Universidad Autónoma Metropolitana Unidad Azcapotzalco

División de Ciencias Básicas e Ingeniería

Licenciatura en Ingeniería en Computación

Modalidad: Experiencia profesional

Cisco *Solution Support* en México

Marco Antonio Domínguez Becerra

Matrícula: 210304686

Empresa: *Cisco Systems, Inc.*

Francesca Laurie

Manager Technical Support

Trimestre lectivo 2017 Primavera

Yo, Francesca Laurie, declaro que aprobé el contenido del presente Reporte de Proyecto de Integración y doy mi autorización para su publicación en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.

Francesca Laurie

Firma

Yo, Marco Antonio Domínguez Becerra, doy mi autorización a la Coordinación de Servicios de Información de la Universidad Autónoma Metropolitana, Unidad Azcapotzalco, para publicar el presente documento en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.

Marco Antonio Domínguez Becerra

Firma

Tabla de contenido

Acrónimos

TI: Tecnología de la Información.
ACI: Infraestructura centralizada en aplicaciones.
APIC: Controlador de aplicaciones de políticas de la infraestructura.
AVS: *Switch* virtual de aplicaciones.
DevOps: Desarrollo y operaciones.
CALO: Laboratorio de operaciones avanzadas de Cisco.
REST: Transferencia de estado representacional.
VM: Máquina virtual.
BD: Dominio de puente.
DNS: Sistema de nombres de dominio.
VRF: Enrutamiento virtual y reenvío.
VPC: Port-channel virtual.

Resumen Ejecutivo

Descripción

Cisco *Systems* es una empresa global con sede en California, Estados Unidos, principalmente dedicada a la fabricación, venta, mantenimiento, consultoría y servicios de dispositivos de conexión para redes informáticas: *routers, switches* y servidores. Cisco es el líder mundial de TI que ayuda a las compañías a aumentar las oportunidades del mañana, promoviendo que cosas sorprendentes pueden pasar, cuando se conecta lo previamente desconectado.

Cisco Global Services Center congrega las áreas de *Global Technical Center*, *Latin America Technical Assistance Center, Global Delivery Center* and *Cisco Solution Support.* El centro brinda apoyo a los clientes de Cisco a nivel mundial.

El GSC equipado con tecnología de punta, está basado al sur de la ciudad de México en la avenida Insurgentes Sur y ocupa más de 9,200 m2. El lugar cuenta con 138 salas de juntas, para trabajo individual y de privacidad para tomar llamadas telefónicas. Veintidós salas cuentan con la generación más reciente de sistemas de Cisco TelePresencencia. El GSC lo conforman cerca de 400 empleados.

Cisco Solution Support es el servicio premier que Cisco ofrece a sus clientes a nivel mundial. Incluye soporte de múltiples proveedores y soporte de productos de Cisco de amplia cobertura, para resolver problemas complejos con un promedio de solución de 41% más rápido que el soporte especializado en un solo producto. La cobertura abarca diferentes soluciones tales como Colaboración, Centro de datos, Soluciones digitales, Internet de las cosas, *Networking*, Seguridad y Proveedor de servicios.

En México, *Cisco Solution Support* está enfocado en las nuevas soluciones de Centro de Datos tales como Infraestructura centralizada en aplicaciones (ACI, por sus siglas en ingles), *Cloud Center, iWAN, Tetration* e Internet de las cosas.

Departamento

ACI Solutions Delivery – Mexico

ACI es una arquitectura integral con automatización centralizada y perfiles de aplicaciones basados en políticas. ACI ofrece flexibilidad de software con la escalabilidad del rendimiento de hardware.
Cisco ACI está compuesta por:

- Los nuevos *switches Nexus* de Cisco de la serie 9000.
- Gestión centralizada de políticas y *Cisco Application Policy Infrastructure Controller* (APIC).

- Un *switch* virtual de aplicaciones (*Application Virtual Switch* o AVS) de Cisco para el perímetro de la red virtual.
- Innovaciones de software y hardware.
- Infraestructura física y virtual integradas.
- Un ecosistema abierto de proveedores de red, almacenamiento, gestión y organización.

Las características fundamentales de ACI incluyen:

- Automatización simplificada mediante un modelo de políticas basado en aplicaciones.
- Visibilidad centralizada con supervisión del rendimiento de las aplicaciones en tiempo real.
- Flexibilidad de software abierto para la integración de los equipos *DevOps* y los compañeros del ecosistema.
- Rendimiento escalable y capacidad para varios arrendatarios incorporados en el hardware.

El futuro de las redes con ACI tiene que ver con proporcionar una red que se pueda implementar, supervisar y gestionar de una forma que admita *DevOps* y rápidos cambios de aplicaciones. ACI lo hace mediante la reducción de la complejidad y un marco común de políticas que permite automatizar el aprovisionamiento y la gestión de recursos.

Un equipo con sede en la Ciudad de México, confirmado por 5 ingenieros de soporte y un líder técnico, que trabajan en conjunto con 2 equipos con sede en Carolina del Norte y California *US*, para dar soporte a los clientes a nivel mundial que están en proceso de implementación o que ya han implementado la solución de ACI en sus centros de datos.

Descripción técnica de actividades asociadas al puesto

- *Resolución de casos.* Actividad principal de un ingeniero de soporte. Consiste en la detección, análisis y solución de problemas presentados en centros de datos que tienen implementada la solución de ACI.
- *Diseño, planeación e implementación de un laboratorio de ACI en la ciudad de México.* En muchas ocasiones durante el proceso de solución de un caso, es necesario replicar el problema del cliente en un ambiente similar, para poder analizar y realizar pruebas sin afectar la red de producción. Es por ello, que surge la necesidad de tener un laboratorio local para el uso de los ingenieros en México, donde puedan realizar pruebas, verificar defectos, estudiar y recrear configuraciones.
- *Creación de documentos técnicos.* ACI es una solución que lleva alrededor de 3 años en el mercado, por lo tanto, no hay gran cantidad de documentación, como son guías de configuración, análisis de problemas, solución de defectos, integración de ACI con otras tecnologías, compatibilidad de servicios e infraestructura, diseño e implementación de servicios, etc. Es por eso que los ingenieros de soporte realizan la constante labor de escribir artículos, los cuales al principio son de uso interno para el resto de los ingenieros de cisco, pero pueden ser revisados y aprobados por expertos para que estos documentos sean públicos y compartidos con los clientes.
- Detección de defectos: ACI al ser una solución de hardware y software está expuesta a diferentes defectos, tanto en diseño como en funcionamiento. Los ingenieros de

soporte trabajan en la detección, solución y documentación de dichos defectos. Esto con el fin de que los desarrolladores de hardware y software arreglen el defecto, por medio de actualizaciones de hardware y software.

- Realización de Scripts: Programación de Scripts para facilitar el análisis de *logs* o registros, detección de problemas y optimización de configuración. El software de los dispositivos que integran ACI está desarrollado en Linux, para detectar la causa raíz de algún problema, es necesario analizar los log, esta tarea puede resultar muy difícil y prolongada. Para optimizar el proceso de análisis los ingenieros realizan Scripts que realizan análisis específicos en los equipos para poder detectar o descartar problemas. Los scripts también son utilizados para optimizar tareas de configuración, en ocasiones los clientes requieren de un Script que les permita configurar algún servicio en su centro de datos de manera sistematizada y eficiente.
- Reclutamiento de ingenieros: Planeación e implementación de estrategias de reclutamiento. El volumen de casos que los clientes abren en *Solution Support*, aumenta constantemente, lo cual impacta en la cantidad de casos asignados a cada ingeniero. Surge la necesidad de crear un plan de reclutamiento de ingenieros que estén a punto de terminar la universidad o recién egresados, los cuáles serán formados técnica y profesionalmente por los ingenieros más experimentados de cada equipo. Para posteriormente ser integrados a los equipos de trabajo y con esto brindar un mejor servicio a los clientes.

Relación de proyectos en los que se ha participado

- POD de ACI en CALO México

  Laboratorio de operaciones avanzadas de Cisco (CALO) en México es parte de la red mundial de laboratorios que pueden ser accedidos en el lugar y de manera remota por los ingenieros de Cisco para resolver los temas más complejos que puedan plantear los clientes. Los laboratorios pueden ayudar a recrear ambientes para probar configuraciones y diseñar previamente a la implementación.

  Para el equipo de ACI México se implementaron 2 *PODs* de ACI en el laboratorio de CALO. Cada POD está conformado por la siguiente infraestructura 2 *Nexus* 9500, 4 *Nexus* 9300, 3 APIC's, 2 *Nexus* 3000, 3 centros de virtualización UCS c220, 2 *Nexus* 2000, 2 *routers* 2900 y 1 *switch* 3750.

  La implementación incluyó la creación de la orden de compra de los dispositivos, a través de la plataforma de CALO; diseño de la topología, instalación de la infraestructura, cableado, configuración e integración de los dispositivos.

  Se realizó una wiki con la información de conectividad y direccionamiento IP de los PODs, con el fin de tener una plataforma de uso interno, como referencia y facilitar la recreación de problemas específicos.

  El uso del laboratorio no solo se limita a los ingenieros locales, también está disponible para los equipos de Sídney, Bruselas, RTP y San José en caso de ser requerido.

Grado de participación: Alto.

- Programa de incubación de ingenieros para *Solution Support*.

  Proyecto enfocado en visitar diferentes universidades del país, con el fin de encontrar candidatos para el programa de incubación. El programa consiste en dar una conferencia en las universidades a estudiantes que estén a punto de terminar la universidad, o recién egresados, que tengan un perfil enfocado a redes informáticas y que tengan el interés de trabajar en Cisco *Solution Support*. Los candidatos seleccionados, son entrenados por los ingenieros de *Solution Support*, tanto técnica como emocionalmente, con el fin de que en un futuro se integren a los diferentes equipos, apoyando en la resolución de casos.

  Grado de participación: Alto.

Proyecto principal

Cisco *Solution Support* México

1 Introducción

Para Cisco, México forma parte fundamental en su estrategia de negocios. La creación de un equipo de soporte de soluciones es un proyecto enfocado en ofrecer a sus clientes, principalmente en el continente americano, un servicio de soporte premier. El soporte en español e incluso portugués, es un servicio extra que Cisco ofrece a sus clientes de Latinoamérica.

Desarrollar técnica y emocionalmente ingenieros bilingües o trilingües que soporten las nuevas soluciones de cisco, es parte fundamental para que los clientes de Latinoamérica adopten las nuevas soluciones en sus redes y sientan la seguridad de que un soporte de excelencia está para solucionar sus problemas.

2 Justificación

Existen diferentes equipos de *Solution Support* para ACI alrededor del mundo. El soporte que se da a los clientes es en el idioma inglés, pero Cisco busca posicionar las nuevas soluciones dentro del mercado latinoamericano. Para lograrlo, Cisco busca ofrecer soporte técnico en el idioma local a sus clientes, principalmente en el idioma español.

En un principio, el equipo de ACI en México, trabaja en conjunto con el equipo de RTP, carolina del norte y San José, California, atendiendo principalmente clientes de Estados Unidos, Canadá y Europa. Pero en el futuro el enfoque será el soporte a clientes de Latinoamérica, ya que el número de clientes que están comprando las nuevas soluciones de Cisco está aumentando de manera muy positiva.

3 Objetivo general

Conformar un equipo en ingenieros con los conocimientos técnicos y emocionales para dar soporte premier a clientes de Cisco que están en proceso de adopción, o que ya han implementado la solución de ACI en sus centros de datos.

4 Objetivos específicos

- Desarrollar en los ingenieros el conocimiento técnico en ACI, *Nexus* 9000, centro de datos, *networking*, sistemas operativos, programación, virtualización, seguridad en sistemas de la información.
- Desarrollar en los ingenieros las habilidades emocionales, para manejar adecuadamente, las diferentes situaciones que se presentan a la hora de resolver los problemas de los clientes como lo son empatía, seguridad, inspirar confianza, trabajo bajo presión, etc.
- Solucionar problemas de clientes que utilizan la tecnología de ACI.
- Posicionar a Latinoamérica como una región en donde Cisco puede tener la seguridad de que sus ingenieros de soporte cuentan con las mismas o mejores capacidades que los ingenieros de soporte de otras partes del mundo.

5 Descripción Técnica

Para la resolución de casos, los ingenieros de *Solution Support* siguen diferentes procesos que sirven de referencia para realizar de manera óptima el análisis de problemas, documentación y resolución. Por cuestiones de privacidad de la empresa no es posible especificar de manera profunda cada uno de los procesos a seguir por los ingenieros.

A continuación, se presenta en términos generales el proceso para la resolución de casos, sin embargo, este flujo no es estrictamente aplicado para cada caso, ya que la solución del mismo puede variar en el orden de los pasos, complejidad, tiempo y severidad:

1. Cliente abre un caso en la plataforma *CSone*, en donde brinda una breve explicación del problema a resolver, el análisis previo del mismo y asigna una severidad al caso, entre 1 y 4. En donde severidad 1 implica que el cliente está teniendo una alta afectación en su servicio, por lo tanto, el ingeniero debe de dar prioridad a resolver ese problema. Severidad 2 implica que el cliente tiene afectación media – alta. Severidad 3 implica que afectación media. Severidad 4 implica que no hay afectación, por lo generar este tipo de casos son abiertos para hacer preguntas o pedir documentación.
2. Ingeniero de soporte acepta el caso, y contacta al cliente por medio de teléfono o correo electrónico, proporcionando la información de contacto.
3. Inicia el proceso de análisis del problema, en donde el ingeniero de soporte solicita información más específica del problema, en base a esto, decide si necesita acceso remoto a los equipos del cliente a través de las herramientas de cisco *WebEx*, para poder analizar y solucionar el problema de manera más eficiente.
4. Dependiendo del problema, los ingenieros de soporte, se apoyan de documentación interna o externa de cisco. Esta documentación se encuentra en la plataforma de *TechZone* o en la página oficial de cisco.
5. Si es requerido el ingeniero de soporte escribe un artículo en donde explica la solución o los pasos a seguir para resolver cierto problema.
6. Si detecta un comportamiento no esperado en la red del cliente, el ingeniero de soporte se apoya del sistema CDTES, para abrir un nuevo defecto, o determinar si un

defecto ya identificado está afectando la red del cliente.

7. Los ingenieros de soporte también se apoyan de la documentación de casos previos, en donde otros ingenieros ya han trabajado en problemas similares y han encontrado la solución. Para facilitar la búsqueda de artículos, defectos y casos, los ingenieros de soportes utilizan el buscador *Topic*.
8. Aplicación de la solución del problema.
9. Los ingenieros de soporte documentan cada uno de los pasos anteriores dentro de las notas del caso, para seguimiento del cliente y futuras referencias.
10. Cierre de caso, en donde se hace un resumen del caso. Descripción de problema, síntomas, análisis hecho, y la solución aplicada.

Existen otros procesos, como escalación de casos, colaboraciones con otras tecnologías, y transferencia de casos, pero no se va a profundizar en ello dentro de este documento.

5.1 CSone

Plataforma web que utilizan tanto clientes como ingenieros para dar seguimiento a cada uno de los casos. Cada caso tiene un único ID, contiene la información del cliente, contacto, número de contrato, nivel de servicio, ingeniero propietario del caso y la documentación de todo el análisis como lo es: descripción del problema, situaciones apreciadas, impacto que provoca el problema, comunicación entre cliente – ingeniero, planes de acción, solución, etc. desde que cliente abre el caso hasta que el ingeniero de cisco provee la solución y cierra el mismo. Además, *CSone* es una base de datos en donde se almacenan todos los casos resueltos y los que se mantienen abiertos. Estos casos pueden ser consultados tanto por ingenieros de Cisco como clientes.

5.2 TechZone o zona técnica

Plataforma web que utilizan los ingenieros de soporte de cisco (todas las tecnologías), en donde se publican artículos de diferente índole, como puedes ser: guías de configuración, guías de análisis de problemas, explicación de algún tema en específico, publicación de preguntas y respuestas, etc. Todos los artículos comienzan siendo exclusivamente para uso interno de los ingenieros de cisco. Pero muchos de estos artículos, son muy útiles no solo para los ingenieros de Cisco, sino para los clientes, por lo tanto, estos artículos son revisados, aprobados y corregidos por expertos, para que después puedan ser publicados en la documentación oficial y publica de Cisco.

5.3 CDTES

Es el sistema de seguimiento de errores para todos los de Cisco. Es utilizado por más de 20.000 empleados de Cisco en todas las fases de desarrollo de productos, ventas y soporte, y en todas las áreas tecnológicas. CDETS se utiliza para los productos de software y hardware, así como para las herramientas internas e incluso la documentación. Esencialmente, si se trata de un

error, se realiza un seguimiento a través de CDETS. Incluso los errores en CDETS (así como otras herramientas) se rastrean a través de CDETS. CDETS también impone el ciclo de vida y las reglas de negocio en las prácticas de desarrollo.

Este sistema permite a los ingenieros de soporte documentar defectos detectados tanto en hardware como software de los dispositivos de cisco. Los desarrolladores lo utilizan para analizar los síntomas y características del defecto, el cual después es solucionado en futuras actualizaciones, si es posible. Los clientes lo utilizan como referencia para saber que defectos fueron detectados en cada una de las versiones de hardware o software, detectar la versión arreglada, o la solución del defecto.

5.4 Topic

Es un buscador interno de Cisco, muy utilizado por los ingenieros de soporte, para poder encontrar de manera rápida y optima, artículos de *TechZone*, defectos, casos, grupos de discusión, e hilos de correos electrónicos. Esta herramienta es de gran utilidad ya que, en una sola plataforma se realiza la búsqueda de toda la documentación interna de cisco, la cual puede ser utilizada para resolver los problemas de los clientes.

5.5 RMA (Autorización de Regreso de Material)

Es una plataforma web, en donde los ingenieros de soporte, crean ordenes de remplazo de hardware que son enviados a los clientes cuando algún dispositivo presenta un problema físico y para su solución es necesario remplazar algún componente del chasis, o incluso el chasis completo.

5.6 NPS

En *Solution Support* existe una forma de evaluar la calidad de servicio que los ingenieros de soporte brindan a los clientes.

Net Promoter Score (NPS): es una encuesta que realiza de manera aleatoria a los clientes, después de que se resolvió su problema. Son 10 preguntas donde el cliente comparte la experiencia que tuvo trabajando con *Solution Support,* y si recomendaría Cisco a sus colegas con una escala de 1 – 10, donde 1 – 6 no lo recomiendo, 7-8 no seguro de recomendar, 9 - 10 si recomiendo. El objetivo general de *Solution Support* en esta encuesta es 6.5 en la escala de recomendación, actualmente Cisco *Solution Support* en México tiene un promedio de 7.9.

6 Descripción general de ACI

La Infraestructura centrada en aplicaciones (ACI) de Cisco es una arquitectura innovadora que simplifica, optimiza y acelera radicalmente todo el ciclo de vida de implementación de la aplicación.

Cisco ACI utiliza un enfoque integral basado en sistemas, con estrecha integración entre elementos físicos y virtuales, un modelo de ecosistema abierto y circuitos integrados para aplicaciones específicas (ASIC) de expansión de innovación, hardware y software. Este enfoque único utiliza un modelo operativo común basado en políticas en la red apta para ACI y elementos de seguridad (computación, almacenamiento en el futuro), lo que supera los silos de TI y reduce significativamente los costos y la complejidad.

Cisco ACI redefine la potencia de la TI, lo que hace que sea más sensible a las necesidades cambiantes de las empresas y aplicaciones, y mejora la agilidad y agrega valor comercial.

