TESIS DE MAESTRÍA

Diseño de una red industrial

por

Mariano Musante

INGENIERO ELECTRÓNICO

PRESENTADO A LA ESCUELA DE POSGRADO DEL ITBA
EN CUMPLIMIENTO PARCIAL
DE LOS REQUERIMIENTOS PARA LA OBTENCIÓN DEL TÍTULO DE

Master en Ingeniería de las Telecomunicaciones

EN EL INSTITUTO TECNOLÓGICO DE BUENOS AIRES
FECHA __ / ____ (MM Y AAAA)

Firma del autor _____

Instituto Tecnológico de Buenos Aires
Fecha __ / __ / ____ (DD, MM y AAAA)

Certificado por _____

Ing. Mag. Uriel Rozenbaum
Instituto Tecnológico de Buenos Aires
Tutor de la Tesis

Miembros del jurado:

_____

_____

_____

AGRADECIMIENTOS

En primer lugar me gustaría agradecer a mi esposa, a mis hijos y a mi familia quienes me apoyaron durante la realización del posgrado y la presente Tesis.

Luego, quisiera destacar la labor de mi tutor de Tesis, Uriel Rozenbaum, quien dedicó su tiempo personal a leer y realizar aportes de gran valor. Antes de recibir su ayuda, me encontraba estancado y desmotivado. No tengo dudas de que sin él no hubiera completado este trabajo.

No quiero tampoco dejar de mencionar a los docentes del instituto quienes aportaron su experiencia y conocimientos durante el posgrado.

También a la empresa para la cual trabajo que me brindó los medios para la realización del posgrado y la oportunidad de contribuir a un proyecto del cual esta Tesis es tan sólo una porción.

Por último, y no por eso menos importante, quiero agradecer a mi compañero de trabajo Ing. Adrián Sampietro responsable de la implementación de la red descripta en esta Tesis. Su aporte ha sido de gran valor técnico y profesional.

ÍNDICE

INTRODUCCIÓN

En los últimos años se ha observado una convergencia de los servicios de comunicaciones hacia Ethernet e IP.

Los sistemas de control industrial no han escapado a esta tendencia y cada vez son más los dispositivos de este segmento que usan Ethernet e IP.

Esto plantea nuevos desafíos para las áreas de redes y de control industrial, a las que se les demanda mayor integración y sinergia.

Si bien es muy costoso y complejo migrar una línea de producción a un modelo de red integrado con el resto de la compañía, no sucede lo mismo cuando el requerimiento es planteado en la fase de diseño de la misma.

El objetivo de la presente tesis se centra en el diseño de una red que cumpla con los requerimientos de los sistemas productivos y a la vez con los de las áreas de tecnología de la información.

Se plantearán dos alternativas, una con tecnología de red tradicional, mientras que la segunda pretenderá ser una opción innovadora basada en el concepto de redes definidas por software.

En el Capítulo 1 de este trabajo se describirán los pasos relevantes por los que pasó la tecnología para llegar al estado actual.

El Capítulo 2 estará dedicado a narrar la situación que impulsó el presente trabajo y a listar los criterios de diseño que debieron ser tenidos en cuenta al momento de evaluar las opciones.

Las alternativas propuestas serán tratadas y analizadas en el Capítulo 3.

Dentro del Capítulo 4 se desarrollarán los conceptos relacionados con la tecnología elegida, así como también se describirá la topología de red, componentes y se contrastarán con los criterios de diseño planteados anteriormente.

Por último, en el Capítulo 5, se presentarán las conclusiones y los siguientes pasos.

CAPÍTULO 1. ANTECEDENTES

1.1 Resumen

Las redes de área local actuales basadas en Ethernet podrían describirse como un conjunto de switches y dispositivos corriendo una serie de protocolos estándar con el objetivo de conmutar tramas entre los diferentes extremos.

Cada uno de estos componentes es independiente del resto y sólo tienen una visión parcial de toda la red. Sólo conocen lo que los demás le informan.

Los llamados plano de control y plano de datos, están individualizados en cada uno de los dispositivos y están estrechamente vinculados entre sí.

Las redes definidas por software o SDN por su sigla en inglés, vienen a romper con el paradigma que rigió el networking en los últimos años, separando los planos antes mencionados. Plantea un control centralizado de la red y un plano de datos distribuido.

En el presente trabajo desarrollaremos el diseño de una red SDN que integre tanto el ambiente industrial como corporativo y se comparará con un diseño tradicional.

1.2 Redes tradicionales

Para poder entender la diferencia entre las redes convencionales y las redes definidas por software, es importante saber que en general, las redes de telecomunicaciones conceptualmente constan de tres partes o planos, llamados así porque pueden considerarse como redes independientes, superpuestas entre sí [I]:

- ***Plano de control:*** lleva la información de control. También se la conoce como señalización. Los protocolos Spanning Tree, BGP y OSPF [II] forman parte de este plano, entre otros.

- ***Plano de datos:*** transmite el tráfico de la red. Contiene la información de cómo deben conmutarse las tramas, paquetes, flujos, circuitos. Las tablas de enrutamiento y de reenvío de tramas, son algunos ejemplos.

- ***Plano de gestión:*** transmite las operaciones y la administración de tráfico necesarias para la gestión de red. En este ámbito, los más comunes son Telnet y SSH.

En los routers y switches convencionales, en los que se basan las redes tradicionales, existe una estrecha vinculación entre los planos antes mencionados.

Cada componente de la red implementa de manera local un plano de control y uno de datos, sin que exista una coordinación central. Al mismo tiempo, la gestión se realiza de forma individual y por lo general, manual sobre cada elemento [III]

Este modelo tiene ventajas y desventajas:

Ventajas:

- ***Independencia de elementos:*** Al no existir un control central, sus componentes son independientes y pueden converger en topologías alternativas frente a la detección de un problema.
- ***Tolerancia a fallos:*** Con un correcto diseño, la falla en uno de sus elementos, no paraliza la gestión del resto, ya que se hace de manera individual.

Desventajas:

- ***Complejidad:*** Para adaptar las redes a las necesidades de los usuarios la industria ha mejorado los protocolos de red para ser más seguros y eficientes. Los mismos tienden a ser definidos en aislamiento, sin embargo, con cada uno resolviendo un problema específico y sin el beneficio de una acción conjunta.

- ***Políticas inconsistentes:*** Para implementar una política que abarque a la red completamente, los administradores, deben configurar miles de mecanismos coherentemente y mantenerlos, por lo general, manual e individualmente.

- ***Imposibilidad de escalabilidad:*** A la vez que las demandas de centros de datos aumentan rápidamente, la red debe crecer de la misma forma. Sin embargo, se vuelve más compleja con la suma de cientos de miles de equipos que deben ser configurados y gestionados.

1.3 Redes definidas por software

El aumento del volumen de tráfico y la necesidad de redes más confiables, predecibles y administrables llevó a los investigadores a buscar mejores enfoques para ciertas funciones de redes como la ingeniería de tráfico, cuyos recursos y métodos usando protocolos de enrutamiento convencionales eran muy limitados.

SDN surge entonces como una arquitectura de red cuyo dinamismo, flexibilidad, rentabilidad y adaptabilidad fueran adecuadas para los requerimientos actuales.

En SDN, se separan los planos de control de la red de las funciones de reenvío y se establece una interfaz (API por sus siglas en inglés) entre ambos, lo que permite la programabilidad del control y la abstracción de la infraestructura subyacente.

Los distintos fabricantes ofrecen una variedad de arquitecturas centradas en el objetivo antes mencionado y formadas por:

Controlador SDN: es el “cerebro” de la red. Retransmite la información de conmutación a los equipos de red mediante la API southbound y se comunica con las aplicaciones del negocio mediante la API northbound.

API Southbound: como se comentó en el punto anterior, esta interfaz facilita el control de la red, permitiendo al controlador realizar cambios dinámicos de acuerdo a las necesidades.

API Northbound: pueden ser usadas para facilitar la innovación, permitir la automatización de tareas y desarrollar la programabilidad de la red. Se podría que decir que son las más críticas ya que soportan una gran variedad de aplicaciones y servicios.

1.4 Redes corporativas y redes de procesos industriales

En cualquier compañía de manufactura podemos encontrar básicamente, dos tipos de redes: la corporativa y la de procesos industriales.

La primera, es la red que la mayoría del personal usa diariamente. Permite el acceso al correo electrónico, internet, sistemas de gestión contable y otros.

La segunda, es una red cuyo objetivo es brindar conectividad entre los diferentes elementos que forman parte de los procesos de fabricación.

Se la suele dividir conceptualmente en cuatro niveles:

Nivel 1: Instrumentación, medición y actuación. Elementos de medición y detección de las variables de procesos (medidores y sensores) y elementos de acción sobre el proceso (actuadores).

Nivel 2: Control local recolección de datos. Dispositivos para integrar los instrumentos. Poseen autonomía formando los sistemas de control junto con los instrumentos y permiten la interconexión con el nivel de supervisión.

Nivel 3: Supervisión y control remoto. Sistemas que permiten visualizar los procesos desde centros de operaciones automatizadas, dando una imagen virtual de la planta. En paneles virtuales se muestran alarmas, fallas, estados y operaciones sobre los procesos.

Nivel 4: Integración, optimización y gestión. Sistema informático de gestión de planta. Comunica distintas organizaciones y mantiene las relaciones con proveedores y clientes a través de un ambiente de integración. Existen aplicaciones de alto nivel que permiten la optimización de procesos y el análisis de datos para la toma de decisiones gerenciales.

Los dos primeros niveles suelen desarrollarse sobre redes aisladas del resto de la organización, mientras que podría considerarse que los sistemas de nivel 3 y 4 están implementados en la red corporativa.

CAPÍTULO 2. PREMISAS

2.1 Situación de la empresa

La empresa sobre la que se realizó el presente trabajo, posee actualmente más 30 plantas distribuidas en 15 países.

La mayor parte de estos centros productivos fueron incorporados a la compañía en los últimos años mediante adquisiciones y si bien se han realizado importantes inversiones en diferentes áreas con el objetivo de unificar y uniformizar las operaciones, las redes industriales presentan en la actualidad una heterogeneidad que no se da en la red corporativa.

Las plantas presentan realidades muy distintas entre sí y se pueden encontrar una gran variedad de escenarios.

Sin embargo, lo que todas tienen en común es que la integración de la red industrial con el resto de la organización es baja o nula.

Para entender a qué se refiere esta falta de integración, basta citar por ejemplo, que aunque muchos de los dispositivos de nivel 1 y 2 hayan evolucionado hacia Ethernet e IP, la gestión debe realizarse de forma local.

Los denominados adquisidores de nivel 2 son los únicos equipos con visibilidad tanto de las capas inferiores como de las superiores, pero por lo general son computadoras con dos placas de red sin capacidad de enrutamiento.

Las desventajas de este modelo son varias, entre las que podemos mencionar:

- Altos costos operativos.
- Baja sinergia operativa con el IT.
- Infraestructura duplicada.
- Baja visibilidad de los niveles inferiores.

2.2 Desafío

En el último tiempo, la empresa ha decidido ampliar su capacidad productiva construyendo una nueva planta en Estados Unidos.

El nuevo centro deberá contar con el estado del arte de las diferentes tecnologías involucradas, siempre enfocadas en lograr la eficiencia operativa.

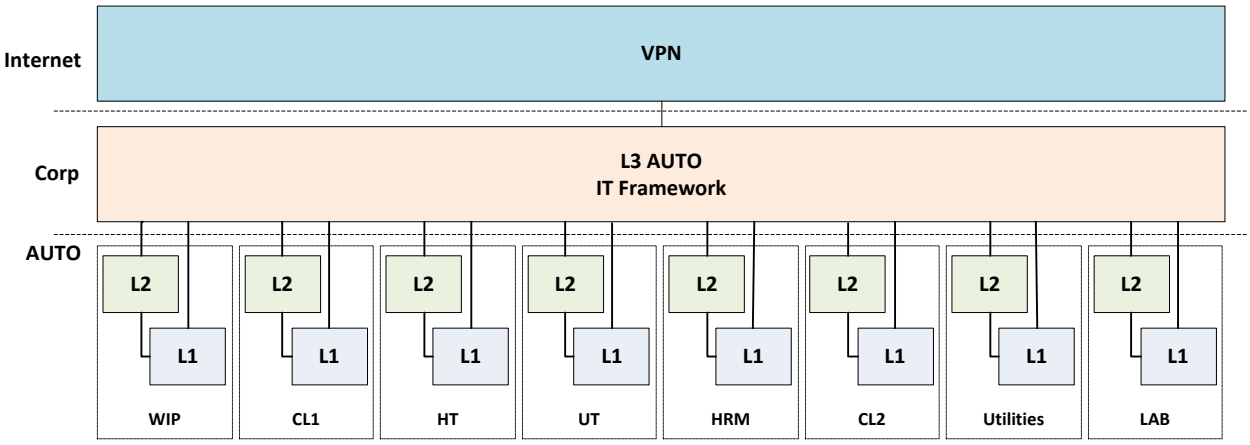
En lo que a comunicaciones y redes se refiere, se plantearon una serie de premisas que se desarrollarán en el siguiente capítulo.

