TRABAJO FIN DE GRADO

Migración del Core de red a SDN Cisco ACI.

Autor: Gregorio De Peña Núñez
Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación.
Consultor: Jaume Jofre Bravo

15/01/2023

Resumen

A consecuencia de la continua digitalización de los servicios, las redes de comunicaciones están experimentando un aumento importante tanto en el nivel de tráfico que soportan como en la cantidad de elementos de red que las componen. Normalmente la gestión de los elementos de red convencionales se hace de manera descentralizada y ante este continuo aumento que se está experimentando, se dificulta su gestión para la provisión de servicios, el mantenimiento o para hacer un simple *Troubleshooting* ante una incidencia en la red.

En este TFG se documenta cómo se migra una red de Core de una entidad bancaria que se ve afectada por estos problemas, los cuales en gran medida son derivados de la digitalización de sus servicios y del continuo aumento de las comunicaciones con otras empresas externas. La red de Core con la que cuenta el banco se sustenta en equipos Cisco C6500 a los que se le va añadiendo cada vez más equipos, lo cual hace que su gestión sea muy compleja ya que cada equipo requiere su propia conexión por *CLI* para gestionarlo. Por otro lado, a esto se le suma que son equipos antiguos y tanto el *throughput* como las velocidades de sus interfaces se quedan desactualizadas para el tipo de servicio y velocidades que se demandan hoy en día. Por todo ello, se ve necesario implementar una solución que permita la gestión centralizada de toda la red Core y que a su vez le otorgue más calidad, estabilidad y escalabilidad a la red.

Para cumplir con los objetivos del banco, se propone migrar la red convencional a una solución SDN que aporte una mejora sustancial en las comunicaciones del banco y a su vez permita tener una gestión unificada de todo el entorno Core. En este documento se detallan las tareas necesarias para llevar a cabo esta migración, sin entrar en detalle de cómo se implementan los protocolos de comunicación dentro de la red SDN y otras cuestiones más técnicas que requerirían otro enfoque de este TFG.

Finalmente, es importante resaltar que, debido a la criticidad del entorno en el que se despliega la solución, el proyecto se ha de llevar a cabo de principio a fin sin afectar en ningún momento al servicio del banco, por lo que todas las tareas de las diferentes fases en las que se ha dividido el proyecto se hacen salvaguardando el funcionamiento del negocio del banco y la calidad del servicio que éste presta a sus clientes.

Abstract

As a result of the continuous digitization of services, communications networks are experiencing a significant increase both in the level of traffic they support and in the number of network elements that compose them. Normally the management of conventional network elements is done in a decentralized manner and given this continuous increase that is being experienced, it is difficult to manage them for the provision of services, maintenance or to carry out a simple Troubleshooting in the event of a network incident.

This TFG documents how a Core network of a bank that is affected by these problems is migrated, which are largely derived from the digitization of its services and the continuous increase in communications with other external companies. The bank's Core network is based on Cisco C6500 equipment to which more and more equipment is being added, which makes its management very complex since each equipment requires its own CLI connection to manage it. On the other hand, to this is added that they are old equipment and both the throughput and the speeds of their interfaces are outdated for the type of service and speeds that are demanded today. For all these reasons, it is necessary to implement a solution that allows the centralized management of the entire Core network and that in turn gives more quality, stability and scalability to the network.

To accomplish the bank's objectives, it is proposed to migrate the conventional network to an SDN solution that provides a substantial improvement in the bank's communications and at the same time allows unified management of the entire Core environment. This document details the tasks necessary to carry out this migration, without going into detail about how the communication protocols are implemented within the SDN network and other more technical issues that would require another focus of this TFG.

Finally, it is important to highlight that, due to the criticality of the environment in which the solution is deployed, the project must be carried out from start to finish without affecting the bank's service at any time, so all the tasks of the different phases into which the project has been divided are carried out safeguarding the operation of the bank's business and the quality of the service it provides to its customers.

ÍNDICE

1. Introducción

1.1. Descripción del proyecto:

En este proyecto se documenta de manera teórica todo el proceso de migración de la capa Core de una entidad bancaria, y a su vez se pretende dejar constancia de la complejidad e importancia que tiene llevar a cabo esta tarea sin que se afecte al servicio en ningún momento.

Se explica el proceso de migración del Core de una red convencional a tecnología SDN (Software Defined Network). Se empezará haciendo un estudio sobre las soluciones que existen en el mercado y se determinará el porqué de la elección del fabricante Cisco, concretamente Cisco ACI (Application Centric Infrastructure), el entorno de prueba de la solución y su despliegue en un entorno que ha de continuar dando servicio a los usuarios 24x7.

1.2. Justificación del proyecto:

Desde hace mucho tiempo las infraestructuras de comunicaciones se han considerado como un elemento fundamental en las empresas y por ello es importante su correcto diseño, gestión y mantenimiento. Debido al continuo aumento de la demanda de servicios informáticos, las redes de comunicaciones han ido creciendo de manera exponencial y paralelamente su complejidad de gestión, lo cual hace necesario que se disponga de una gestión lo más centralizada y robusta posible que facilite estas tareas a los administradores de las redes de comunicaciones.

1.3. Motivación para realizar el proyecto:

El motivo principal por el que se hace este TFG es por la necesidad de controlar una red de Core que cada vez se hace más grande y a que su vez requiere grandes capacidades de rendimiento a nivel de velocidad, disponibilidad, throughputs, etc. Por ello, en vista de los requerimientos de red de hoy en día, es necesario conocer las diferentes tecnologías de SDN que nos podemos encontrar en el mercado para poder gestionar de manera centralizada las redes de comunicaciones de gran tamaño y una vez elegida la solución, detallar el proceso de migración de una red convencional basada en *hardware* hacia SDN sin que se afecte al servicio en ningún momento tanto durante como después de la migración.

1.4. Ámbito de aplicación del proyecto:

Este tipo de solución se aplica en la capa Core de la Red. Al tratarse del Core de un banco, se ha de tener en cuenta que cualquier caída o pérdida en la calidad del servicio puede tener consecuencias económicas negativas sobre la entidad, empresas colaboradoras y/o clientes, por lo que es muy importante realizar la migración de manera controlada y salvaguardando el servicio (comunicación con oficinas, comunicación con otras entidades financieras, transferencias de divisas, acceso a cuentas vía *app* o web, etc.). Con la elección de SDN se

cumple con estos requisitos de seguridad, fiabilidad y escalabilidad que han de mantenerse durante todo el tiempo para poder prestar el servicio de manera eficiente.

1.5. Objetivos del proyecto:

Los objetivos principales del proyecto son los siguientes:

- Identificar claramente los componentes de la red de Core actual.
- Avanzar hacia un entorno de gestión centralizada de toda la capa Core.
- Aumentar la calidad del servicio de comunicaciones del Banco.
- Disponer de una red actual, escalable, fiable y segura.
- Preparar la red para poder aumentar la experiencia de usuario interno y externo al Banco.
- Aumentar los niveles de seguridad y fiabilidad de las comunicaciones corporativas y con las demás entidades financieras.
- Disponer de conexiones capaces de mantener una velocidad de transferencia de 100 Gbs.
- Homogeneizar los elementos de la red de los dos CPDs que existen actualmente.
- Llevar a cabo la migración sin que haya impacto negativo a nivel de comunicaciones ni de reputación del Banco.

1.6. Tareas del proyecto de migración:

Para que la migración del Core a SDN sea un éxito, se han de llevar a cabo las tareas que se detallan a continuación:

- Análisis de la red actual de Core: Se realizará un estudio exhaustivo de la red actual de Core con el objetivo de identificar claramente todos los equipos que la componen y las diferentes configuraciones que hay implementadas.

- Estudio de fabricantes con tecnología SDN: Se trata de ver qué opciones existen en el mercado y cuál es la idónea según las necesidades de la empresa y de la red.

- Formación SDN a administradores de la red: Una vez elegida la solución, se ha de hacer una formación específica a los administradores de la red para que por un lado se pueda hacer la migración correctamente y por otro para que la continúen explotando y evolucionando con nuevos servicios o ampliación de equipamiento que pueda haber en un futuro.

- Estudio de migración: Se lleva a cabo un estudio de migración en el que se valoran los posibles riesgos y se minimizan al máximo para evitar cualquier incidencia que pueda conllevar un corte o disminución del servicio.

- Compra de equipamiento: Seleccionado el fabricante, se ha de dar el paso a la compra del material necesario según la dimensión de la red y las características que se

requieran en cuanto a velocidad, tipos de conexiones, throughput, etc.

- Configuración de equipamiento en laboratorio: Recibido el material, se procederá a su configuración adaptándolo a la configuración actual o incluso realizando mejoras que se detecten durante la fase de análisis de la red actual.

- Diseño del plan de pruebas: Se diseña este plan de pruebas para validar que la solución se adapta a lo que se necesita y que se va en buen camino. A su vez servirá para detectar posibles errores de configuración, incompatibilidades entre tecnología actual y la futura o conexión que se puedan llevar a cabo en el momento en que entre en funcionamiento la nueva solución. Un dato importante a tener en cuenta es que, para que la migración tenga éxito, ambas tecnologías han de convivir durante un tiempo y ser compatibles con todo lo que hay actualmente configurado y conectado sobre la actual electrónica de red.

- Montaje e interconexión de equipos en CPDs: Una vez configurados, se instalarán e interconexionará todo el *hardware* que compone la solución SDN. Esta instalación se hará de forma totalmente aislada a la red actual y permanecerá así hasta el momento en que empiece la migración.

- Pruebas de entorno SDN: Se trata de una prueba concentrada en los elementos que componen la solución con el fin de certificar que todo está correctamente conectado, configurado y preparado para dar el paso a la migración.

- Migración de la red: Es el punto en el que se empieza a pasar todos los equipos desde la antigua electrónica a la nueva.

1.7. Tareas del TFG

Para la elaboración del TFG, básicamente se documentará cada uno de los puntos definidos en la propuesta de índice que se muestra al principio de este plan de trabajo, los cuales se detallan a continuación:

- Realizar propuesta de trabajo: Se trata de la confección del documento inicial en el que se explica por primera vez de qué trata el proyecto y cómo se va a ejecutar tanto en metodología como en tiempo.

- Estudio sobre soluciones SDN: Es la parte en la que se analizará las posibles soluciones que existen para sustituir la electrónica de red actual. Con el fin de no extender demasiado el documento, se analizarán las dos o tres opciones que más se adaptan a las necesidades actuales y futuras de la organización.

- Revisión y corrección: Será una tarea recurrente que se llevará a cabo cada vez que se tenga un feedback del profesor del TFG después de cada entrega. Con esta se pretende pulir aquellos puntos que haya que mejorar y corregir los errores cometidos durante todo el proyecto y así llegar a cada entrega, y por supuesto a la fecha de

entrega final, con un entregable que cumpla con los requerimientos mínimos.

- Análisis y documentación sobre red actual: Se documentará cómo está desplegada y configurada la red actual, apoyándonos en explicaciones sobre configuración y topología de red que pongan en contexto al lector del documento.

- Documentación sobre migración y pruebas de funcionamiento: Se documentará los pasos a seguir para que la migración sea satisfactoria sin que se produzca ningún fallo que comprometa al proyecto. También se explicarán las pruebas que se han de realizar para validar el funcionamiento de la solución en el entorno productivo.

- Preparativos y documentación de anexos y bibliografía: Se incluirá todo tipo de documentación (diagramas de red, documentación oficial del fabricante, etc.) que apoye o sirva de complemento a lo explicado en cada uno de los puntos que conforman el TFG.

- Conclusión final: Servirá para hacer una valoración sobre el proyecto en la que se indicará hasta qué punto el proyecto cumple o no con lo exigido, en qué punto se queda la red a nivel de despliegue y cuáles serán las siguientes fases a realizar en caso de que se quiera ampliar la red o incluir nuevos servicios sobre la red.

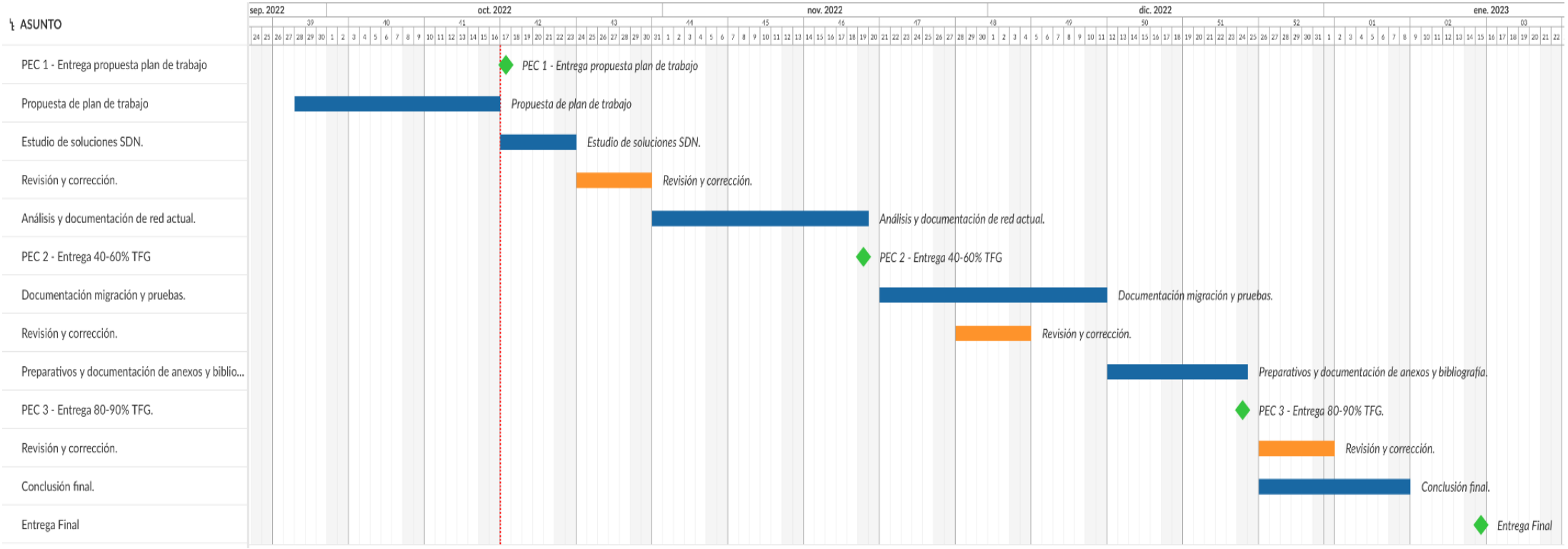
1.8. Cronograma del TFG

En el siguiente cronograma se indican las semanas de las que se dispone para hacer el TFG y las actividades que se van a llevar a cabo en cada una de ellas hasta llegar a la entrega final, la cual está planificada para el 15 de Enero de 2023:

	Semana	**Actividad**	**Comentario**
1	26 Sept - 02 Oct.	Inicio propuesta de plan de trabajo TFG.	
2	03 Oct. - 09 Oct.		
3	10 Oct. - 16 Oct.	Entrega propuesta de plan de trabajo TFG.	PEC 1
4	17 Oct. - 23 Oct.	Estudio de soluciones SDN.	
5	24 Oct. - 30 Oct.	Revisión y corrección.	
6	31 Oct. - 06 Nov.	Análisis y documentación de red actual.	
7	07 Nov. - 13 Nov.	Análisis y documentación de red actual.	