6.1 ACI: Aborda el panorama cambiante

Los cambios en la industria están redefiniendo la tecnología de la información (TI) en todos los niveles. Los modelos de consumo de TI están cambiando a servicios basados en la nube. La TI como servicio (ITaaS) está dando paso a las aplicaciones como servicio. El desarrollo y las operaciones, anteriormente separados, avanzan hacia su integración (DevOps). Los modelos de administración centrada en dispositivos están migrando a administración centrada en aplicaciones.

El dinamismo empresarial requiere dinamismo de aplicaciones, por lo que los equipos de TI deben aprovisionar aplicaciones en horas en vez de meses. Los recursos deben poder ampliarse y reducirse en minutos, no en horas.

Las estrategias tradicionales utilizan un enfoque operativo fragmentado, sin un modelo operativo común entre los equipos de aplicaciones, redes y la nube. Un modelo operativo común ofrece agilidad de aplicaciones, operaciones simplificadas, rendimiento garantizado y escala.

Las aplicaciones en la nube, de movilidad y datos masivos están generando un cambio en el modelo de centro de datos. Las nuevas aplicaciones generan nuevos tipos de demandas en la infraestructura. Las aplicaciones distribuidas (por ejemplo, datos masivos); las aplicaciones de bases de datos (como las de Oracle y SAP) que se ejecutan en aplicaciones virtualizadas, instaladas directamente en el hardware, y funcionan en entornos de múltiples hipervisores; y las aplicaciones basadas en la nube que están disponibles a pedido, imponen distintas demandas sobre la infraestructura. Estas demandas se describen brevemente a continuación:

- La infraestructura debe reconocer las aplicaciones y ser más ágil para respaldar tanto la creación de instancias como la eliminación de aplicaciones dinámicas.
- La naturaleza no virtual de las nuevas aplicaciones emergentes implica que la

infraestructura deba respaldar la integración física, virtual y en la nube con visibilidad Completa.

- Las aplicaciones independientes de la infraestructura tratan al centro de datos como un grupo dinámico de recursos compartidos.
- Los modelos de ampliación promueven más tráfico de este a oeste, con la necesidad de mayor rendimiento y escalabilidad de la red.
- Los modelos de múltiples nubes requieren que la infraestructura sea segura y sensible a diversos clientes.

Estos cambios aumentan la complejidad operativa y limitan el dinamismo y la capacidad de respuesta de la empresa. Cisco ACI brinda un centro de datos ágil con operaciones simplificadas y mayor capacidad de respuesta de la aplicación para brindar soporte a una nueva generación de aplicaciones distribuidas mientras tiene en cuenta los entornos virtualizados y no virtualizados existentes.

6.2 La solución: Un enfoque centrado en aplicaciones para administrar su infraestructura

Infraestructura centrada en aplicaciones (ACI) es una arquitectura integral con automatización centralizada y perfiles de aplicaciones basados en políticas centralizados. ACI ofrece flexibilidad de software con la capacidad de escala del rendimiento de hardware.

Cisco ACI está compuesta por:

- Los nuevos *Switches* Cisco *Nexus* de la serie 9000.
- Administración centralizada de políticas y Controlador de infraestructura de políticas de aplicaciones (APIC) de Cisco.
- Un *switch* virtual de aplicaciones (AVS) de Cisco para el perímetro de la red virtual
- Innovaciones de software y hardware.
- Infraestructura física y virtual integradas.
- Un ecosistema abierto de proveedores de red, almacenamiento, administración y organización.

Las características fundamentales de ACI incluyen:

- Automatización simplificada mediante un modelo de políticas basado en aplicaciones.
- Visibilidad centralizada con supervisión del rendimiento de aplicaciones en tiempo real.
- Flexibilidad de software abierto para la integración de los equipos *DevOps* y los *partners* del ecosistema.
- Rendimiento escalable y capacidad de múltiples clientes incorporados en el hardware.

El futuro de las redes con ACI tiene que ver con proporcionar una red que se pueda implementar, supervisar y administrar de una forma que admita *DevOps* y rápidos cambios de

aplicaciones. ACI lo hace mediante la reducción de la complejidad y un marco común de políticas que permite automatizar el aprovisionamiento y la administración de recursos.

Cisco ACI brinda un modelo operativo transformacional para las aplicaciones en la nube y el centro de datos de próxima generación.

En el marco de Cisco ACI, las aplicaciones guían el comportamiento de las redes, no a la inversa. Las descripciones y los requisitos predefinidos de las aplicaciones (perfiles de políticas) automatizan el aprovisionamiento de la red, los servicios de aplicación, las políticas de seguridad, las subredes de clientes y la ubicación de cargas de trabajo.

Como automatiza el aprovisionamiento de toda la red de la aplicación, Cisco ACI permite disminuir los costos de TI, reducir errores, acelerar la implementación y agilizar más el negocio.

El nuevo modelo de Cisco ACI utiliza un enfoque basado en la estructura diseñado para respaldar las demandas emergentes de la industria y mantener un camino de migración para arquitecturas ya vigentes. Este enfoque permite a las aplicaciones empresariales tradicionales y a las aplicaciones desarrolladas internamente ejecutarse en forma paralela en una infraestructura de red diseñada para brindarles soporte de manera dinámica y escalable. Las políticas de red y las topologías lógicas, que tradicionalmente establecían el diseño de las aplicaciones, se aplican, en cambio, según las necesidades de aplicaciones. La estructura está diseñada para respaldar la migración a la automatización de administración, la política definida mediante programación y las cargas de trabajo dinámicas en cualquier dispositivo, en cualquier lugar. Cisco ACI logra este objetivo con una combinación de hardware y software en estrecha colaboración para brindar ventajas que no son posibles en otros modelos (Figura 1).

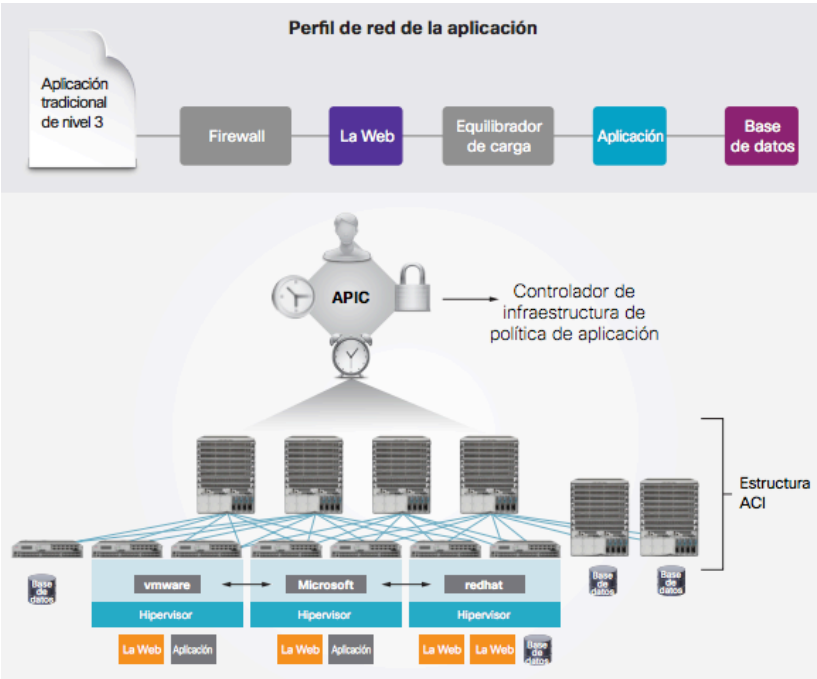

Figura 1. Cisco ACI: Controlador de infraestructura de política de aplicación de Cisco, perfil de red de la aplicación y estructura que respalda Cisco ACI.

6.3 Principales componentes de Cisco ACI

Controlador de infraestructura de política de aplicación de Cisco

El Controlador de infraestructura de política de aplicación (APIC) de Cisco es el principal componente arquitectónico de la solución ACI de Cisco. Es el punto unificado de automatización y administración para la estructura de Cisco ACI, la aplicación de políticas y la supervisión de estado. El APIC de Cisco es un controlador agrupado centralizado que optimiza el rendimiento, brinda soporte a cualquier aplicación en cualquier lugar, y unifica la operación de entornos físicos y virtuales. El controlador administra y opera una estructura de Cisco ACI escalable, de diversos clientes.

El APIC de Cisco es responsable de tareas como la activación de la estructura, el mantenimiento del firmware del *switch* y la configuración y la creación de instancias de políticas de red. El APIC de Cisco se elimina por completo de la ruta de datos. Esto significa que la estructura aún puede enviar tráfico cuando se pierde comunicación con el APIC.

El APIC propiamente dicho se proporciona como un dispositivo y, por lo general, se ejecutará como tres o más dispositivos para rendimiento y disponibilidad. El APIC de Cisco está diseñado sobre la base de la programabilidad y la administración centralizada. El APIC de Cisco expone una API ascendente a través de XML y JSON, y brinda una interfaz de línea de comandos (CLI) y una GUI que utilizan esta API para administrar la estructura. El sistema también proporciona una API descendente de código abierto que permite que los proveedores de servicios de red de terceros implementen el control de políticas de los dispositivos proporcionados a través del APIC de Cisco.

Perfiles de redes de aplicaciones

Un perfil de red de la aplicación dentro de la estructura es una recopilación de grupos de terminales (una agrupación lógica de terminales similares que representa un nivel de aplicación o conjunto de servicios que requieren una política similar), sus conexiones y las políticas que definen esas conexiones. El perfil de red de la aplicación es la representación lógica de todos los componentes de la aplicación y sus interdependencias en la estructura de la aplicación.

Los perfiles de redes de aplicaciones están diseñados para modelarse de una forma lógica que coincida con la manera en que se diseñan y se implementan dichas aplicaciones. A continuación, el sistema maneja la configuración y aplicación de políticas y la conectividad a través del APIC de Cisco en lugar de un administrador.

6.4 Beneficios

Cisco ACI ayuda a disolver los silos de TI en cuanto a implementación de aplicaciones, seguridad, servicios de red y personal de configuración de red, ya que les permite colaborar a través de una plataforma común. Los principales beneficios incluyen:

- Velocidad de la aplicación: cualquier aplicación, en cualquier lugar.
- Arquitectura de servicios que permite una visión integral de las aplicaciones, con visibilidad integrada y centralizada a nivel de la aplicación, y supervisión en tiempo real del estado de la aplicación en entornos físicos y virtuales.
- Plataforma común para administrar entornos físicos, virtuales y basados en la nube.
- Entorno seguro de diversos clientes con control detallado para aplicaciones y clientes.
- Rendimiento escalable que combina la flexibilidad del software y el rendimiento del hardware.
- Rendimiento superior de la aplicación, que mejora el tiempo de finalización del flujo de la aplicación hasta un 80 %.
- Simplicidad operativa, con modelos comunes de políticas, administración y operación en los recursos de aplicación, red y seguridad (y los recursos de computación y almacenamiento en el futuro).
- Las API abiertas, los estándares abiertos y los elementos de código abierto permiten la flexibilidad del software para los equipos de desarrollo y operaciones (DevOps), y la integración del socio en el ecosistema.

7 Fundamentos de ACI

A continuación, se presentan los fundamentos esenciales para el entendimiento de la solución ACI de Cisco.

7.1 Acerca de la infraestructura centralizada en aplicaciones de Cisco

ACI permite requerimientos de aplicaciones para definir la red. Esta arquitectura simplifica, optimiza, y acelera el ciclo de vida del despliegue de las aplicaciones.

7.2 Acerca del Controlador de Aplicaciones de la infraestructura de aplicaciones de Cisco

El Controlador de Aplicaciones de la infraestructura de aplicaciones (APIC por sus siglas en ingles) permite a las aplicaciones conectarse directamente con un conjunto de recursos, seguros y compartidos de alto rendimiento; que incluye capacidades de red, de cálculo y de almacenamiento. La siguiente figura proporciona un
a visión general del APIC.

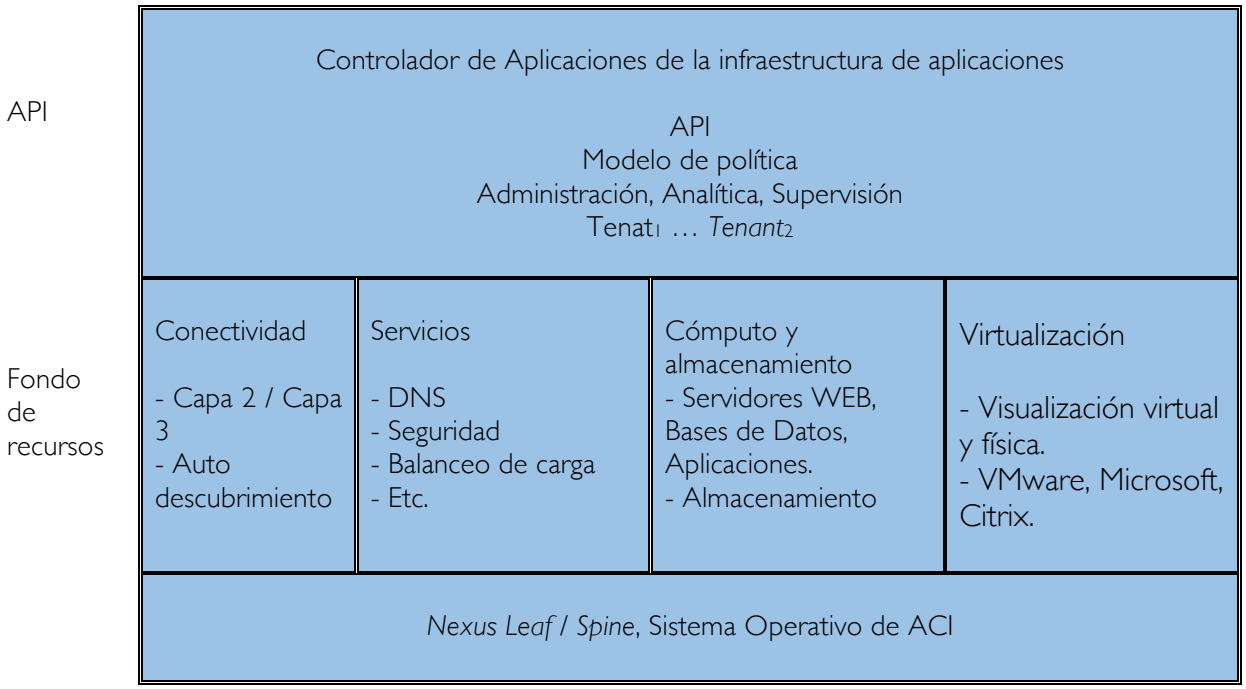

Figura 2. Visión general del APIC.

El APIC proporciona un punto unificado de automatización y administración, programación de políticas, implementación de aplicaciones y monitoreo de la salud para el *fabric* (nombre que

recibe la infraestructura de ACI). El APIC, que se implementa como un controlador de clúster sincronizado a través de réplicas, optimiza el rendimiento, admite cualquier aplicación en cualquier lugar y proporciona una operación unificada de la infraestructura física y virtual. El APIC permite a los administradores de red, definir fácilmente la red óptima para las aplicaciones. Los operadores de centros de datos pueden ver claramente cómo las aplicaciones consumen recursos de red, aíslan fácilmente y solucionan problemas de aplicaciones y de infraestructura, supervisan y perfilan los patrones de uso de recursos.

7.3 Acerca del fabric de la infraestructura centralizada en aplicaciones

El *fabric* de ACI incluye *switches* Cisco *Nexus* serie 9000 con el APIC para funcionar como *leaf*s y *spines* en modo ACI. Estos *switches* forman una red de "árbol" conectando cada nodo *leaf* con cada nodo *spine*; todos los demás dispositivos se conectan a los nodos *leaf*. El APIC administra el *fabric* de ACI. La configuración mínima recomendada para el APIC es un clúster de tres hosts replicados. Las funciones de gestión del *fabric* del APIC no funcionan en la ruta de datos del *fabric*. La figura siguiente muestra una vista general del *fabric* ACI *leaf* / spine.

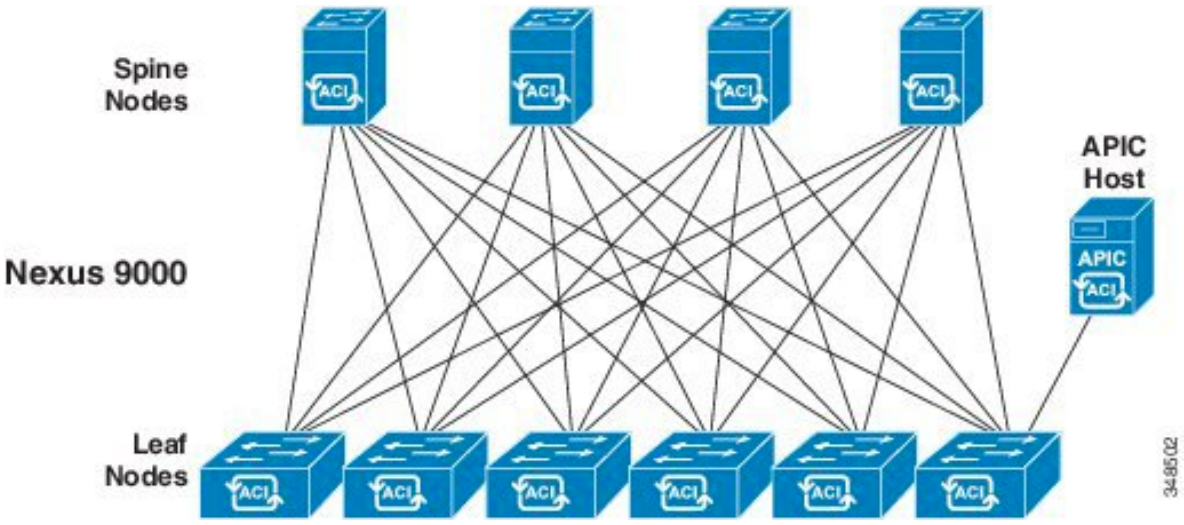

Figura 3. Visión general del *fabric* de ACI.

El *fabric* de ACI proporciona un reenvío consistente de baja latencia a través de enlaces de alto ancho de banda (40 Gbps, con una capacidad futura de 100 Gbps). El tráfico con el origen y el destino en el mismo *switch leaf* se maneja localmente, y todo el otro tráfico viaja desde el *leaf* de entrada hasta el *leaf* de salida a través de un *spine switch*. Aunque esta arquitectura aparece como dos saltos desde una perspectiva física, en realidad es un único salto de capa 3, porque el *fabric* funciona como un solo *switch* de capa 3.

El sistema operativo (OS) orientado a objetos de ACI se ejecuta en cada nodo de la serie Cisco *Nexus* 900. Permite la programación de objetos para cada elemento configurable del sistema.

El sistema operativo del *Fabric* de ACI de ACI transforma las políticas del APIC en un modelo concreto que se ejecuta en la infraestructura física. El modelo concreto es análogo al software compilado; Es la forma del modelo que el sistema operativo del *switch* puede ejecutar. La siguiente figura muestra la relación del modelo lógico con el modelo concreto y el sistema operativo del *switch*.

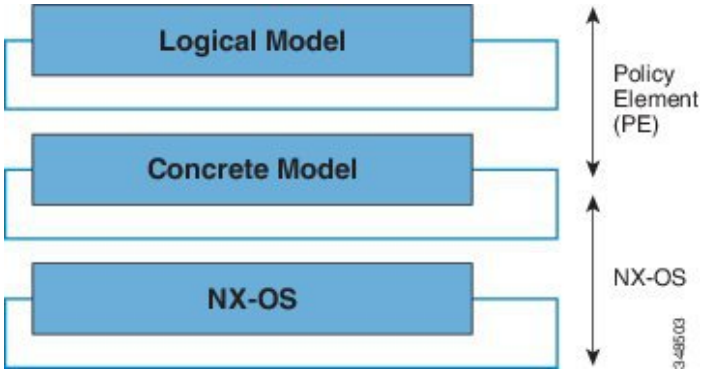

Figura 4. Modelo lógico transformado a modelo concreto

Todos los nodos *switch* contienen una copia completa del modelo concreto. Cuando un administrador crea una política en el APIC que representa una configuración, el APIC actualiza el modelo lógico. El APIC realiza entonces el paso intermedio de crear una política completamente elaborada que es empujada en todos los nodos *switch* donde se actualiza el modelo concreto.