2.3 Criterios de diseño

Los siguientes criterios de diseño fueron acordados al inicio del proyecto con el área de automatización de procesos (AUTO):

- Alta disponibilidad
  - Redundancia de conexiones.
  - Redundancia de los equipamientos de red.
- Baja latencia.
- Dos centros de datos con el mismo nivel de servicios de red.
- Procesamiento del nivel 2 y 3 de AUTO en el mismo centro de datos de IT.
- Consolidación de hardware entre IT y AUTO siempre que sea posible.
- Posibilidad de coexistencia de las redes lógicas de IT y AUTO en cualquier dispositivo de red.
- Redes de nivel 1 enrutadas localmente en cada línea de producción, pero con conectividad al resto de la organización.
- Segregación lógica entre IT y AUTO a través de reglas de acceso.
- Conectividad controlada a cada nivel de cada línea de producción desde la red corporativa e Internet.

2.3.1 Conectividad entre niveles



WIP, CL1, HT, UT, HRM, CL2, Utilities y LAB son líneas de producción.

2.3.2 Relaciones entre los niveles

Internet: Conectividad limitada y controlada con la red corporativa.

Nivel 3 – IT: La conectividad con cada nivel 1 y 2 de cada línea es controlada por reglas de tráfico por usuario.

Nivel 2: La conectividad entre el nivel 1 y 2 de la misma línea es controlada por reglas de tráfico.

Niveles de líneas: No hay restricciones dentro de cada red del mismo nivel y de la misma línea. Nivel 1 y 2 de diferentes líneas no deben tener conectividad.

El siguiente cuadro resume lo anterior:

	Internet	Nivel 3 - IT	Nivel 2	Nivel 1
Internet	X	VPN + OTP	VPN + OTP + Reglas por usuario	VPN + OTP + Reglas por usuario
Nivel 3 - IT	Proxy / Reglas por tráfico	X	Reglas por usuario	Reglas por usuario
Nivel 2	Sin acceso	Reglas por tráfico	X	Reglas por tráfico
Nivel 1	Sin acceso	Sin acceso	Reglas por tráfico	X

CAPÍTULO 3. ALTERNATIVAS

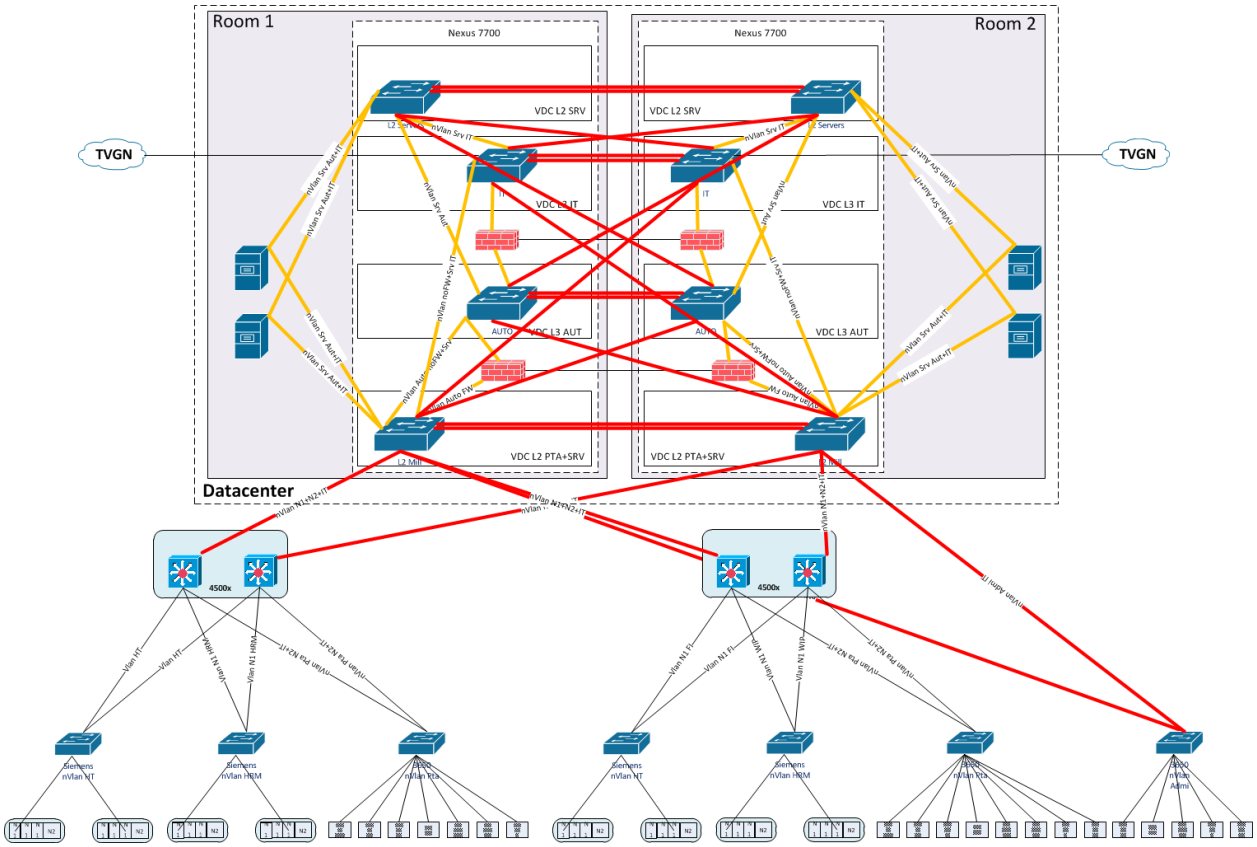
Con las premisas de diseño claras se plantearon dos alternativas, una basada en la tecnología tradicional y otra basada en SDN.

Dado que Cisco es el estándar de red de la compañía, la primera opción se desarrolló con Cisco Nexus 7700, mientras que la segunda con Cisco ACI.

3.1 Diseño tradicional

Se basa fundamentalmente en la separación de los dominios de conmutación y enrutamiento de IT y AUTO y en la instalación de firewalls en los puntos donde se requiera control por tráfico y/o usuario.

Como en muchos otros diseños, se pueden observar las capas de acceso, distribución y core. Adicionalmente, fue necesario incluir una capa de segregación y otra de control de tráficos, propias de la solución, a fin de poder cumplir con la sinergia de equipamiento y los niveles de seguridad.



3.1.1 Acceso Nivel 2 y Nivel 3 – IT

La componen los switches a los que se conectan los dispositivos y usuarios finales, como impresoras, computadoras, teléfonos IP y algunos elementos de AUTO.

Pueden estar en edificios administrativos, en planta o en el centro de datos. Cuentan en su configuración con las VLANs de Nivel 3 – IT y/o Nivel 2, por lo que brindan acceso a ellos.

3.1.2 Acceso Nivel 1

La componen los switches a los que se conectan los sensores, actuadores y medidores del Nivel 1.

Se encuentran exclusivamente en planta y cuentan en su configuración con las VLANs de Nivel 1.

Es importante aclarar que estas VLANs se enrutan localmente en switches de capa 3 que forman parte de la solución de automatización provista en este caso, por Siemens.

3.1.3 Distribución

Los switches de distribución cumplen con la función de concentrar varios accesos y disminuir el cableado hacia el centro de datos.

Por las distancias que deben conectar, tienen en su mayoría puertos de fibra óptica.

Luego de un análisis de capacidad, se definió que se conectarían a los accesos con troncales de 1Gbit Ethernet, mientras que subirían al centro de datos con vínculos de 10Gbit Ethernet.

Se encuentran varios nodos en planta o edificios administrativos y cuentan en su configuración con las VLANs de todos los niveles.

3.1.4 Segregación

Es la primera capa que se puede encontrar en el centro de datos. Su función, propia de la solución, es la de separar las diferentes VLANs para poder aplicarles los niveles de seguridad establecidos.

3.1.5 Core IT

Concentra y enruta todas las VLANs de IT. Así mismo se conecta con el resto de la red corporativa e Internet.

A fin de lograr la sinergia de equipamiento requerida, se planteó como una partición lógica de un único switch core.

3.1.6 Core AUTO

Concentra y enruta todas las VLANs de Nivel 2. Es otra partición lógica del mismo hardware que utiliza el core de IT. Sin embargo, el grado de virtualización es tan grande que la manera de comunicar ambos ambientes es mediante conexiones físicas (cables de cobre o fibra óptica externos).

3.1.7 Control de tráfico

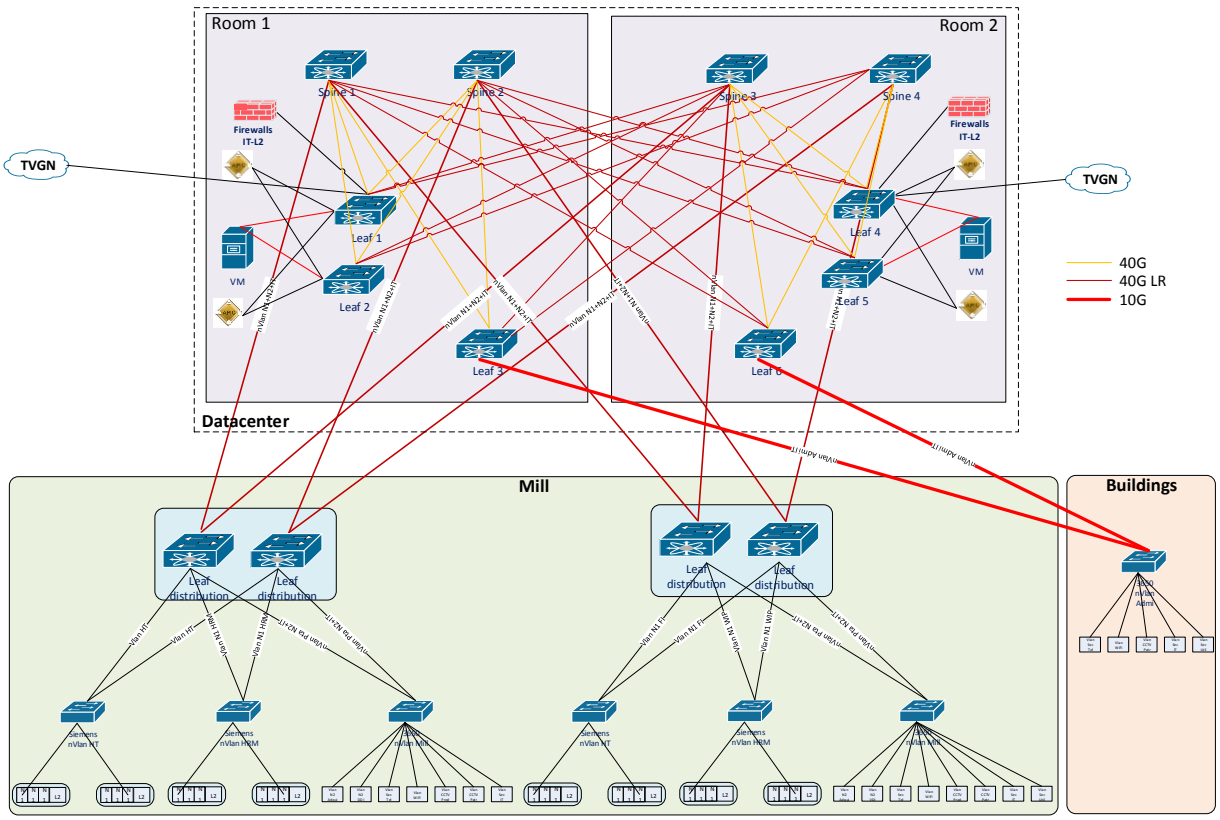
El control de tráfico se logra mediante la instalación de firewalls entre los niveles que se quieren aislar.

Las reglas pueden ser definidas por usuario, direcciones IP y/o puertos.

3.2 Diseño SDN

La alternativa basada en Cisco ACI simplifica en gran medida el cableado, la configuración y la operación ya que elimina la necesidad de separar los cores de IT y AUTO mediante firewalls.

En el modelo SDN de Cisco, por defecto ningún host puede comunicarse con otro host. Es necesario crear reglas similares a las de los firewalls.



3.2.1 Acceso Nivel 2 y Nivel 3 – IT

Al igual que en el modelo tradicional, la componen los switches a los que se conectan los dispositivos y usuarios finales, como impresoras, computadoras, teléfonos IP y algunos elementos de AUTO.

Pueden estar en edificios administrativos, en planta o en el centro de datos. Cuentan en su configuración con las VLANs de Nivel 3 – IT y/o Nivel 2, por lo que brindan acceso a ellos.

3.2.2 Acceso Nivel 1

También es igual al modelo tradicional. La componen los switches a los que se conectan los sensores, actuadores y medidores del Nivel 1.

Se encuentran exclusivamente en planta y cuentan en su configuración con las VLANs de Nivel 1.

Es importante aclarar que estas VLANs se enrutan localmente en switches de capa 3 que forman parte de la solución de automatización provista en este caso, por Siemens.

3.2.3 Distribución

Aquí se presenta la primera diferencia importante con el modelo anterior.

La distribución es eliminada y reemplazada por una extensión del core, extendiendo de esta manera las ventajas de SDN. En el siguiente capítulo se detallara la arquitectura Cisco ACI, ampliando este punto.

3.2.4 Core y control de tráfico

Se elimina la necesidad de una duplicación de cores. Tanto IT como AUTO comparten la infraestructura sin resignar ninguna de las premisas planteadas mientras que el control de tráfico es inherente a la tecnología.