8	14 Nov. - 20 Nov.	- Análisis y documentación de red actual. - Día 19: Entrega 40-60% TFG.	PEC 2
9	21 Nov. - 27 Nov.	Documentación migración y pruebas.	
10	28 Nov. - 04 Dic.	- Revisión y corrección. - Documentación migración y pruebas.	
11	05 Dic. - 11 Dic.	Documentación migración y pruebas.	
12	12 Dic. - 18 Dic.	Preparativos y documentación de anexos y bibliografía.	
13	19 Dic. - 25 Dic.	- Preparativos y documentación de anexos y bibliografía. - Día 24: Entrega 80-90% TFG.	PEC 3
14	26 Dic. - 01 Ene.	- Revisión y corrección. - Conclusión final.	
15	02 Ene. - 08 Ene.	Conclusión final.	
16	09 Ene. - 15 Ene.	Día 15: Entrega Final, 100% TFG.	Entrega Final

1.9. Diagrama de Gantt del TFG



1.10. Recursos

Para la realización del TFG se dispondrá de los siguientes recursos:

- Ordenador iMac.
- Paquete ofimático de Google Suite.
- Diagramas de red.
- Documentación oficial de fabricantes (Anexo 1).

2. Estudio de soluciones SDN

2.1. Introducción al concepto SDN.

La tecnología *Software-Defined Network (*de aquí en adelante *SDN),* tal y como se entiende por su nombre, es un conjunto de técnicas que permiten el control y gestión de la red a través de un *software* que gestiona de manera centralizada todos los elementos de *hardware* que componen la red*.* Su principal objetivo es facilitar la implementación e implantación de servicios de red con un dinamismo y escalabilidad que hasta ahora no era posible con las redes basadas en *hardware* con gestión descentralizada*.*

2.2. Elementos de una solución SDN

Con el objetivo de tener una visión más exacta de los diferentes elementos que componen una solución SDN, a continuación se cita y explica el rol de cada uno de ellos:

- Controlador: Es el hardware en el que se instala el software de control de la solución SDN y viene a ser el “cerebro” de la red. Se trata de una serie de servidores que normalmente están dimensionados para evitar la pérdida de control de la red en caso de fallo de alguno de ellos.

- Software de control SDN: Se trata del *software* que decide, previa configuración a través de una API, qué se debe hacer con cada paquete de comunicación.

- Elementos de red: Es el *hardware* que se encarga de conmutar o enrutar, con switches de nivel 2 o 3 y/o routers, los paquetes a través de la red. También son identificados como nodos y se localizan en la capa de infraestructura.

- Aplicación de negocio: Es la aplicación o API que se suministra para gestionar el *software* de control. Está separada de todo el plano de control y sólo se utiliza para enviar órdenes de configuración o consultar estado de la red, no interviene en el funcionamiento normal de la red, sólo sirve para gestión.

2.3. Arquitectura SDN

Para conseguir una gestión centralizada, la tecnología SDN separa el plano de control del plano de datos y a su vez divide la arquitectura en las siguientes capas:

- Capa de aplicación: En ella residen todas las aplicaciones y/o recursos que permiten a los administradores la gestión de las comunicaciones. Mediante el uso de aplicaciones del tipo REST, JSON, XML, Java, etc. se simplifica y automatiza la configuración, provisión y gestión de los servicios de la red.

- Capa de control: Se trata del Sistema Operativo o *software,* que se instala en un ordenador central y en los elementos de *hardware*, con el que se tiene control exclusivo de los diferentes nodos de la red. Por otro lado, habilita la gestión de capacidades de la red de manera global, sin importar el tipo de topología o protocolos de red que se utilice, permitiendo así que se pueda llevar a cabo configuraciones y parametrizaciones de la red sin necesidad de tener un alto conocimiento de los equipos que conforman la red o sobre la configuración de protocolos de comunicaciones.

- Capa de infraestructura o datos: Son todos los elementos de *hardware* de la red y es la encargada de la conmutación y enrutamiento de los paquetes por todos los nodos. Estos elementos de *hardware,* generalmente switches de alta capacidad con SO sencillos, no contienen programas muy complejos en su implementación, de esta forma, delegando el plano de control, consiguen una menor latencia en la red y un mayor aprovechamiento de los recursos del propio *hardware*.

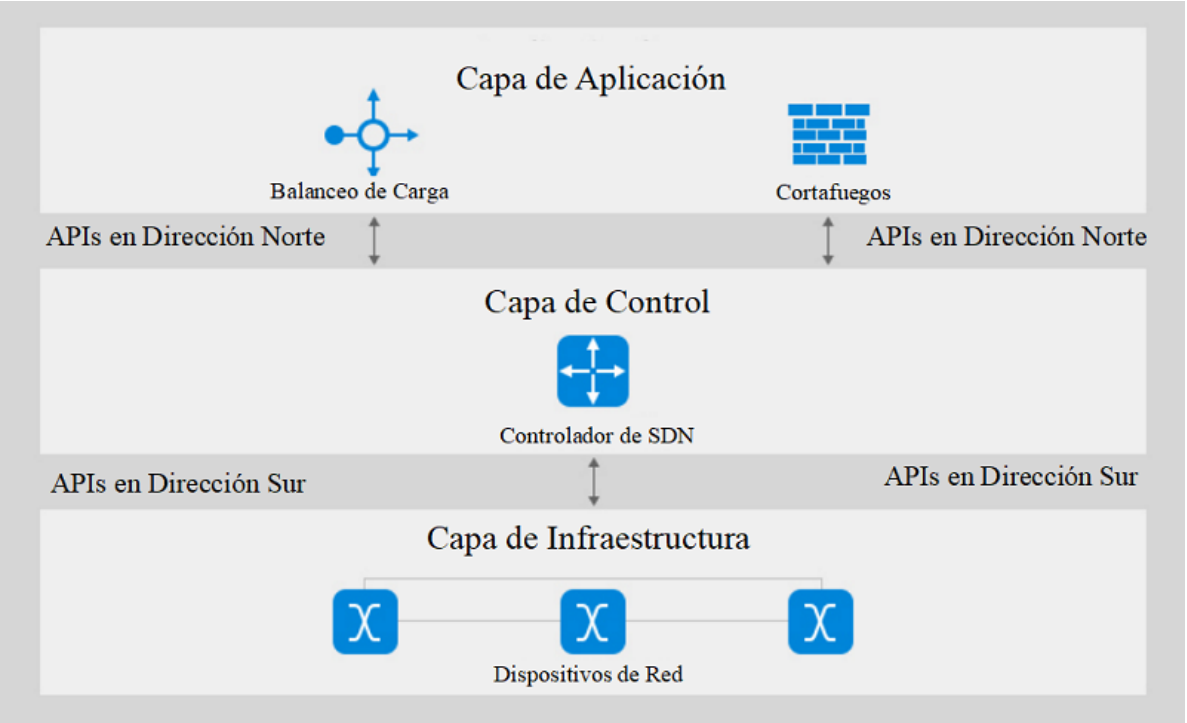


Figura 1 - Arquitectura SDN

Con esta separación por capas, los administradores de la red sólo actuarán sobre la capa de aplicación a través de un software específico desarrollado por el fabricante. Será esta capa de aplicación la encargada de comunicarse con la capa de control y a su vez esta última le enviará las órdenes necesarias a la de infraestructura para indicarle a los dispositivos de red qué hacer con los paquetes a través de la red.

La comunicación entre capas se realiza a través de interfaces API. Básicamente existen dos tipos:

- Northbound API: Interfaz que permite la comunicación entre las aplicaciones de negocio y la capa de control. Posibilita que la aplicación de negocio no se aloje en la misma máquina que el controlador. Gracias a esta comunicación se llega a obtener información en tiempo real del estado de la red y a su vez se envían órdenes hacia el controlador para que éste las procese antes de enviarlas hacia los elementos de red a través de la interfaz de *southbound*.

- Southbound API: Interfaz que se encarga de gestionar la comunicación entre el controlador y los dispositivos de red. Podemos afirmar que es en este punto donde se separa el plano de control del plano de datos. Para intercambiar toda la información entre ambos planos, se utiliza el protocolo OpenFlow, por lo que la electrónica de red que se emplee en la solución SDN ha de ser capaz de utilizar este protocolo. Con ello se delega todo el control y los elementos de red sólo han de cumplir las órdenes enviadas desde la capa de control y reportar hacia ésta cuando se le consulte cierta información desde capas superiores.

Con esta arquitectura todo el control de de los elementos de red reside en el software, de forma que cuando un elemento de *hardware* recibe un paquete éste no tiene conocimiento sobre cómo tratarlo y le pregunta al *software* para saber de qué manera transitar los paquete en la red.

El desplegar este tipo de tecnología tiene sus ventajas y desventajas. Como ventajas podemos destacar:

- **Sencillez de los equipos:** Se utiliza un *hardware* muy sencillo que delega toda la parte de control sobre el *software* de control SDN, consiguiendo así una dedicación plena de la electrónica de red en la conmutación o enrutamiento de los paquetes y liberación de procesos complejos.

- **Encaminamiento dinámico:** Con a la centralización del control de la red, se tiene la capacidad de encaminar el tráfico de los paquetes de manera más eficiente con un mayor aprovechamiento de los recursos que dispone la red, por ejemplo, utilizando enlaces con mayor capacidad de ancho de banda y disminuyendo así la latencia en las comunicaciones críticas de la entidad.

- **Escalabilidad de la red:** El hecho de tener una capa de control desvinculada de la electrónica de red, permite que la red sea muy escalable tanto para el aumento del número de dispositivos como para su reducción en caso de que haya que hacer alguna modificación en la topología de la red.

- **Versatilidad de la red:** Mediante la capa de aplicación se permite a los administradores de la red, a través de las APIs implementadas en la solución SDN, el despliegue de nuevos entornos o modificarlos en tiempo real y de manera cómoda, adaptando la red a las necesidades que se requiera en cada momento.

- **Monitorización de la red:** El propio *software* implementa una monitorización continua de los elementos y el tráfico de la red, lo cual permite que los administradores conozcan en todo momento el estado de la red y puedan tomar decisiones importantes en base a esta información, bien de manera proactiva o reactiva ante un problema que se presente en cualquier momento.

- **Ahorro de costos:** Al optimizar el uso de los recursos de la red de manera centralizada se reducen los costes de manejo de altos volúmenes de información.

Como desventajas podemos citar las siguientes:

- **Permisos Centralizados:** El hecho de que esté todo centralizado conlleva que la seguridad también resida en un único punto. Por ello los atacantes se centran en detectar las vulnerabilidades de este equipo y una vez dentro desde aquí poder tomar control de toda la red.

- **Centralización del control:** La esencia de SDN es que se centraliza toda la inteligencia del sistema en un único punto, lo cual puede suponer que ante una caída del centro de control, los demás elementos de la red perderían el plano de control y con ello la operatividad de la red.

Para evitar que los efectos mencionados en estas desventajas tengan lugar y afecten así al correcto funcionamiento de la solución SDN, existe una serie de técnicas como por ejemplo; la escalabilidad de permisos, *backups* automáticos*,* actualización continua del *software*, redundancia de controladores y elementos de red, etc. que dotan a la solución de una robustez que complementa las ventajas mencionadas anteriormente.

2.4. Soluciones candidatas para el despliegue

Con la tecnología SDN existen numerosas opciones de implementación, tanto libres como privadas. Por tratarse de un entorno bancario, el cual requiere un soporte continuo y está sometido a numerosas normativas a nivel europeo e internacional en cuanto a seguridad y cumplimiento del servicio, la opción de software libre se ha descartado desde un primer momento. Es por ello que se pasa directamente a valorar las diferentes opciones de fabricantes o marcas privadas que llevan consigo un soporte y mantenimiento que asegura el cumplimiento de los requisitos antes mencionados. Así pues, a continuación se enumera brevemente las soluciones consideradas antes de empezar el proyecto de migración:

- SDN Huawei: Se trata de una solución del fabricante Huawei basada en los conceptos básicos de las redes SDN explicados anteriormente. Se tuvo en cuenta la solución, pero al tratarse de un fabricante del cual no se disponía de ningún elemento de red instalado y tampoco había en el equipo de comunicaciones una experiencia sobre equipos de este fabricante que diera la confianza suficiente a la hora de gestionar estos equipos, se descartó esta opción.

- Aruba SDN: Se trata de una solución del fabricante Aruba basada en protocolos libres como OpenFlow lo cual le permite funcionar con equipos de diferentes fabricantes que admiten este protocolo. Desde el punto de vista del departamento de Comunicaciones se le daba más sentido a este fabricante para la red de campus, donde ya existe un parque bastante extenso de electrónica Aruba, que para el Core donde ya se tenía Cisco y por ello se desestimó su adquisición.