El APIC es responsable de la activación del *fabric*, la gestión del firmware de los *switches*, la configuración de la política de red y la creación de instancias. Mientras que el APIC actúa como la política centralizada y el motor de gestión de red para el *fabric*, esta se elimina completamente de la ruta de datos, incluida la topología de reenvío. Por lo tanto, la tela todavía puede reenviar tráfico incluso cuando se pierde la comunicación con el APIC.

Los *switches* de la serie Cisco *Nexus* 9000 ofrecen configuraciones de módulos que soportan Ethernet de 1, 10 y 40 Gigabits que funcionan en cualquiera de los modos independientes de Cisco NX-OS o en modo ACI para aprovechar al máximo los servicios de APIC basados en las políticas de aplicación y las características de automatización de la infraestructura.

***Nota**: Los switches de la serie Cisco Nexus 9000 sólo pueden ejecutar el modelo concreto. Cada switch tiene una copia del modelo concreto. Si el APIC se desconecta, el fabric sigue funcionando, pero no se pueden realizar modificaciones en sus políticas.*

7.4 Determinando el comportamiento del Fabric

El *fabric* de ACI permite a los clientes automatizar y orquestar recursos escalables y de alto rendimiento de red, computación y almacenamiento para implementaciones en la nube. Los actores clave que definen cómo se comporta el *fabric* de ACI incluyen los siguientes:

Planificadores de TI, ingenieros de red e ingenieros de seguridad, los desarrolladores que acceden al sistema a través de las API de APIC, administradores de aplicaciones y de red.
La arquitectura *Representational State Transfer* (REST) es un método de desarrollo clave que soporta el *cloud computing*. El API de ACI está basado en REST. La *World Wide Web* representa la implementación más grande de un sistema que se ajusta al estilo arquitectónico REST.

El *cloud computing* difiere de la computación convencional en escala y enfoque. Los entornos convencionales incluyen requisitos de software y mantenimiento con sus conjuntos de habilidades asociadas que consumen sustanciales gastos operativos. Las aplicaciones en la nube utilizan diseños de sistemas que están soportados por una infraestructura de gran escala que se despliega a lo largo de una curva de costos que se reduce rápidamente. En este tipo de infraestructura, el administrador del sistema, los equipos de desarrollo y los profesionales de la red colaboran para proporcionar una contribución mayor valorada.

En los ajustes convencionales, el acceso a la red para recursos de cálculo y terminales se gestiona a través de LANs virtuales (VLAN) o capas sobrepuestas (*overlay*) rígidas, como MPLS (*Multiprotocol Label Switching),* que forzan el tráfico a través de servicios de red rígidamente definidos, como equilibradores de carga y firewalls. El APIC está diseñado para la programación y la gestión centralizada. Al abstraer la red, el *Fabric* ACI permite a los operadores suministrar dinámicamente recursos en la red en lugar de hacerlo de manera estática. El resultado es que el tiempo hasta el desarrollo (tiempo hasta el mercado) se puede reducir de meses o semanas a minutos. Los cambios en la configuración de *switches* virtuales o físicos, adaptadores, políticas y otros componentes de hardware y software pueden realizarse en minutos con llamadas API.

La transformación de las prácticas convencionales en métodos de *cloud computing* aumenta la demanda de servicios flexibles y escalables desde los centros de datos. Estos cambios exigen una gran reserva de personal altamente calificado que permita esta transformación. El APIC está diseñado para la programación y la gestión centralizada. Una característica clave de la APIC es la API web denominada REST. La APIC REST API acepta y devuelve mensajes HTTP o HTTPS que contienen documentos de *JavaScript Object Notation* (JSON) o *Extensible Markup Language* (XML). Hoy en día, muchos desarrolladores web utilizan métodos *RESTful*. La adopción de *APIs* web a través de la red permite a las empresas abrir y combinar fácilmente servicios con otros proveedores internos o externos. Este proceso transforma la red de una mezcla compleja de recursos estáticos a un intercambio dinámico de servicios que se ofrecen.

7.5 Acerca del Modelo de Política ACI

El modelo de política ACI permite especificar las políticas que las aplicaciones requieren. El APIC automáticamente crea las políticas en la infraestructura del *fabric*. Cuando un usuario o proceso inicia un cambio administrativo en un objeto del *fabric*, el APIC aplica primero ese

cambio al modelo de políticas. Este modelo de política activa un cambio en el manejo de *endpoints* (dispositivos finales).

7.6 Características clave del modelo de política

Las características clave del modelo de política son las siguientes:

- Como una arquitectura modelo-impulsado, el software mantiene una representación completa del estado administrativo y operativo del sistema (el modelo). El modelo se aplica de manera uniforme al *fabric*, los servicios, los comportamientos del sistema y los dispositivos físicos y virtuales conectados a la red.
- Los dominios lógico y concreto están separados; las configuraciones lógicas se transforman en configuraciones concretas aplicando las políticas en relación con los recursos físicos disponibles. No se realiza ninguna configuración con entidades concretas. Las entidades concretas se configuran implícitamente como un efecto secundario de los cambios en el modelo de política APIC. Las entidades concretas pueden ser, pero no tienen que ser, físicas (como una máquina virtual o una VLAN).
- El sistema prohíbe las comunicaciones con dispositivos recién conectados hasta que el modelo de políticas se actualice para incluir el nuevo dispositivo.
- Los administradores de red no configuran directamente los recursos del sistema lógico y físico, sino que definen configuraciones lógicas (independientes del hardware) y políticas en el APIC que controlan diferentes aspectos del comportamiento del sistema.

La manipulación de objetos administrados en el modelo libera a los ingenieros de la tarea de administrar configuraciones aisladas de componentes individuales. Estas características permiten la automatización y el aprovisionamiento flexible de la carga de trabajo, que puede localizar cualquier carga de trabajo en cualquier lugar de la infraestructura. Los servicios conectados a la red se pueden implementar fácilmente y el APIC proporciona un marco de automatización para administrar el ciclo de vida de los servicios conectados a la red.

7.7 Construcciones lógicas

El modelo de políticas administra todo el *fabric*, incluyendo la infraestructura, autenticación, seguridad, servicios, aplicaciones y diagnósticos. Las construcciones lógicas en el modelo de política definen cómo el *fabric* atiende las necesidades de cualquiera de sus funciones. La figura siguiente proporciona una visión general de las construcciones lógicas del modelo de políticas ACI.

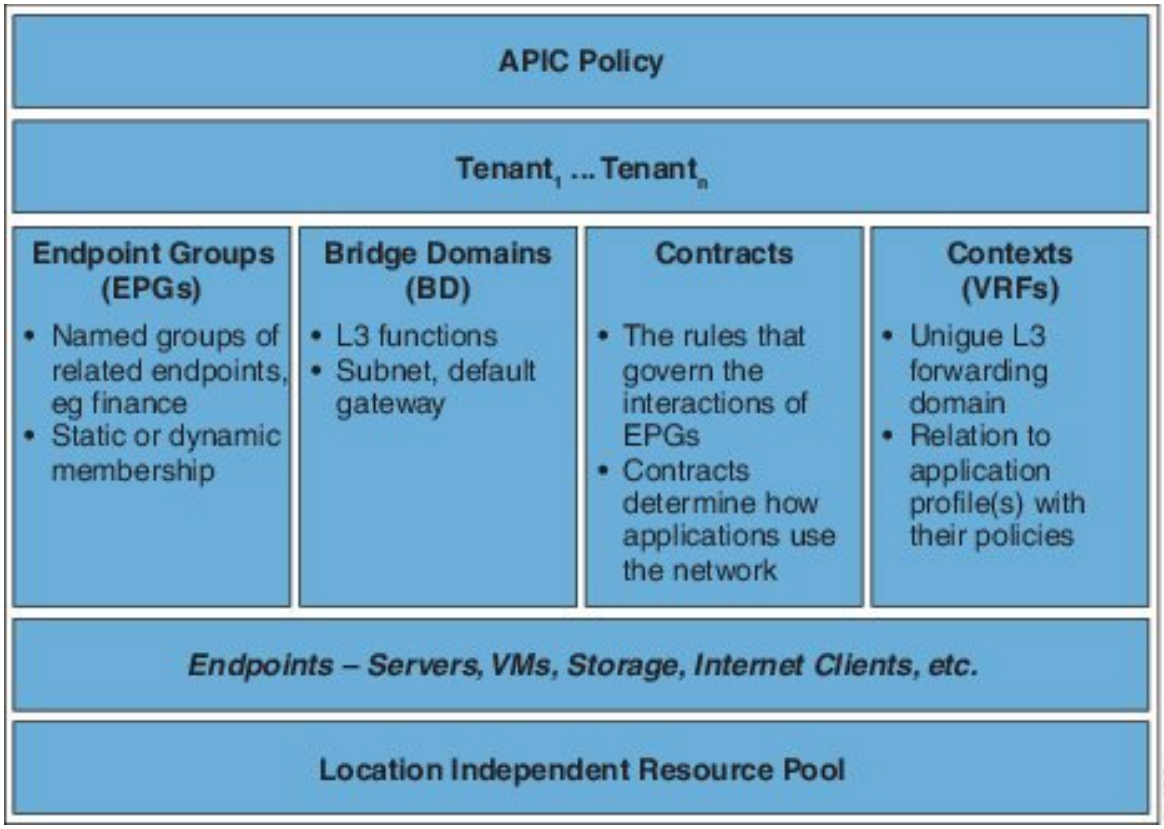

Figura 5. Acerca del modelo de construcciones logias en ACI

Los administradores *tenant*, crean políticas predefinidas que contienen aplicaciones o recursos compartidos. Estas políticas automatizan el aprovisionamiento de aplicaciones, servicios conectados a la red, políticas de seguridad y subredes de *tenant*, lo que coloca a los administradores en la posición de acercarse al grupo de recursos en términos de aplicaciones en lugar de bloques de construcción de infraestructura. La aplicación necesita manejar el comportamiento de la red, no al revés.

7.8 Tenant

Un *tenant* (fv*Tenant*) es un contenedor lógico para las políticas de aplicación que permiten al administrador ejercer control de acceso basado en el dominio. Un *tenant* representa una unidad de aislamiento desde una perspectiva de política, pero no representa una red privada. Los *tenant*s pueden representar a un cliente en una configuración de proveedor de servicios, una organización o dominio en una configuración empresarial o simplemente una agrupación conveniente de políticas. La siguiente figura proporciona una visión general de la porción de inquilino del árbol de información de administración.

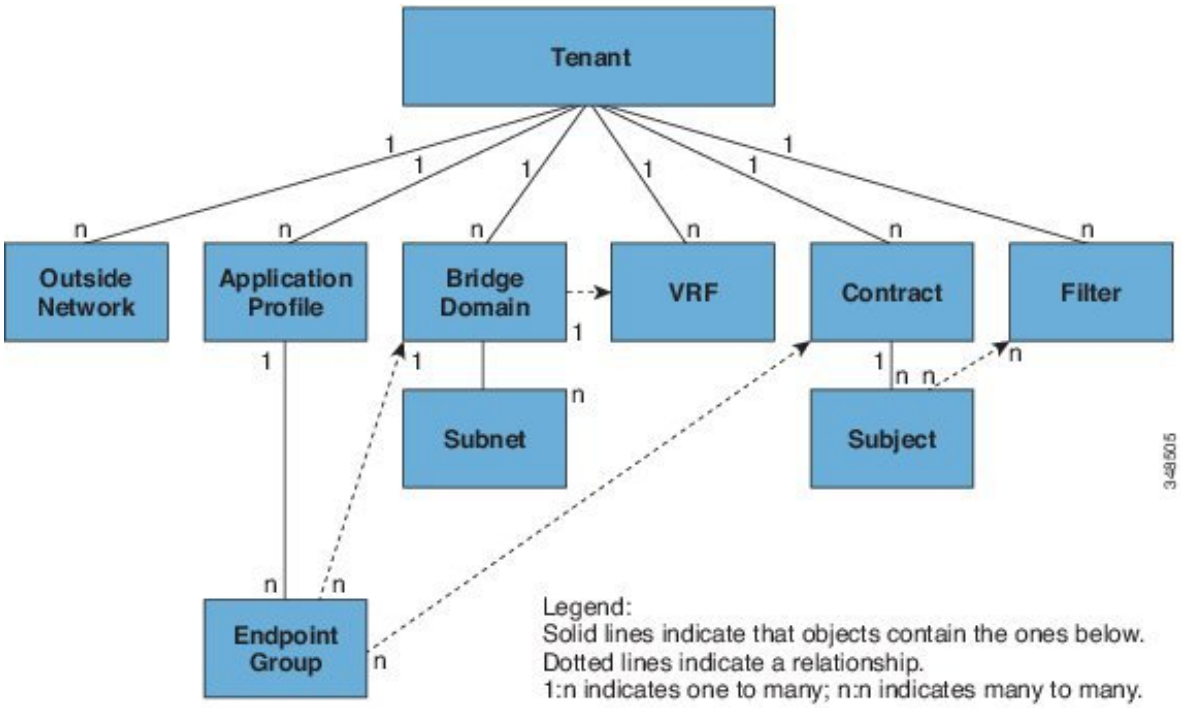

Figura 6. *Tenant.*

Los *tenants* pueden aislarse unos de otros o pueden compartir recursos. Los elementos principales que contiene el *tenant* son los filtros, los contratos, las redes externas, los *bridges domain (*BD), las instancias de enrutamiento y reenvío virtuales (VRF) y los perfiles de aplicación que contienen grupos de dispositivos finales (EPG). Las entidades del *tenant* heredan sus políticas. Los VRF también se conocen como contextos; Cada VRF puede asociarse con múltiples *bridges domains*.

Los *tenants* son contenedores lógicos para las políticas de aplicación. El *fabric* puede contener varios *tenants*. Debe configurar un *tenant* antes de poder implementar cualquier servicio de Capa 4 a Capa 7. El *fabric* de ACI admite configuraciones IPv4 e IPv6.

7.9 El modelo de información de gestión de políticas ACI de Cisco

El *fabric* comprende los componentes físicos y lógicos registrados en el Modelo de información de gestión (MIM), que puede representarse en un árbol de información de gestión jerárquica (MIT). El modelo de información es almacenado y administrado por procesos que se ejecutan en el APIC. Al igual que el Protocolo Común de Información de Gestión (CMIP) OSI y otras variantes X.500, el APIC permite el control de recursos gestionados presentando sus características manejables como propiedades de objeto que pueden ser heredadas de acuerdo con la ubicación del objeto dentro de la estructura jerárquica del MIT.

Cada nodo del árbol representa un objeto gestionado (MO) o grupo de objetos. MO son abstracciones de los recursos del *fabric*. Un MO puede representar un objeto concreto, como

un *switch*, adaptador o un objeto lógico, como un perfil de aplicación, un grupo de dispositivos finales o una falla. La siguiente figura proporciona una visión general del MIT.

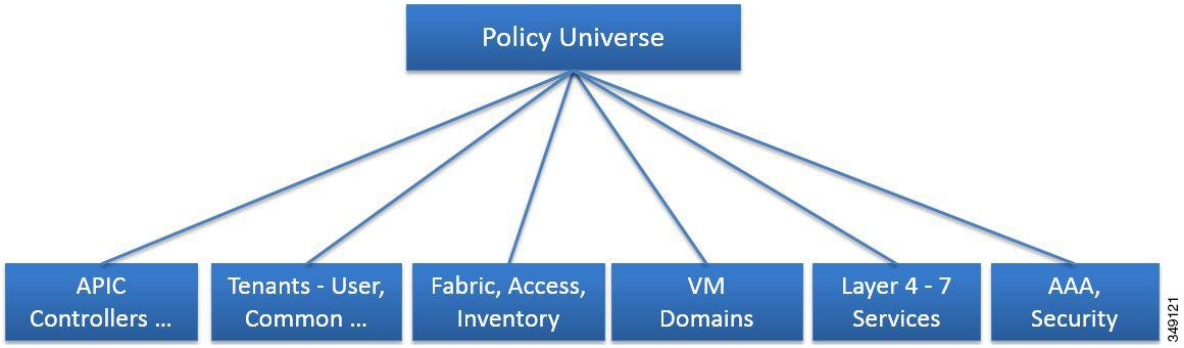

Figura 6. Cisco ACI modelo de información de gestión de políticas ACI de Cisco

La estructura jerárquica comienza con el universo de políticas en la parte superior (raíz) y contiene nodos padre e hijo. Cada nodo en el árbol es un MO y cada objeto en el tejido tiene un nombre distinguido único (DN) que describe el objeto y localiza su lugar en el árbol.
Los siguientes objetos administrados contienen las políticas que rigen el funcionamiento del sistema:

- Los controladores APIC comprenden un controlador de clúster sincronizado con replicas que proporciona administración, programación de políticas, despliegue de aplicaciones y supervisión de la integridad para el *fabric multitenant*.
- Un *tenant* es un contenedor para directivas que permiten a un administrador ejercer control de acceso basado en dominio. El sistema proporciona los siguientes tipos de t*enants*:
    - Los *tenats* de usuarios son definidos por el administrador de acuerdo con las necesidades de los usuarios. Contienen políticas que rigen el funcionamiento de recursos como aplicaciones, bases de datos, servidores web, almacenamiento conectado a la red, máquinas virtuales, etc.
    - El *tenant* común es proporcionado por el sistema, pero puede ser configurado por el administrador del *fabric*. Contiene políticas que rigen el funcionamiento de los recursos accesibles a todos los *tenant*, como Firewalls, balanceadores de carga, servicios de Capa 4 - Capa 7, dispositivos de detección de intrusiones, etc.
    - El *tenant* de la infraestructura es proporcionado por el sistema, pero puede ser configurado por el administrador del *fabric*. Contiene políticas que rigen el funcionamiento de los recursos de infraestructura, como la superposición de VXLAN. También permite que un proveedor de *fabric*s despliegue recursos selectivamente a uno o más *tenant*s de usuarios. Las políticas de *tenant* de infraestructura son configurables por el administrador del *fabric*.
    - El *tenant* de gestión es proporcionado por el sistema, pero puede ser configurado por el administrador del *fabric*. Contiene políticas que rigen el funcionamiento de las funciones de gestión del *fabric* utilizadas para la

configuración *in-band* y *out-of-band* de los nodos del *fabric*. El *tenant* de administración contiene un espacio de direcciones privado fuera de del camino de datos del *fabric*, para las comunicaciones internas de APIC / *Fabric*, que proporciona acceso a través del puerto de administración de los *switches*. El *tenant* de gestión permite la detección y automatización de comunicaciones con controladores de máquinas virtuales.