3.3 Análisis y conclusiones preliminares

3.3.1 Análisis técnico

	Tradicional (Cisco Nexus 7700)	*SDN (Cisco Nexus ACI)*	
☒	Tareas sencillas de configuración, como por ejemplo agregar una VLAN, se convierten en intervenciones de alto riesgo e impacto sobre toda la red.	Tareas sencillas de configuración tienen un riesgo e impacto acotado.	☑
☒	Los firewalls incluidos en el diseño son un punto de falla adicional con un alto impacto en las líneas de producción.	No hay necesidad de incluir firewalls para controlar el tráfico productivo.	☑
☒	Múltiples conexiones entre los Centros de Datos.	Pocas conexiones entre los Centros de Datos.	☑
☒	Las configuraciones sobre el core son hechas individualmente sobre cada equipo, con la consecuente posibilidad de inconsistencias.	La configuración se realiza de forma centralizada en el controlador, evitando inconsistencias.	☑
☒	Las configuraciones de red del entorno virtual deben realizarse sobre la plataforma de gestión del mismo.	La gestión de red del entorno virtual se encuentra integrado al controlador SDN Cisco ACI.	☑
☑	Existe dentro de la compañía un alto nivel de experiencia sobre la plataforma.	Por ser una nueva tecnología, no existe experiencia dentro de la compañía.	☒

3.3.2 Análisis económico

	Tradicional (Cisco Nexus 7700)	*SDN (Cisco Nexus ACI)*
Producto	Cisco Nexus 7710	Cisco Nexus 9300
Descripción	1x N7K por sala con doble supervisora.	Cisco ACI, 2x Spine + 2x Leaf por sala + 4x APIC
Puertos de 10Gbits	198	198
Puertos de 40Gbits LR	32 (16 conexiones entre los Centros de Datos)	16 (8 conexiones entre los Centros de Datos)
Costo [kUSD] [1]	**$ 1143**	**$ 594**

[1] Precio de lista para Estados Unidos publicado en el website de Cisco.

3.3.3 Conclusiones

Las conclusiones preliminares se basaron en documentación de producto, presentaciones técnicas, consultas específicas y precios de lista. Se determinó así que la solución SDN cumple con las premisas propuestas, es técnicamente superior al diseño tradicional y económicamente más competitiva.

De acuerdo a la bibliografía, los tiempos de configuración inicial son bajos, lo que acelera el despliegue de la red.

Al mismo tiempo, el sistema escala rápida y sencillamente con alta disponibilidad: en una solución tradicional de networking, para alcanzar un nivel similar de redundancia, habría que realizar un mallado completo de las conexiones. Siendo N el número de nodos, la ecuación que define la cantidad C de conexiones, es:

$$C = \frac{N\ (N-1)}{2}$$

Si se considera que la cantidad de interfaces a configurar es el doble de C y que debe hacerse manualmente, se puede apreciar la complejidad de la tarea. Adicionalmente, hay que tener en cuenta que en un sistema tradicional, varios links quedarían bloqueados por el protocolo spanning-tree. La alternativa propuesta, no ejecuta spanning-tree, utiliza todos vínculos y la escalabilidad viene dada por el agregado de nodos que se configuran mediante scripts.

La posibilidad de automatizar tareas mediante el uso de APIs, es otra ventaja que debería reducir los costos operativos y disminuir las fallas por errores humanos.

Por último, la característica nativa que tiene el sistema de no permitir el tráfico entre dos nodos cualquiera, elimina la necesidad de un firewall simplificando la implementación y el mantenimiento.

Dicho esto y luego de acordar con las áreas incumbentes, se definió sin más, avanzar con la propuesta de Cisco ACI.

CAPÍTULO 4. DESARROLLO

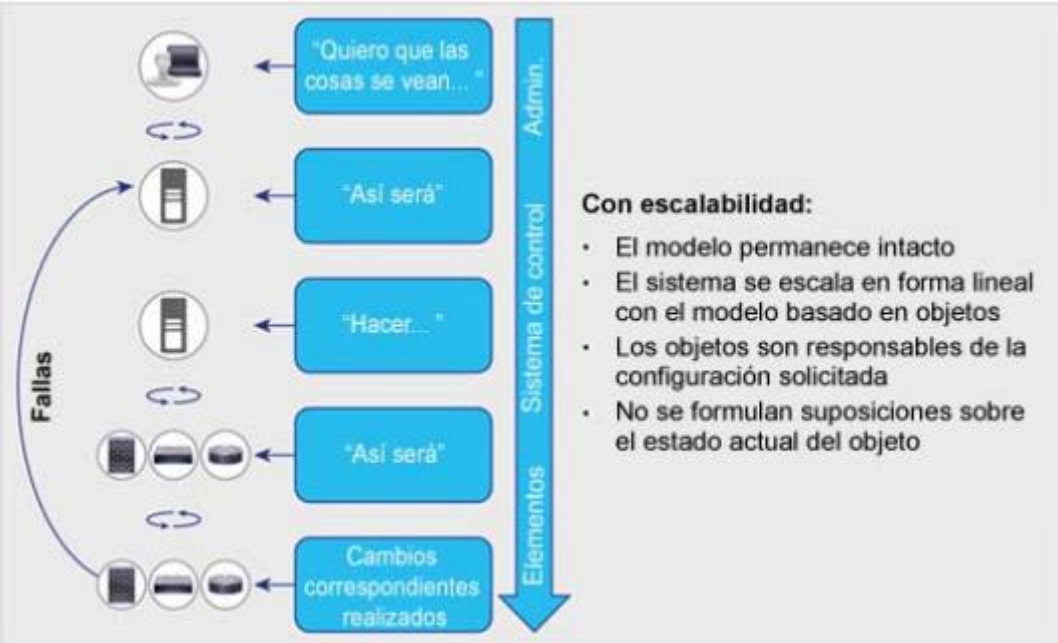
4.1 Principios de la arquitectura Cisco ACI

Una de las principales innovaciones de la infraestructura centrada en aplicaciones ACI [IV], por su sigla en inglés, es la incorporación de una interfaz sumamente abstracta para expresar la conectividad de los componentes de la aplicación junto con políticas de alto nivel que controlan esa conectividad.

4.2 Teoría de la política de ACI

La política de ACI es un modelo orientado a objetos basado en la teoría de promesa, que tiene como característica, el control escalable de objetos inteligentes y depende de estos objetos subyacentes para manejar los cambios de estado en la configuración iniciados por el sistema de control mismo como "cambios de estado deseados". De este modo, los objetos son responsables de devolver las excepciones o faltas al sistema de control. Este enfoque reduce la carga y la complejidad del sistema de control y permite una mayor escalabilidad (Figura 1).

FIGURA 1: ENFOQUE DE LA TEORÍA DE PROMESA PARA EL CONTROL DE SISTEMAS A GRAN ESCALA



Dentro de este modelo teórico, ACI crea una alternativa para la implementación de aplicaciones, con enfoque principal en ellas. En los modelos tradicionales, las aplicaciones sufren las restricciones de las capacidades de la red.

Conceptos como asignación de direcciones, VLAN y seguridad siempre estuvieron relacionados, lo que limita la escalabilidad y movilidad de las aplicaciones, lo que con el advenimiento del Cloud Computing es altamente apreciado.

En el modelo de política ACI, no se impone nada sobre la estructura de la red subyacente. Según lo determina la teoría de promesa, se requiere un elemento perimetral, llamado iLeaf, para administrar las conexiones con varios dispositivos.

4.3 Modelo de objeto

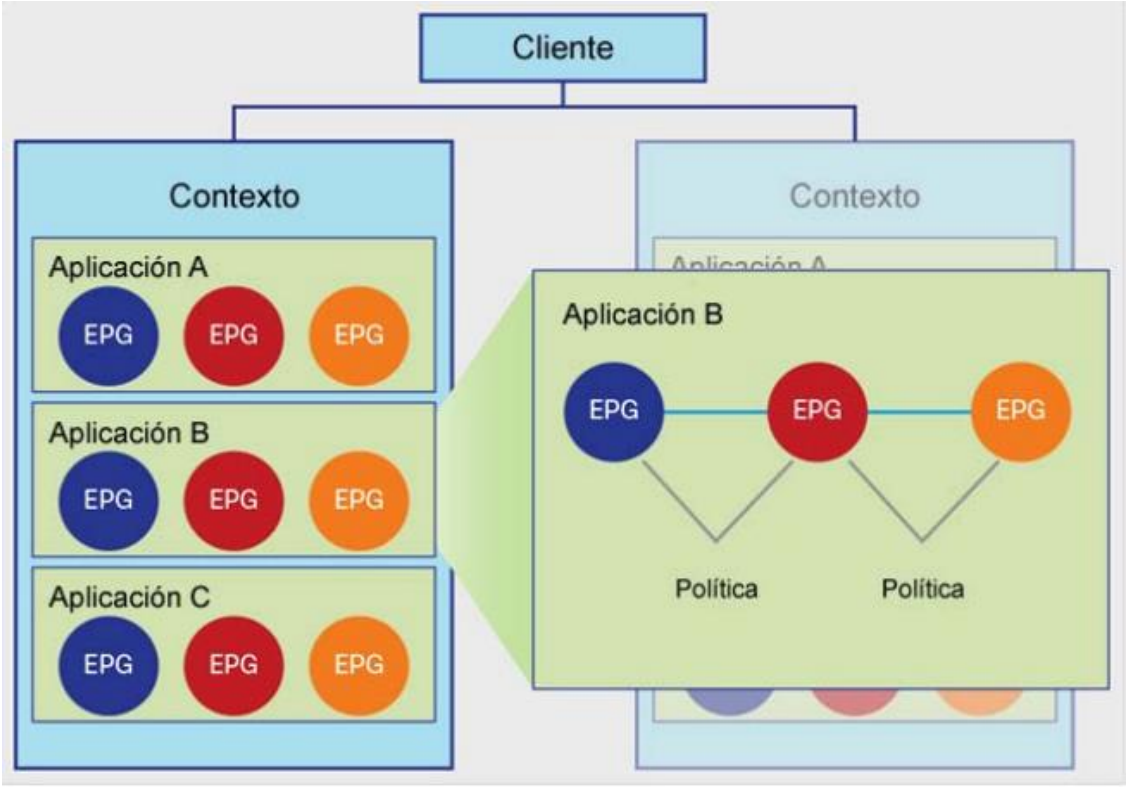
En el nivel más alto, el modelo de objeto ACI se construye según un grupo de uno o más usuarios, lo que permite que la administración de la red y el flujo de datos se separen. Los usuarios pueden ser clientes, unidades de negocios o grupos. Por ejemplo, una empresa puede utilizar un usuario para toda la organización mientras que un proveedor de la nube puede tener varios clientes que utilizan un usuario o más de uno para representar a sus organizaciones.

Los usuarios, a su vez, se pueden dividir en contextos, lo cual se relaciona directamente con instancias virtuales de enrutamiento (VRF) o espacios de IP separados. Cada usuario puede tener uno o más contextos.

Los contextos proporcionan una manera de separar aún más los requisitos organizativos de cada usuario y dado que usan instancias de enrutamiento diferentes, la asignación de IP se puede duplicar en contextos diferentes.

En cada contexto, el modelo ofrece una serie de objetos que definen a la aplicación. Estos objetos son EP (End Points), EPG (End Point Groups) y las políticas que definen las relaciones entre ellos (Figura 2). Puede observarse que las políticas son más que listas de control de acceso e incluyen un conjunto de filtros de entradas y salidas, configuración de calidad de servicio, reglas de marcado y enrutamiento.

FIGURA 2: MODELO DE OBJETO LÓGICO



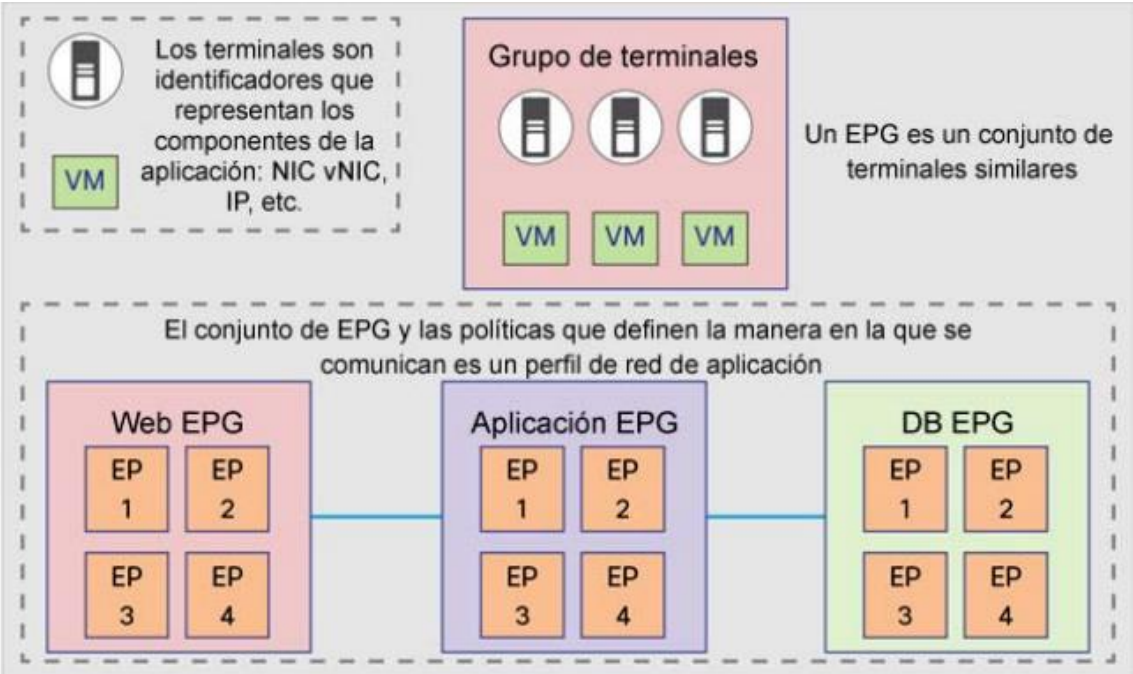
En la Figura 2 se muestra un usuario con dos contextos y las aplicaciones que los componen. Los EPG que se muestran son grupos de terminales que conforman un nivel de aplicaciones u otra agrupación lógica de aplicaciones. Por ejemplo, la aplicación B, que se muestra expandida en el lado derecho de la figura, está compuesta por un nivel web (azul), un nivel de aplicaciones (rojo) y un nivel de base de datos (anaranjado). La combinación de los EPG y las políticas que definen sus interacciones es un perfil de red de aplicación en el modelo de ACI.