- Cisco ACI (*Application Centric Infrastructure*): Solución SDN del fabricante Cisco que se basa en la arquitectura presentada en la figura “2.3.1 - Arquitectura SDN”. A parte de utilizar el protocolo libre OpenFlow, también se apoya en su protocolo propietario CDP (Cisco Discovery Protocol). Los equipos que componen la infraestructura han de ser del propio fabricante y esto, junto con el expertise del equipo técnico en los diferentes elementos de red de Cisco, fue fundamental para elegir esta opción como la idónea para llevar a cabo la migración del Core de la red a una solución SDN. Otro de los puntos importantes por el que se decidió elegir este fabricante, es porque la experiencia con el soporte técnico de Cisco, ante las múltiples implementaciones, incidencias y anteriores migraciones que ha habido en la red, ha sido muy buena. Desde un primer momento se era consciente de que se contaba con un soporte competente que daba toda la confianza necesaria para llevar a cabo la migración a SDN.

Cada una de las soluciones de estos fabricantes se puede consultar con más detalles en los enlaces proporcionados en “***Anexo 1 - Documentación de fabricantes***”.

2.5. Solución elegida: Cisco ACI

Como ya se ha comentado antes, la solución del fabricante Cisco ya contaba con cierta ventaja por parte del departamento de Comunicaciones del banco. Concretamente el departamento estaba muy interesado en la solución Cisco ACI (*Application Centric Infrastructure*), la cual hace especial enfoque en contrarrestar las desventajas mencionadas en el punto “2.1 introducción al concepto SDN”. Especialmente destacan las siguientes ventajas que a su vez los diferencia de otros fabricantes:

- **Seguridad:** A través de una monitorización continua desde su centro de soporte, Cisco se encarga de detectar e implementar las últimas actualizaciones de seguridad o vulnerabilidades detectadas en todos los equipos que componen la arquitectura SDN.

- **Integración con otros entornos:** Permite la integración con entornos virtualizados como *VMWare, Microsoft y OpenStack, etc.* haciendo que éstos se comporten como si fuesen un componente más de la red y posibilitando así su gestión desde la propia aplicación de Cisco ACI; Cisco APIC (*Application Policy Infrastructure Controller*).

- **Interfaz gráfica de gestión centralizada:** Permite gestionar la solución SDN desde una interfaz web que actúa sobre el APIC. Este APIC está compuesto por unos controladores -servidores físicos- sincronizados en todo momento que tienen el rol de configurar, gestionar y monitorizar todos los elementos que componen la red.

- **Redundancia de nodos de control:** Para asegurar el servicio de gestión en todo momento, Cisco ACI requiere la existencia de al menos tres controladores. Uno de ellos será designado como el nodo principal y los otros dos se categorizan como de respaldo. La configuración y cualquier modificación que se realice está sincronizada en todo momento entre los tres nodos. De esta manera siempre habrá un equipo disponible en caso de caída del nodo principal o secundario.

- **Copias de seguridad automatizada:** La solución de Cisco ACI realiza backups automáticos cada cierto tiempo y siempre que se realiza alguna modificación en la configuración. De esta manera se asegura la posibilidad de remediar rápidamente cualquier impacto negativo a causa de una configuración errónea y además se tiene un versionado completo de todas las configuraciones realizadas durante un tiempo determinado.

Como desventaja o puntos a tener en cuenta, podemos citar los siguientes:

- **Equipamiento específico:** Al ser una solución propietaria, ésta sólo funciona con un equipamiento del mismo fabricante y electrónica de red concreta; switches Cisco Nexus de la familia 9000. Además este modelo de switches tiene un coste muy elevado en comparación con la electrónica basada en Cisco IOS que es la que se tiene en producción antes de la migración; punto importante a tener en cuenta de cara al presupuesto.

- **Licenciamiento:** Puesto que la solución es propietaria de Cisco y los elementos de red también son de la misma empresa, ésta se asegura que todos los elementos se integren correctamente en la arquitectura SDN a través de un licenciamiento. Sin licencia los equipos no son capaces de reconocerse y vincularse a los controladores de la red, por lo que sin ella no son funcionales; son simples “cajas tontas”.

2.5.1. Introducción a Cisco ACI

Como ya se ha comentado, Cisco ACI se basa en la estructura tipo de una red SDN, separando su arquitectura en las capas de aplicación, control e infraestructura.

En la capa de aplicación utiliza el software de gestión a través de una interfaz web. Esta interfaz web utiliza una API que actúa sobre el APIC ya mencionado en el apartado anterior. Al acceder a la web de gestión se presenta un portal donde se ha de loguear el administrador que quiere tener acceso, tal y como se muestra en la siguiente imagen:

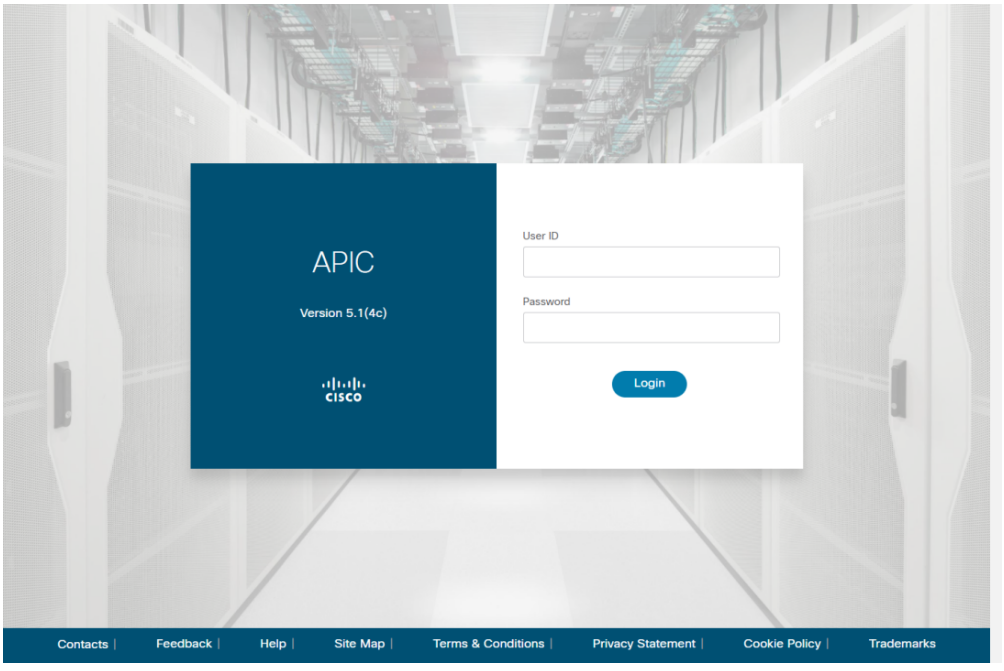


Figura 2 - interfaz web APIC.

Una vez logueado el usuario, éste puede navegar por los diferentes módulos que permiten realizar acciones de configuración, gestión, sobre el sistema, los tenants, el fabric, etc.

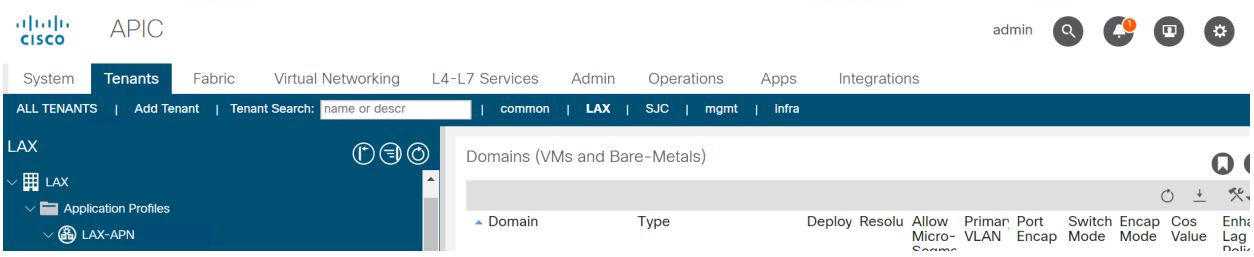


Figura 3 - Secciones de interfaz web APIC.

Como elementos de **la capa de control** están los controladores específicos de Cisco llamados “APIC Controller”. Estos tienen toda la inteligencia para controlar y gestionar los nodos de la red. El *software* de estos controladores permite que la gestión se pueda llevar a cabo bien por la interfaz web o a través de una consola *CLI (Command Line Interface)* con comandos que desencadenan acciones específicas a enviar hacia la electrónica de red.

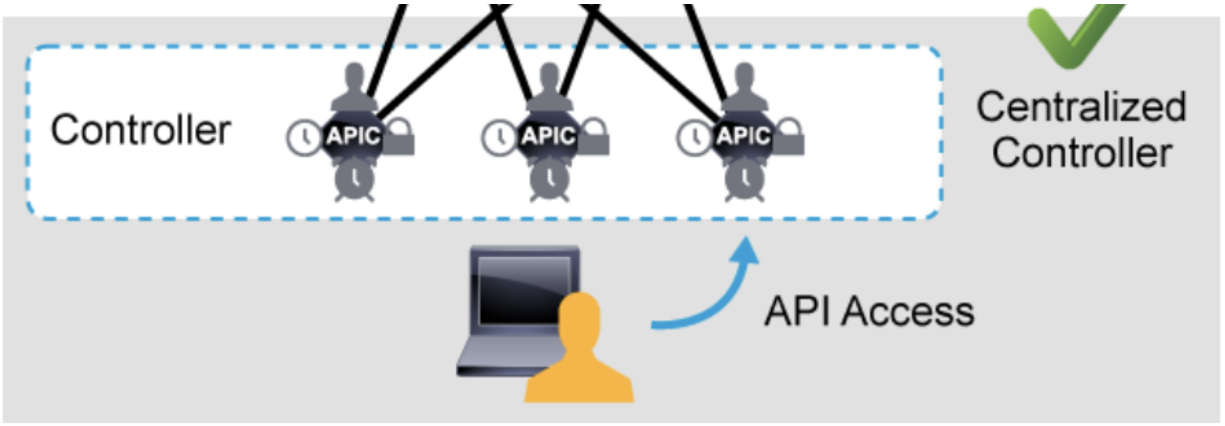


Figura 4 - Gestión unificada del APIC.

En nuestro caso, el APIC está formado por un total de cuatro servidores Cisco APIC M3/L3 sincronizados entre ellos. La conexión a la red de cada uno de los servidores se hace de manera redundada con un doble enlace hacia los *Leafs* (más adelante se explica qué es un *Leaf*) a través de los puertos del Bond0 y a parte se habilita una conexión OOB (Out Of Band) por los puertos del Bond1 para su gestión o mantenimiento desde una red diferente a la de datos llamada comúnmente MGMT (Management). Tal y como se puede apreciar en la siguiente imagen, las conexiones redundadas tienen un puerto en activo -línea continua- y otro de backup -línea discontinua-.

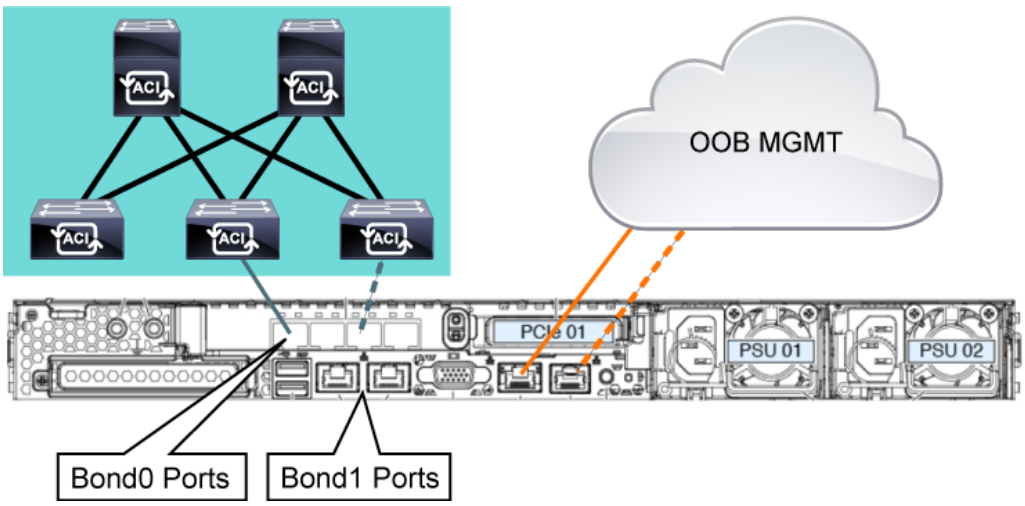


Figura 5 - Conexión a la red de los APICs Servers.

Aunque el cluster del APIC está formado por cuatro servidores, en realidad los que prestan el servicio son tres y uno se queda en *Stanby.* Como requerimiento mínimo, Cisco específica que ha de existir siempre tres servidores prestando el servicio y uno o dos como *standby*. Los tres que están operativos se reparten la carga de trabajo de manera sincronizada y en caso de fallo de uno de los tres, el cuarto entra en acción sin necesidad de acción humana ni configuración alguna.