- Las políticas de acceso rigen la operación de los puertos de acceso del *switch* que proporcionan conectividad a recursos tales como almacenamiento, computación, conectividad de Capa 2 y Capa 3, hipervisores de máquinas virtuales, dispositivos de Capa 4 a Capa 7, etc. Si un *tenant* requiere configuraciones de interfaz distintas a las que se proporcionan en el vínculo predeterminado, el Protocolo de detección de vínculos (LLDP), el Protocolo de control de agregación de vínculos (LACP) o el *Spanning Tree*, un administrador debe configurar políticas de acceso para habilitar tales configuraciones en los puertos de acceso de los *switch leaf*.
- Las políticas del *fabric* gobiernan la operación de los puertos de los *switches* del *fabric*, incluyendo funciones como la sincronización del servidor del protocolo de la hora de la red (NTP), protocolo intermedio del sistema a intermedio del sistema (IS-IS), reflectores de la ruta del protocolo de la frontera del paso (BGP), Domino de Nombres del Sistema (DNS) etc. El tejido MO contiene objetos tales como fuentes de alimentación, ventiladores, chasis, etc.
- Dominios de controladores de máquinas virtuales (VM), con requisitos de directiva de red similares. Los controladores de VM pueden compartir espacio de la red VLAN o *Virtual Extensible Local Area Network* (VXLAN) y grupos dispositivos finales (EPGs). El APIC se comunica con el controlador de VM para publicar configuraciones de red como grupos de puertos que se aplican a las cargas de trabajo virtuales.
- El marco de automatización del ciclo de vida de la integración de servicios de capa 4 a capa 7 permite al sistema responder dinámicamente cuando un servicio se pone en línea o se desconecta. Las políticas proporcionan funciones de administración de paquetes y funciones de administración de inventario.
- Las políticas de acceso, autenticación y contabilidad (AAA) rigen los privilegios de usuario, las funciones y los dominios de seguridad del *fabric* Cisco ACI.

El modelo de política jerárquica encaja bien con la interfaz REST API. Cuando se invoca, la API lee o escribe en objetos en el MIT. Las URL se asignan directamente a nombres distinguidos que identifican objetos en el MIT. Cualquier dato en el MIT puede ser descrito como un documento de texto de árbol estructurado autónomo codificado en XML o JSON.

7.10 VRF's

Un objeto de enrutamiento y reenvío virtual (VRF) (fvCtx) o contexto es una red de *tenant* (llamada una red privada en la GUI de APIC). Un *tenant* puede tener varios VRF. Un VRF es un dominio de reenvío y aplicación de la Capa 3 único. La siguiente figura muestra la ubicación de VRF en el árbol de información de gestión (MIT) y su relación con otros objetos del inquilino.

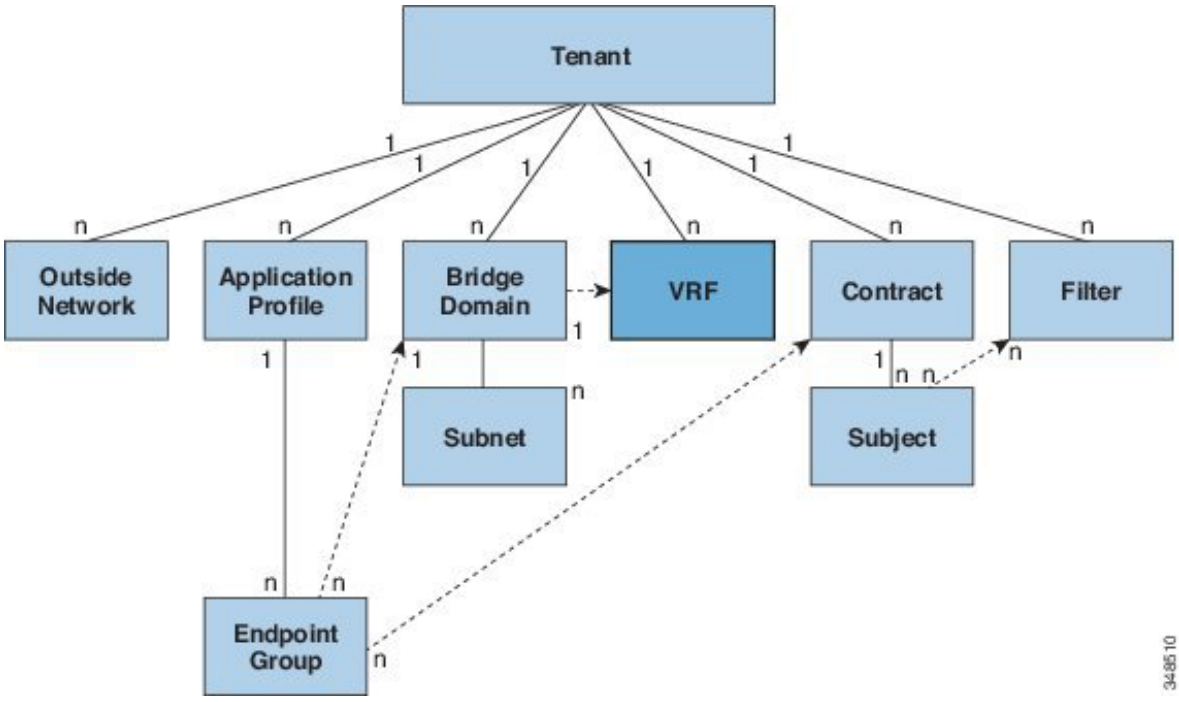

Figura 8. VRF's.

Un VRF define un dominio de dirección de Capa 3. Uno o más *bridge domain* están asociados con un VRF. Todos los dispositivos finales (*endpoints*) dentro del dominio de Capa 3 deben tener direcciones IP únicas porque es posible reenviar paquetes directamente entre estos dispositivos si la política lo permite.

7.11 Perfiles de aplicación

Un perfil de aplicación (fvAp) define las políticas, los servicios y las relaciones entre grupos de dispositivos finales (EPG). La siguiente figura muestra la ubicación de perfiles de aplicación en el árbol de información de gestión y su relación con otros objetos del inquilino.

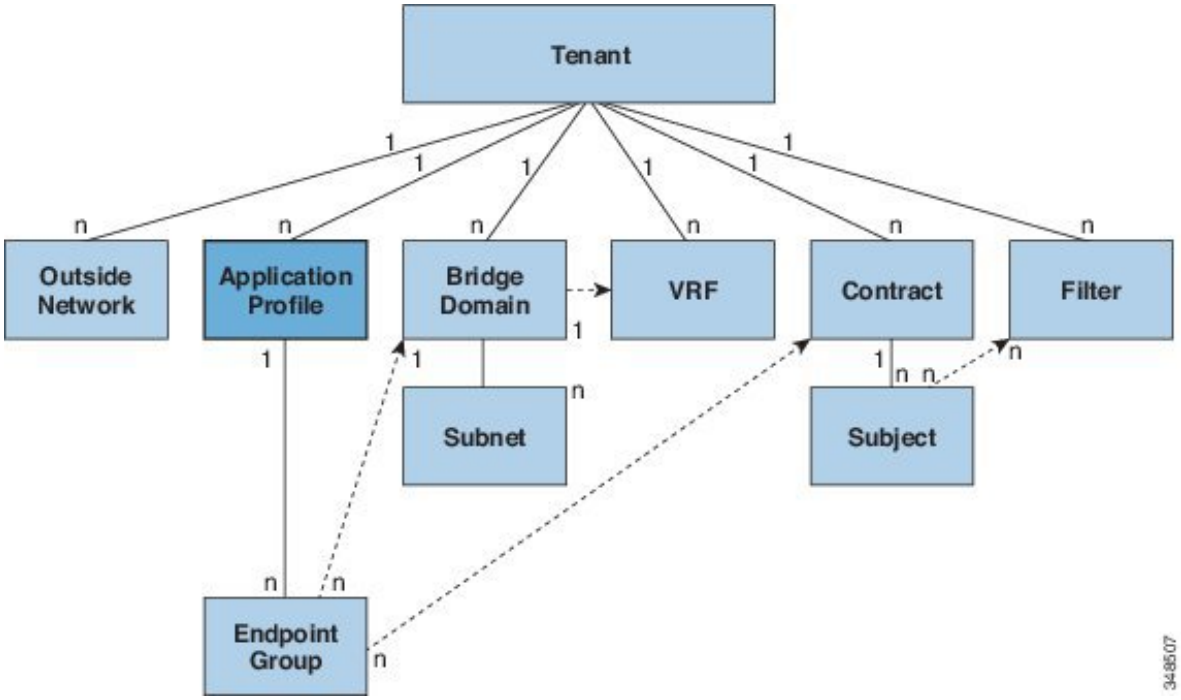

Figura 9. Perfiles de aplicaciones

Los perfiles de aplicación contienen uno o más EPG. Las aplicaciones modernas contienen múltiples componentes. Por ejemplo, una aplicación de comercio electrónico podría requerir un servidor web, un servidor de base de datos, datos ubicados en una red de área de almacenamiento y acceso a recursos externos que permitan transacciones financieras. El perfil de aplicación contiene tantos (o tan pocos) EPG como sea necesario que estén relacionados lógicamente con las capacidades de una aplicación.

Los EPG's se pueden organizar de acuerdo con uno de los siguientes:

- La aplicación que proporcionan, como un servidor DNS.
- La función que proporcionan (como la infraestructura).
- Donde están en la estructura del centro de datos (como DMZ).
- Sea cual sea el principio organizativo que el administrador de un *fabric* o un te*nant* elija utilizar.

7.12 Grupos de dispositivos finales

El grupo de dispositivos finales o *enpoints*, es el objeto más importante en el modelo de política. La siguiente figura muestra dónde se encuentran los EPG de la aplicación en el árbol de información de gestión (MIT) y su relación con otros objetos del *tenant*.

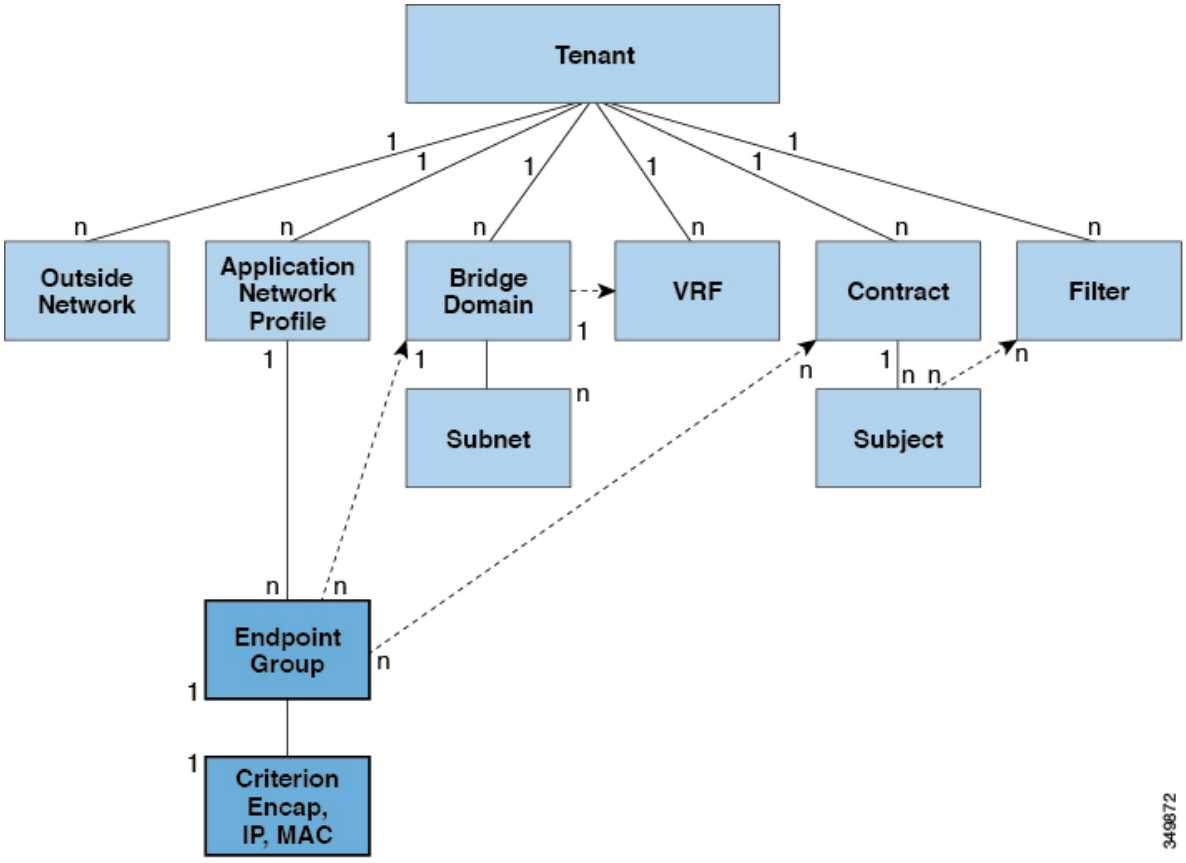

Figura 10. Grupos de *endpoints*.

Un EPG es un objeto gestionado que es nombrado como una entidad lógica, que contiene una colección de *endpoints*. Los *endpoints* son dispositivos que están conectados a la red directa o indirectamente. Tienen una dirección (identidad), una ubicación, atributos (como versión o nivel de parche) y pueden ser físicos o virtuales. Saber la dirección de un *endpoint* también permite el acceso a todos sus otros detalles de identidad. Los EPGs están totalmente desacoplados de la topología física y lógica. Los ejemplos de *endpoints* incluyen servidores, máquinas virtuales, almacenamiento conectado a la red o clientes en Internet. La pertenencia a un *endpoint* en un EPG puede ser dinámica o estática.

El *fabric* de ACI puede contener los siguientes tipos de EPG:

- Aplicación de grupos de *endpoints* (fvAEPg).
- Grupo de *endpoints* de red externa de capa 2 (l2extInstP).
- Grupo de *endpoints* de red externa de capa 3 (l3extInstP).
- Grupos de administración de *endpoints* para el acceso fuera de banda (mgmtOoB) o dentro de banda (mgmtInB).

Los EPG contienen *endpoints* que tienen requisitos de política comunes como, por ejemplo, seguridad, movilidad de la máquina virtual (VMM), calidad de servicio (QoS) o servicios de capa

4 a capa 7. En lugar de configurar y administrar *endpoints* individualmente, se colocan en un EPG y se administran como un grupo.

Las políticas se aplican al EPG, nunca a los *endpoints* individuales. Una EPG puede ser configurado estáticamente por un administrador en el APIC, o configurada dinámicamente por un sistema automatizado como *vCenter* o *OpenStack*.

7.13 Políticas de acceso automatizan la asignación de VLAN a los EPG

Mientras las políticas de red del *tenant* se configuran por separado de las políticas de acceso del *fabric*, las políticas del *tenant* no se activan a menos que sus políticas de acceso subyacentes estén en su lugar. Las interfaces con acceso externo del *fabric* se conectan a dispositivos externos como controladores de máquinas virtuales e hipervisores, hosts, *router*s o extensores de *fabric*s (FEX). Las políticas de acceso permiten a un administrador configurar port-channel y virtual *port-channel,* protocolos tales como LLDP, CDP o LACP, y funciones tales como monitoreo o diagnóstico.

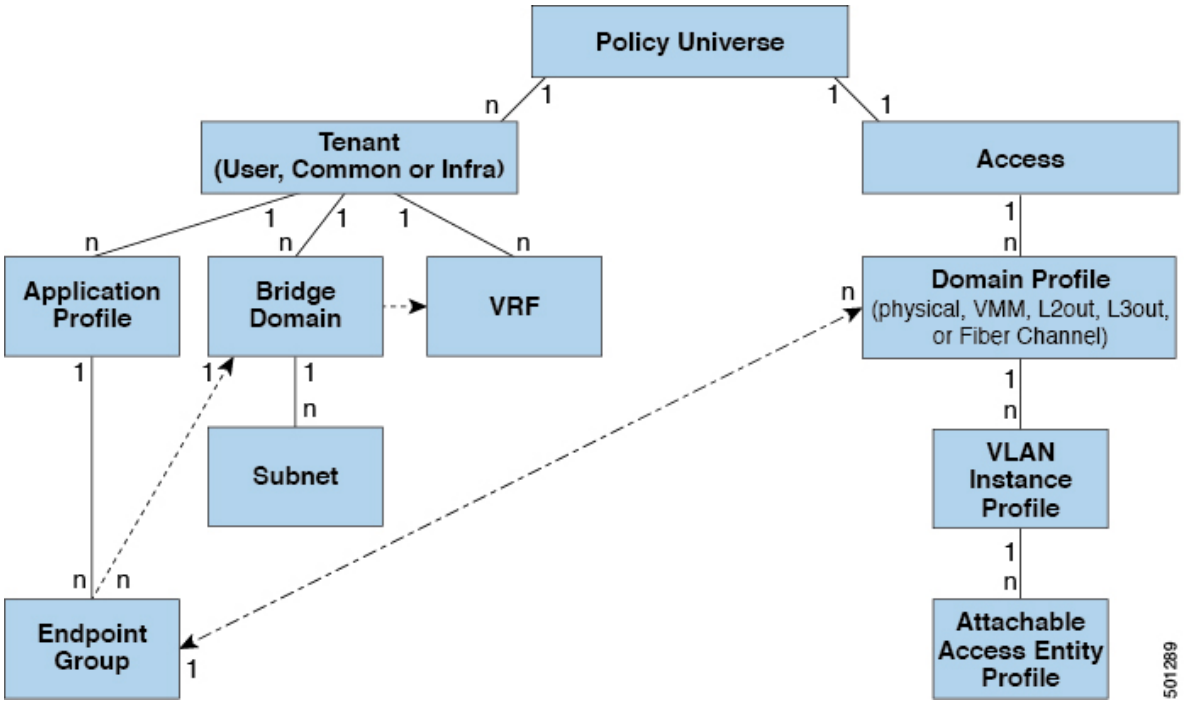

Figura 11. Asociación de EPG con las políticas de acceso.

En el modelo de política, los EPG están estrechamente acopladas con las VLAN. Para que el tráfico fluya, un EPG debe implementarse en un puerto del *leaf* con una VLAN en un dominio físico, VMM, L2out, L3out o *Fiber Channel*.

En el modelo de política, el perfil de dominio asociado al EPG contiene el perfil de instancia VLAN. El perfil de dominio contiene tanto el perfil de instancia de VLAN (conjunto de VLAN) como el perfil de entidad adjunto (AEP) asociado, que está asociado directamente con los EPG de la aplicación. El AEP despliega la aplicación asociada al EPG a todos los puertos a los que está conectado y automatiza la tarea de asignar VLANs. Mientras que un centro de datos grande podría tener fácilmente miles de máquinas virtuales activas provisionadas en cientos de VLAN, el tejido ACI puede asignar automáticamente ID de VLAN a los pools de VLAN. Esto ahorra una tremenda cantidad de tiempo, en comparación con el *trunking* de las VLAN en un centro de datos tradicional.

7.14 Perfil de entidad adjunto AEP

El *fabric* de ACI proporciona múltiples puntos de conexión que se conectan a través de puertos de los *leaf* a varias entidades externas, como servidores *barel metal*, hipervisores de máquinas virtuales, *switches* de Capa 2 o enrutadores de Capa 3 (por ejemplo, Cisco *Nexus* 7000 Serie). Estos puntos de conexión pueden ser puertos físicos, puertos FEX, *port-channel* o *virtual port-channel* (vPC) en los *leaf switches.*

Un AEP representa un grupo de entidades externas con requisitos de política de infraestructura similares. Las políticas de infraestructura consisten en políticas de interfaz física que configuran varias opciones de protocolo, tales como *Cisco Discovery Protocol* (CDP), Protocolo de detección de capa de enlace (LLDP) o protocolo de control de agregación de vínculos (LACP)

Se requiere un AEP para desplegar agrupaciones de VLAN en los *leaf*. Las agrupaciones de encapsulación (y las VLAN asociadas) son reutilizables a través de los *leaf*s. Un AEP proporciona implícitamente el ámbito del conjunto de VLAN a la infraestructura física.

Los siguientes requisitos y dependencias de AEP deben tenerse en cuenta en varios escenarios de configuración, incluida la conectividad de red, los dominios VMM.