4.3.1 End point groups

Los EPG son una recopilación de terminales similares que representan un nivel de aplicaciones o un conjunto de servicios. Proporcionan una agrupación lógica de objetos que requieren políticas similares. Por ejemplo, un EPG puede ser el grupo de elementos que componen un nivel web de la aplicación. Los terminales se definen mediante el uso de la placa de red (NIC), la NIC virtual (vNIC), la dirección IP o el nombre (DNS), que se puede extender con métodos futuros de identificación de componentes de aplicación.

Asimismo, los EPG se usan para representar entidades como redes externas, servicios de red, dispositivos de seguridad y almacenamiento en red. Los EPG son conjuntos de uno o más terminales que ofrecen funciones similares. Son una agrupación lógica con varias opciones de uso, según el modelo de implementación de la aplicación en uso (Figura 3).

FIGURA 3: RELACIONES EN EL GRUPO DE TERMINALES



Los EPG se diseñan para brindar flexibilidad y adaptabilidad a las necesidades de cada implementación y está contemplado que el futuro, permitan la aplicación de políticas dentro de sí mismos.

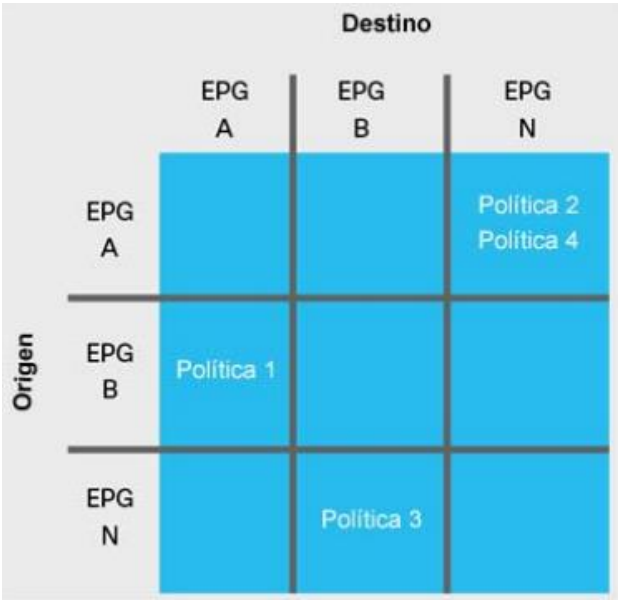
A continuación, se presentan algunos ejemplos de uso de EPG:

- EPG definido por las VLANs de redes tradicionales: serán parte de él, todos los terminales conectados a una VLAN dada ubicada dentro de un EPG.
- EPG definido por una VXLAN: igual que el caso anterior, sólo que se utiliza una VXLAN.
- EPG asignado a un grupo de puertos de VMWare.
- EPG definido por una IP o una subred.
- EPG definido por nombres de DNS o dominios de DNS. Por ejemplo, ejemplo.sdn.com o *.sdn.com

4.3.2 Aplicación de políticas

Se puede entender la relación entre los EPG y las políticas como una matriz con un eje que representa el EPG de origen (sEPG) y otro que representa el EPG de destino (dEPG). En la intersección de los sEPG y dEPG correspondientes, habrá una o más políticas. En la mayoría de los casos, la matriz se completará mínimamente debido a que muchos EPG no necesitan comunicarse entre sí (Figura 4).

FIGURA 4: MATRIZ DE APLICACIÓN DE POLÍTICAS



Las políticas se dividen por filtros para calidad de servicios (QoS), control de acceso, inserción de servicios, etc. Los filtros son reglas específicas para la política que afecta a dos EPG. Los filtros consisten en reglas de entrada y de salida: permitir, rechazar, redirigir, iniciar sesión, copiar y marcar. Permiten funciones de comodín en las definiciones (Figura 5). Por lo general, la aplicación de políticas utiliza un enfoque de coincidencia con el más específico primero.

FIGURA 5: REGLAS DE APLICACIÓN DEL COMODÍN

sEPG	dEPG	Aplicación	Comentarios
totalmente calificados	totalmente calificados	totalmente calificados	Reglas totalmente calificadas (S, D, A)
totalmente calificados	totalmente calificados	*	Reglas (S, D, *)
totalmente calificados	*	totalmente calificados	Reglas (S, *, A)
*	totalmente calificados	totalmente calificados	Reglas (*, D, A)
totalmente calificados	*	*	Reglas (S, *, *)
*	totalmente calificados	*	Reglas (*, D, *)
*	*	totalmente calificados	Reglas (*, *, A)
*	*	*	Predeterminado (por ejemplo, rechazo implícito)

Ejecución

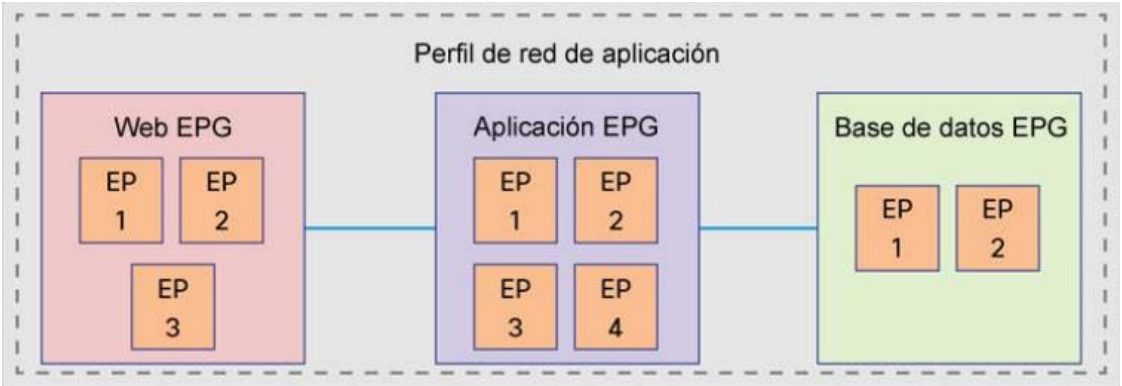
4.3.3 Perfiles de red de aplicación

El perfil de red de aplicación es un conjunto de EPG, sus conexiones y las políticas que definen esas conexiones. Constituyen una representación lógica de una aplicación y sus interdependencias en la estructura de red.

El sistema realiza integralmente la configuración, aplicación de políticas y enrutamiento, sin necesidad de que un administrador lo haga manualmente.

En la Figura 6 se muestra un ejemplo de perfil de acceso.

FIGURA 6: PERFILES DE RED DE APLICACIÓN



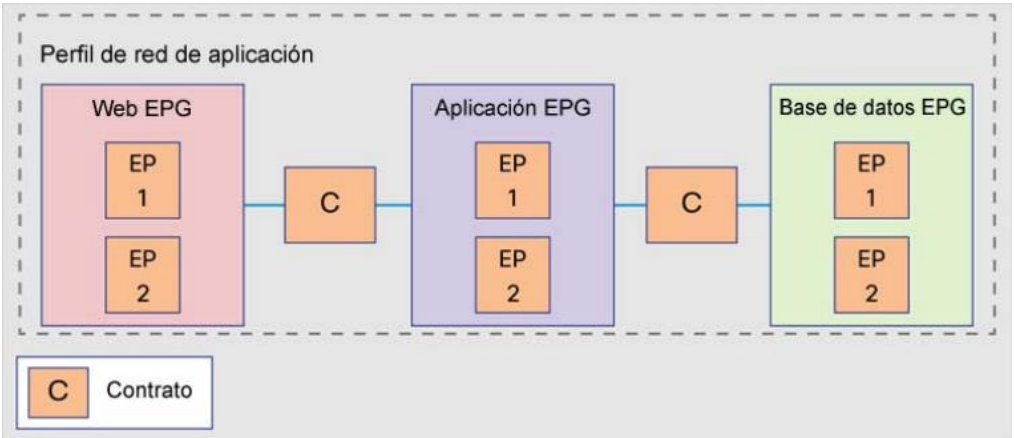
Para crear un perfil es necesario seguir los siguientes pasos generales:

1. Crear un EPG (como se indicó anteriormente)
2. Crear las políticas que definen la conectividad con estas reglas:
   - Permitir
   - Rechazar
   - Iniciar sesión
   - Marcar
   - Redirigir
   - Copiar
3. Crear puntos de conexión entre los EPG mediante políticas conocidas como contratos.

4.3.4 Contratos

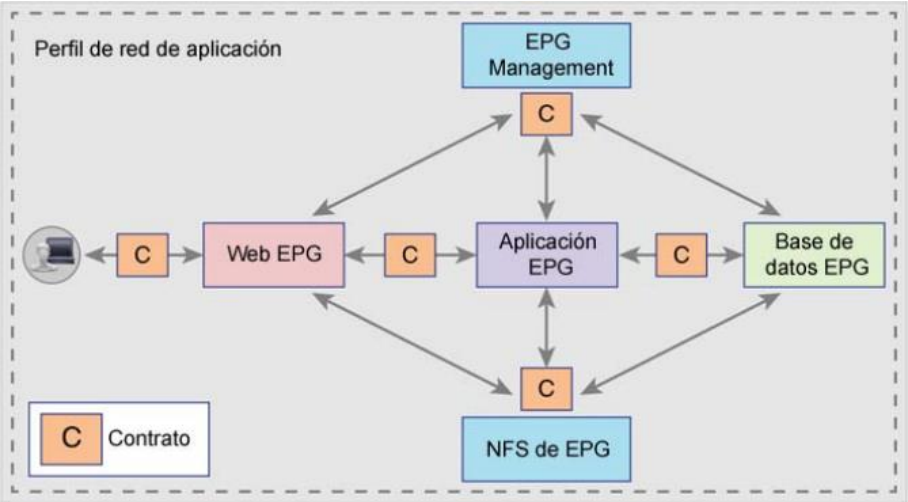
Los contratos definen los permisos, los rechazos de entrada y de salida, las reglas de calidad de servicio y como re direccionar el tráfico. Permiten tanto la definición simple como la compleja de la manera en que un EPG se comunica con otros EPG. Básicamente, un EPG proporciona un contrato y los demás EPG lo respetan. Por ejemplo, un servidor web puede ofrecer HTTP y HTTPS, por lo que a este servidor lo puede regir un contrato que permita solo estos servicios. Además, el modelo de contrato entre proveedor y consumidor promueve la seguridad gracias a que permite que se realicen actualizaciones simples y uniformes de políticas a un objeto de política única en lugar de los diversos enlaces que puede representar un contrato. Los contratos también ofrecen simplicidad, ya que permiten que las políticas se definan una vez y se reutilicen muchas veces (Figura 7).

FIGURA 7: CONTRATOS



En la Figura 8 se muestra la relación entre los tres niveles de una aplicación web definida por la conectividad del EPG y los contratos que determinan su comunicación. La suma de estas partes constituye un perfil de red de aplicación. Los contratos también facilitan la reutilización y uniformidad de políticas para los servicios que, generalmente, se comunican con varios EPG.