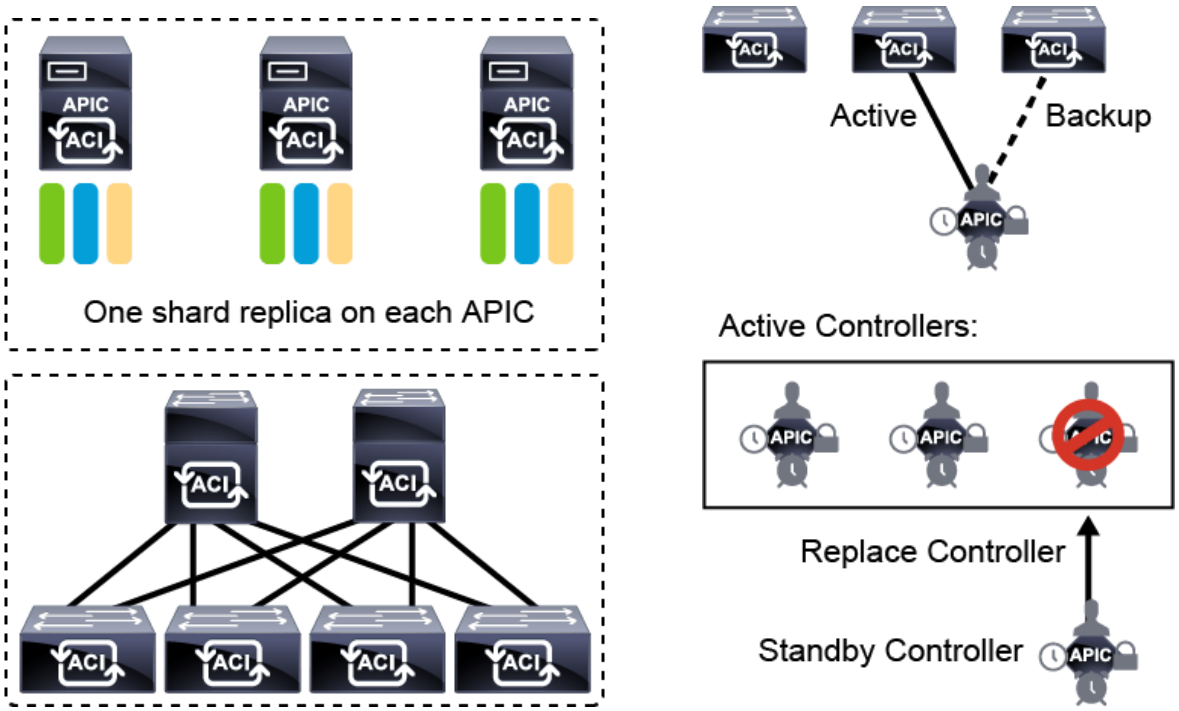


Figura 6 - Replica de BD y roles de los APIC Servers.

En cuanto a **la capa de infraestructura,** está compuesta por los switches Cisco Nexus de la serie 9000 pero con *software* ACI en vez de NX-OS. Como elemento diferenciador, en la solución Cisco ACI la capa de infraestructura a su vez se subdivide

en dos con los siguientes elementos:

- Spines: Switches que hacen el rol de agregadores e interconectan a todos los de la capa de acceso (Leafs) a través de ellos.

- Leafs: Switches de acceso a los cuales se conectan los equipos finales del CPD: servidores, firewalls, balanceadores, etc.. La función principal de estos switches es enviar los paquetes hasta otro Leaf a través de los Spines a los que se conectan.

Figura 7 - Distribución de Spine y Leafs

Una de las premisas de la solución Cisco ACI es que no se permite la conexión física de *Leaf* a *Leaf* ni de *Spine* a *Spine*. Cada uno de los *Spine* tiene un enlace físico hacia cada *Leaf* existente en la red y con ello se consigue que:

- Todo equipo conectado a dos *Leaf,* en caso de caída de cualquier nodo de la red, tenga siempre al menos un activo. Ante este tipo de situación la red se autogestiona y encamina los paquetes por los enlaces disponibles hasta llegar al *Leaf* donde se encuentra el destino del paquete.

- Todo equipo conectado a la red ACI tiene una distancia máxima de 4 saltos con su destino (Origen→Leaf, Leaf→Spine, Spine→Leaf, Leaf→Destino). Esto hace que la infraestructura ACI sea conocedora en todo momento de la latencia existente en la red y gestione mejor la conmutación de los paquetes en función de esta.

Así pues, gracias a esta topología y modelo de gestión, con Cisco ACI el departamento de Comunicaciones pasa de tener una red compleja y de difícil gestión a otra más escalable y completamente gestionable desde un solo punto; Cisco APIC.

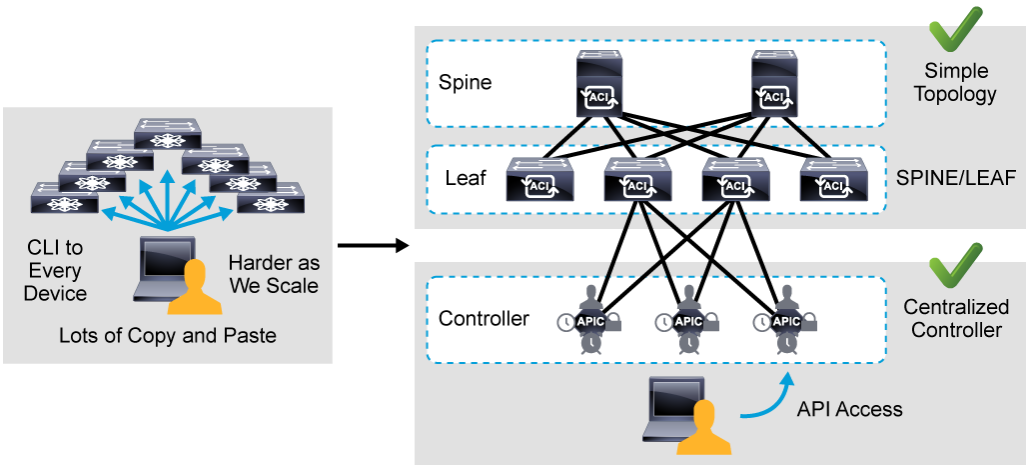


Figura 8 - Topología y gestión actual vs Cisco ACI

2.5.2. Tipos de despliegues en ACI.

Debemos de tener en cuenta que físicamente todos estos elementos pueden estar localizados en un solo CPD o en varios. Para identificar a los diferentes elementos y su ubicación, Cisco ha normalizado las siguientes nomenclaturas que nos serán útiles para comprender a qué se hace referencia cuando se nombren en los siguientes puntos del documento:

- *Pod*: Se refiere a la ubicación física en la que están instalados los *Spines* y *Leafs*, viene a ser lo que comúnmente se conoce como CPD (Centro de Procesamiento de Datos). Pueden haber tantos como la empresa tenga desplegados -tantos físicos como en cloud- y cada uno de ellos tiene su propio plano de control en cuanto a los protocolos de IS-IS, BGP, COOP, etc.

- *Fabric:* Es el conjunto que componen todos los Pods que forman la infraestructura ACI y se considera como un ente único que es gestionado en su totalidad por el APIC.

Así pues, teniendo en cuenta esta terminología, en función del número de CPDs con el que cuente la empresa, la solución se puede desplegar con las siguientes topologías:

- Single APIC Cluster/Single Domain: Existe un cluster de APIC único para todos los *Pods* que componen el *Fabric*. Toda la gestión se hace desde el APIC (vía web) y las políticas que se definan en él serán aplicadas a todos los elementos distribuidos en los diferentes *Pods* que componen el *Fabric.* A este tipo de despliegue también se le llama Multi-Pod y es el que se aplica en nuestro caso.

- Multiple APIC Cluster/Multiple Domains: Se caracteriza por tener un cluster de APICs en cada CPD que gestiona su propio *Fabric* de manera independiente.

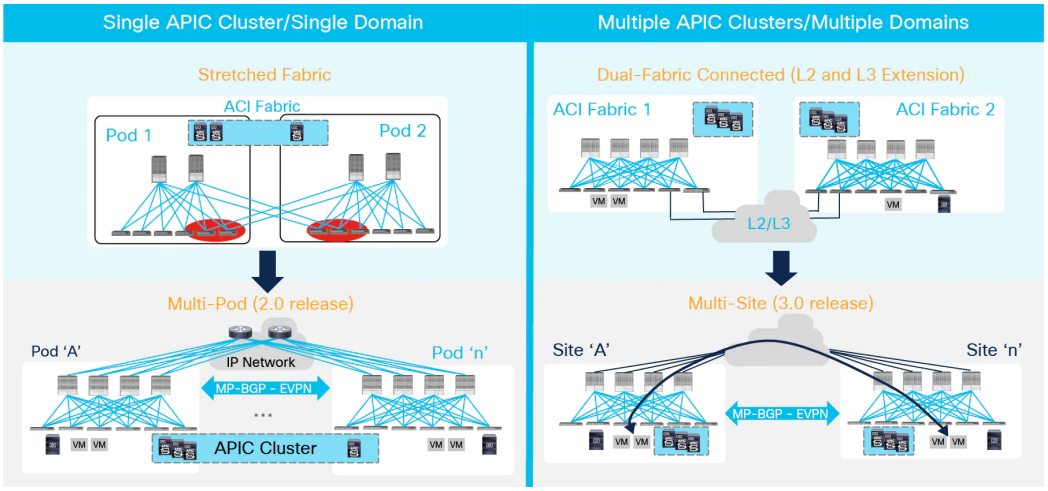


Figura 9 - Tipos de despliegues en ACI.

3. Análisis de red actual de Core

En este punto se explica la red de Core que se va a migrar, entrando en detalles sobre los elementos que la componen, explicando el tipo de topología y el despliegue de los equipos. La idea es que este capítulo sirva para poner en contexto el escenario que se va a migrar y se tenga en cuenta la complejidad que supone llevar a cabo la migración a una nueva red basada en SDN.

3.1. Topología de la red de Core actual

Actualmente la topología de la red de Core es de tipo estrella. Hay una pareja de switches C6500, uno en cada CPD e interconectados por fibra oscura (DWDM), que hacen de nodos principales. Estos se encargan de enrutar y conmutar todos los paquetes de las comunicaciones que se establecen a través del Core. A parte de tener funcionalidad de capa 2 y 3, también tienen configuradas ACLs para descartar o permitir ciertas conexiones hacia según qué entorno.

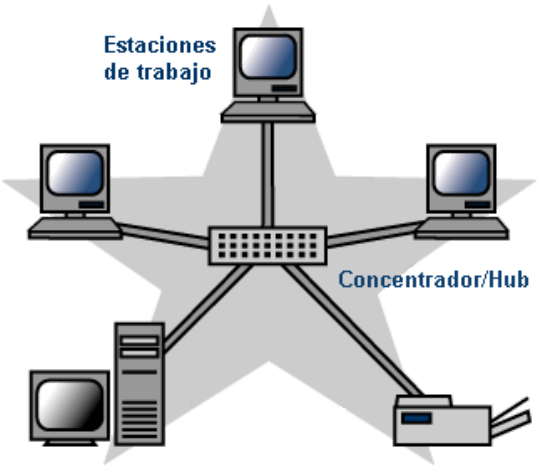


Figura 10 - Ejemplo de topología en estrella.

Hace unos años esta electrónica y topología de red era más que suficiente para el funcionamiento del banco, pero con el paso de los años y la continua demanda de nuevos servicios de red, y con ello la necesidad de disponer de mayor ancho de banda, se ha tomado la decisión de migrar este modelo a un entorno que cumpla con todos las necesidades de las comunicaciones de hoy en día y que a su vez permita continuar evolucionando con las exigencias futuras.

3.2. Equipamientos que componen la red actual.

La red actual está compuesta por múltiples dispositivos que tienen una función específica en el funcionamiento diario de la entidad. Estos equipos están ubicados lógicamente en segmentos de red diferenciados tanto a nivel 2 -con sus *Vlans IDs* correspondientes- como a nivel 3 -con direccionamiento IP-. Algunos de estos equipos son:

- **Servidores:** Se trata de ordenadores físicos y virtualizados que albergan las aplicaciones de gestión o del negocio de la empresa.

- **Clientes:** Ordenadores corporativos, físicos y virtuales, que consumen las aplicaciones antes citadas para el trabajo diario.

- **Cabinas de almacenamiento:** Equipos que contienen grandes *cabinets* de almacenamiento donde se guarda toda la información y BDs del banco.

- **Switches Core:** Conjunto de switches Cisco 6500 que hacen de punto neurálgico de la red. Estos se encargan del enrutamiento y/o conmutación de todos los paquetes que trasiegan la red del banco.

- **Firewalls:** Equipos de seguridad que protegen la red del banco frente a posibles ataques. Se dispone de varios dispuestos en diferentes zonas para garantizar la seguridad tanto de equipos expuestos al exterior como aquellos que pueden verse comprometidos por un ataque procedente de la red interna.

- **Cajeros**: Están desplegados en oficinas remotas o en puntos específicos donde hay uno instalado para poder dar servicio a los clientes, pero su comunicación pasa por el Core y por ello se tienen en cuenta como un tipo de equipamiento que está presente en la red.

Todos estos equipos establecen sus comunicaciones a través del Core y son vitales para el negocio.

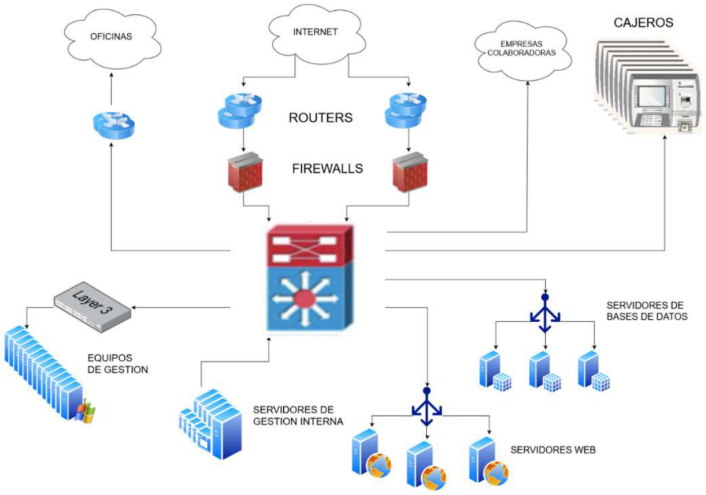


Figura 11 - Ejemplo del equipamiento que compone la red actual

Debido a la importancia de estos equipos, y para prevenir cualquier tipo de incidencia que pueda suponer un perjuicio para los intereses del banco, todos han de estar redundados para que en caso de fallo el servicio se continúe prestando en todo momento.