El AEP define el rango de VLANs permitidas, pero no las proporciona. No hay tráfico a menos que se despliegue un EPG en el puerto. Sin definir un grupo de VLAN en un AEP, una VLAN no está habilitada en el puerto del *leaf* aunque se provea un EPG.

Una VLAN particular se habilita en el puerto del *leaf* que está asociado a un EPG, ya sea vinculado estáticamente en un puerto del *leaf* o basado en eventos de VM de controladores externos como *VMware vCenter* o *Microsoft Azure Service Center Virtual Machine Manager* (SCVMM).

Los AEP pueden asociarse directamente con los EPG de aplicación, que despliegan los EPG de aplicación asociados a todos los puertos asociados con el AEP. El AEP tiene una función genérica configurable, que contiene una relación con un EPG, que se despliega en todas las interfaces que forman parte de los selectores que están asociados con el AEP.
Un dominio de administrador de máquina virtual (VMM) deriva automáticamente las políticas interfaz física de las políticas de grupos de interfaces de un AEP.

7.15 Bridge domain y subredes

Un dominio de puente o *bridge domain* representa una construcción de reenvío de Capa 2 dentro del *fabric*. La siguiente figura muestra la ubicación de los *bridge domain* en el árbol de información de gestión y su relación con otros objetos del *tenant*.

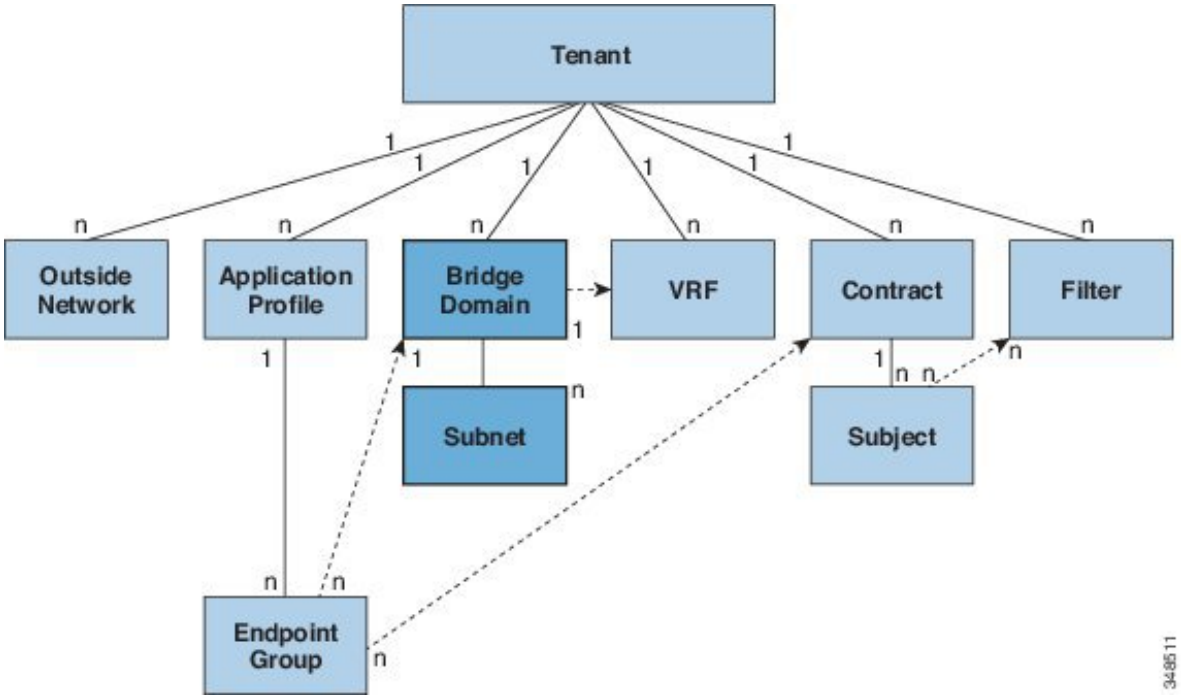

Figura 12. *Bridge domian*

Un *bridge domain* debe estar vinculado a un VRF (también conocido como contexto o red privada). Debe tener al menos una subred asociada a ella. El *bridge domain* define el espacio de dirección MAC de Capa 2 único y un dominio de inundación de Capa 2 si está habilitado. Mientras que un VRF define un espacio de dirección IP único, ese espacio de direcciones puede consistir en varias subredes. Estas subredes se definen en uno o más *bridge domains* que hacen referencia al VRF correspondiente.

Las opciones para una subred bajo un *bridge domain* o bajo un EPG son las siguientes:

- Público: la subred se puede exportar a una conexión enrutada.
- Privado: la subred sólo se aplica a su *tenant*.
- Compartida: la subred se puede compartir y exportar a varios VRF en el mismo *tenant* o entre *tenants* como parte de un servicio compartido. Un ejemplo de un servicio compartido es una conexión enrutada a un EPG presente en otro VRF en un *tenant* diferente. Esto permite que el tráfico pase en ambas direcciones a través de VRFs. Un EPG que proporciona un servicio compartido debe tener su subred configurada bajo

ese EPG (no bajo un bridge domain), y su ámbito debe configurarse para anunciarse externamente y compartido entre VRF.

7.16 Contratos

Además de los EPG, los contratos son objetos clave en el modelo de política. Los EPG sólo pueden comunicarse con otros EPG de acuerdo con las reglas del contrato. La siguiente figura muestra la ubicación de los contratos en el árbol de información de gestión y su relación con otros objetos del *tenant*.

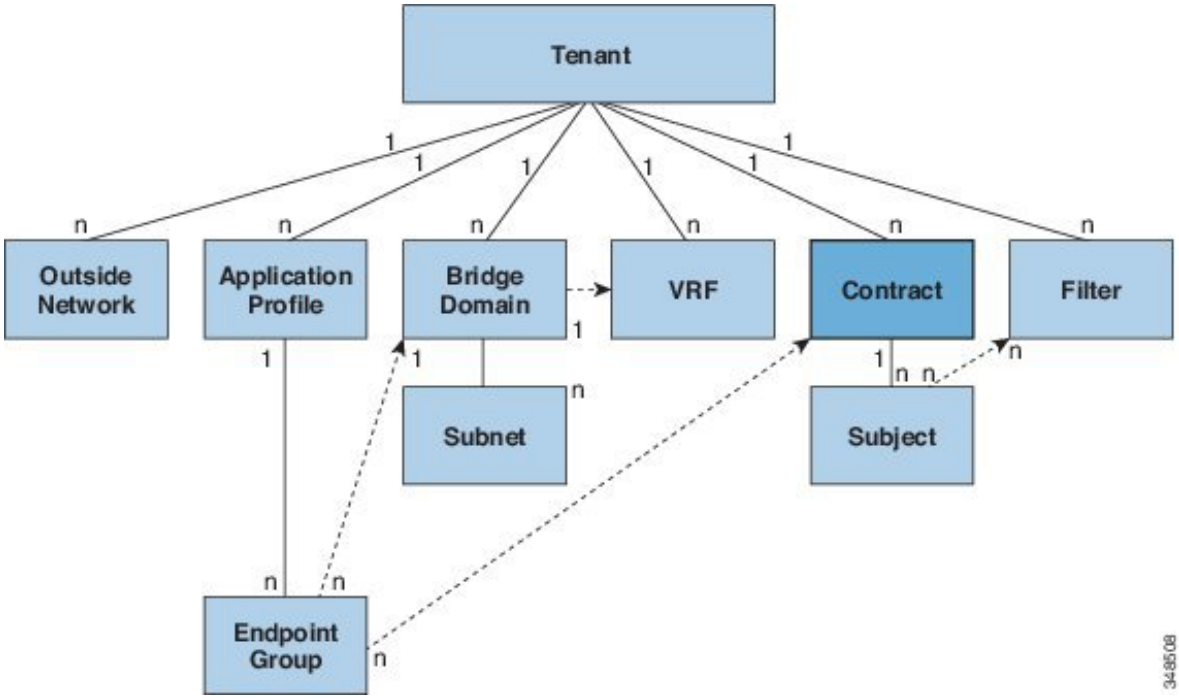

Figura 13. Contratos.

Un administrador utiliza un contrato para seleccionar el tipo de tráfico que puede pasar entre EPGs, incluidos los protocolos y puertos permitidos. Si no hay contrato, la comunicación entre EPG está desactivada de forma predeterminada. No hay contrato necesario para la comunicación intra-EPG; la comunicación intra-EPG siempre está implícitamente permitida.

Los contratos rigen los siguientes tipos de comunicaciones de EPG:

- Entre los EPG de aplicación del *fabric* de ACI, tanto *intra-tenant* como *inter-tenant*.
- Entre los EPG de aplicación del *fabric* de ACI y los EPG de la instancia de red externa de capa 2.
- Entre los EPG de aplicación del *fabric* de ACI y los EPG de la instancia de red externa de capa 3.

- Entre los EPGs de gestión de la banda ACI fuera de banda (*Out-of-band*) o dentro de banda (in-band).

Los contratos rigen la comunicación entre EPGs que son proveedores, consumidores o ambos. Los proveedores de EPG exponen los contratos con los que debe cumplir un EPG consumidor. La relación entre un EPG y un contrato puede ser un proveedor o consumidor. Cuando un EPG proporciona un contrato, la comunicación con el EPG puede iniciarse desde otros EPG siempre y cuando la comunicación cumpla con el contrato proporcionado. Cuando un EPG consume un contrato, los *endpoints* en el EPG consumidor pueden iniciar la comunicación con cualquier *endpoint* en un EPG que esté proporcionando ese contrato.

7.17 Redes externas

Las políticas de red externas controlan la conectividad con el exterior. Un *tenant* puede contener varios objetos de red externos. La siguiente figura muestra la ubicación de las redes externas en el árbol de información de gestión y su relación con otros objetos del *tenant*.

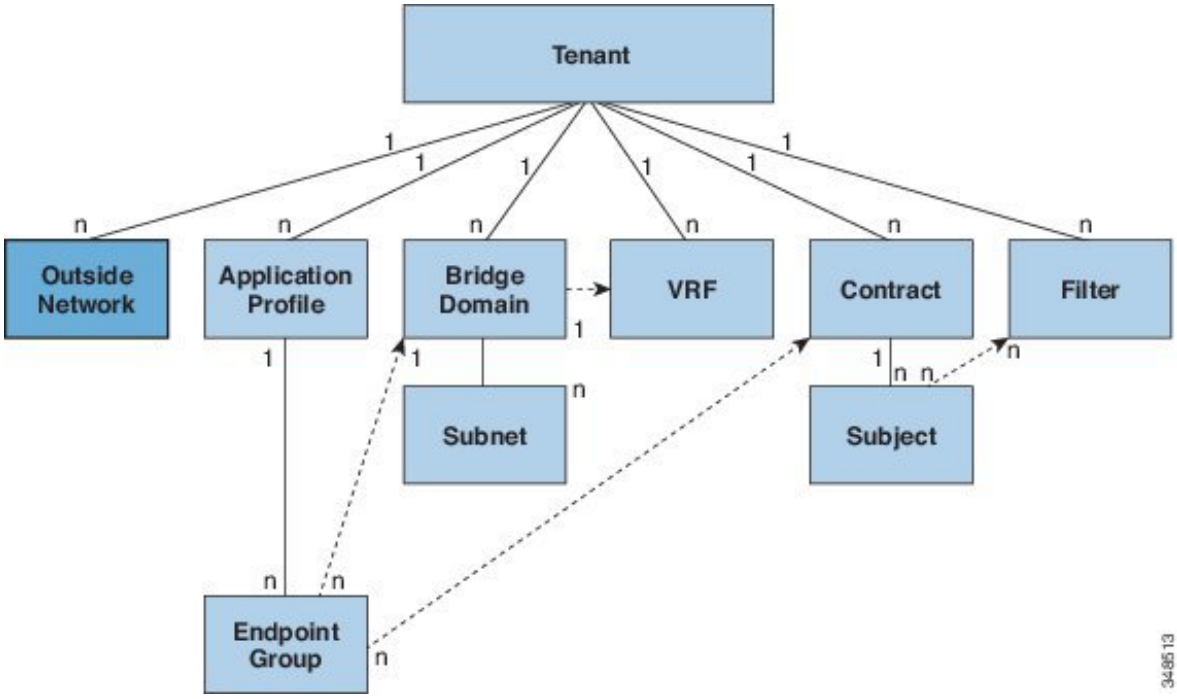

Figura 14. Redes externas

Las políticas de red externas especifican las propiedades relevantes de Capa 2 (l2extOut) o Capa 3 (l3extOut) que controlan las comunicaciones entre una red pública o privada externa y el *fabric* de ACI. Los dispositivos externos, como los enrutadores que se conectan a la WAN y el núcleo de la empresa, o los *switches* de capa 2 existentes, se conectan a la interfaz del panel frontal de un *leaf switch*. El *leaf switch* que proporciona dicha conectividad se conoce como *leaf* de borde. La interfaz del *leaf* de borde que conecta con un dispositivo externo se

puede configurar como interfaz puenteada o enrutada. En el caso de una interfaz enrutada, puede utilizarse enrutamiento estático o dinámico. El *leaf* de borde también puede realizar todas las funciones de un *leaf* normal.

7.18 Descripción general de la GUI

La GUI del APIC es una interfaz gráfica basada en navegador para la APIC que se comunica internamente con el motor APIC intercambiando mensajes de la API REST. La GUI contiene varias áreas y paneles.

7.18.1 Advertencia de implementación e información de uso de políticas

Cuando inicia sesión por primera vez en la GUI de APIC, se abre el cuadro de diálogo Configuración de advertencia de implementación que le permite habilitar y modificar el ámbito de la notificación de implementación que muestra la información de uso de políticas.

La información de uso de políticas permite a los usuarios identificar qué recursos y políticas están siendo utilizados por la política que el usuario está modificando o eliminando actualmente. Las tablas muestran los nodos donde se utiliza la política dada y otras políticas que utilizan esta política. De forma predeterminada, la información de uso se muestra en un cuadro de diálogo cada vez que el usuario intenta modificar una directiva. Además, en cualquier momento, puede hacer clic en el botón "Mostrar uso" en la parte inferior de la pantalla para ver la misma información.

7.18.2 Alternar entre los modos básico y avanzado de GUI

Cuando inicie sesión en la GUI de APIC, puede verificar el modo de GUI en el que se encuentra. El modo que ha ingresado se muestra en la esquina superior derecha de la GUI. Puede optar por operar en uno de los dos modos siguientes: avanzado y básico.

Cuando realiza una configuración en cualquiera de los modos y cambia la configuración utilizando el otro modo, pueden producirse cambios no deseados. Por ejemplo, si aplica una política de interfaz a dos puertos utilizando el modo Avanzado y, a continuación, cambia la configuración de un puerto mediante el modo básico, es posible que los cambios se apliquen a ambos puertos.

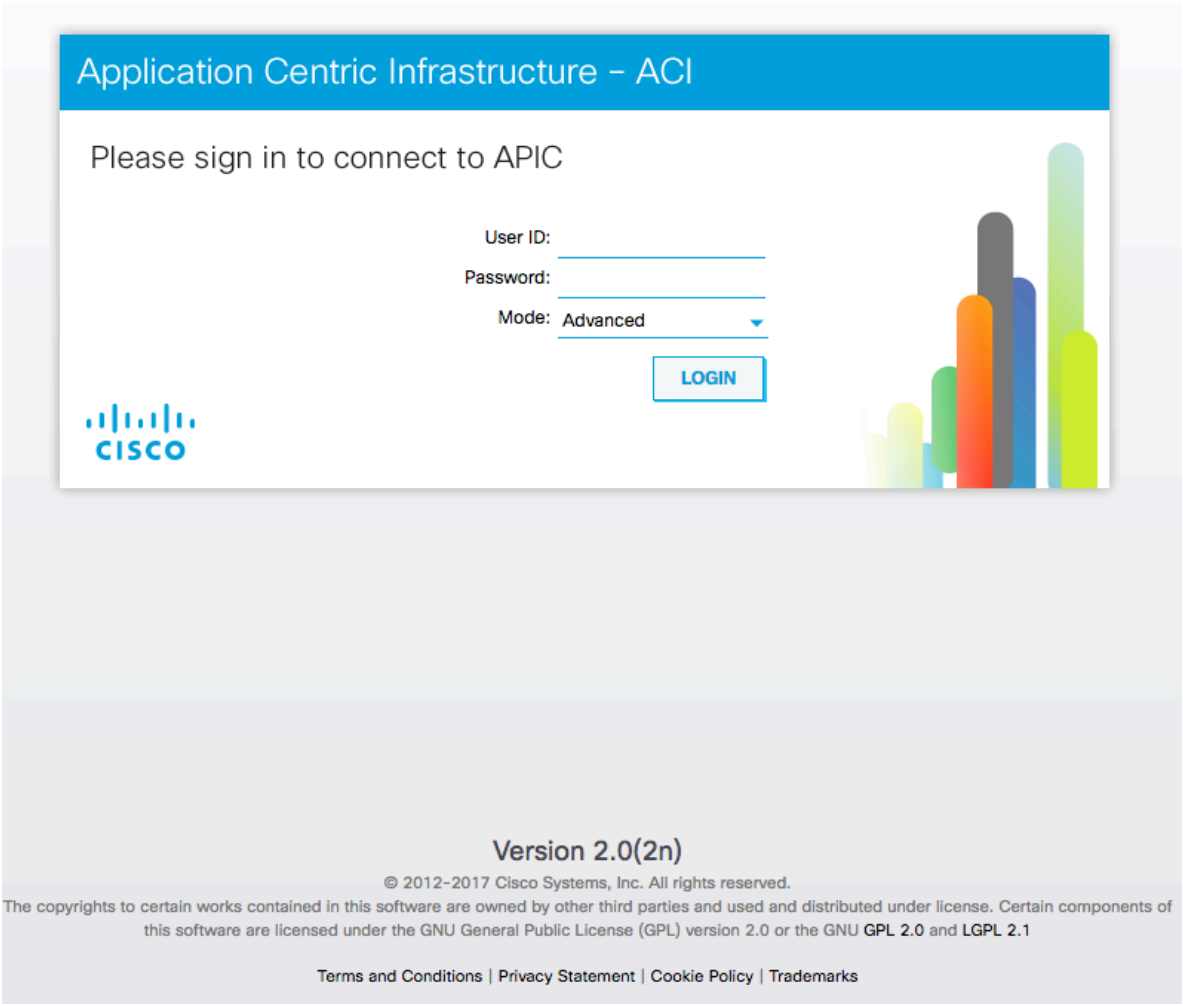

Figura 15. Pantalla de inicio de APIC GUI.

7.18.3 Barra de menús y barra de submenús

La barra de menús se muestra en la parte superior de la GUI APIC (consulte la figura siguiente). Proporciona acceso a las pestañas principales.

Figura 16. Barra de menús GUI de APIC.

Puede desplazarse hasta la barra de submenús (consulte la siguiente figura) haciendo clic en una de las pestañas de la barra de menús. Al hacer clic en una pestaña de la barra de menús, se muestra la barra de submenús para esa pestaña. La barra de submenús es diferente para cada pestaña de la barra de menús y también puede variar dependiendo de sus configuraciones específicas.

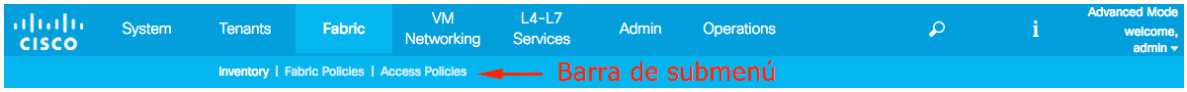

Figura 17. Barra de submenús GUI del APIC.