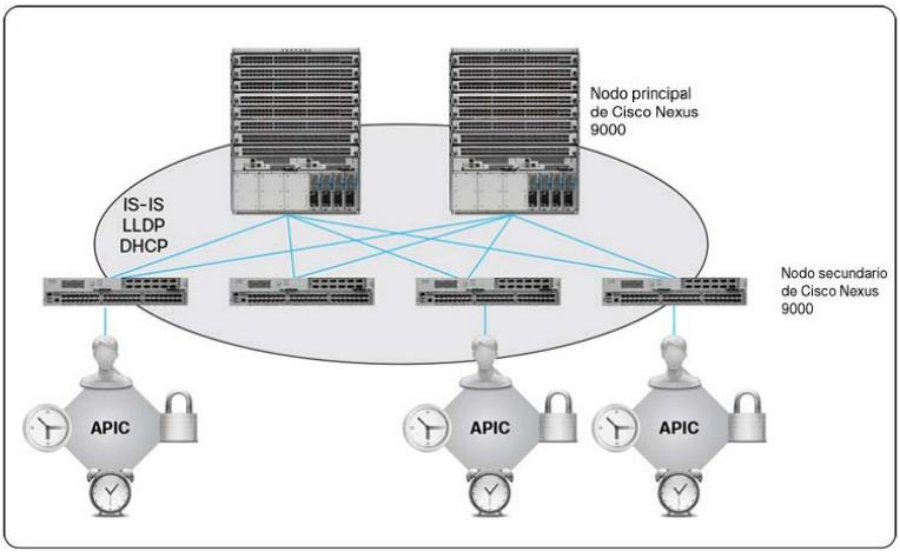
FIGURA 8: PERFIL DE RED DE APLICACIÓN COMPLETO



4.3.5 Topología y componentes de Cisco ACI

La estructura Cisco ACI (Figura 9), llamada Fabric, es una arquitectura de nodos principales y secundarios, del tipo grafo bipartito[2]. Pensado como una arquitectura de alto rendimiento, gran escalabilidad y redundante, implementa también el concepto de espacio de la infraestructura, en donde se llevan a cabo de manera segura y aislada, la detección de topología, la administración y el direccionamiento del sistema. [V]

FIGURA 9: ESTRUCTURA CISCO ACI



[2] En teoría de grafos, un grafo bipartito es aquel en que los vértices de un conjunto, sólo pueden conectarse mediante aristas, a los vértices del otro conjunto.

La topología de Cisco ACI está compuesta por un controlador llamado APIC (Application Policy Infrastructure Controller) y los switches de la familia Cisco Nexus 9000 principales y secundarios llamados spine y leaf respectivamente. Como en todo grafo bipartito, los leaves ubicados en la parte superior del rack (ToR) se conectan a los spines, pero nunca entre sí. De igual forma, los spines se conectan sólo a los leaves. Tanto el controlador APIC como el resto de los dispositivos del centro de datos se conectan sólo a los leaves.

4.3.6 Controlador Cisco APIC

Es un controlador físicamente distribuido, pero lógicamente centralizado, que proporciona al sistema el protocolo DHCP, la configuración de arranque y la administración de imágenes para inicio y actualizaciones automatizadas.

El software de la estructura ACI conforma un paquete como una imagen ISO, que se puede instalar en el servidor del APIC a través de la consola serial. Contiene la imagen del propio APIC, como así también los firmwares de los nodos spine y leaf, las políticas predeterminadas de la infraestructura y los protocolos necesarios para la operación.

4.3.7 Inicio de ACI con detección y configuración automáticas

La secuencia de arranque comienza con las imágenes instaladas en fábrica en todos los switches. Los componentes que ejecutan el firmware ACI y los APIC usan una capa reservada para el proceso de arranque, que se encuentra pregrabado en los switches.

Luego de realizar una mínima configuración en el controlador, el Fabric ACI se construye en forma de cascada, con inicio en los leaves directamente conectados a los APIC. Utiliza los protocolos DHCP y LLDP para detectar automáticamente los switches, asignar las direcciones e instalar el firmware.

Toda la comunicación de gestión dentro del Fabric ocurre en el espacio de la infraestructura, mediante el uso de direcciones IP privadas e internas.

4.3.8 Actualización del Fabric

Las políticas de firmware determinan la versión necesaria para cada uno los nodos, mientras las políticas de mantenimiento determinan grupos de nodos que se pueden actualizar en conjunto. Por último, existen los programas de mantenimiento que determinan cómo y cuándo varios nodos de un grupo se pueden actualizar.

Los grupos predeterminados incluyen “todos los leaves”, “todos los spines” y “todos los APIC” y actualizar el sistema, es tan sencillo como seleccionar una política y programarla para su ejecución.

El APIC conserva un catálogo de firmware basándose en los metadatos de las imágenes que identifican los tipos y modelos de switches compatibles.

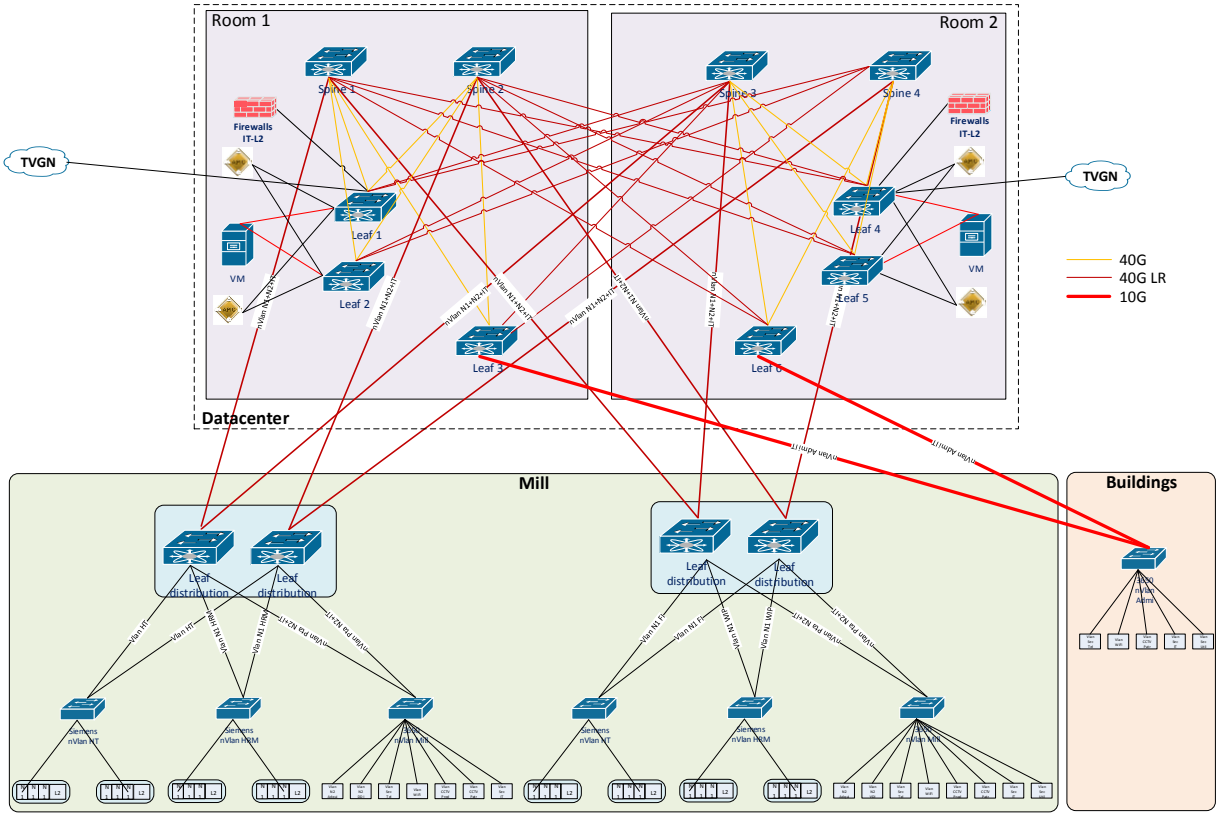
4.4 Implementación

La tecnología Cisco ACI fue desarrollada para funcionar como core de la red del centro de datos, por lo que hubo que ajustar el diseño para que pudiera funcionar también como core de la red de usuarios o red de campus.

Una definición importante en este sentido, fue llevar los switches leaf fuera del centro de datos y extender así, las funcionalidades del Fabric.

El resultado es una red homogénea con un core SDN ACI y un acceso basado en networking tradicional, tal como se observa en la Figura 10.

FIGURA 10: DISEÑO COMPLETO DE LA RED



4.4.1 Componentes de la topología

Switches Ethernet Layer 3 de Nivel 1. Cada línea de producción cuenta con un switch de capa 3 en donde se enrutan las VLANs de nivel 1, es decir que es el default gateway de todas las redes de Nivel 1 pertenecientes a una línea en particular.

Estos dispositivos, forman parte de la solución de control industrial provista por el fabricante y a ellos se conectan los PLCs y otros equipos ethernet de Nivel 1.

Switches Ethernet Layer 2 de Nivel 2 e IT para acceso. Tanto en planta como en los edificios administrativos, existen switches de capa 2 que podrán recibir tanto VLANs de Nivel 2 como así también VLANs de IT.

Estos equipos forman parte de la solución de networking diseñada por IT a ellos se conectan usuarios, access-points, impresoras y otros.

Switches Leaf. Como se mencionó en la descripción de la arquitectura ACI, estos equipos son los puntos de acceso al Fabric. Normalmente se deberían encontrar en el centro de datos, pero en el caso de referencia, se decidió desplegarlos como nodos de distribución en planta.

Switches Spine. Según el diseño de grafo bipartito explicado anteriormente, los spine sólo se conectan a los leaves. Estos equipos se encuentran únicamente en el centro de datos.

Firewalls. Son los responsables del control de acceso a las redes de Nivel 1 y 2, basándose en la autenticación de usuario.

APIC Controller. Son necesarios un mínimo de tres APIC para administrar la solución. Debido a que la planta cuenta con dos centros de datos físicamente separados, se optó por instalar dos controladores en cada sala, es decir, un total de cuatro controladores.

TVGN. Representa el acceso a la red internacional de la compañía.

4.4.2 Integración entre SDN y el networking tradicional de acceso

Dentro de la infraestructura ACI, todo debe ser administrado mediante el uso de End Points, End Point Groups y Contratos.

La granularidad para gestionar estos EPG dentro del entorno ACI es muy alta, sin embargo, al pasar la frontera del Fabric, ya no es posible contar con ese grado de segregación. Se decidió por tal motivo, separar por VLANs, asignando cada una a un EPG diferente.

4.5 Resultados

Retomando el cuadro de accesos planteados al principio del trabajo, se detalla a continuación la forma en la que un usuario o dispositivo interactuaría con otro.

	Internet	***Nivel 3 - IT***	***Nivel 2***	***Nivel 1***
Internet	X	VPN + OTP	VPN + OTP + Reglas por usuario	VPN + OTP + Reglas por usuario
Nivel 3 - IT	Proxy / Reglas por tráfico	X	Reglas por usuario	Reglas por usuario
Nivel 2	Sin acceso	Reglas por tráfico	X	Reglas por tráfico
Nivel 1	Sin acceso	Sin acceso	Reglas por tráfico	X

Internet a Nivel 3 – IT: un usuario conectado a Internet, puede mediante el uso de un cliente VPN y autenticación de clave de única vez (One Time Password – OTP), acceder a las redes de nivel 3 (Figura 11).

FIGURA 11: INTERNET A NIVEL 3 - IT

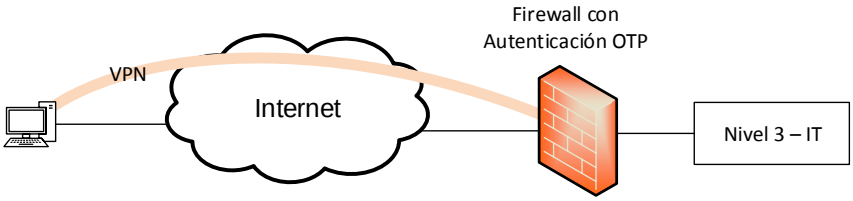
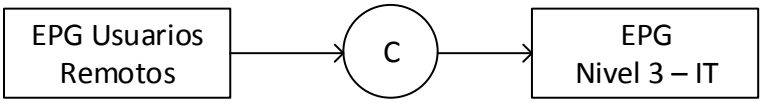


FIGURA 12: ESQUEMA ACI. INTERNET A NIVEL 3 – IT



En la Figura 12 se puede observar el modelo ACI en donde el EPG Usuarios Remotos se define por el segmento IP de red asignado y el EPG Nivel 3 – IT está formado por VLANs de usuarios, segmentos de red y máquinas virtuales.

Internet a Nivel 2 o Nivel 1: a la conexión anterior, se le suma que el usuario debe validarse una vez más en un portal web y en base a su perfil, se aplican los permisos que le correspondan (Figura 13)

FIGURA 13: INTERNET A NIVEL 1 O NIVEL 2

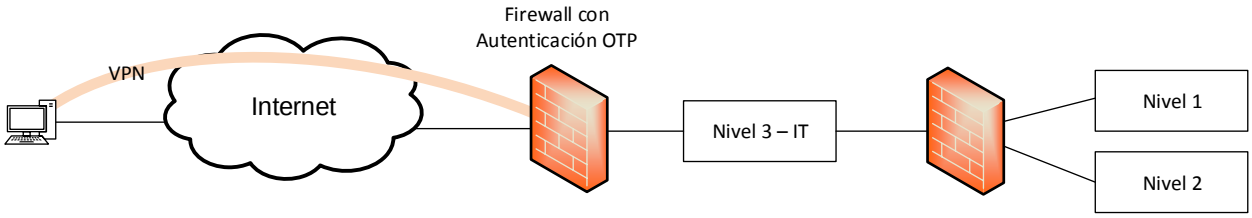
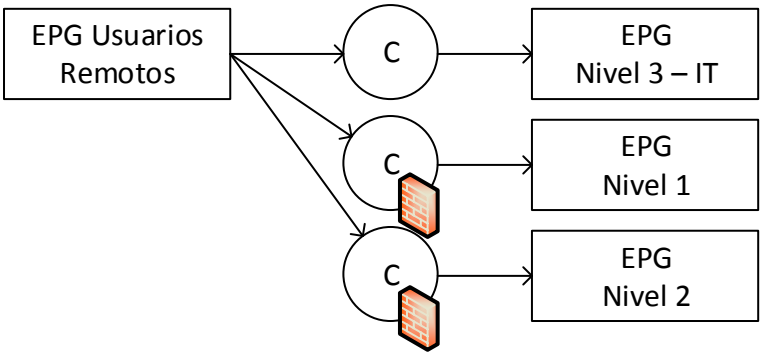


FIGURA 14: ESQUEMA ACI. INTERNET A NIVEL 1 O NIVEL 2



A diferencia del punto anterior, dentro de los contratos hacia Nivel 1 y Nivel 2, se especifica una derivación del tráfico hacia el firewall de autenticación, llamada Service Graph (Figura 14).