Para conseguir esta redundancia tanto a nivel lógico como físico, se cuenta con dos CPDs físicos que tienen toda la estructura replicada. De esta forma, en el caso de que en el CPD1 -"Edificio-Principal"- haya algún problema que le impida continuar prestando el servicio, el CPD2 -"Edificio-Secundario"- entra en funcionamiento. Esta redundancia se consigue interconectando los equipos a través del enlace de *DWDM* -más adelante se explica de qué se trata- y aplicando configuraciones de alta disponibilidad en los siguientes equipos considerados como los más importantes:

- **Firewalls:** Están instalados en modo Stack activo/pasivo de manera que cada uno de ellos, los perimetrales e internos, tienen su homólogo en el otro CPD.

- **Routers externos:** Instalados de forma que existe una pareja en cada CPD. Esta pareja está compuesta por un router de dos ISPs diferentes. De esta forma se consigue redundancia tanto a nivel de equipamiento como a nivel de operador.

- **Balanceadores:** Al igual que los *firewalls*, están instalados en modo Stack con rol activo/pasivo.

- **Servidores de aplicaciones:** Tanto los físicos como los virtuales están redundados y pueden funcionar tanto en el CPD1 como en el CPD2 en función de la necesidad del negocio ya que están conectados a un balanceador que permite dicha funcionalidad.

- **Switch principal:** Se trata de una pareja de switches C6500 por cada CPD que forman un VSS (Virtual Switching System). Gracias a la funcionalidad del VSS la pareja de switches se comporta como si fuese uno único, pero en caso de fallo del VSS principal, por ejemplo, entra en funcionamiento el secundario por la configuración de HSRP que existe entre las parejas de cada CPD.

Para conseguir la comunicación entre las parejas de los elementos comentados, existe una conexión de "fibra oscura" (DWDM - Dense Wavelength Division Multiplexing, ofertado por operador) entre los dos CPDs que a su vez tiene redundancia de equipos y trayecto de la fibra óptica, de forma que el funcionamiento está asegurado en caso de que el operador que presta este servicio tenga un problema en cualquiera de los puntos de la red.

A continuación se muestra un esquema a alto nivel donde se puede apreciar cómo queda distribuida esta redundancia física de todos los elementos comentados:

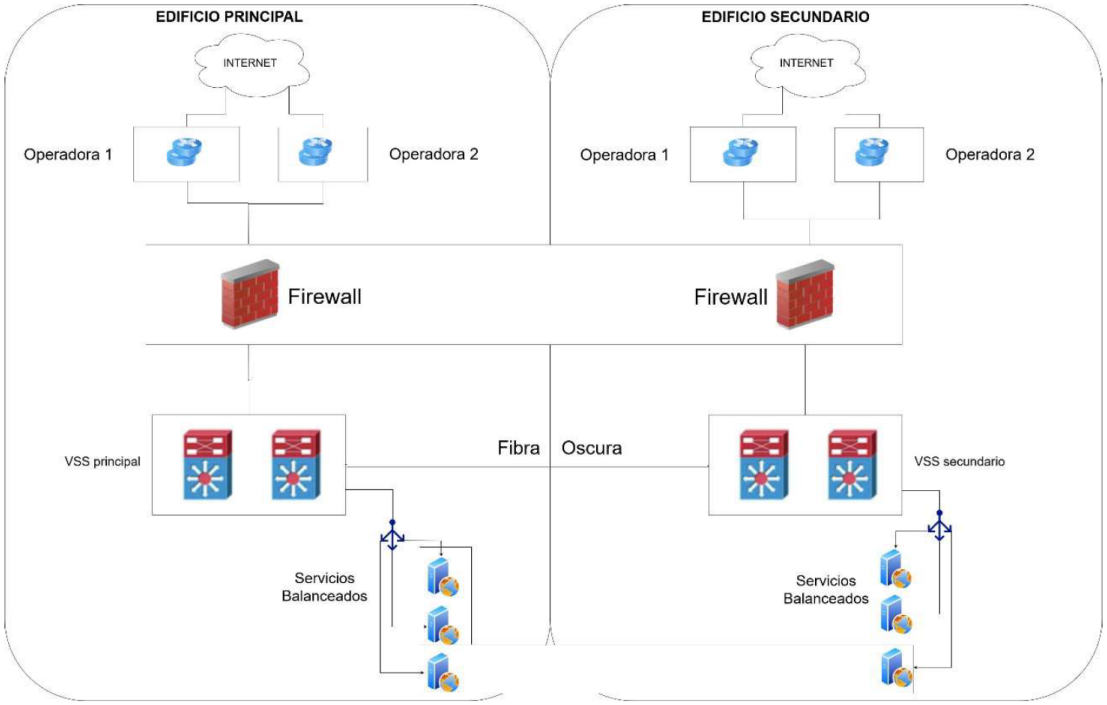


Figura 12 - Entornos redundados actualmente.

3.3. Consideraciones a tener en cuenta antes de la migración.

El objetivo de este apartado es recopilar, a modo de resumen, todos los puntos importantes que se han de tener en cuenta de cara a la migración futura de la red de Core, los cuales son los siguientes:

- La topología de red es de tipo estrella.
- Se dispone de dos CPDs en ubicaciones diferentes y unidos por fibra bajo la modalidad de DWDM.
- Los equipos que sustentan el servicio y negocio están redundados.
- Los servicios internos están separados tanto a nivel 2 como a nivel 3.
- Se dispone de enrutamiento estático configurado en los C6500.
- Todos los equipos de los CPDs son gestionados a través de una red de gestión diferenciada de la red de datos (OOB).

4. Migración a infraestructura ACI.

El objetivo de este capítulo es explicar la manera en la que se va a llevar a cabo la migración a lo largo del proyecto, durante la cual se ha de dedicar especial importancia a la seguridad, al control de los procesos y la continuidad del negocio.

4.1. Configuración y aspectos técnicos a tener en cuenta.

Para poder entender mejor las cuestiones técnicas de la solución Cisco ACI, antes de entrar en detalles de la migración, se considera importante conocer los conceptos básicos de configuración de este entorno. En Cisco ACI el concepto de Vlan no existe, lo más parecido son los *EPGs* (End Point Groups), los cuales se configuran a nivel de *Fabric* y se asocian a los puertos de los *Leafs.* Estos *EPGs* son agrupados en *BDs* (Bridge Domains) que vienen a ser agrupaciones de puertos. A su vez los BDs se juntan con VRFs (Virtual Routing and Forwarding) a través de los cuales se permiten las comunicaciones a nivel 3 entre los diferentes *BDs*. A continuación se muestra una imagen que ayuda a entender estos conceptos visualmente:

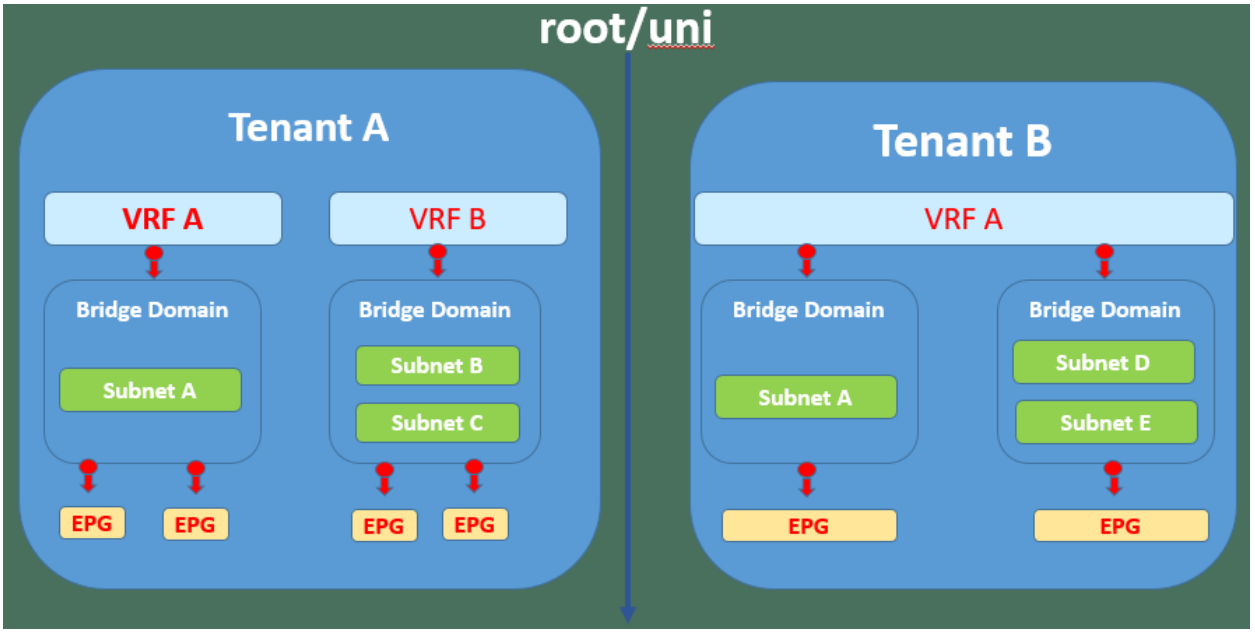


Figura 13 - Asociación gráfica de EPG, BD y VRF.

Teniendo en cuenta estos conceptos, la recomendación del fabricante a la hora de migrar, es crear un *EPG* por cada máquina que se desea migrar y un *BD* por *Vlan* que agrupa a todos los *EPGs* de la Vlan existente en la red actual. En caso de que sea necesario routing entre diferentes Vlans, se creará un VRF que permitirá la comunicación entre los diferentes BDs.

En este punto, aplicando la configuración básica, los equipos migrados serían capaces de comunicar entre todos ellos sin ningún elemento de restricción como sí existe en los equipos actuales C6500 (a través de ACLs - *Access List*). Para evitar esta brecha de seguridad, la solución de Cisco ACI nos permite utilizar las siguientes funcionalidades:

- Contratos: Son políticas que se aplican a los *EPGs* y en función de su configuración (reglas) permiten la comunicación o no con otros *EPGs*. A modo de ejemplo, es como si se configura una regla de firewall en la que sólo se permite la comunicación entre dos *EPGs* a través de un puerto concreto.

- Perfiles de aplicación: Es un perfil en el que se definen las políticas, servicios y relaciones entre los *EPGs*.

- Etiquetas: Nombres que se le pueden asociar a los objetos creados en ACI para poder catalogarlos correctamente.

- Filtros: La solución de ACI permite crear filtros desde la capa 2 hasta la capa 4.

Aplicando estas medidas de seguridad conseguiremos que la nueva red se comporte igual que la actual, de forma que todos los entornos continúen securizados y se haga el

proceso de migración con todas las garantías de que los equipos migrados no quedarían expuestos a entornos que no interese.

4.2. Proceso de migración.

Tal y como se ha indicado en el punto “2.5.2 Tipos de despliegues en ACI”, el tipo de despliegue que se va a emplear es un “Multi-Pod” con la modalidad de *Network Centric (ACI basado en red previo a evolución a Application Centric)*. Con esta modalidad cubrimos los dos CPDs físicos que tiene actualmente el banco, los cuales se comunican entre sí por *DWDM*, tipo de conexión que cumple con las recomendaciones de Cisco para asegurar los tiempos de latencias máximos y tasa de velocidad que requiere este tipo de despliegue.

Como ya es sabido, una de las premisas del proyecto es que no se ha de interrumpir el servicio en ningún momento y que ambos entornos, actual y Cisco ACI, sean capaces de convivir durante el periodo de migración. Para cumplir con este requerimiento se decide programar varias ventanas de intervención en las que se asegurará en todo momento la posible vuelta atrás en caso de que se detectase un fallo de configuración o conexión al migrar cualquier equipo al nuevo entorno. A su vez se ha dividido la migración en las siguientes fases:

- Fase de conexión a nivel físico de los elementos de red.
- Fase de migración a nivel 2 de la comunicación.
- Fase de migración a nivel 3 de la comunicación.
- Fase de migración a nivel físico de los equipos finales.

En cada una de las fases indicadas, se ejecutan pruebas de funcionamiento que aseguran el correcto funcionamiento. Estas pruebas se detallan en “***Anexo 3 - Pruebas de funcionamiento”*** del documento.

4.2.1. Fase de conexión a nivel físico de los elementos de red.

El objetivo de esta fase es conectar a nivel físico todos los elementos de la nueva infraestructura Cisco ACI con la red antigua. Para ello se subdivide la fase en dos partes; una primera parte se dedica para la instalación e interconexión de todos los elementos del *Fabric* y en una segunda, una vez esté en funcionamiento la infraestructura ACI en ambos CPDs, se conectarán las dos infraestructuras, antigua y nueva, para que convivan mientras se hace la migración.