7.18.4 Pestaña Sistema

Utilice la pestaña Sistema para recopilar y mostrar un resumen de la integridad general del sistema, su historial y una tabla de fallos a nivel de sistema.

7.18.5 Pestaña Tenants

Utilice la pestaña *Tenants* de la barra de menús para realizar la gestión de *tenants*. En la barra de submenús, se ve un vínculo Añadir *tenant* y una lista desplegable que contiene todos los *tenants*. Hasta cinco de los *tenants* más recientemente utilizados también se muestran en la barra de submenús.

Un *tenant* contiene políticas que permiten a los usuarios cualificados el control de acceso basado en el dominio. Los usuarios cualificados pueden acceder a privilegios como administración de *tenants* y administración de redes.
Un usuario necesita privilegios de lectura/escritura para acceder y configurar políticas en un dominio. Un usuario *tenant* puede tener privilegios específicos en uno o más dominios.

7.18.6 Pestaña Fabric

La pestaña *Fabric* contiene las siguientes pestañas en la barra de submenús:

- Pestaña Inventario: muestra los componentes individuales del *fabric*.
- Pestaña Políticas del *fabric*: muestra las políticas de supervisión y solución de problemas, además de los ajustes de protocolo del *fabric* o los ajustes de unidad de transmisión máxima (MTU) del *fabric*.
- Pestaña Políticas de Acceso: muestra las políticas de acceso que se aplican a los puertos de borde del sistema. Estos puertos están en los *switches leaf* que se comunican externamente.

7.18.7 Pestaña VM Networking

Utilice la pestaña VM *Networking* para ver y configurar el inventario de los administradores de máquinas virtuales (VM). Puede configurar y crear varios dominios de administración en los que se pueden configurar conexiones a sistemas de gestión individuales (como *VMware vCenters o*

VMware vShield). Utilice la pestaña Inventario en la barra de submenús para ver los hipervisores y VMs que son administrados por estos sistemas de administración de VM.

7.18.8 Pestaña Servicios Capa4 – Capa7

Utilice la pestaña Servicios Capa4 – Capa7 para realizar servicios como la importación de paquetes que definen los dispositivos de la capa 4 a la capa 7. Puede ver los nodos de servicio existentes en la pestaña del submenú Inventario.

7.18.9 Pestaña Administración

Utilice la pestaña Administración para realizar funciones administrativas tales como funciones de autenticación, autorización y contabilidad, programar políticas, retener y purgar registros, actualizar el firmware y controlar funciones como *syslog, Call Home* y SNMP.

7.18.10 Icono de búsqueda

Haga clic en el icono Buscar para mostrar el campo de búsqueda. El campo de búsqueda le permite localizar objetos por nombre u otros campos distintivos.

7.18.11 Panel de navegación

Utilice el panel de navegación, que está en el lado izquierdo de la GUI de APIC debajo de la barra de submenús, para navegar a todos los elementos de la categoría de submenú. Cuando selecciona un componente en el panel de navegación, el objeto se muestra en el panel Trabajo. Consulte la siguiente figura para obtener una vista de ejemplo del panel de navegación.

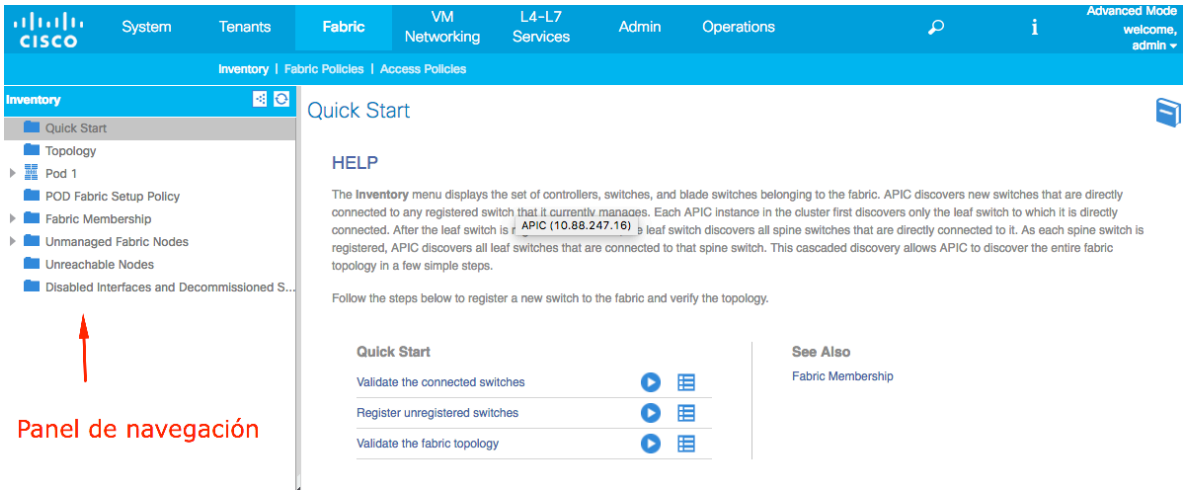

Figura 18. Panel de navegación.

7.18.12 Panel de trabajo

Utilice el panel de Trabajo, que se encuentra en el lado derecho de la GUI de APIC, para mostrar detalles sobre el componente que seleccionó en el panel de navegación. Consulte la siguiente figura para obtener una vista de ejemplo del panel de trabajo.

Un área de contenido que muestra pestañas. Estas pestañas le permiten acceder a la información relacionada con el componente que eligió en el panel de navegación. Las pestañas mostradas en el área de contenido dependen del componente seleccionado.

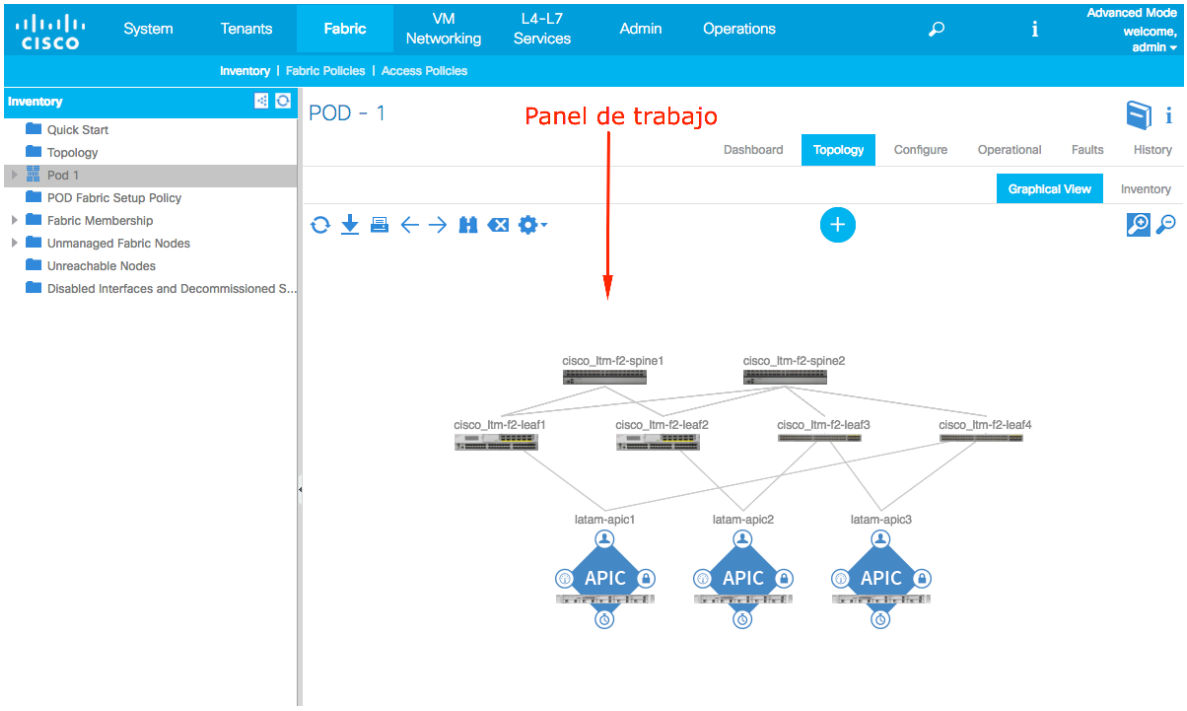

Figura 19. Panel de trabajo.

7.18.13 Iconos GUI

Icono	Descripción
	Flecha de control para el panel de navegación
	Muestra información de ayuda en línea
	Información de inicio rápido
	Descarga la tabla en formato XML o JSON
	Muestra la vista de la tabla
	Muestra la vista de la tabla de componentes que se selecciona en el panel de navegación
	Actualiza el contexto del panel.
	Configuraciones
	Siguiente vista
	Vista anterior
	Muestra el camino
	Limpia el camino

Tabla 1. Iconos mostrados con frecuencia en la GUI del APIC.

7.18.14 Iconos de fallas, estadísticas y niveles de salud

Iconos	Descripción
	Crítico. Este icono muestra un nivel de falla con gravedad crítica.
	Mayor. Este icono muestra un nivel de falla con gravedad mayor.
	Menor. Este icono muestra un nivel de falla con gravedad menor.
	Advertencia. Este icono muestra un nivel de falla que requiere atención.

Tabla 2. Niveles de gravedad de los fallos mostrados en la GUI de APIC

8 Resolución de casos de ACI

A continuación, se presentan el proceso de solución de uno de los casos más significativos que he resuelto durante mi experiencia profesional. Los ingenieros no solo de *Solution Support* sino de cualquier área de soporte alrededor del mundo, utilizan el método *Kepner Tregoe* (ver referencia 1) para analizar, documentar y resolver los problemas de los clientes.

8.1 ACI || 2.0(2f) || Sesión de SPAN no captura trafico bidireccional

Este es uno de los casos más representativos, debido a que, durante la resolución del problema, se encontró una limitante de hardware y software dentro de los *switches* leaf de segunda generación. Esta limitante podría afectar el monitoreo del trafico dentro de la red de ACI, además de que los clientes podrían ser susceptibles a comprar equipos para monitoreo de red de millones de dólares, sin tener en cuenta que el diseño de la red de monitoreo podría no desempeñarse de la forma esperada.

8.1.1 Introducción

Se presenta la información con la que el cliente reporta el problema y abre el caso en la herramienta *CSone*.

Cliente: ETERPRISE HOLDING INC.
Fecha: 25 de octubre de 2016
Tecnología: *Data Center and Storage Networking*
Subtecnología: WW-ACI-Solutions
Código del problema: Falla de software
Severidad: 3

Detalles del problema: La configuración de SPAN de entrada no está capturando los paquetes en el host conectado hacia el *fabric* de ACI. Sin embargo, yo estoy recibiendo datos unidireccionales (sólo saliente) cuando en la opción de direccionamiento se especifica ambos.

Resolución del problema realizado: Las investigaciones sugieren que un *switch Nexus* 9000 es capaz de manejar 4 sesiones SPAN (3 Tx / Rx y 1 Rx). Intenté configurar un SPAN entrante solamente en un *switch leaf* del *tenant* que es parte del *fabric* de ACI. Esta fue la única sesión definida en este *switch* y la herramienta de supervisión no registró ningún tráfico. Yo estaba apuntando a una interfaz individual que era miembro de un vPC usando un acceso tradicional SPAN. Procedí a cambiar la dirección a ambos y comencé a recibir un flujo de tráfico unidireccional (sólo saliente). Entonces intenté reflejar otra interfaz que no era un miembro de un vPC y recibió los mismos resultados. Tengo otra sesión SPAN establecida en un *switch leaf* de borde y está registrando tráfico en ambas direcciones. También tengo una disposición idéntica del *fabric* de ACI en un ambiente del laboratorio y los resultados sugirieron que también estaba registrando tráfico en ambas direcciones.

8.1.2 Presentación del problema

Para poder iniciar con el análisis del problema, es necesario aclarar algunos términos presentes en los detalles y resolución del problema que proporcionó el cliente.

SPAN dentro del ambiente de ACI

ACI tiene la característica SPAN (Analizador de puerto conmutado), así como otros productos de Cisco. En general, hay tres tipos de SPAN. SPAN local, SPAN remoto (RSPAN) y SPAN remoto encapsulado (ERSPAN). Las diferencias de estos SPAN son principalmente un destino de los paquetes copiados. Cisco ACI admite SPAN local y ERSPAN.

Cisco ACI tiene tres tipos de SPAN; *Fabric* SPAN, *Tenant* SPAN y Access SPAN. La diferencia de cada SPAN es la fuente de los paquetes copiados:

- *Fabric* SPAN es para capturar los paquetes que entran y salen de las interfaces entre los swtiches *leaf* y *spine*.
- Access SPAN es capturar paquetes que entran y salen de interfaces entre *switches Leaf* y dispositivos externos.
- *Tenant* SPAN es capturar los paquetes que entran y salen de *EndPoint* Group (EPG) en los *switches* ACI *Leaf*.

Este nombre SPAN corresponde al lugar en el que se va a configurar en la interfaz gráfica de usuario de Cisco ACI.

- *Fabric* SPAN está configurado en "*Fabric*> Políticas del *Fabric*"
- Access SPAN está configurado bajo "*Fabric*> Políticas de acceso"
- *Tenant* SPAN se configura bajo "*Tenant*> {cada *tenant*}"

En cuanto al destino de cada SPAN, sólo Access SPAN es capaz de SPAN local y ERSPAN. Otros dos SPAN (*fabric* y *tenant*) son solamente capaces de ERSPAN.

VPC

Los *port-channels* virtuales (vPCs) permiten que los enlaces físicamente conectados a dos *switches* Cisco diferentes aparezcan en un tercer dispositivo descendente procedentes de un solo dispositivo y como parte de un único *port-channels* l. El tercer dispositivo puede ser un *switch*, un servidor o cualquier otro dispositivo de red que admita *port-channels* IEEE 802.3ad.

Los vPCs se componen de dos pares de *swtiches* de vPC conectados mediante un enlace entre iguales. De los pares de vPC, uno es primario y uno secundario. El sistema formado por los *switches* se denomina un dominio vPC.

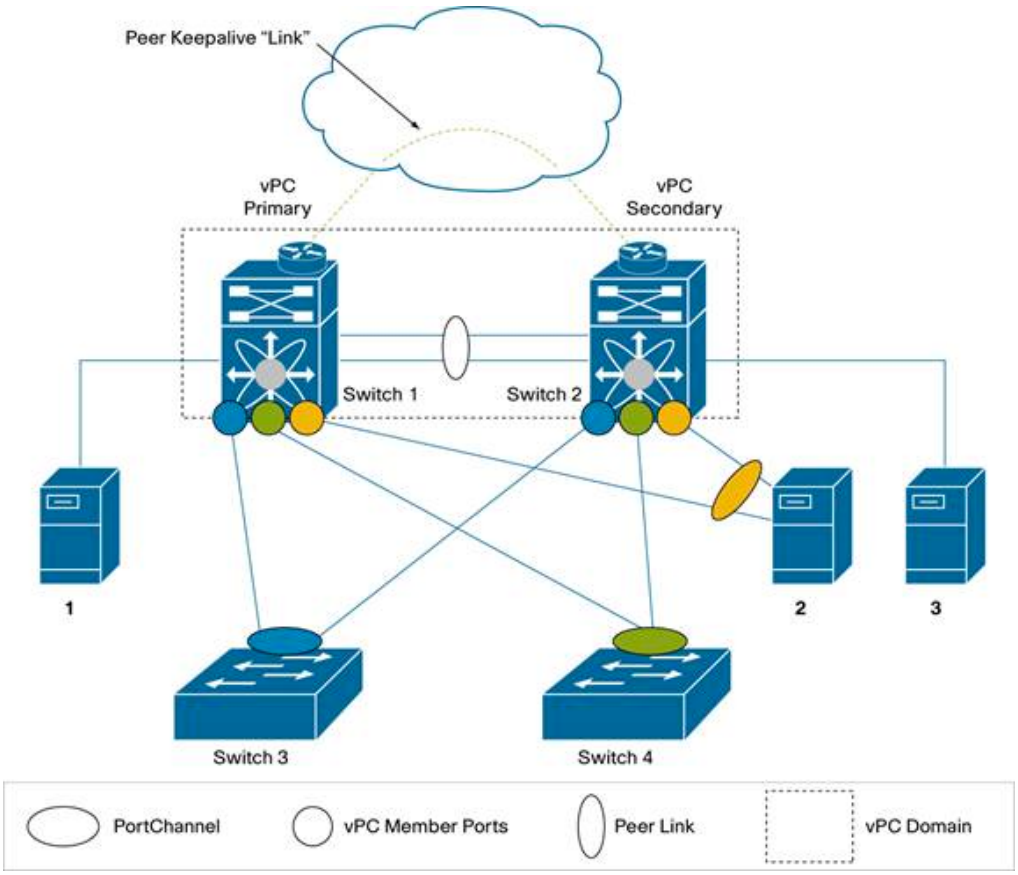

Figura 17. Componente de un VPC

Para más información acerca de VCP se puede consultar la referencia 2.

Una vez que se entienden los principios del funcionamiento de SPAN en ACI y los VPC, el comprender el problema se vuelve más intuitivo para el ingeniero de soporte.

Para iniciar con el proceso de solución del problema, contacté al cliente vía Email. Envié mi información de contacto e hice un par de preguntas.

***Nota**: La documentación de casos siempre es realizada en idioma inglés, pero por fines prácticos del reporte serán traducida y presentada en español.*

E-mail de primer contacto con el cliente:

25-10-2016 14:14

Hola Ryan,

Mi nombre es Marco Domínguez de Cisco TAC. Le envío este correo como un punto inicial de contacto, para hacerle saber que le ayudaré en esta solicitud de servicio.

Por lo que entiendo, la descripción del problema es la siguiente: "SPAN no está recolectando paquetes bidireccionales procedentes de un host conectado por VPC en un par de switches leaf en el fabric de ACI. Sin embargo, cuando se selecciona la opción de dirección 'ambos' SPAN captura unidireccional solo de entrada". Por favor, siéntase libre de corregirme si mi comprensión no es correcta o si desea añadir algo a mi descripción.

También, por favor hágame saber lo siguiente:

1. ¿Cuál es la versión del APIC?

2. ¿Tienes tiempo para una reunión webex?

3. Por favor, tome un poco de tiempo para documentar el impacto comercial relacionado con esta Solicitud de Servicio (si es relevante), para poder concentrarme en el problema en consecuencia.

Por favor, asegúrese de marcar un cc a attach@cisco.com en toda nuestra comunicación y eliminar los mensajes anteriores y sólo mantener la nueva. Esto actualizará las notas de caso automáticamente y ayudará a mantener la coherencia de la solicitud de servicio.

He incluido mi horario de trabajo y los datos de contacto a continuación para su referencia. Si necesita asistencia inmediata y no estoy disponible, llame a su número local de Cisco TAC y solicite al próximo ingeniero disponible que se le asigne a su caso.

