switches Spine**					
Propósito:		Verificar que se ha asignado correctamente el direccionamiento TEP en los distintos nodos que actúan como Spine.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Acceder vía HTTPS al APIC. 2. Realizar las revisiones necesarias descritas abajo.					
Verificar:							
1. Acceder al controlador APIC.				Aprobado [X] No Aprobado [ ]			
2. Comprobar el direccionamiento TEP asignado en Tenant >Infra > Policies > Protocol > Fabric Ext Connection Policies > Fabric Ext Connection Policy default y verificar que se ha asignado un Data Plane TEP por cada uno de los Pods. 3. En Tenant >Infra > Policies > Protocol > Fabric Ext Connection Policies > Fabric Ext Connection Policy default, verificar en el apartado Fabric External Routing Profile que aparecen todas las subredes de interconexión entre los nodos IPNs y los Spines.				Aprobado [X] No Aprobado [ ] Aprobado [X] No Aprobado [ ]			

Resultados Esperados:	Existe direccionamiento TEP asignado a cada uno de los Pods. Todas las subredes de interconexión entre IPNs y Spines están definidas correctamente.
Paso: (Inicial)	
Fallo: (Inicial)	
Razón de la No Aprobación:	
Observaciones:	

Núm.	7.4	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas red IPN					
Equipo		Nexus 93600GD-CX; APIC-CLUSTER					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**MP-BGP eVPN**					
Propósito:		Verificar que las adyacencias BGP se establecen correctamente y que se anuncian las rutas adecuadamente.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Acceder vía HTTPS al APIC. 2. Realizar las revisiones necesarias descritas abajo.					
Verificar:							
1. Acceder al controlador APIC.					Aprobado [X]		No Aprobado [ ]
2. Comprobar las adyacencias en cada nodo Spine con el comando **show bgp l2vpn evpn summary vrf overlay-1**.					Aprobado [X]		No Aprobado [ ]
Resultados Esperados:		Las adyacencias BGP se han formado y se aprenden rutas correctamente.					
Paso: (Inicial)							
Fallo: (Inicial)							
Razón de la No Aprobación:							
Observaciones:							

Núm.	7.5	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas red IPN					
Equipo		Nexus 93600GD-CX; APIC-CLUSTER					
Tecnología:		Centros de datos			**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**Verificar base de datos COOP**					
Propósito:		En un switch spine remoto, verificar la base de datos COOP y chequear que las entradas se conocen por el túnel proxy entre spines de distintos Pods.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					

Procedimiento:	1. Acceder por línea de comando a un spine. 2. Realizar las revisiones necesarias descritas abajo.	
Verificar:		
1. Acceder a un switch spine por CLI.		Aprobado [X] No Aprobado [ ]
2. Comprobar la base de datos de COOP con el comando **show coop internal info ip-db**.		Aprobado [X] No Aprobado [ ]
Resultados Esperados:	La salida del comando muestra la información correspondiente.	
Paso: (Inicial)		
Fallo: (Inicial)		
Razón de la No Aprobación:		
Observaciones:		

Núm.	7.6	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas red IPN					
Equipo		Nexus 93XX, APIC-CLUSTER					
Tecnología:		Centros de datos		**Prueba de Conformidad**		Estándar	
Nombre del Fabric ACI:		FABRIC_ACI					
Titulo:		**Comprobar túneles dinámicos**					
Propósito:		En un switch Spine comprobar que se establecen los túneles dinámicos para los endpoints remotos.					
Preparación:		Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.					
Procedimiento:		1. Acceder por línea de comando a un switch Leaf. 2. Realizar las revisiones necesarias descritas abajo.					
Verificar:							
1. Acceder a un switch Leaf por CLI.						Aprobado [X] No Aprobado [ ]	
2. Lanzar un ping entre un PC o VM del Pod1 a un PC o VM del Pod2 dentro del mismo BD/EPG. Ejecutar el comando **show endpoint** y comprobar que se forma el túnel dinámico correspondiente. Repetir la misma prueba contra un PC de un BD/EPG distinto.						Aprobado [X] No Aprobado [ ]	
Resultados Esperados:		La salida del comando muestra la información de túneles dinámicos correspondiente.					
Paso: (Inicial)							
Fallo: (Inicial)							
Razón de la No Aprobación:							
Observaciones:							

Núm.	7.7	Revisión	1.0	Autor:		Fecha:	
Categoría		Pruebas red IPN					
Equipo		Nexus 93XX					