La primera parte se inicia con la instalación de los elementos de red y servidores en los *racks* destinados para tal fin en cada CPD. Luego se conectan de tal manera que se cumpla la premisa comentada en el punto ”2.5.1 Introducción a Cisco ACI”; no se permite la conexión física de *Leaf* a *Leaf* ni de *Spine* a *Spine*. Cumpliendo con todo ello, el esquema a alto nivel de la conexión a nivel 2 ó físico queda como se muestra en la siguiente imagen:

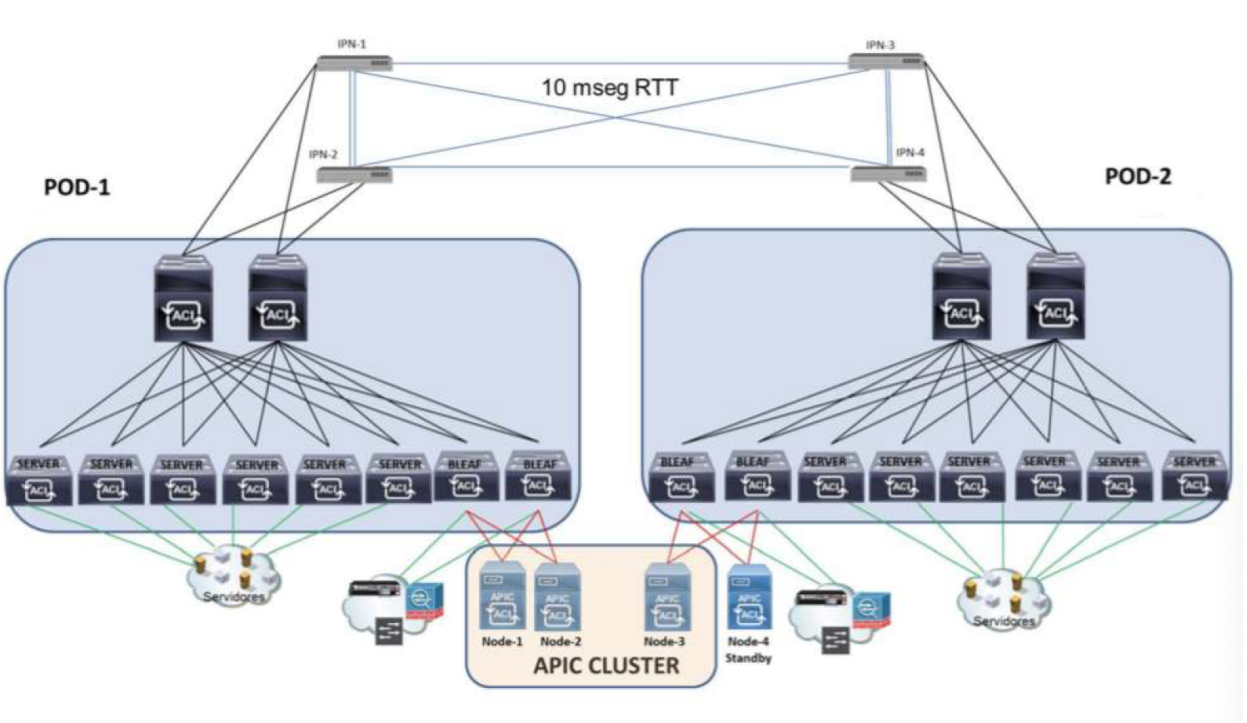


Figura 14 - Conexión de elementos del Fabric.

En la figura 14 se puede ver cómo se interconecta todo el fabric, los servidores de la empresa en ambos CPDs que van conectados directamente a los *Leafs* para que a través de los *Spines* comuniquen con otros *Leafs* del mismo *Pod* y si fuese necesario comunicar con el otro *Pod* (por ejemplo del *Pod-1* hacia el *Pod-2*) se utilizaría la conexión que existe a través de los *IPNs* por el DWDM.

Con el *Fabric* en funcionamiento, ahora se ha de pasar a la segunda fase de este apartado; interconexión entre infraestructura antigua y la nueva. La conexión se hace utilizando los VSS y dos *Leafs* de cada CPD. De cada VSS se harán cuatro conexiones físicas con el Fabric de ACI, de forma que dos de estas vayan hacia un Leaf y otras dos a otro Leaf diferente. En total serán ocho conexiones físicas -cuatro en cada CPD- que en realidad suponen dos lógicas ya que se configura un *VPC* (Virtual Port Channel) por cada conexión entre ACI y los VSS. Con el *VPC* se consigue tener tanto redundancia física como mayor ancho de banda en el enlace entre ambos entornos puesto que se aprovechan cuatro conexiones físicas de 1Gbs para convertirlas en una lógica de 4Gbs.

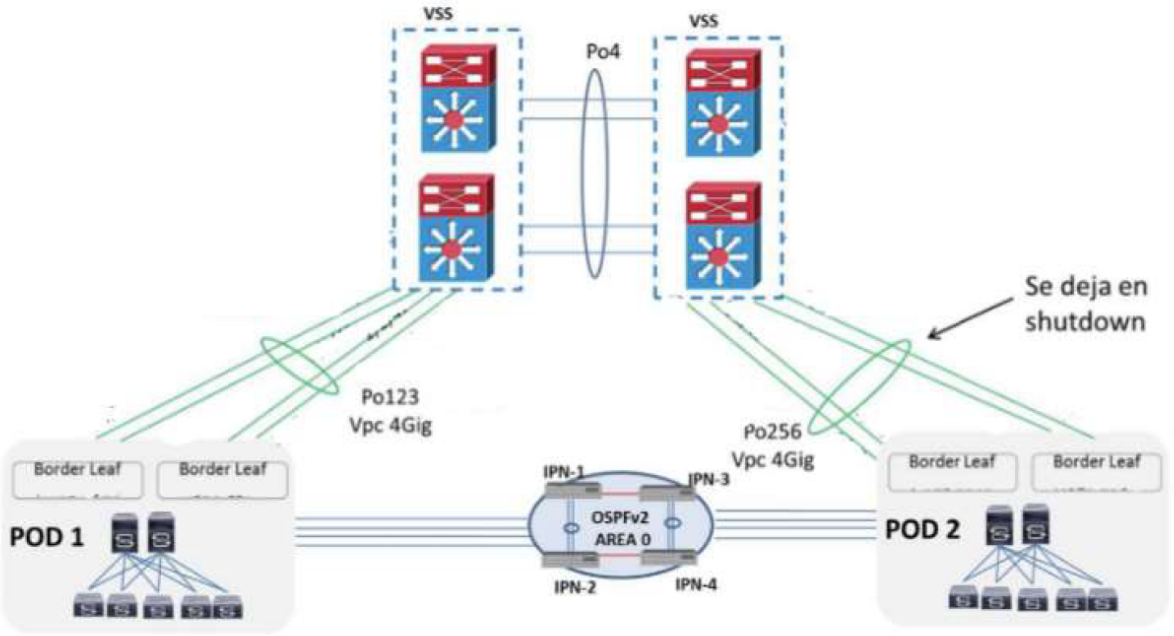


Figura 15 - Conexión entre infraestructura antigua y ACI

Tal y como se puede observar en la figura 15, para evitar cualquier tipo de bucle de nivel 2 en la red (aunque más adelante se configura *STP, Spanning Tree Protocol*), se deja uno de los VPC deshabilitado -concretamente el VPC256 del Pod-2- y así tener más controlado el entorno y evitar cualquier tipo de incidencia que pueda propagarse hacia la red en producción.

4.2.2. Fase de migración a nivel 2 de la comunicación.

Una vez que ambas infraestructuras están comunicadas a nivel físico, ahora es el momento de habilitar la comunicación a nivel 2. Se trata de progresar todas aquellas Vlans que se están utilizando en la red antigua hacia la nueva red de ACI, de manera que cuando se conecten los equipos finales en los *Leafs*, estos puedan comunicar a nivel 2 con los que aún existen en la red antigua.

Antes de configurar las Vlans y propagarlas por los enlaces habilitados, primero se configura *STP*. Con ello se consigue eliminar cualquier posibilidad de que se produzca un bucle en la red que pueda afectar al servicio y a su vez se garantiza que la red converja rápidamente ante un cambio de topología. Para tener un mayor control del tráfico, se configuran diferentes costes para cada uno de los enlaces, de forma que en el edificio principal se tendrá un menor coste que en el secundario y así tener este camino como el principal a la hora de comunicar con la infraestructura de ACI.

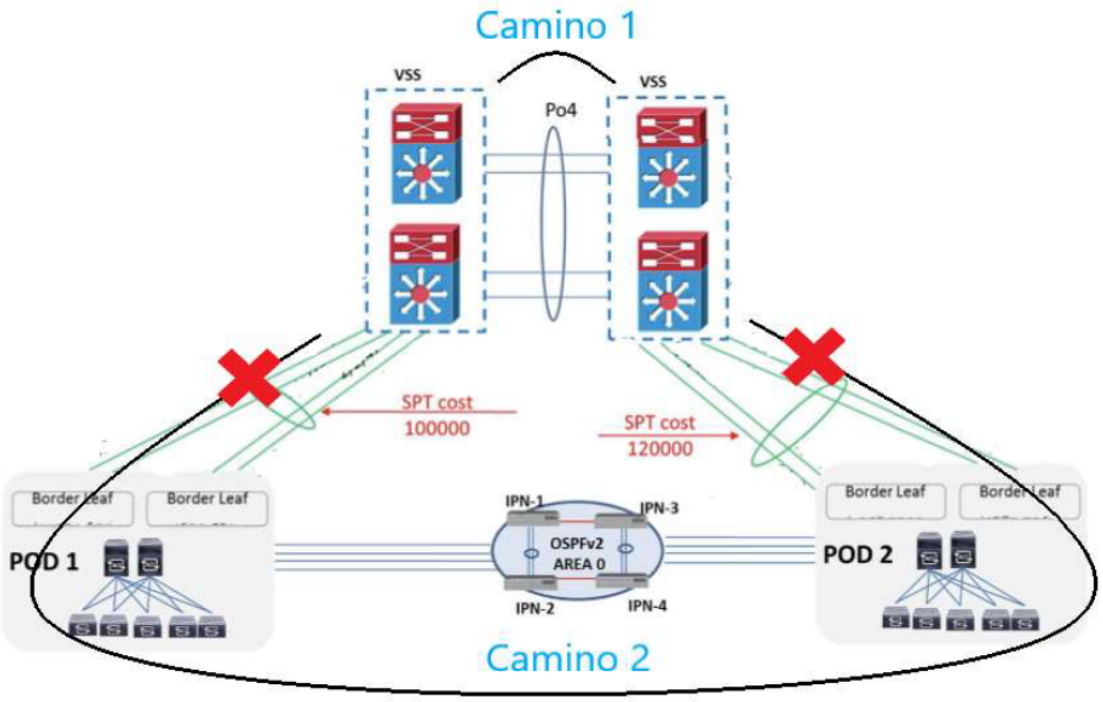


Figura 16 - Costes de STP configurados en los enlaces.

Tras tener lista la configuración de STP, se configuran en ACI y los VPC las Vlans que se están utilizando en la red antigua y con ello se deja preparado el entorno para que haya comunicación a nivel 2 entre todos los equipos independientemente de donde estén conectados.

4.2.3. Fase de migración a nivel 3 de la comunicación.

Conseguida la comunicación a nivel 2, se ve necesario hacer lo mismo con la comunicación a nivel 3.

Para que ambas infraestructuras tengan conocimiento de las redes que residen en cada una de ellas, y así poder enrutar el tráfico correctamente hacia donde corresponda, se configura el protocolo de enrutamiento dinámico *OSPF (Open Shortest Path First).* Con la configuración de *OSPF* se consigue que tanto ACI como los VSS tengan conocimiento de las redes y rutas estáticas que residen en cada entorno a través de los anuncios que comparten. Así mismo, es importante recalcar que en la parte de ACI, se configuran los *L3Outs* correspondientes en cada una de las interfaces que conectan con entornos externos al *Fabric* donde se espera tener este tipo de anuncios o comunicación a nivel 3, como es el caso del enlace con los VSS.

Durante todo el proceso de migración es necesario tener un alto control sobre el enrutamiento y la redistribución de las rutas estáticas, para ello se hace uso de las funcionalidades de *prefix-list y route-map* en los VSS que nos permitirán tener controladas cuántas y qué rutas redistribuir y/o aprender en cada entorno.

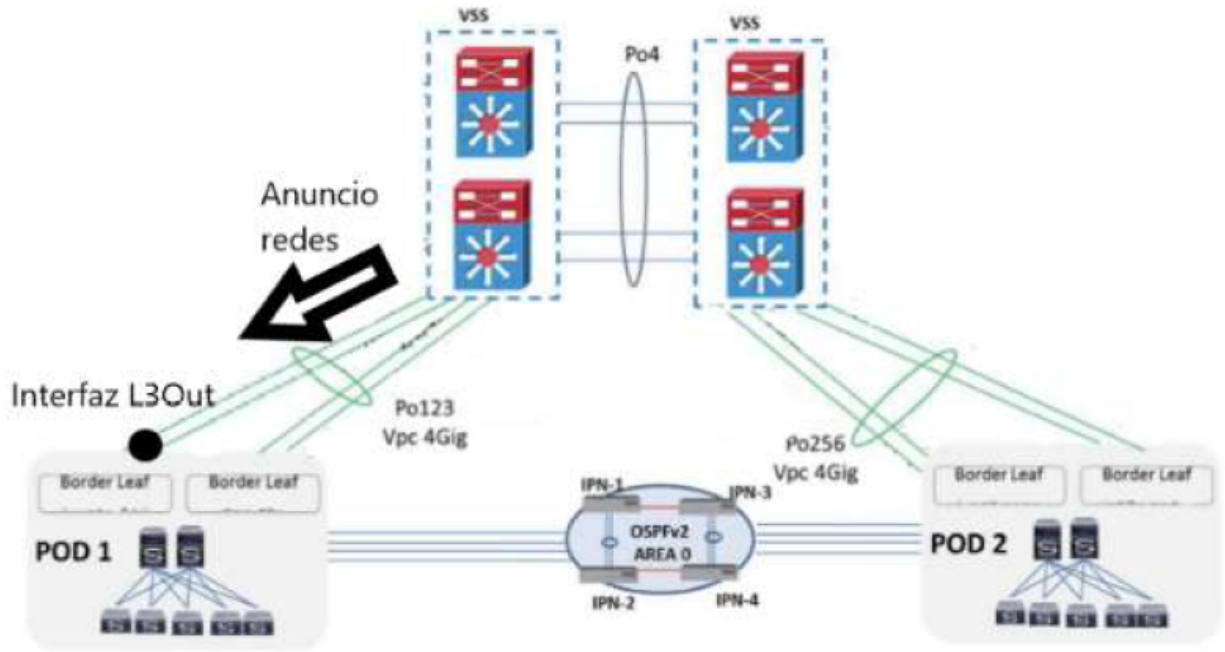


Figura 17 - Anuncio de rutas a través de OSPF.

Con el enrutamiento dinámico configurado, ya podemos plantear la migración del nivel 3, pero antes se ha de tener en cuenta que, por el diseño de red y funcionamiento de según qué aplicaciones y servicios del banco, existen Vlans cuyo nivel 3 (IP de Gateway o routing) puede residir en el VSS, un *Firewall* o *Balanceador*. Esto es importante ya que en función de donde se encuentre el Gateway de la red, el tráfico llegará hasta el VSS o transcurrirá a través de este (hacia el *Firewall* o *Balanceador* por ejemplo). Así pues, en función de donde se encuentre el routing los pasos para la migración del nivel 3 se hará de una manera u otra:

- **Para Vlans con nivel 3 en VSS:**

    1. Deshabilitar interface Vlan en VSS: Se pone en *shutdown* la “interface vlan” o *SVI (Switch Virtual Interface)* que se vaya a migrar para obligar que los paquetes se vayan hacia ACI.