Atentamente,

.:|:.:|:.
Marco Antonio Domínguez Becerra
Marcdomi@cisco.com
Ingeniero de Soporte al Cliente
Horario: M-F 11:00 am a 7:00 pm CST -5

Siempre es importante saber que versión de software se está utilizando en ACI, ya que en cada versión se presenta diferente funcionalidad, capacidad, escalabilidad y bugs/defectos. Esto ayuda a saber si la configuración que realiza el cliente está soportada, o en caso de que se encuentre un defecto, saber que versión es la afectada y en cual el defecto es arreglado.

```
Respuesta al e-mail de primer contacto:

25-10-2016 14:38

Hola Marco,

¡Gracias por la respuesta inmediata!


1. La versión APIC es 2.0(2f)

2. Estoy programado para salir de la oficina en ~ 45 minutos, por lo que mañana
a las 11 AM CST o 12 AM CST sería ideal. Mi horario es de 6:30 AM a 3:30 PM CST
M-F.

3. El Fabric de ACI es un despliegue bastante nuevo y actualmente tenemos dos
aplicaciones migradas a este entorno. Este problema fue identificado
recientemente mientras se realizaba una demostración al CON para la captura de
datos. Como mencioné en las notas de caso, las sesiones SPAN del leaf de borde
han estado funcionando como se diseñó, así como las pruebas realizadas en
nuestro entorno de laboratorio. Este problema existe en un entorno de
producción, así que tenga en cuenta que la solución de problemas puede ser
limitada.

Espero trabajar juntos.

Ryan
```

En base a la respuesta del cliente y verificar las notas de la versión 2.0(2f) de ACI, confirmé que la configuración de SPAN estaba soportada. Además de que debería de ser muy cuidadoso en caso de cambiar alguna configuración dentro de ACI, debido a que el *fabric* está en producción y cualquier cambio indebido, puede afectar de manera alta la producción y servicios del cliente.

Le hice saber al cliente mi disponibilidad para poder trabajar con él a través de la herramienta *WebEx*. Acordamos la hora y fecha para realizar el proceso de análisis del problema.

La reunión *WebEx* fue realizada en el tiempo establecido, durante la sesión, el cliente pudo compartir el escritorio de su computadora, para tener acceso al APIC GUI, permitir tener el control de su computadora para revisar la configuración de SPAN. En base a lo revisado en la reunión, pude obtener la siguiente descripción del problema:

8.1.3 Descripción del problema

Hardware: APIC
Versión: 2.0 (2f)
Impacto empresarial: el *fabric* de ACI es un despliegue bastante nuevo y actualmente el cliente tiene dos aplicaciones migradas a este entorno, pero necesita realizar el monitoreo los puertos pertenecientes al vPC para obtener una telemetría del tráfico generado por los clientes de la red.

Problema: El cliente configuro SPAN local en ACI para analizar las interfaces ethernet 1/5 del *leaf* 105 y 106. Estas interfaces forman parte de un VPC que conecta un centro de datos, el cual contiene cientos de máquinas virtuales que se comunican a través de la infraestructura de ACI.

Configuración de SPAN local en ACI:

SPAN Grupo de origen: Dirección: ambos Rutas de origen: Pod-1 / *leaf*-105 / eth1 / 5 ← Este puerto forma parte de un VPC Grupo de destino SPAN Ruta de destino: Pod-1 / *leaf*-105 / eth1 / 48 ← Recolector de SPAN conectado a este puerto

En el momento de generar una captura de paquetes, la herramienta de supervisión no registra ningún tráfico.

Además, se realizaron una serie de pruebas para obtener información de cómo el trafico estaban siendo cambiando los contadores TX y RX en la interface eth 1/48 utilizando cada una de las direcciones de captura de SPAN (Entrada, Salida y Ambas):

8.1.3.1 Prueba 1

SPAN grupo origen: Dirección: Ambas Camino del origen: *Pod-1/leaf-105/eht1/5* SPAN grupo destino: Camino del destino: *Pod-1/leaf-105/eth1/48*

Analicé los contadores de paquetes en la interface del *leaf* de destino, para esto, accedí al *leaf* 105 por medio de SSH. El acceso vía SSH permite ejecutar comandos del tipo del sistema operativo NXOs de los *Nexus* 9000. Para mostrar los contadores utilicé el comando show interface eth1/48:

```
ETC-ACI-LF105# show interface eth1/48
Ethernet1/48 is up
admin state is up, Dedicated Interface
  Hardware: 1000/10000/25000/auto Ethernet, address: 00f6.63ca.6434
(bia 00f6.63ca.6434)
  MTU 9000 bytes, BW 10000000 Kbit, DLY 1 usec
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, medium is broadcast
  Port mode is trunk
  full-duplex, 10 Gb/s, media type is 10G
  FEC (forward-error-correction) : disable-fec
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned off
  Rate mode is dedicated
  Switchport monitor is on
  EtherType is 0x8100
  EEE (efficient-ethernet) : n/a
  Last link flapped 4d20h
  Last clearing of "show interface" counters 2d03h
  12 interface resets
  30 seconds input rate 0 bits/sec, 0 packets/sec
  30 seconds output rate 0 bits/sec, 0 packets/sec
  Load-Interval #2: 5 minute (300 seconds)
    input rate 0 bps, 0 pps; output rate 13856352 bps, 1367 pps
  RX
    0 unicast packets  0 multicast packets  0 broadcast
packets                        <------------  0 paquetes recibidos
    0 input packets  0 bytes
    0 jumbo packets  0 storm suppression bytes
    0 runts  0 giants  0 CRC  0 no buffer
    0 input error  0 short frame  0 overrun   0 underrun  0 ignored
    0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
    0 input with dribble  0 input discard
    0 Rx pause
  TX
    965004 unicast packets  491 multicast packets  0 broadcast packets
       <------------  965004 paquetes transmitidos
    965495 output packets  1179616549 bytes
    0 jumbo packets
    0 output error  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble  0 output discard
    0 Tx pause
```

Ejecutando el comando nuevamente para observar los cambios en los contadores:

```
ETC-ACI-LF105# show interface eth1/48
Ethernet1/48 is up
admin state is up, Dedicated Interface
  Hardware: 1000/10000/25000/auto Ethernet, address: 00f6.63ca.6434
(bia 00f6.63ca.6434)
  MTU 9000 bytes, BW 10000000 Kbit, DLY 1 usec
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, medium is broadcast
  Port mode is trunk
  full-duplex, 10 Gb/s, media type is 10G
  FEC (forward-error-correction) : disable-fec
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned off
  Rate mode is dedicated
  Switchport monitor is on
  EtherType is 0x8100
  EEE (efficient-ethernet) : n/a
  Last link flapped 4d20h
  Last clearing of "show interface" counters 2d03h
  12 interface resets
  30 seconds input rate 0 bits/sec, 0 packets/sec
  30 seconds output rate 0 bits/sec, 0 packets/sec
  Load-Interval #2: 5 minute (300 seconds)
    input rate 0 bps, 0 pps; output rate 12677088 bps, 1251 pps
  RX
    0 unicast packets  0 multicast packets  0 broadcast packets
       <------------  0
    0 input packets  0 bytes
    0 jumbo packets  0 storm suppression bytes
    0 runts  0 giants  0 CRC  0 no buffer
    0 input error  0 short frame  0 overrun   0 underrun  0 ignored
    0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
    0 input with dribble  0 input discard
    0 Rx pause
  TX
    985654 unicast packets  491 multicast packets  0 broadcast packets
       <------------  985654
    965495 output packets  1179616549 bytes
    0 jumbo packets
    0 output error  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble  0 output discard
    0 Tx pause
```

Se puede observar que en la interface eth 1/48 no se estaban recibiendo paquetes (RX), pero se estaban transmitiendo (Tx). Confirmé el síntoma que el cliente reportó cuando abrió el caso. El colector de SPAN solo está registrando tráfico de salida.

8.1.3.2 Prueba 2

SPAN grupo origen:
Dirección: Entrada
Camino del origen: Pod-1/leaf-105/eht1/5

SPAN grupo destino:
Camino del destino: Pod-1/leaf-105/eth1/48

```
ETC-ACI-LF105# show interface eth1/48
Ethernet1/48 is up
admin state is up, Dedicated Interface
  Hardware: 1000/10000/25000/auto Ethernet, address: 00f6.63ca.6434
(bia 00f6.63ca.6434)
  MTU 9000 bytes, BW 10000000 Kbit, DLY 1 usec
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, medium is broadcast
  Port mode is trunk
  full-duplex, 10 Gb/s, media type is 10G
  FEC (forward-error-correction) : disable-fec
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned off
  Rate mode is dedicated
  Switchport monitor is on
  EtherType is 0x8100
  EEE (efficient-ethernet) : n/a
  Last link flapped 4d20h
  Last clearing of "show interface" counters 2d03h
  12 interface resets
  30 seconds input rate 0 bits/sec, 0 packets/sec
  30 seconds output rate 0 bits/sec, 0 packets/sec
  Load-Interval #2: 5 minute (300 seconds)
    input rate 0 bps, 0 pps; output rate 0 bps, 0 pps
  RX
    0 unicast packets  0 multicast packets  0 broadcast
packets                          <------------  0
    0 input packets  0 bytes
    0 jumbo packets  0 storm suppression bytes
    0 runts  0 giants  0 CRC  0 no buffer
    0 input error  0 short frame  0 overrun   0 underrun  0 ignored
    0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
    0 input with dribble  0 input discard
    0 Rx pause
  TX
    968944 unicast packets  498 multicast packets  0 broadcast packets
        <--------------- 968944
    969442 output packets  1181813646 bytes
    0 jumbo packets
    0 output error  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble  0 output discard
    0 Tx pause
```

A pesar de cambiar la dirección de captura a "entrada", en los contadores de la interface solamente se observó un incremento en paquetes transmitidos. Lo esperado es que aumentara el contador de paquetes recibidos.

8.1.3.3 Prueba 3

SPAN Source group:
Direction: Outgoing
Source Paths: Pod-1/leaf-105/eht1/5

SPAN Destination Group
Destination Path: Pod-1/leaf-105/eth1/48

```
ETC-ACI-LF105# show interface eth1/48
Ethernet1/48 is up
admin state is up, Dedicated Interface
  Hardware: 1000/10000/25000/auto Ethernet, address:
00f6.63ca.6434 (bia 00f6.63ca.6434)
  MTU 9000 bytes, BW 10000000 Kbit, DLY 1 usec
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, medium is broadcast
  Port mode is trunk
  full-duplex, 10 Gb/s, media type is 10G
  FEC (forward-error-correction) : disable-fec
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned off
  Rate mode is dedicated
  Switchport monitor is on
  EtherType is 0x8100
  EEE (efficient-ethernet) : n/a
  Last link flapped 4d20h
  Last clearing of "show interface" counters 2d04h
  12 interface resets
  30 seconds input rate 0 bits/sec, 0 packets/sec
  30 seconds output rate 25739952 bits/sec, 3087 packets/sec
  Load-Interval #2: 5 minute (300 seconds)
    input rate 0 bps, 0 pps; output rate 20560432 bps, 2398 pps
  RX
    0 unicast packets  0 multicast packets  0 broadcast
packets                <------------  0
    0 input packets  0 bytes
    0 jumbo packets  0 storm suppression bytes
    0 runts  0 giants  0 CRC  0 no buffer
    0 input error  0 short frame  0 overrun   0 underrun  0
ignored
    0 watchdog  0 bad etype drop  0 bad proto drop  0 if down
drop
    0 input with dribble  0 input discard
    0 Rx pause
  TX
    4501376 unicast packets  2289 multicast packets  14 broadcast
packets <------------ 4501376
    4503679 output packets  5308153230 bytes
```

Ejecutando el comando nuevamente para observar los cambios en los contadores:

```
ETC-ACI-LF105# show interface eth1/48
Ethernet1/48 is up
admin state is up, Dedicated Interface
  Hardware: 1000/10000/25000/auto Ethernet, address: 00f6.63ca.6434 (bia
00f6.63ca.6434)
  MTU 9000 bytes, BW 10000000 Kbit, DLY 1 usec
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, medium is broadcast
  Port mode is trunk
  full-duplex, 10 Gb/s, media type is 10G
  FEC (forward-error-correction) : disable-fec
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned off
  Rate mode is dedicated
  Switchport monitor is on
  EtherType is 0x8100
  EEE (efficient-ethernet) : n/a
  Last link flapped 4d20h
  Last clearing of "show interface" counters 2d04h
  12 interface resets
  30 seconds input rate 0 bits/sec, 0 packets/sec
  30 seconds output rate 3148544 bits/sec, 336 packets/sec
  Load-Interval #2: 5 minute (300 seconds)
    input rate 0 bps, 0 pps; output rate 15337152 bps, 1780 pps
  RX
    0 unicast packets  0 multicast packets  0 broadcast
packets                <------------  0
    0 input packets  0 bytes
    0 jumbo packets  0 storm suppression bytes
    0 runts  0 giants  0 CRC  0 no buffer
    0 input error  0 short frame  0 overrun   0 underrun  0 ignored
    0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
    0 input with dribble  0 input discard
    0 Rx pause
  TX
    4507414 unicast packets  2307 multicast packets  14 broadcast
packets <------------ 4507414
    4509735 output packets  5315230995 bytes
    0 jumbo packets
    0 output error  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble  0 output discard
    0 Tx pause
```

En esta prueba se puede observar que los contadores de paquetes transmitidos (TX) tuvieron un incremento, sin embargo, no hubo cambio en los contadores de paquetes recibidos (RX). Mismo comportamiento que la prueba 2.

Definitivamente el comportamiento de esta sesión de SPAN estaba generando resultados inesperados. Le pedí al cliente tiempo para recrear esta configuración en mi entorno de laboratorio de CALO. El cliente aceptó, terminamos la llamada.

8.1.4 Análisis del problema

Realice una prueba con los siguientes elementos:

- *Fabric* de ACI versión 2.0(2f).
- Configurar un VPC (puertos ethernet 1/17 de los *leaf* 101 y 102) para integrar un servidor UCS con ACI.
- Crear 2 EPGs, con 2 subredes diferentes. Asocie un *endpoint* (Máquina Virtual) en cada EPG para poder mandar tráfico de un EPG hacia otro. Una vez que los dos *endpoints* se podían comunicar entre ellos proseguí con la configuración de SPAN en ACI.
- SPAN local configurado, grupo de origen un puerto que forma parte del VPC (puerto ethernet 1/17, *leaf* 101), dirección "ambas".
- Destino SPAN una laptop conectada puerto ethernet1/13 en *leaf* 101.
- Enviar tráfico desde la máquina virtual de EPG 1 hacia la máquina virtual en el EPG 2 (ping).
- En la captura de paquetes, vi tráfico en ambas direcciones.
- Cambiar la dirección de SPAN a entrada.
- Enviar tráfico desde la máquina virtual de EPG 1 hacia la máquina virtual en el EPG 2 (ping).
- En el análisis de los contadores en el puerto ethernet1/13 en *leaf* 101, sólo se detectó tráfico en dirección entrante.
- Cambiar la dirección de SPAN a saliente.
- Enviar tráfico desde la máquina virtual de EPG 1 hacia la máquina virtual en el EPG 2 (ping).
- En el análisis de los contadores en el puerto ethernet1/13 en *leaf* 10, sólo se detectó tráfico en dirección saliente.

En este momento y con esa configuración, SPAN funcionó como se espera. Después, realicé una segunda prueba para comprobar cómo se estaba transmitiendo el tráfico en la otra interface del VPC:

- Configurar SPAN local, grupo de origen un puerto que forma parte del VPC (puerto ethernet 1/17, *leaf* 102), dirección "ambos".
- Configurar destino SPAN, puerto 1/13, *leaf* 102, como se está configurando SPAN local el destino debe de estar en el mismo *leaf* que el origen.
- Enviar tráfico desde la máquina virtual de EPG 1 hacia la máquina virtual en el EPG 2 (ping).

- En el análisis de los contadores en el puerto ethernet1/13 en *leaf* 102, no se detectó ningún incremente en los contadores TX y RX, lo que indica que no se estaba transmitiendo tráfico en ninguna dirección a través de ese puerto.
- Cambiar la dirección de SPAN a "entrante".
- En el análisis de los contadores en el puerto ethernet1/13 en *leaf* 102, no se detectó ningún incremente en los contadores TX y RX, lo que indica que no se estaba transmitiendo tráfico en ninguna dirección a través de ese puerto.
- Cambiar la dirección de SPAN a "saliente".
- En el análisis de los contadores en el puerto ethernet1/13 en *leaf* 102, no se detectó ningún incremente en los contadores TX y RX, lo que indica que no se estaba transmitiendo tráfico en ninguna dirección a través de ese puerto.

En la base de la prueba anterior, el tráfico sólo estaba siendo transmitido a través de un puerto del VPC (ethernet 1/13 *leaf* 101), esto debido a que el algoritmo de balanceo de carga (LACP) del VPC solo estaba utilizando un solo puerto del VPC para él envió de tráfico.

En mi laboratorio el comportamiento de SPAN estaba funcionando de manera correcta. El siguiente paso fue pedir al cliente realizar un test similar al segundo que hice en mi laboratorio. Mi teoría era que, probablemente el tráfico que se transmitía por el VPC, estaba siendo enviado por el otro puerto del VPC (Pod-1/*leaf*-106/eht1/5), en vez de la que se analizó inicialmente (Pod-1/*leaf*-105/eht1/5).

Compartí mis resultados de las pruebas de laboratorio con el cliente por medio de un e-mail, además de realizar pruebas similares en su ambiente de ACI. Esta fue su respuesta:

Marco,

Parece que mi experiencia es diferente...

Primera prueba;
+ Configuré un SPAN local, puerto de origen eth 1/5 que es miembro de un VPC (leaf 105), dirección "ambos".
+ Destino SPAN, puerto 1/48 en leaf 105.
+ Envió de tráfico de múltiples EPGs.
+ En la captura de paquetes, vi tráfico en una dirección. Tráfico procedente de otros EPGs al puerto 1/5.
+ Cambie la dirección de SPAN a "entrante".
+ En la captura de paquetes, he observado unos paquetes LLDP Multicast
+ Cambie la dirección de SPAN a "saliente".
+ En la captura de paquetes, vi el tráfico sólo en dirección saliente.
+ En este momento y con esa configuración, SPAN es unidireccional.

Segunda prueba;
+ Configuré un SPAN local, puerto de origen eth 1/5 que es un miembro de un VPC (leaf 106), dirección "ambos".
+ Destino SPAN, puerto eth 1/48 en leaf 106.
+ Recopilación de tráfico de múltiples EPGs.
+ En la captura de paquetes, vi tráfico en una dirección. Tráfico procedente de otros EPGS al puerto 1/5. El volumen de tráfico no fue tan significativo, pero los datos fueron recolectados.
+ Cambie la dirección de SPAN a "entrante".
+ En la captura de paquetes, he observado unos paquetes LLDP Multicast
+ Cambie la dirección de SPAN a "saliente".
+ En la captura de paquetes, vi el tráfico sólo en dirección saliente.
+ En este momento y con esa configuración, SPAN es unidireccional y no parece llevar tanto tráfico como en el puerto 1/5 del leaf 105.

Gracias,
Ryan

A pesar de haber realizado un par de pruebas similares a las realizadas en el laboratorio, los resultados seguían variando. En ese momento me surgió la necesidad de saber por qué el cliente quería monitorear individualmente cada una de las interfaces de los *leaf* en lugar de monitorear las dos interfaces a la vez y utilizar ERSPAN en lugar de SPAN local. Así que envié un e-mail al cliente para verificar el uso de local SPAN.

Esta fue su respuesta:

> *Hola Marco,*
>
> *Se trata de una configuración SPAN sencilla, y es imperativo para nuestro diseño de monitoreo que tenemos, la capacidad de monitorear port-channels utilizando SPAN local. Tengo una disposición similar fuera del fabric de ACI, donde un vPC se configura entre dos dispositivos de Cisco. Para capturar los datos simplemente agrego el port-channel a la sesión de monitoreo en cada switch. Cuando se configura el grupo SPAN de origen en ACI, no hay opciones en el menú desplegable, pare seleccionar port-channel, por lo que espero que solo tengamos que actualizar el software para que estos port-channel directos sean visibles.*

El diseño de monitoreo del cliente estaba pensado para analizar específicamente el tráfico de los puertos de cada uno de los *leaf*, por lo que proveer una solución al cliente era de suma importancia, ya que si se proponía un nuevo diseño de monitoreo de red, podría causar un retraso en la implementación del mismo. Este monitoreo está funcionando en otros dispositivos de cisco, el cual podría ser un indicio de que por alguna razón en ACI no está funcionando de la manera adecuada. Además de que en el ambiente de laboratorio había tenido resultados pósitos.