Tecnología:	Centros de datos	**Prueba de Conformidad**	Estándar
Nombre del Fabric ACI:	FABRIC_ACI		
Titulo:	**Comprobar redundancia de conexión Inter-CPDs**		
Propósito:	Apagar o desconectar un switch de la red IPN conectado a uno enlaces Inter-CPDs.		
Preparación:	Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.		
Procedimiento:	1. Acceder a la línea de comando de un PC o VM de prueba de uno de los Pod. 2. Realizar las revisiones necesarias descritas abajo.		
Verificar:			
1. Acceder a la línea de comando de un PC o VM en cada uno de los dos Pods.	Aprobado ☒ No Aprobado ☐		
2. Lanzar un ping entre un PC o VM del Pod1 a un PC o VM del Pod2 dentro del mismo o distinto BD/EPG. Verificar que la conectividad se mantiene cuando se apaga/desconecta el Nexus que conecta con uno de los enlaces entre los Datacenters. Restaurar la conectividad y repetir la prueba con el segundo enlace.	Aprobado ☒ No Aprobado ☐		
Resultados Esperados:	La conectividad entre los hosts se mantiene cuando se corta uno de los circuitos de interconexión entre los Data Centers.		
Paso: (Inicial)			
Fallo: (Inicial)			
Razón de la No Aprobación:			
Observaciones:	Pruebas realizadas con ping entre portátil en Pod1 y switch de pod Pod2.		

Núm.	7.8	Revisión	1.0	Autor:		Fecha:	
Categoría	Pruebas red IPN						
Equipo	Nexus 93XX						
Tecnología:	Centros de datos				**Prueba de Conformidad**		Estándar
Nombre del Fabric ACI:	FABRIC_ACI						
Titulo:	**Comprobar seguridad de conexión Inter-CPDs MACSEC**						
Propósito:	Comprobar que la seguridad proporcionada por MACSEC se encuentra configurada y activa entre los 2 enlaces entre CPDs.						
Preparación:	Supone que todo el hardware incluido se instaló correctamente, además de que las configuraciones para la integración de los componentes fueron completadas.						
Procedimiento:	1. Acceder a la línea de comando de un PC o VM de prueba de uno de los Pod. 2. Realizar las revisiones necesarias descritas abajo.						
Verificar:							
1. Acceder a la línea de comando de un PC o VM en uno de los dos Pods, y a conectarse a uno de los IPN.	Aprobado ☒ No Aprobado ☐						
2. Ejecutar el comando ***show macsec mka summary*** y comprobar que en el status aparece ***Secured,*** repetir la prueba con el segundo enlace.	Aprobado ☒ No Aprobado ☐						
Resultados Esperados:	La conexión entre los 2 pares de IPNs se encuentra en modo *Secured*.						

Paso: (Inicial)	
Fallo: (Inicial)	
Razón de la No Aprobación:	
Observaciones:	

ANEXO II: ACRÓNIMOS

Sigla	Significado
ACI	Application Centric Infrastructure
APIC	Application Policy Infrastructure Controller
API	Application Programming Interface
ASIC	Application-Specific Integrated Circuit
BGP	Border Gateway Protocol
CLI	Command Line Interface
CPD	Centro de Procesamiento de Datos
CPU	Central Processing Unit
DC	Data Center
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DWDM	Dense Wavelength Division Multiplexing
EIGRP	Enhanced Interior Gateway Routing Protocol
eVPN	Ethernet Virtual Private Network
GPU	Graphics Processing Unit
GUI	Graphical User Interface
IA	Artificial Intelligence
IaaS	Infrastructure as a Service
IEEE	Institute of Electrical and Electronics Engineers
IDS	Intrusion Detection System
IP	Internet Protocol
IPN	Inter Pod Network
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
L2	Layer 2 (Capa de enlace)

L3	Layer 3 (Capa de red)
LAN	Local Area Network
MACSEC	Media Access Control Security
MPLS	Multiprotocol Label Switching
NFV	Network Function Virtualization
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PaaS	Platform as a Service
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RTT	Round Trip Time
SaaS	Software as a Service
SDN	Software Defined Networking
SD-WAN	Software-Defined Wide Area Network
SSH	Secure Shell (shell seguro)
STP	Spanning Tree Protocol
TACACS	Terminal Access Controller Access Control System
TCP/IP	Transmission Control Protocol/Internet Protocol
TI	Tecnologías de la Información
TIC	Tecnología de la Información y las Comunicaciones
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
VxLAN	Virtual Extensible Local Area Network
WAN	Wide Area Network (red de área extensa)