    2. Deshabilitar IP de gateway configurada en HSRP de la Vlan: Para evitar conflicto de IP ya que esta será configurada en ACI en el siguiente paso.

3. Configuración de IP de gateway en ACI: Se configura la IP de gateway de la Vlan a migrar en ACI para que los equipos de la red en cuestión que requieran comunicación o enrutamiento hacia otras redes lo hagan a través de ACI. A su vez, al haber configurado OSPF, ACI incluirá esta red en sus anuncios para que los vecinos sepan de su existencia en ACI.

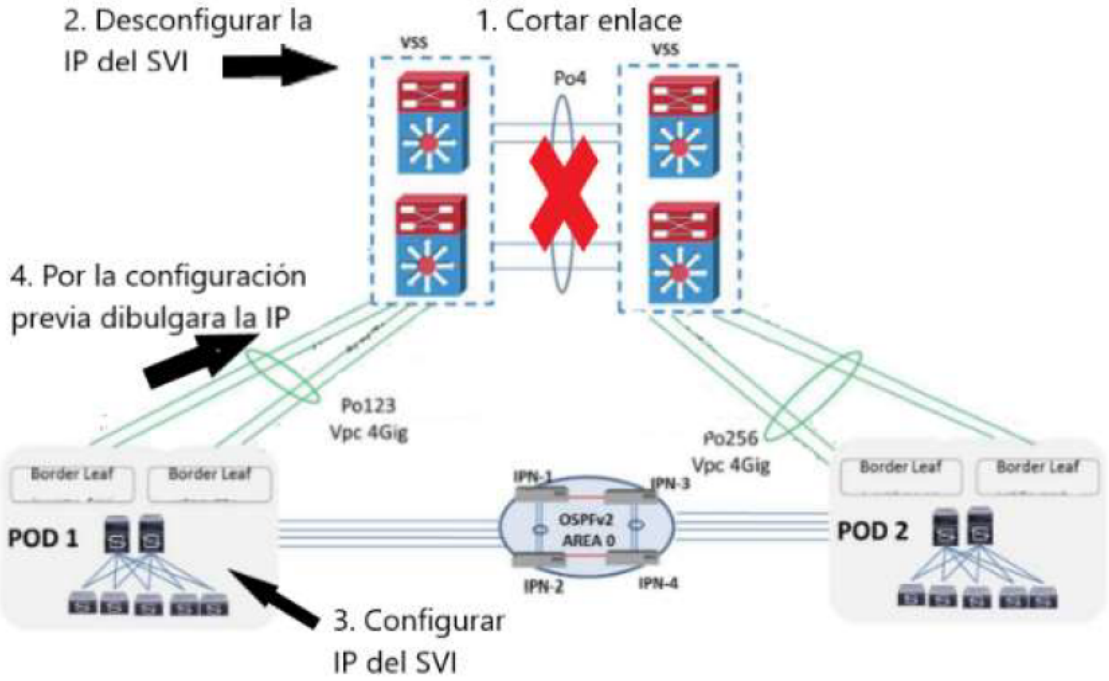


Figura 18 - Pasos para migración de red con Nivel 3 en VSS

- **Para Vlans con nivel 3 en otros equipos:**

1. Deshabilitar interface Vlan en VSS: Se pone en *shutdown* la "interface vlan" o *SVI* que se vaya a migrar para obligar que los paquetes se vayan hacia ACI.

2. Eliminación de rutas estáticas en los VSS: Antes de la migración, para que los paquetes pasasen a través de los VSS y llegasen a los elementos donde realmente estaba el gateway (por ejemplo un *firewall*), se configuraban diferentes *"policy route-map"* para reconducir este tráfico. En este punto de la migración se eliminan aquellos *"route-maps"* que estén relacionados con la Vlan de nivel 3 o red a migrar para que el tráfico se dirija hacia ACI en vez de al equipo de destino directamente.

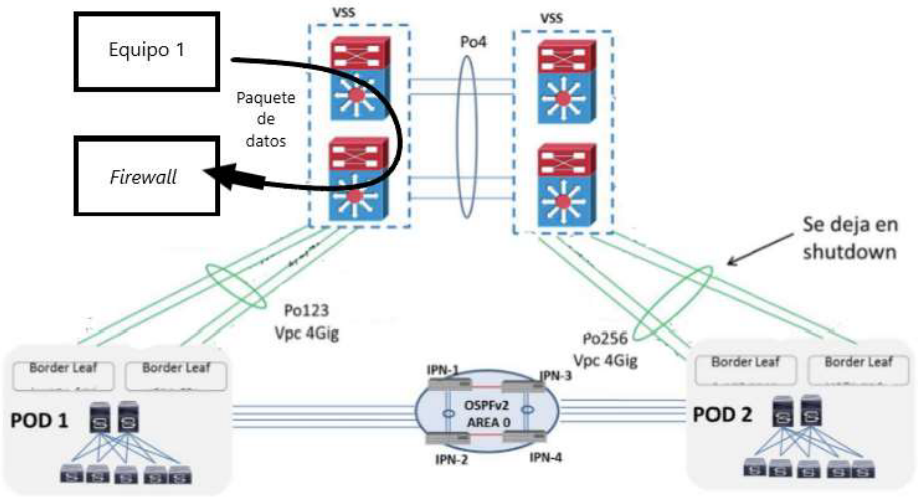


Figura 19 - Ejemplo de enrutamiento con policy route-map aplicado en VSS.

3. Configuración de redes a migrar en L3Outs: Se configuran las redes a migrar en los L3Out con el objetivo de indicarle a ACI cual es su *gateway* y a su vez anunciarlas dentro del *Fabric* para que los elementos de red de ACI sepan por dónde encontrar estas redes externas a ACI y así enrutar los paquetes correctamente.

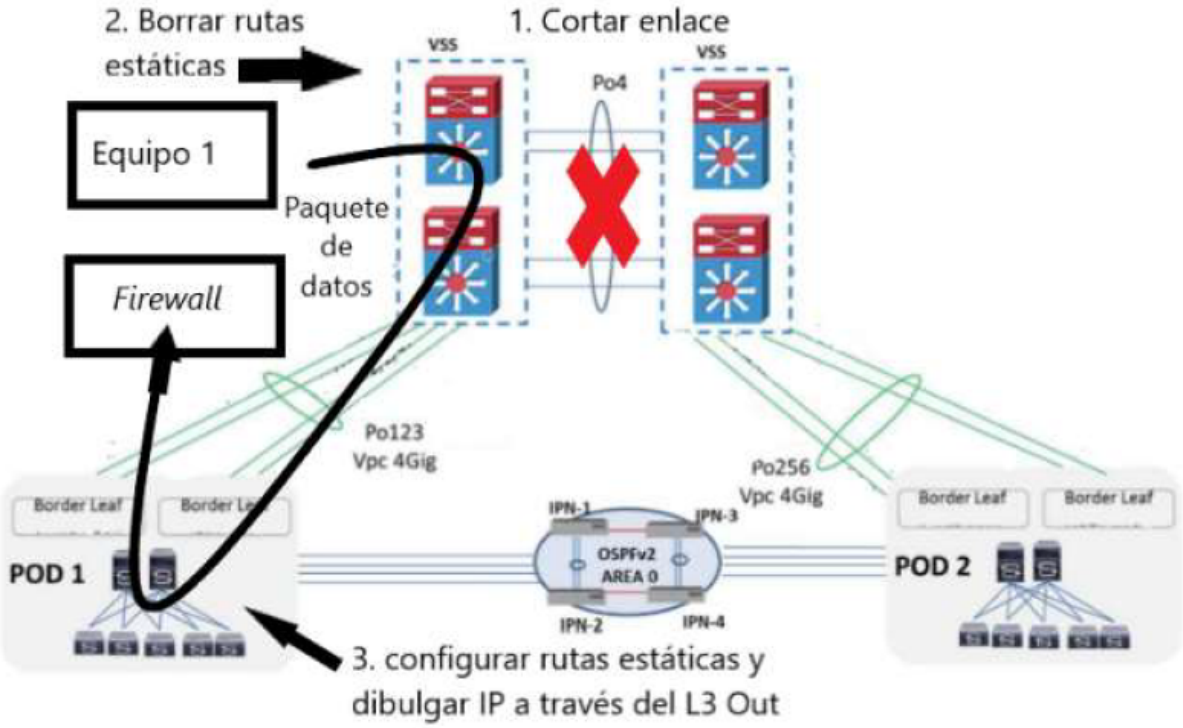


Figura 20 - Pasos para migración de red con Nivel 3 en otros equipos.

Con el nivel 2 y 3 de red configurado en ACI, se procede a eliminar la configuración de routing dinámico (OSPF), ya que no hace falta divulgar las redes entre el entorno

antiguo y el nuevo. Los equipos de ambos entornos ya son capaces de verse en ambos niveles y la red está preparada para empezar con la migración física de los equipos que están conectados en los VSS hacia los *Leafs* de ACI.

4.2.4. Fase de migración a nivel físico de los equipos finales.

El objetivo de esta fase es mover todos los equipos que están conectados en los VSS hacia la infraestructura de ACI, concretamente a los *Leafs.* Se ha de tener en cuenta que en este punto toda la infraestructura de ACI está configurada -tanto a nivel de comunicaciones como de parámetros específicos como EPG, BD, VRF, etc- para que al conectar el equipo que se vaya a migrar éste entre automáticamente en funcionamiento.

Dado que el proceso de migración supone la desconexión del equipo a migrar, hay que tener especial cuidado de no incidir en el corte del servicio. Tal y como se ha comentado en puntos anteriores, los equipos que prestan servicios están redundados en ambos CPDs, lo cual facilita en cierto modo la migración ya que mientras se está prestando el servicio desde un equipo situado en un CPD (activo), se puede mover el del otro que no está en servicio (pasivo).

Teniendo en cuenta esta redundancia y modo de funcionamiento de los equipos, antes de realizar la migración de un equipo se pasa el servicio hacia el CPD contrario al que se va a intervenir. Por ejemplo; para migrar el firewall del CPD del edificio principal, los pasos serían los siguientes:

1. Se pasa el servicio al firewall en el CPD del edificio secundario: A través de la consola de gestión de los firewalls declaramos al firewall ubicado en el CPD2 como “activo” y el del CPD1 se queda en modo pasivo.

2. Desconectamos el firewall del VSS principal: Se desconecta el cable ethernet del puerto en el que está conectado en el VSS (línea negra en la figura-21). En este punto el servicio se presta a través del Firewall del CPD2 (línea verde en la figura-21) sin que haya afección para los usuarios y clientes del banco.

3. Conectamos el cable en el puerto del *Leaf* en ACI: Se conecta el extremo del cable que va a la electrónica de red al puerto del *Leaf* que se haya configurado para este equipo. Tras conectarlo los firewalls se vuelven a comunicar entre ellos y sincronizan sus configuraciones y tablas de sesiones.

4. Volvemos a dejar el servicio en CPD del edificio principal: Con los firewalls sincronizados, volvemos a declarar al firewall del edificio principal como “activo” y de forma automática todo el tráfico vuelve a transitar por este firewall.

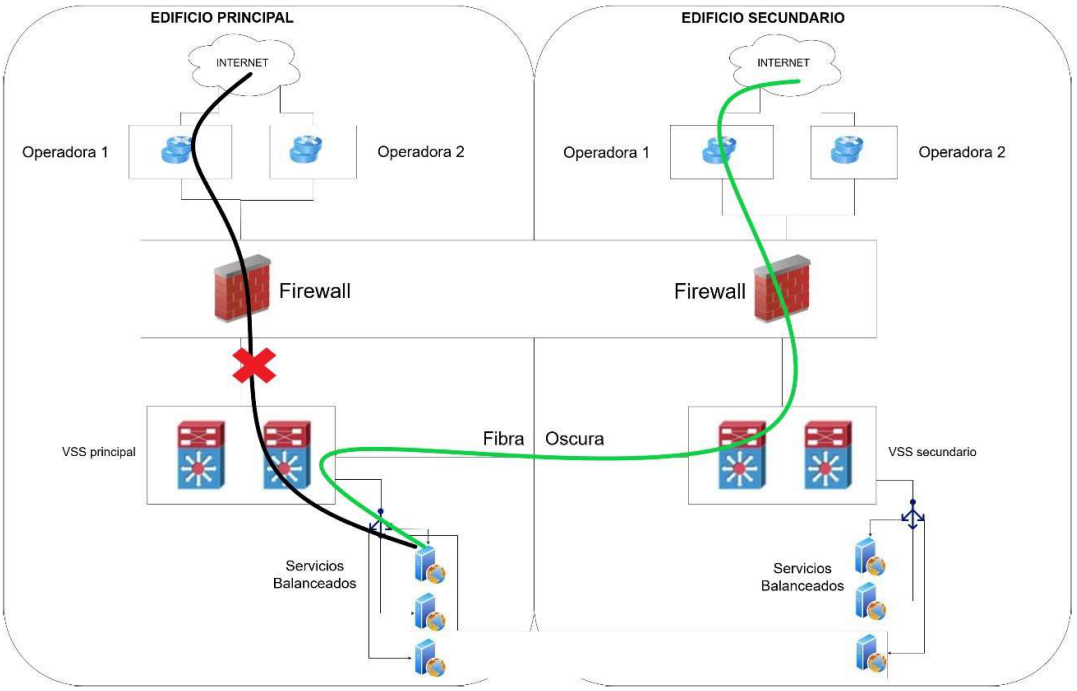


Figura-21 - Comunicación del Firewall en proceso de migración.

Para cada uno de los elementos que se vaya a migrar se ejecutarán estas 4 acciones ya que al tenerlos todos redundados podemos decidir en todo momento donde se presta el servicio; si en CPD1 o CPD2.