Nivel 3 – IT a Internet: por regla general, el acceso a Internet se realiza mediante el uso de un Proxy corporativo. Para el caso de servidores o accesos especiales que no pueden usar Proxy, se crean reglas basadas en IP o nombre de usuario.

FIGURA 15: NIVEL 3 – IT A INTERNET

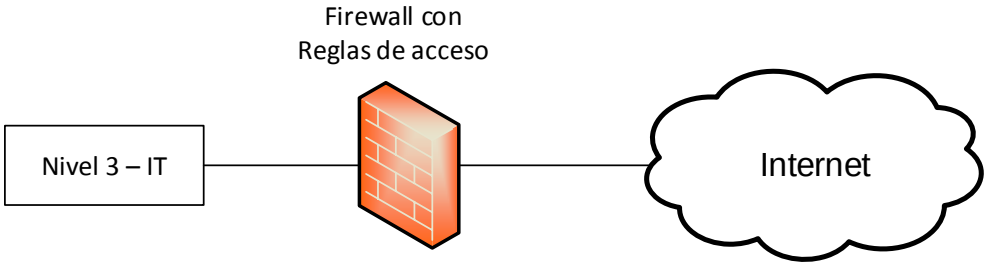
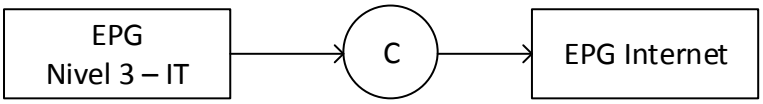


FIGURA 16: ESQUEMA ACI. NIVEL 3 – IT A INTERNET



Por razones de simplicidad operativa, el Proxy de navegación a Internet se encuentra en el mismo EPG, junto con Nivel 3 – IT (Figura 16)

Nivel 3 – IT a Nivel 2 o Nivel 1: el usuario debe validarse en un portal web y en base a su perfil, se aplican los permisos que le correspondan.

FIGURA 17: NIVEL 3 – IT A NIVEL 1 O NIVEL 2

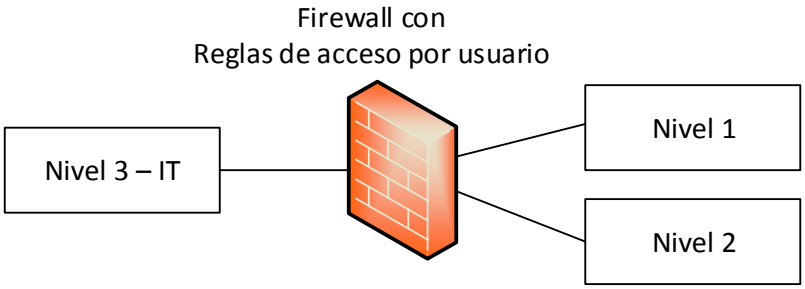
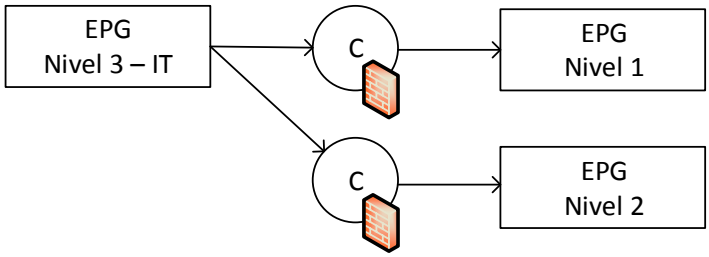


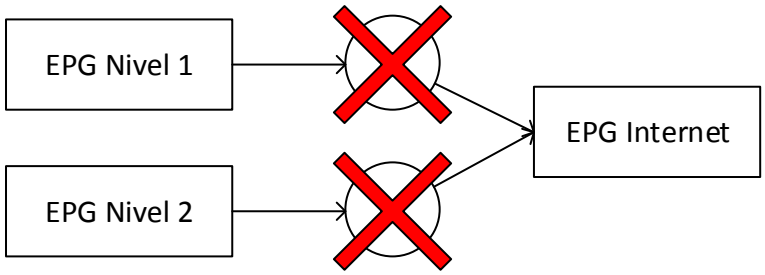
FIGURA 18: ESQUEMA ACI. NIVEL 3 – IT A NIVEL 1 O NIVEL 2



Como se mencionó con anterioridad, los contratos entre Nivel 3 – IT y Nivel 1 y entre Nivel 3 – IT y Nivel 2 contienen un Service Graph para derivar el tráfico a un firewall de autenticación (Figura 18).

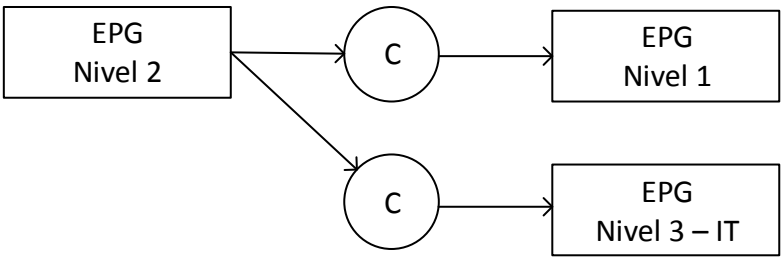
Nivel 2 o Nivel 1 a Internet: estos segmentos no cuentan con acceso a Internet, es decir que no existen contratos entre estos EPG (Figura 19).

FIGURA 19: ESQUEMA ACI. NIVEL 1 O NIVEL 2 A INTERNET



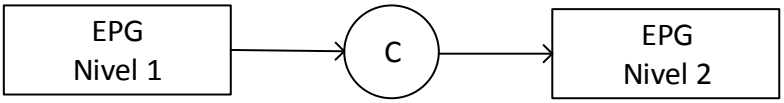
Nivel 2 a Nivel 3 – IT o Nivel 1: los dispositivos de estos segmentos podrán conectarse entre sí, en función de los contratos que se establezcan, basándose en IP, nombre o segmento de red (Figura 20).

FIGURA 20: ESQUEMA ACI. NIVEL 2 A NIVEL 3 – IT O NIVEL 1



Nivel 1 a Nivel 2: sólo podrán comunicarse los dispositivos habilitados en los contratos (Figura 21)

FIGURA 21: ESQUEMA ACI. NIVEL 1 A NIVEL 2



CAPÍTULO 5. CONCLUSIONES

5.1 Metodología de evaluación

Al momento de la evaluación de las alternativas, se tuvieron en cuenta el grado de cumplimiento de las premisas planteadas en el capítulo 2 y la operación posterior.

Considerando que la tecnología tradicional es conocida y está ampliamente desarrollada en la empresa, solamente se realizó una prueba de concepto con la nueva tecnología SDN.

Se planteó en un ambiente de laboratorio, una versión reducida, pero que debió simular cada uno de los ambientes reales. Es decir, que se simuló un core de red distribuido utilizando grandes longitudes de fibra óptica, se estableció un nodo de distribución con sus accesos con el fin de emular una línea de producción, se configuraron servidores de aplicación, se conectaron a la red elementos de control industrial y se realizaron pruebas de acceso y gestión como se harían en la implementación final.

En la prueba participaron cuatro personas del área de tecnología de redes, dos personas del grupo de tecnología de plataforma (servidores, virtualización y almacenamiento), dos integrantes del equipo de control industrial y un especialista de Cisco. Cabe aclarar, que de las nueve personas involucradas, siete son argentinos y dos, estadounidenses.

Por último, se acordó entre los sectores, una matriz de evaluación dividida en áreas de importancia ponderadas y un puntaje de 1 a 5 siendo 1 el más bajo.

5.2 Resultados de la prueba de concepto

El laboratorio se desarrolló durante el mes de mayo de 2016 en las nuevas instalaciones de la empresa en Estados Unidos y se pudieron validar las conclusiones preliminares expresadas en el punto 3.3.3:

- ACI es una arquitectura innovadora que provee centralizadamente, la gestión y visibilidad tanto de la red física como de la virtual.
- La configuración inicial de ACI tomó aproximadamente, 15 minutos usando PXE (Entorno de ejecución de pre inicio) para instalar los controladores APIC. También se pudo verificar que la solución escala rápidamente mediante el agregado de nuevos switches LEAF que son configurados con scripts personalizables.
- Reemplazar o agregar un miembro al Fabric (SPINE o LEAF) fue una tarea automática que se pudo realizar en pocos minutos sin alterar al resto de la red.
- Dentro del Fabric, por defecto, ningún dispositivo se pudo comunicar con otro, excepto que un contrato fuera definido explícitamente, lo que permitió la separación lógica de aplicaciones, independientemente del segmento de red o VLAN.
- ACI se integra nativamente con la infraestructura virtual, de forma que es posible tener gestión y visibilidad de los switches virtuales.

5.3 Matriz de evaluación

Área	Ponderación del área	Requerimiento	Ponderación del requerimiento	Ponderación total	Diseño tradicional	Diseño SDN
Disponibilidad	4	Redundancia de conexiones	5	7.33%	5	5
		Redundancia de los equipos de red	4	5.86%	5	5
		Dos centros de datos con el mismo nivel de servicios de red	4	5.86%	5	5
Performance	5	Baja latencia	5	23.81%	4	4
Sinergia	3	Procesamiento del Nivel 2 y 3 de AUTO en el mismo centro de datos de IT	4	5.19%	5	5
		Consolidación de hardware entre IT y AUTO siempre que sea posible	3	3.90%	3	5
		Posibilidad de coexistencia de las redes lógicas de IT y AUTO en cualquier dispositivo de red	4	5.19%	4	5
Seguridad	5	Redes de nivel 1 enrutadas localmente en cada línea de producción, pero con conectividad al resto de la organización	5	8.50%	5	5
		Segregación lógica entre IT y AUTO a través de reglas de acceso	4	6.80%	3	5
		Conectividad controlada a cada nivel de cada línea de producción desde la red corporativa e Internet	5	8.50%	3	5
Operación	4	Simplicidad en la operación	4	4.23%	3	4
		Automatización de tareas rutinarias	3	3.17%	2	4
		Estabilidad frente a errores comunes	5	5.29%	2	4
		Troubleshooting	4	4.23%	4	3
		Grado de expertise	2	2.12%	4	2
				100%	3.92	4.49

Si bien ambas soluciones podrían cumplir con los requerimientos, el esfuerzo necesario para implementar la solución con un modelo de networking tradicional sería significativamente mayor que con un modelo SDN Cisco ACI y al mismo tiempo, la operación diaria sería considerablemente más compleja.

5.4 Próximos pasos

Una de las ventajas que brinda ACI es la integración con otros sistemas mediante APIs, lo que abre la puerta a un sinfín de posibilidades.

Será el desafío de los próximos años desarrollar portales que permitan la automatización de tareas cotidianas como creación de VLANs, asignación de servidores a EPG, configuración de contratos o provisión de máquinas virtuales.

GLOSARIO

ACI. *Application Centric Infrastructure.* Infraestructura centrada en la aplicación. Es el nombre comercial que recibe la arquitectura de red definida por software de Cisco.

API. *Applicaton Programming Interface.* Interfaz de programación de aplicaciones. Es el conjunto de subrutinas, funciones y procedimientos que ofrece cierta biblioteca para ser utilizado por otro programa como una capa de abstracción.

APIC. *Application Policy Infrastructure Controller.* Controlador de la infraestructura de política de aplicación. Es el nombre comercial del controlador de la solución ACI de Cisco.

AUTO. Nombre interno que recibe el área de control industrial o automatización de procesos industriales.

BGP. *Border Gateway Protocol.* Protocolo de puerta de enlace de borde. Es un protocolo exterior estándar diseñado para intercambiar rutas e información de disponibilidad entre sistemas autónomos. Es el protocolo de enrutamiento utilizado en Internet.

Broadcast. En telecomunicaciones, es un método para transferir un mensaje a todos destinatarios, simultáneamente.

Broadcast domain. Dominio de broadcast. Es una porción de la red en la que todos los dispositivos pueden alcanzarse entre sí mediante broadcast. Grandes dominios de broadcast, con muchos dispositivos, reducen notablemente el desempeño de la red.

Cloud Computing. Computación en la nube. Es un tipo de cómputo basado en internet que provee procesamiento mediante el uso de recursos compartidos.

Core (networking). Núcleo. Se refiere al núcleo de una red, al conjunto de dispositivos centrales de una topología.

DHCP. *Dynamic Host Configuration Protocol.* Protocolo de configuración dinámica de dispositivo. Es un protocolo del tipo cliente-servidor que establece la forma en la que se deben solicitar y asignar dinámicamente, direcciones IP en una red.