Lo siguiente que había que averiguar es como era el flujo del tráfico que pasaba a través del VPC que el cliente quería monitorear. Para esto, le pedí al cliente que realizamos otra reunión de *WebEx* para realizar una captura de paquete a nivel de hardware ELAM, para darnos cuenta como el trafico estaba siendo enviado dentro del *fabric* de ACI, esto nos daría una pista para saber si realmente el tráfico estaba siendo mandado de la forma correcta, y con esto verificar si el problema de SPAN era debido a un mal flujo de tráfico y no propio del mismo SPAN.

La reunión de *WebEx* se llevó a cabo, el resultado de la captura ELAM, fue que efectivamente el trafico está siendo mandado desde la interface del VPC hacía el *endpoint* destino a través del *fabric* de ACI. Por ejemplo, si un *endpoint* A conectado a través del VPC en *leaf* 105-106 mandaba tráfico hacia otro *endpoint* B conectado al *leaf* 101, el flujo de tráfico era de la siguiente manera:
El trafico entraba al *fabric* de ACI a través de la interface ethernet 1/5 *leaf* 105, después era enviado hacia uno de los *switch spine*, este lo enviaba hacia el *leaf* 101, y finalmente el *leaf* 101 envía el tráfico a través de la interface que conecta al *endpoint* destino. Con esto se confirmó que el trafico dentro del *fabric* de ACI estaba utilizando el flujo esperado. Lo que reducía el problema a que SPAN no estaba copiando de manera adecuada el tráfico de los puertos del VPC.

Al final de la reunión *WebEx* pedimos al cliente que nos proporcionara retroalimentación del otro escenario donde había configurado SPAN y había podido monitorear exitosamente los puertos del VPC.

Hola Marco,

Para reiterar mis comentarios durante la llamada ... Estamos utilizando un SPAN local para capturar tráfico en VPCs fuera del fabric, pero hay una ligera diferencia al origen de SPAN. Aquí hay un ejemplo de cada entorno;

No ACI
Tengo dos switches N9K-C93180YC-EX que contienen un VPC. Hay un nodo conectado a Eth1 / 32 en cada switch que pertenece al port-channel 132, los port-channel de cada switch están configurados para pertenecer al VPC 132. Tengo un SPAN local establecido en cada swtich (Interfaz de destino Eth1 / 45) Y puedo con éxito capturar tráfico en el origen del SPAN, especificando el port-channel local en cada swtich que participa en el VPC. Si intento agregar el miembro (por ejemplo, interfaz física Eth1 / 32) al SPAN, recibo el siguiente error;

ERROR: Eth1 / 32: Interface es un miembro de PC.

ACI

El APIC sólo nos permite seleccionar los miembros del port-channel (por ejemplo, interfaces físicas) en el puerto de origen del SPAN. Hay una pestaña dentro de la APIC para mostrar los port-channel, pero la lista desplegable no genera ningún resultado. Cuando especifico una interfaz física como fuente sólo observo el tráfico saliente en mi SPAN local (Access SPAN). Tengo la esperanza de que hay algo en el software que podríamos actualizar que nos permitiría monitorear los port-channel locales o directos, al igual que el procedimiento fuera de ACI.

Como mencioné anteriormente nuestro diseño de monitoreo completo se basa en la utilización de sesiones SPAN locales (Access SPAN) para capturar tráfico para todos los hosts, y se espera que los VPC representen más del 70% de las conexiones. Además, los SPANs locales nos permiten capturar hasta 40Gb / s por switch (sesiones SPAN de 4x10Gb), y estamos planeando desplegar 87 switches a la terminación del proyecto. Tenemos una infraestructura de monitorización completa para terminar todos los 348 destinos de 10Gb SPAN, y es imprescindible que nuestra solución de captura aproveche todas las 348 interfaces. Me temo que ERSPAN limitará severamente la cantidad de tráfico que podremos capturar y no podremos utilizar las cuatro sesiones SPAN por switch. Mi otra preocupación es dónde terminar el ERSPANs como nuestra solución de monitoreo sólo es capaz de terminar 6 sesiones para un total de 60Gb / s.

¡Gracias!
Ryan

Para continuar con el proceso de análisis del problema decidimos realizar un par de pruebas más utilizando diferentes interfaces de los *leaf* del cliente, además de utilizar un ordenador portátil que fungiría como el destino/monitoreador del tráfico. Esto, con el fin de analizar cómo se comporta SPAN en ambas direcciones cuando se utiliza como origen un puerto que pertenece a un VPC, y cuando el origen es un puerto de acceso.

Prueba 1: Se configura un VPC para analizar el flujo del tráfico en el destino del SPAN (Resultado: Salida unidireccional en el destino SPAN):

- Dirección IP aplicada 10.21.224.20 a una computadora portátil independiente.
- Se configuró un VPC en el *leaf*105 - *leaf* 106 eth1/ 2, y luego se conectó el portátil solo a Eth1/32 en la hoja 105 (No conectó nada en *leaf* 106 eth1/32).
- Conectado un segundo ordenador portátil al *leaf* 105 eth 1/34 y se añadió Eth1/34 como un destino SPAN utilizando un Access SPAN.
- Iniciado un ping desde el *leaf* 105 utilizando iping a 10.21.224.20.
- Se observó comunicación desde el *switch* hacia el host (no hay tráfico capturado desde el host de vuelta al *switch*) en el portátil conectado al destino SPAN.
- Se corrió una captura con el analizador de trafico wireshark en host 10.21.224.20 durante la prueba y el tráfico observado en dirección saliente.

Prueba 2: Se configura un Puerto de Acceso para analizar el flujo del tráfico en el destino del SPAN (Resultado: salida bidireccional en el destino SPAN).

- Dirección IP aplicada 10.21.224.20 a una computadora portátil independiente.
- Se configuró el *leaf* 105 eth1/35 como un puerto de acceso, y luego se conectó el computador portátil sólo a eth 1/35 en *leaf* 105.
- Se conectó un segundo ordenador portátil al *leaf*105 Eth1/34 y se añadió Eth1/34 como un destino SPAN utilizando un Access SPAN.
- Iniciado un ping desde el *leaf* 105 utilizando iping a 10.21.224.20
- Tráfico observado en ambas direcciones en el portátil conectado al destino SPAN.
- Se corrió una captura con el analizador de trafico wireshark en host 10.21.224.20 durante la prueba y el tráfico observado en ambas direcciones.

Al final de la prueba concluí que SPAN bidireccional funciona correctamente cuando el puerto de origen cuando se configura como acceso. El síntoma era muy claro, si el puerto de origen es configurado como un *port-channel* que es parte de un VPC, SPAN local solo captura tráfico de salida en el puerto de destino.

Sin embargo, no había una razón clara del por qué los resultados de las pruebas en el laboratorio eran diferentes a las obtenidas con el cliente. Analizando las notas del caso, noté una diferencia entre las pruebas del laboratorio y las del cliente. En mi laboratorio utilice *switches* leaf modelo N9K-C9396PX en lugar de N9K-C93180YC-EX, como los que tiene en su *fabric* de ACI el cliente.

Lo *switches* del modelo N9K-C9396PX pertenecen a la primera generación de *Nexus* 9000, los N9K-C93180YC-EX son de la segunda generación. Se puede consultar las diferencias entre los dos modelos de *switches* en la referencia 3.

Mi primera prueba la realice en la plataforma N9K-C93180YC-EX, debido a que, en ese momento, la cantidad de equipo en nuestro laboratorio de CALO era limitada. Existían dos *leaf* N9K-C9396PX, dos *spine* N9K-C9336PQ y un controlador APIC.

Para poder para poder recrear el problema tuve que utilizar un *fabric* de ACI que cuenta con los *switches* N9K-C93180YC-EX, en el laboratorio de CALO en San José California. Como la red de administración de CALO es accesible para todos los ingenieros de soporte, pude acceder remotamente a los dispositivos y configurar SPAN local y realizar las pruebas con éxito.

Al realizar las pruebas con lo *leaf* N9K-C93180YC-EX, obtuve los mismos resultados que los obtenidos en el *fabric* del cliente. Sin embargo, el problema en el que SPAN no captura el tráfico entrante no es sólo para vPC sino que también ocurre con *port-channel* normal. Es decir, que los puertos de origen pueden estar configurados como *port-channel* que pertenecen a un VPC, o como puertos en *port-channel* normal.

El siguiente paso fue informar al cliente sobre los resultados obtenidos en el laboratorio, además de llenar un nuevo bug, explicando a los desarrolladores de ACI el problema encontrado. Probablemente este problema es debido a una limitación de software en la segunda generación de *switches* leaf.

Detalles del BUG:

ID: CSCvc11053
Severidad: 4
Versiones conocidas afectadas: 12.0(2f)
Producto: N9K-C93180YC-EX y 93108TC-EX

Síntoma:
El tráfico entrante no es capturado por SPAN o ERSPAN.
Esta es una limitación actual en la 2ª generación ASIC ACI LEAF *(N9K-C93180YC-EX y 93108TC-EX).*

Condiciones:
Cuando el origen SPAN o ERPSAN está configurada utilizando un puerto individual, que es miembro de port-channel o un vPC, en la 2ª generación de ASIC ACI LEAF.

Solución:
Ninguna.
Para Local SPAN: Configure el port-channel propio (la combinación SPAN local y VPC no está soportada)
Para ERSPAN: Por favor, configure el propio port-channel como origen en caso de port-channel, por favor configure el propio vPC como origen de ERSPAN en lugar los alguno de los puertos miembros del VPC.

Después de que el bug fue abierto, hubo una discusión interna con los desarrolladores de software, se acordó abrir un nuevo de mejora, para que en la GUI de ACI se habilite la opción de poder seleccionar como origen de SPAN un *port-channel* que es miembro de un VPC, además se proporcionó una solución provisional, la cual consiste configurar SPAN local a través de la línea de comandos. Los detalles del bug se presentan a continuación.

ID: CSCvc44643
Severidad: 4
Versiones conocidas afectadas: 12.0(2f)
Producto: N9K-C93180YC-EX y 93108TC-EX

Síntoma:
Esta mejora consiste en implementar la característica donde configuramos un port-channel miembro de vPC como origen de SPAN local en ACI.
Actualmente, APIC GUI solo permite al usuario configurar todo el vPC, (en ambos *leaf*s) o un componente de interfaz física que es miembro de un port-channel.

Condiciones:
Al intentar configurar el origen SPAN para vPC, los siguientes escenarios son posibles en este momento.

1. Configurar el componente de interfaz física de vPC como origen de SPAN local y ERSPAN.
2. Configurar vPC como origen sólo para ERSPAN.

Sin embargo, la segunda generación de hardware como N9K-C93180YC-EX en modo ACI no admite el primer escenario anterior.
Lo que significa que no hay forma de hacer Local SPAN con vPC en hardware de segunda generación en ACI.

Solución:
Una solución provisional por ahora es configurar un port-channel miembro de un vPC desde la consola de comandos CLI del estilo NX-OS o la API REST.

Un ejemplo de CLI de estilo NX-OS

```
monitor access session x1
  source interface port-channel accBndlGrp_1018_1019_vpc1 leaf 1018
    exit
  destination interface ethernet 1/5 leaf 1018
  exit
```

Un ejemplo para REST API

```
<infraInfra>
   <spanDestGrp name="MyDstGrp">
      <spanDest name="dst1018">
          <spanRsDestPathEp tDn="topology/pod-1/paths-1018/pathep-[eth1/5]" />
      </spanDest>
   </spanDestGrp>

<spanSrcGrp name="MySrcGrp">
      <spanSpanLbl name=" MyDstGrp " />
      <spanSrc name="src1018">
         <spanRsSrcToPathEp tDn="topology/pod-1/paths-1018/pathep-
[accBndlGrp_1018_1019_vpc1]" />
      </spanSrc>
   </spanSrcGrp>
</infraInfra>
```

8.1.5 Solución del Problema

La solución provisional para SPAN local fue probada en el laboratorio.

En la GUI del APIC no podemos seleccionar un *port-channel* o un VPC, origen de SPAN local. Sin embargo, podemos hacerlo vía CLI. En nuestra prueba usamos 2 *port-channel* como origen. Se puede utilizar la siguiente consulta para obtener el nombre de los perfiles vPC configurado en las políticas de acceso en el *fabric* de ACI:

```
moquery -c infraAccBndlGrp -f 'infra.AccBndlGrp.lagT=="node"' | grep dn
```

Se utilizaron los *leaf*:
-1018
-1019

Dos VPC's:
- accBndlGrp_1018_1019_vpc1
- accBndlGrp_1018_1019_vpc2

Puertos destino dedicados para trafico TX y RX:
-Tx – eth1/5
-Rx – eth1/6

Configuración en *leaf* 1018:

```
monitor access session Tx1
    source interface port-channel accBndlGrp_1018_1019_vpc1 leaf 1018
    source interface port-channel accBndlGrp_1018_1019_vpc2 leaf 1018
    direction tx
      exit
    destination interface ethernet 1/5 leaf 1018
```

```
monitor access session Rx1
    source interface port-channel accBndlGrp_1018_1019_vpc1 leaf 1018
    source interface port-channel accBndlGrp_1018_1019_vpc2 leaf 1018
    direction rx
      exit
    destination interface ethernet 1/6 leaf 1018
    exit
```

En el análisis de contadores TX y RX de las interfaces ethernet 1/5 y ethernet 1/6, se observó un aumento en los respectivos contadores al momento de enviar tráfico a través de VPC's "accBndlGrp_1018_1019_vpc1" y "accBndlGrp_1018_1019_vpc2":

Incremento de contador TX en interface eth1/5:

```
ACI-leaf1018# show interface eth1/5
.
.
.
RX
    1249 unicast packets  0 multicast packets  0 broadcast
packets
    0 input packets  0 bytes
    0 jumbo packets  0 storm suppression bytes
    0 runts  0 giants  0 CRC  0 no buffer
    0 input error  0 short frame  0 overrun   0 underrun  0 ignored
    0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
    0 input with dribble  0 input discard
    0 Rx pause
  TX
    6240 unicast packets  2289 multicast packets  14 broadcast
packets              <------------ 6240
    4503679 output packets  5308153230 bytes
    0 jumbo packets
    0 output error  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble  0 output discard
    0 Tx pause
```

```
ACI-leaf1018# show interface eth1/5
.
.
.
RX
    1249 unicast packets  0 multicast packets  0 broadcast
packets
    0 input packets  0 bytes
    0 jumbo packets  0 storm suppression bytes
    0 runts  0 giants  0 CRC  0 no buffer
    0 input error  0 short frame  0 overrun   0 underrun  0 ignored
    0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
    0 input with dribble  0 input discard
    0 Rx pause
```

```
  TX
    8063 unicast packets  2289 multicast packets  14 broadcast
packets              <------------ 8063
    4503679 output packets  5308153230 bytes
    0 jumbo packets
    0 output error  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble  0 output discard
    0 Tx pause
```

Incremento de contador RX en interface eth1/5:

```
ACI-leaf1018# show interface eth1/5
.
.
.
RX
    2748 unicast packets  0 multicast packets  0 broadcast
packets               <------------  2748
    0 input packets  0 bytes
    0 jumbo packets  0 storm suppression bytes
    0 runts  0 giants  0 CRC  0 no buffer
    0 input error  0 short frame  0 overrun   0 underrun  0 ignored
    0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
    0 input with dribble  0 input discard
    0 Rx pause
  TX
    9450 unicast packets  2289 multicast packets  14 broadcast
packets
    4503679 output packets  5308153230 bytes
    0 jumbo packets
    0 output error  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble  0 output discard
    0 Tx pause
```

```
ACI-leaf1018# show interface eth1/5
.
.
.
RX
    2961 unicast packets  0 multicast packets  0 broadcast
packets               <------------  2961
    0 input packets  0 bytes
    0 jumbo packets  0 storm suppression bytes
    0 runts  0 giants  0 CRC  0 no buffer
    0 input error  0 short frame  0 overrun   0 underrun  0 ignored
    0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
    0 input with dribble  0 input discard
    0 Rx pause
  TX
    9803 unicast packets  2289 multicast packets  14 broadcast
packets
    4503679 output packets  5308153230 bytes
    0 jumbo packets
    0 output error  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble  0 output discard
    0 Tx pause
```

Básicamente, en la prueba anterior se puede observar que el tráfico que está capturando SPAN local es bidireccional.

9 Conclusión

Con la solución verificada y funcional en el laboratorio, el último paso fue aplicar la solución en el *fabric* de ACI del cliente. Los pasos para solucionar el problema fueron proporcionados al cliente via e-mail. Esta fue su respuesta:

```
Buenos días Marco,

He podido confirmar que la solución que proporcionaste captura el tráfico en ambas
direcciones para los nodos / interfaces que participan en un vPC.


Estamos trabajando con nuestro equipo de cuentas de Cisco para realizar un
seguimiento de una futura versión de software que nos permitirá aprovechar la
interfaz gráfica de usuario a través del navegador web para supervisar los vPC.
Dicho esto, debemos ser capaces de seguir adelante y marcar este caso como
resuelto.

Ryan
```

Actualmente la mejora solicitada en el bug *CSCvc44643* esta implementada en las versiones: 2.1(2e) y 2.2(2e) de ACI.

El cliente autorizó el cierre del caso el 4 de enero de 2017, el tiempo de resolución de este caso tomo aproximadamente 2 meses y 10 días.

Eso no significa que exclusivamente trabajé en este caso durante ese periodo de tiempo. En general los ingenieros de *Solution Support* en la tecnología de ACI toman entre 1a 3 casos al día, lo que implica trabajar en la solución de múltiples casos a la vez. Es de vital importancia para los ingenieros de soporte administrar su tiempo, para hacer recreaciones en el laboratorio, atender sesiones *Webex* con los clientes, escribir documentación, llenar bugs, documentar casos y sobre todo estudiar. Un ingeniero de soporte debe de ser experto en la tecnología que atiende, pero además debe de poseer excelentes habilidades en manejo de emociones, no solo las propias, incluso las de los clientes.

Durante mi experiencia en *Solution Support* (1 año con 5 meses) he resuelto alrededor de 350 casos, en donde he enfrentado muchos retos, desde aprender un protocolo en algunos minutos. hasta lidiar con clientes muy enojados debido a que un problema en ACI ocasiona pérdida de miles de dólares al día a su compañía. Todos los días aprendo algo nuevo, al mismo tiempo que desarrollo mis capacidades técnicas y emocionales. Trabajar en Cisco México para mí, es una de las más grandes oportunidades que he tenido. Sé lo que significa esta empresa para el mundo del *networking* y la responsabilidad que recae en todos sus empleados para seguir cambiado y evolucionando la forma en que el mundo se comunica. Es por eso que día a día sigo preparándome para poder brindar el mejor servicio posible.

Referencias

[1]. "Kepner Tregoe", kepner-tregoe.com, 2017. [Online]. Disponible: http://www.kepner-tregoe.com/
[2]. "Cisco NX-OS Software Virtual PortChannel: Fundamental Concepts 5.0", www.cisco.com, 2017. [Online]. Disponible: http://www.cisco.com/c/en/us/products/collateral/switches/nexus-5000-series-switches/design_guide_c07-625857.html#_Toc271759437
[3]. "Cisco Nexus 9000 Series Switches", www.cisco.com, 2017. [Online]. Disponible: http://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/tsd-products-support-series-home.html