Se ha de tener en cuenta que, a pesar de tener la redundancia que nos presta cierta libertad y seguridad a la hora de hacer la migración, se está interviniendo en un entorno crítico y por ello la migración de los equipos se planifica de manera que se cumplan los siguientes criterios:

- La intervención se ha de hacer de manera presencial.

- La migración se ha de hacer de manera coordinada con los departamentos o empresas externas implicadas en el entorno/equipo que se vaya a migrar.

- No puede haber corte del servicio interno ni externo.

- En el momento de la migración, el equipo a migrar ha de tener un nivel de demanda bajo o casi nulo.

- Tras la migración se ha de hacer pruebas de validación de todo el servicio.

Todas estas limitaciones y las características especiales de algunos equipos, hacen que esta fase de migración física se prolongue durante muchos meses, por lo que podemos decir que es la fase más larga del proyecto.

Una vez migrados todos los equipos, se comprueba que las comunicaciones se establecen completamente a través de la red de ACI, pero por precaución durante un tiempo se mantienen encendidos los VSS por si hubiese que volver a conectar algún entorno por cualquier circunstancia que pudiese surgir.

Pasado un mes de la migración de todos los equipos, se valida el buen funcionamiento de la solución Cisco ACI y es el momento de poder apagar los VSS. Con el apagado de los equipos se da por concluída la migración y por tanto el proyecto.

5. Conclusiones finales y líneas de trabajo futuras.

5.1. Conclusión final.

En este Trabajo de Fin de Grado se ha llevado a cabo la documentación de todo el proceso de migración de una red Core con *hardware* convencional a una red SDN. Antes de elegir a la solución definitiva se han valorado diferentes soluciones de varios fabricantes, pero debido a la experiencia, seguridad y escalabilidad del producto finalmente se eligió la solución de Cisco ACI.

Elegida la solución, se ha hecho una introducción a la solución Cisco ACI detallando su arquitectura, los elementos que la componen y los diferentes tipos de despliegues que se pueden implementar en función de la infraestructura física de la que se disponga. Este punto ha permitido aprender diferentes formas de interconectar entornos remotos y la importancia de disponer de una red estable, redundada y adecuada en cuanto a requerimientos necesarios para comunicaciones entre CPDs.

Previo a la migración se ha hecho un estudio exhaustivo de la red a migrar a nivel de configuración, servicios, dimensionamiento, topología, etc. y se ha tenido en cuenta todas aquellas consideraciones específicas de la red que podrían influir en el nuevo entorno. Este trabajo de análisis se considera crucial ya que con él se ha minimizado al máximo el riesgo de cometer algún error en la configuración de la solución Cisco ACI y a su vez ha permitido realizar un inventario e identificación de los equipos importantes de la red.

Una vez identificados los elementos a migrar, se ha explicado a alto nivel las configuraciones y técnicas que se llevarían a cabo en ACI para adaptar la solución a los requerimientos técnicos identificados en la fase de análisis de la red antigua. La

adaptación de la configuración en ACI nos ha permitido ser conscientes del cambio de paradigma que supone la tecnología SDN, hemos conocido algunas de las diferencias que existe entre las redes convencionales y las de SDN como son: separación del plano de control, uso de nuevas metodologías para identificar a los equipos de la red con EPGs, segmentación de las redes con el uso de Bridge Domains, VRFs para la comunicación entre diferentes BDs y el uso de contratos para restringir la comunicación entre EPGs o BDs en caso de que sea necesario.

En el documento se ha detallado el proceso de migración, el cual se ha hecho de manera controlada empezando desde las capas inferiores del modelo *OSI*: se empieza por la fase de conexión física, se continúa con la de enlace de datos y después con la de red. Esto ha permitido probar la infraestructura a medida que se han ido migrando los diferentes entornos y validar que el funcionamiento era el esperado en base a la configuración que se aplicaba en cada fase. La migración se completó con la migración de los equipos finales, los cuales se conectaron a los *Leafs* y, una vez pasado un tiempo y comprobado que la nueva infraestructura ACI era estable, se procedió al apagado de los VSS que soportaban todo el tráfico de la red Core antigua, dando así por finalizado el proyecto de migración.

Todo el proyecto se llevó a cabo sin afectar en ningún momento al servicio del banco, lo cual fue muy gratificante para el equipo técnico y valorado muy positivamente por la entidad. Con él se consiguió cumplir el objetivo de disponer de una red altamente escalable, enlaces de red con velocidades de 100 Gbs y que tuviese una gestión centralizada. Además permitió conocer a fondo todos los conceptos técnicos de las redes SDN y en especial la de Cisco ACI, cuestión que es de gran interés puesto que las redes de hoy en día van encaminadas hacia este modelo de funcionamiento y gestión.

5.2. Líneas de trabajo futuras

Tal y como se ha indicado en el punto *"4.2 Proceso de migración"*, la modalidad de ACI implementada en este proyecto es la de *Network Centric*. Esta modalidad está centrada en la red y, entre otras muchas ventajas, permite gestionar de manera centralizada todos sus elementos gracias a la implementación de la tecnología SDN, pero no explota al máximo el potencial de SDN.

Podemos decir que Network Centric es un primer paso para adentrarse en el ecosistema SDN de Cisco, pero el objetivo es llegar a implementar la modalidad de *Application Centric* con lo que la red pasa a un escenario en el que el protagonismo lo tiene el flujo de las aplicaciones. Con esta modalidad ACI aporta un mayor control de la red, hasta tal punto que los conceptos de subredes, Vlans, VRF, etc. desaparecen para los administradores ya que pasan a ser entidades intrínsecas del propio sistema obligando a estos a centrarse sólo en las capas se aplicación. El uso de contratos para gestionar los accesos a según qué aplicaciones o entornos adquiere un mayor protagonismo y disminuye la dependencia de direccionamientos IPs para la segmentación de la red.

Por otro lado, aprovechando la tecnología SDN ya implementada con Cisco ACI, otra línea de trabajo que se ha de tener en cuenta más adelante es la implementación de microsegmentación. Con ello se podrá tener un mayor control del tráfico específico de ciertos equipos de la red de forma que podamos desviarlo por donde nos interese en función del servicio a consumir. Por ejemplo; aplicando esta técnica podemos desviar sólo el tráfico https a través de cierto *firewall* de la red para descongestionar a otros de este tipo de comunicaciones.

En cuanto a seguridad, una mejora que se implementará será el análisis de patrones. Con ello, a través de ciertos patrones detectados en las comunicaciones, se podrá identificar aquellos equipos que no tienen un comportamiento categorizado como normal para inmediatamente cortar sus comunicaciones antes de que continúen con este comportamiento y comprometan a la red. Los equipos entrarían en modo de cuarentena y hasta que los administradores no den el visto bueno para su vuelta a la actividad quedarán bloqueados.

En definitiva, como se ha podido comprobar, Cisco ACI nos ha hecho dar un salto de calidad en todas las comunicaciones de la entidad, pero aún nos puede aportar mucho más con el siguiente salto a la modalidad Application Centric. Pero para poder llegar a este punto, al igual que se ha hecho con la red de comunicaciones, es necesario un estudio previo a nivel de aplicaciones con el fin de tener muy claro el flujo de todas ellas y así poder hacer la evolución a ACI Application Centric con las mayores garantías de éxito sin que se afecte al servicio en ningún momento.

ANEXOS

ANEXO 1 - Documentación de fabricantes.

- Información solución Aruba:
  https://www.arubanetworks.com/techdocs/ArubaOS_83_Web_Help/Content/ArubaFrameStyles/Connecting_Managed%20Device_AP_Wrd_Network/basic_user_centr_netw.htm#

- Información solución Huawei:
  https://actfornet.com/huawei-cloud/sdn.html

- Información Cisco ACI:

  https://www.cisco.com/c/es_es/solutions/data-center-virtualization/application-centric-infrastructure/index.html#~integrations

  https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-737855.html

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/aci-fundamentals/b_ACI-Fundamentals/b_ACI-Fundamentals_chapter_010001.html#concept_9241D40AD01249C0992D486359CF46

ANEXO 2 - Network Centric vs Application Centric

Comparativa entre modalidad de Network Centric y Application Centric de Cisco ACI:

PARAMETER	NETWORK CENTRIC	APPLICATION CENTRIC
Terminology	Network Centric approach allows existing network architecture and flows to remain the same, henceforth allowing IT resources enough period to get acclimatized with the new terminologies of ACI fabric.	Application Centric approach is comparatively a new approach model where application tiers are defined by EPGs . In this setup, Application Profiles are created for each application with EPGs based on the application architecture tiers.
Approach	Considers traditional approach of using Subnets, VLANs and VRFs	Hides traditional network related terminologies (such as VRFs, VLANs, and subnets).
Default Gateway	May or may not reside in ACI Fabric, subject to requirement.	Generally resides in ACI fabric
Defining of Policies	Policies are defined based on existing network setup like how VLANs are created.	Policies are defined and created based on application details like application names, application security requirement etc
Mapping	Maps BD and EPG to VLAN	Maps applications with same functions to same EPGs
Usage scenario	When gradual migration from existing setup to new infrastructure is required.	When a greenfield Network environment is being setup
Focus area	Network focussed	Application Orchestration focussed
Benefits	• Close to traditional design and simpler for network resources to operate. • Routes leaking across VRFs becomes easier	• Less dependency on IP Subnet planning • Limited dependency of application developers on network team
https://ipwithease.com		

ANEXO 3 - Pruebas de funcionamiento.

En este anexo se detallan las diferentes pruebas realizadas después de completar cada una de las fases de la migración:

- **Fase de conexión a nivel físico de los elementos de red.**

El objetivo de estas pruebas es comprobar que las conexiones físicas y configuración de los elementos de la infraestructura ACI son correctas. Para ello se lleva a cabo:

- ☐ Comprobación del correcto funcionamiento de los equipos recibidos: Se comprueba que el equipamiento viene de fábrica en buen estado, comprobando que las interfaces responden como deben ante las conexiones físicas.

- ☐ Comprobación de configuración aplicada: Se comprueba que la configuración global aplicada tiene efecto y que los elementos comunican correctamente con la nube de Cisco para un seguimiento del mantenimiento de fabricante.

- ☐ Comprobación acceso a GUI de los APIC y autenticación local.
- ☐ Comprobación de acceso a CIMC de APIC.
- ☐ Comprobación de DNS con APIC.
- ☐ Comprobación NTP con APIC.
- ☐ Comprobación SYSLOG con APIC.
- ☐ Comprobación SNMP de APIC.
- ☐ Comprobación POD1.
- ☐ Comprobación del POD2.
- ☐ Comprobación del cableado del Fabric.
- ☐ Comprobación NTP con Leaf & Spine.
- ☐ Comprobación SYSLOG con Leaf & Spine.
- ☐ Comprobación SNMP de Leaf & Spine.
- ☐ Comprobación POD1.
- ☐ Comprobación de cableado.
- ☐ Comprobación OSPF.
- ☐ Comprobación MP-BGP EVPN en SPINE.
- ☐ Comprobación NTP con IPN.

- ☐ Comprobación SYSLOG con IPN.
- ☐ Comprobación SNMP de IPN.
- ☐ Comprobación MTU en IPN.
- ☐ Comprobación RP en IPN.
- ☐ Comprobación PIM en IPN.
- ☐ Comprobación INBAND en OOB.
- ☐ Comprobación del cableado en OOB.
- ☐ Comprobación del stack OOB.
- ☐ Comprobación NTP con OOB.
- ☐ Comprobación SYSLOG con OOB.
- ☐ Comprobación SNMP de OOB.
- ☐ Comprobación cableado Agregación.
- ☐ Comprobación NTP en Agregación.
- ☐ Comprobación SYSLOG en Agregación.
- ☐ Comprobación SNMP en Agregación.

- **Fase de migración a nivel 2 de la comunicación.**

Tras conectar los equipos y configurar el STP, se comprueba que:

- ☐ Las MACs de los equipos conectados en la red antigua se transmiten correctamente hacia entorno ACI. Con ello validamos que los enlaces troncales están correctamente configurados.

- ☐ ACI responde correctamente ante un cambio de topología en la red antigua.

- ☐ Equipos en diferentes Vlans no son capaces de verse entre ellos.

- ☐ Ante un bucle en la red, ACI no sufre afección y STP actúa correctamente.

- **Fase de migración a nivel 3 de la comunicación.**

Antes de migrar los equipos, en esta fase se comprueba que todo el routing funciona adecuadamente en función de la configuración aplicada. Para validar la configuración, con un equipo conectado en la infraestructura ACI y otro en la antigua, se hacen las siguientes pruebas:

- ☐ Se comprueba que, con un equipo conectado a la Vlan/red que se migra, se llega al Gateway migrado a ACI y viceversa.

- ☐ Se comprueba que, con un equipo conectado a una Vlan en la red antigua que no se migra, se puede comunicar con un equipo de la red que se migra conectado en ACI. Con esto comprobamos que el routing funciona correctamente.

Referencias:

SDN en Wikipedia [en línea] [fecha de consulta: 5 de diciembre 2022].
Disponible en:
https://es.wikipedia.org/wiki/Redes_definidas_por_software#Separación_de_plano_de_control_y_datos

IT Exams [en línea] [fecha de consulta: 13 de diciembre 2022].
Disponible en:
https://itexamtools.com/cisco-data-center-exams/ccnp-data-center-300-620-dcaci-data-center-aci-implementation/

How does internet work [en línea] [fecha de consulta: 13 de diciembre 2022].
Disponible en: https://howdoesinternetwork.com/2019/aci-multipod

Curso DCAC9K (21-11-2019). De esta formación no se puede aportar ningún enlace con el contenido de esta, pero en el siguiente enlace se puede consultar el plan de formación y los temas que se tratan:

Mira Telecomunicaciones [en línea] [fecha de consulta: 13 de diciembre 2022].
Disponible en:
https://miratelecomunicacions.com/cisco-data-center-cloud/configuring-cisco-nexus-9000-switches-in-aci-mode-v1-0-dcac9k/