DNS. *Domain Name Server.* Servidor de nombres de dominio. Es un conjunto de protocolos y entidades jerárquicas que estable la forma en la que nombres de dominio deben ser traducidos a direcciones IP.

EP. *End Point. Dispositivo.* En nomenclatura ACI, es cualquier elemento terminal del sistema.

EPG, sEPG, dEPG. *End Point Group.* Grupo de dispositivos. En nomenclatura ACI, es un grupo de end points.

Ethernet. También conocido como IEEE 802.3, es un protocolo que, de acuerdo al modelo OSI, establece parámetros de capa 1 y 2 como los niveles de tensión, cableado, acceso al medio y formato de tramas.

Fabric. Sistema o matriz de conmutación. En nomenclatura ACI, es el nombre que recibe el sistema de conmutación distribuido integrado por los diferentes switches.

Firewall. Cortafuego. Elemento de seguridad de red que cuenta en su configuración con reglas que permiten o rechazan determinados patrones de tráfico.

Firmware. Es un tipo de programa que establece instrucciones de bajo nivel para controlar físicamente el hardware.

HTTP. *Hypertext Transfer Protocol.* Protocolo de transferencia de hipertexto. Es un protocolo de comunicaciones que permite las transferencias de información de páginas web.

HTTPS. *Hypertext Transfer Protocol Secure.* Protocolo seguro de transferencia de hipertexto. Es igual a HTTP sólo que cuenta con encripción de datos.

IP. *Internet Protocol.* Protocolo de Internet. Es el principal protocolo de comunicaciones de internet. Está encargado del enrutamiento de los paquetes a través de las diferentes redes.

IS-IS. *Intermediate System to Intermediate System.* Sistema intermedio a sistema intermedio. Es un protocolo de enrutamiento interior diseñado para mover paquetes en una red de datos eligiendo el mejor camino.

ISO (image). *Imagen ISO.* Es un formato de almacenamiento de archivos en formato óptico. Una imagen del disco que contiene cada uno de los sectores, incluyendo el sistema de archivos del disco.

IT. *Information Technology.* Tecnología de la información. En el contexto del presente trabajo, se refiere al área de la empresa encargada de la gestión de los sistemas informáticos y su infraestructura.

LAN. *Local Area Network.* Red de área local. Es un tipo de red que interconecta dispositivos en geográficamente próximos, como dentro de un edificio, campus o empresa.

LEAF. Hoja de árbol. En la nomenclatura ACI, se refiere a los switches extremos o secundarios a donde se conectan todos los dispositivos.

LLDP. *Link Layer Discovery Protocol.* Protocolo de descubrimiento de capa de enlace. Es un protocolo estándar diseñado para publicar la identidad y capacidades de un dispositivo a sus vecinos en un ambiente LAN.

NIC. *Network Interface Card.* Placa de interfaz de red. Es la placa de un dispositivo que lo conecta con la red.

OSPF. *Open Shortest Path First.* Primero el camino más corto. Es un protocolo de enrutamiento interior, diseñado para calcular la mejor ruta entre dos dispositivos de un mismo sistema.

OSI Model. *Open System Interconnection Model.* Modelo de interconexión de sistemas abiertos. Es un modelo de referencia para los protocolos de la red de arquitectura en capas. Está separado en siete niveles y establece las funciones de cada uno: Capa física, capa de enlace, capa de red, capa de transporte, capa de sesión, capa de presentación y capa de aplicación.

OTP. *One Time Password.* Contraseña de única vez. Es un tipo de contraseña que sólo es válida para una única autenticación. Una vez usada, es desechada. Por lo general, se implementa mediante una aplicación que se ejecuta en algún dispositivo portátil y que solicita alguna clave para iniciar.

Proxy. Es un sistema o aplicación que actúa como intermediario entre los clientes y los recursos. Típicamente, se utilizan para que los usuarios no accedan directamente a Internet. Posibilitan además, el filtrado de contenido, el control de acceso y mejoran la performance, almacenado parte del contenido de forma local.

PXE. *Preboot Execution Enviroment.* Entorno de ejecución de pre arranque. Es un estándar que establece cómo un dispositivo que soporta PXE debe iniciarse descargando de un servidor el programa necesario.

Router. Enrutador. De acuerdo al modelo OSI, es un dispositivo de capa 3 que interconecta redes. Su función principal es conmutar paquetes entre diferentes segmentos de red.

SDN. *Software Defined Networks.* Redes definidas por software. Es un concepto que define una arquitectura para desacoplar el plano de control del plano de datos y permite a un administrador tener mayor gestión sobre la red.

Service Chaining. Encadenamiento de servicios. En SDN, es una funcionalidad que permite que el flujo de datos entre dos dispositivos de la red, sea derivado previamente a un tercer dispositivo, como un balanceador de tráfico o un firewall.

Service Graph. Gráfico de servicio. En nomenclatura ACI, representa el mismo concepto de Service Chaining.

SPINE. Espina. En nomenclatura ACI, son los switches principales a los que sólo se conectan los LEAVES.

SSH. *Secure Shell.* Shell seguro. Es un protocolo que sirve para operar sistemas de forma remota. Implementa criptografía para cifrar los datos de gestión entre el cliente SSH y el sistema que se quiere administrar.

STP. *Spanning Tree Protocol.* Protocolo del árbol de expansión. De acuerdo al modelo OSI, es un protocolo de capa 2, diseñado para evitar bucles en redes Ethernet.

Switch. Conmutador. De acuerdo al modelo OSI, es un dispositivo de capa 2 que conmuta tramas. En el contexto del presente trabajo, siempre se hace referencia a switches Ethernet.

Telnet. Es un protocolo similar a SSH, pero sin cifrado de datos.

ToR. *Top of the Rack.* Arriba del gabinete. En diseño de centro de datos, es un criterio que establece la instalación de algún dispositivo concentrador, por lo general switches, en la parte superior del rack, para simplificar el cableado.

VLAN. *Virtual Local Area Network.* Red de área local virtual. Es la subdivisión lógica de una LAN que permite agrupar dispositivos de funciones similares y reducir los dominios de broadcast.

VMWare. Es una compañía que provee una plataforma de virtualización sobre arquitectura de procesadores x86. Un sistema operativo llamado hipervisor, crea una capa de abstracción del hardware subyacente permitiendo un uso eficiente de los recursos de procesamiento. Cada uno de los sistemas que se ejecutan sobre el hipervisor se los llama máquinas virtuales.

vNIC. *Virtual Network Interface Card.* Placa de interfaz de red virtual. Similar a la NIC, pero en un entorno de virtualización.

VPN. *Virtual Private Network.* Red privada virtual. Es una red privada que se extiende sobre otra red pública o compartida. En el contexto del presente trabajo, es una conexión cifrada hacia la compañía, que pueden establecer los usuarios, desde cualquier lugar del mundo, con el objeto de acceder a servicios corporativos como correo electrónico, intranet, archivos compartidos y otros.

VRF. *Virtual Routing and Forwarding.* Enrutamiento y reenvío virtual. Es una tecnología que permite múltiples instancias de enrutamiento en un mismo dispositivo. Como las tablas de rutas son

independientes, es posible que los espacios de direcciones IP estén superpuestos, sin que eso represente un problema.

VXLAN. *Virtual Extensible Local Area Network.* Red de área local virtual extensible. Es una tecnología que encapsula tramas Ethernet de capa 2 en paquetes IP. Esto permite extender una LAN a través de una red IP.

BIBLIOGRAFÍA

I. Andrew S. Tanenbaum, David J. Wetherall. *"Computer Networks. 5th Edition"*. Pearson. 2011.

II. Dr. Sidnie Feit. *"TCP/IP. Arquitectura, protocolos e implementación con IPv6 y seguridad de IP"*. McGraw-Hill. 1998.

III. Craig Hunt. *"TCP/IP. Network Administration. 3rd Edition."* O´Reilly Media. 2002.

IV. Cisco. *"Principles of Application Centric Infrastructure"*. White Paper. Cisco, Nov. 2013. http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps13004/ps13460/white-paper-c11-729906_ns1261_Networking_Solutions_White_Paper.html

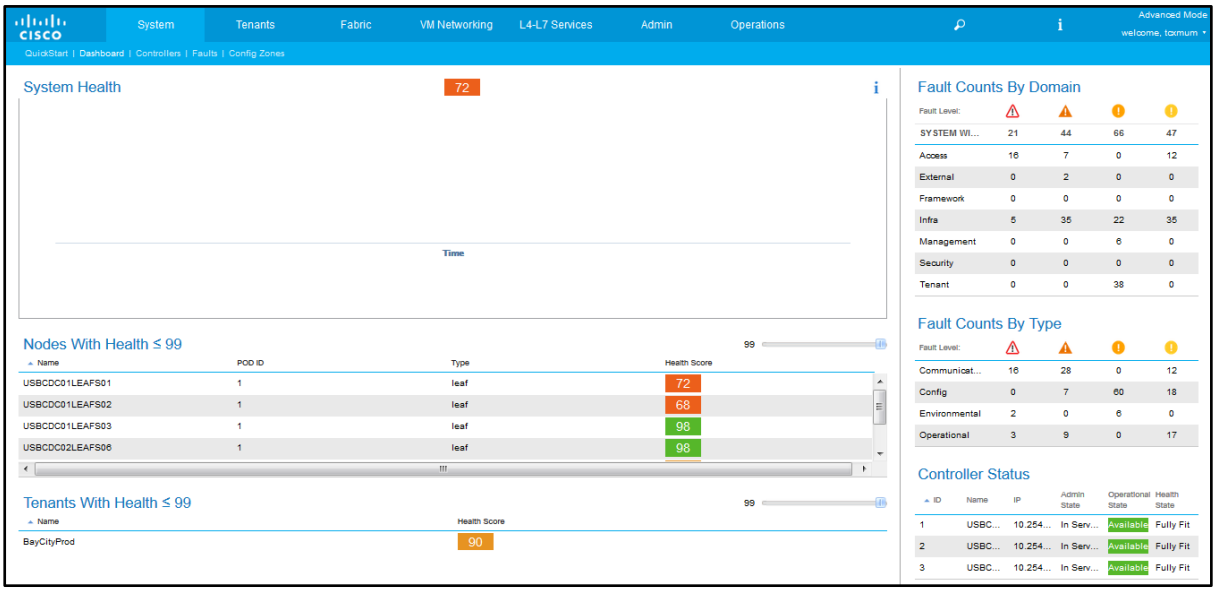
V. Cisco. *"Cisco Application Centric Infrastructure Zero-Touch Fabric"*. Application Note. Cisco, Nov. 2013. http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/aci-fabric-controller/application-note-c27-729997.html

APÉNDICE I. EJEMPLOS DEL SISTEMA

I. Pantalla de inicio. Dashboard

Vista general al ingresar al sistema. Se pueden observar distintos indicadores de salud del sistema y un resumen de alarmas y errores.

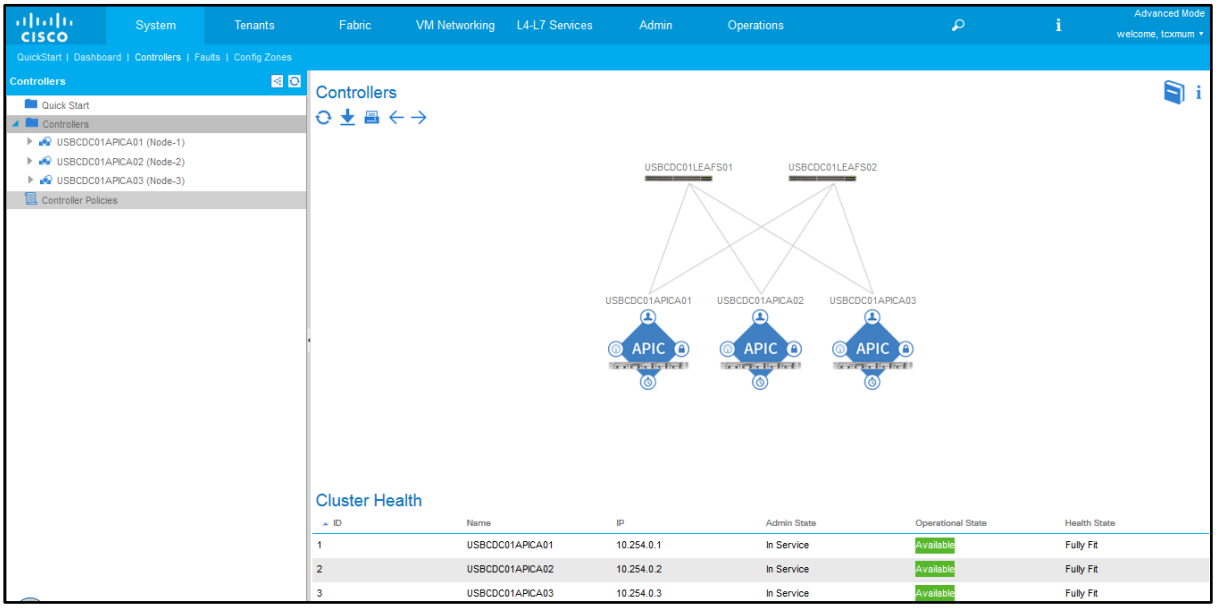
Captura 5:



CAPTURA 1: DASHBOARD DE INICIO

II. Vista de los controladores

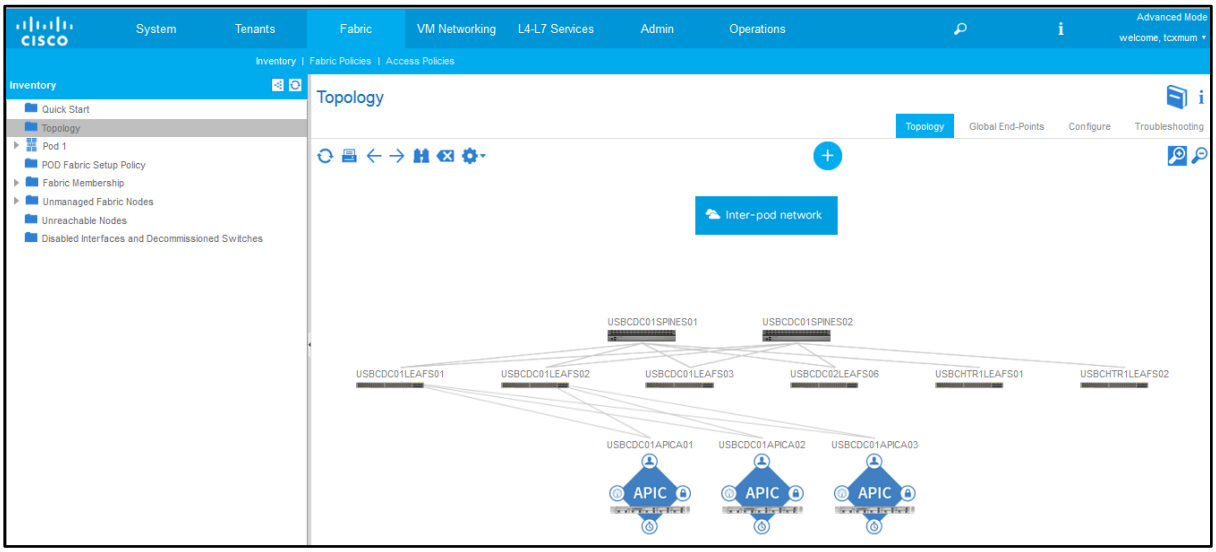
Vista topológica y del estado de los controladores APIC.



CAPTURA 2: TOPOLOGÍA DE CONTROLADORES

III. Fabric

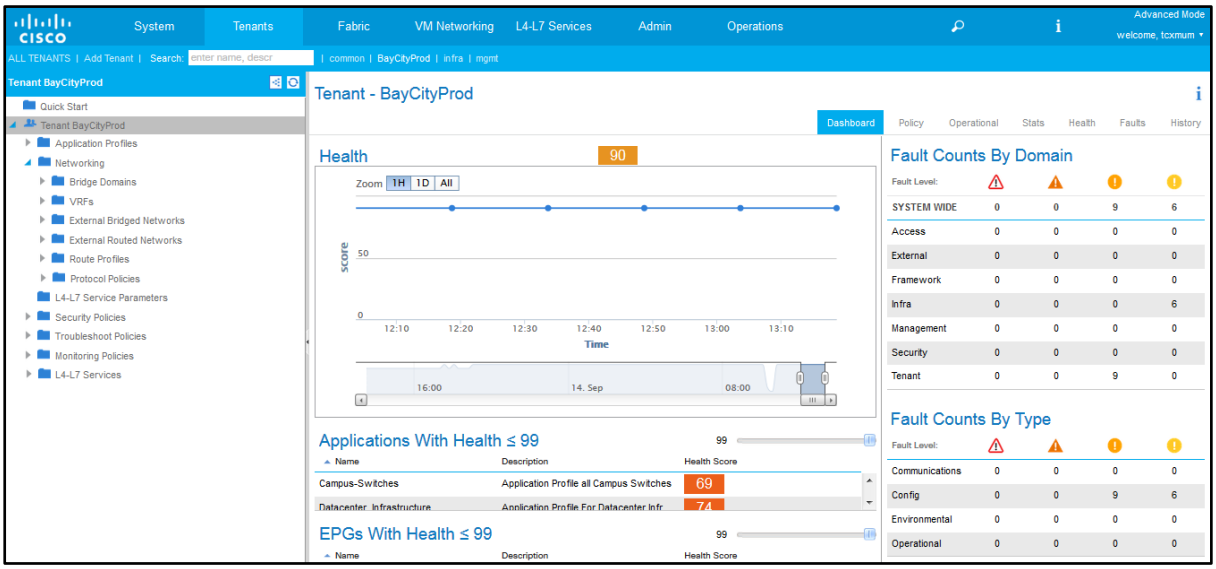
Vista general del Fabric. Desde esta parte del menú, se pueden realizar las configuraciones que tienen que ver más con la parte física de la topología.



CAPTURA 3: TOPOLOGÍA DEL FABRIC

IV. Tenants

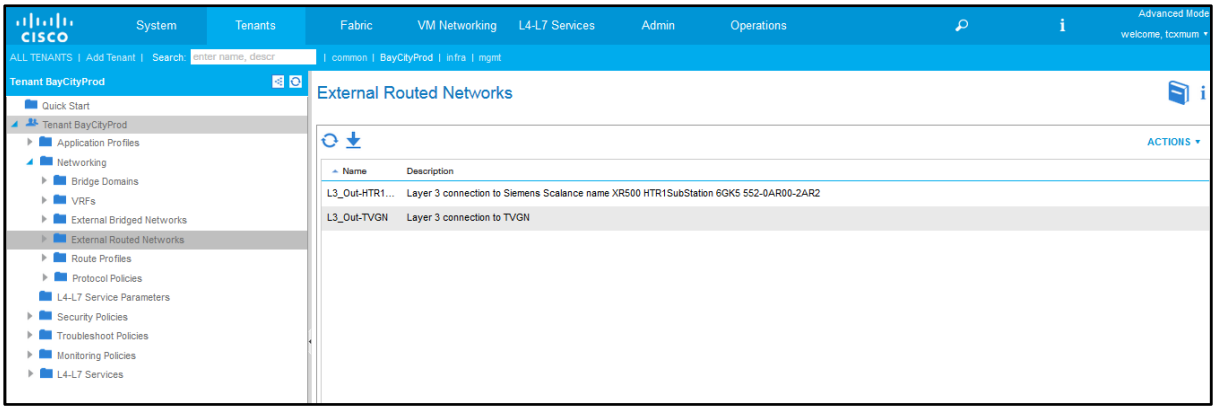
En esta sección, se configura todo lo concerniente a la lógica del sistema. La mayoría de los conceptos vistos en el presente trabajo se crean y modifican desde aquí.



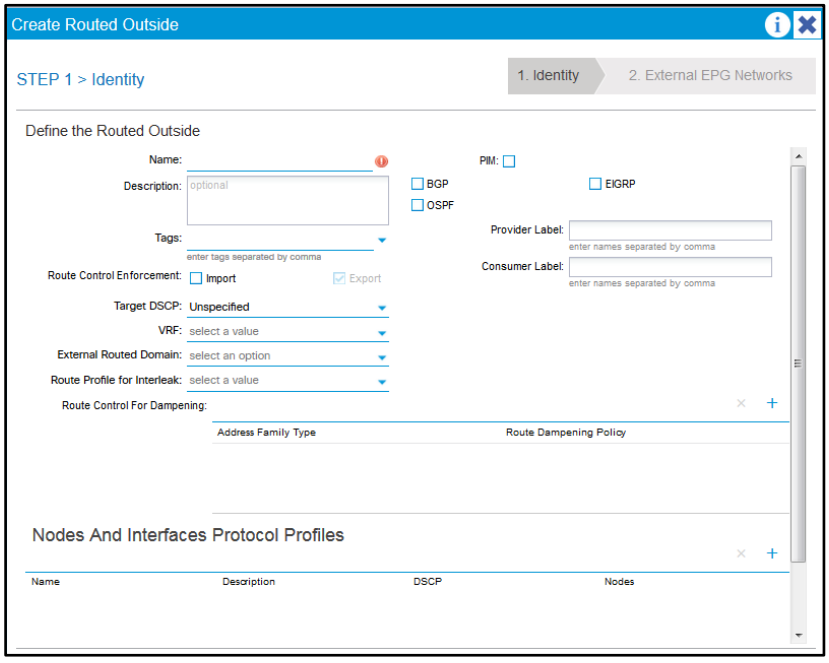
CAPTURA 4: VISTA PRINCIPAL DEL TENANT

V. Enrutamiento hacia fuera del Fabric

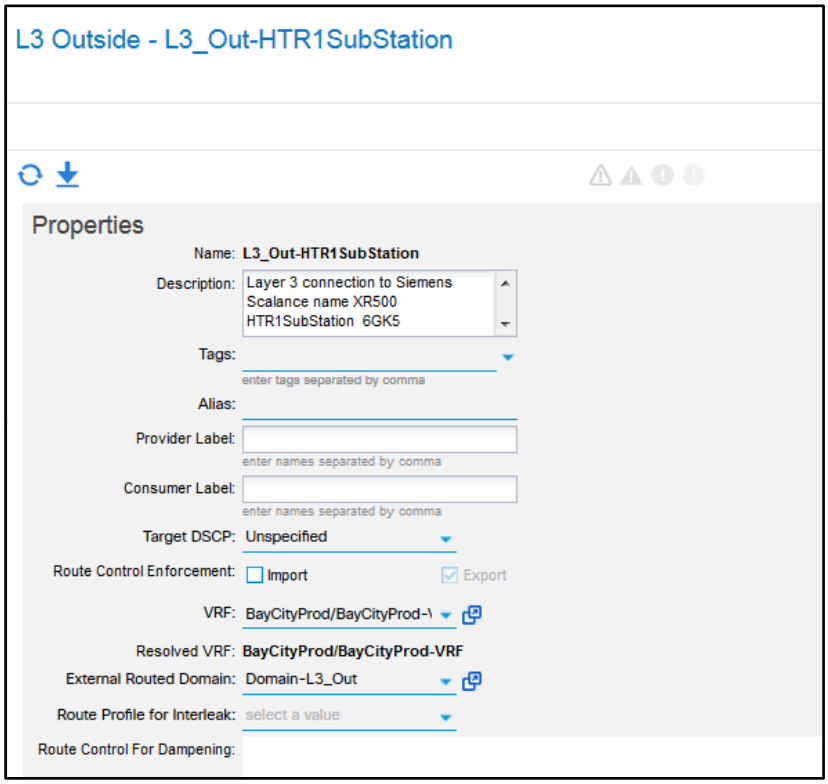
Llamados L3-out, son las rutas estáticas que direccionan los segmentos de Nivel 1 y el enrutamiento dinámico que comunica el Fabric con el resto de la compañía. Se configuran desde el menú de Tenants mencionado en el punto anterior.



CAPTURA 5: VISTA PRINCIPAL DE SALIDAS DE ENRUTAMIENTO

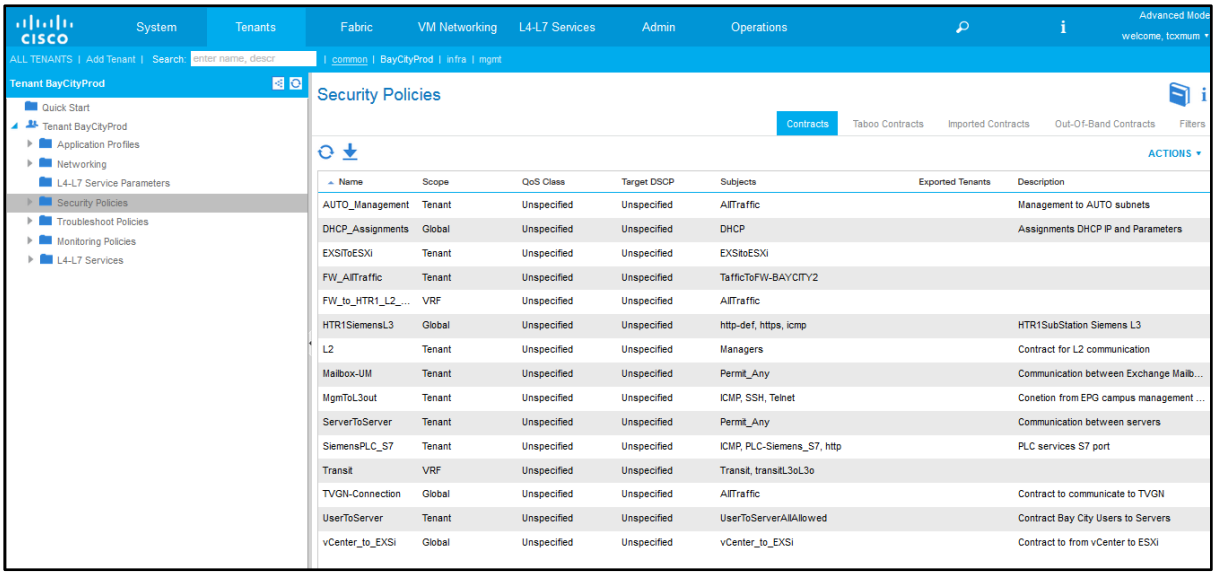


CAPTURA 6: PANTALLA DE CARGA DE UNA SALIDA DE ENRUTAMIENTO

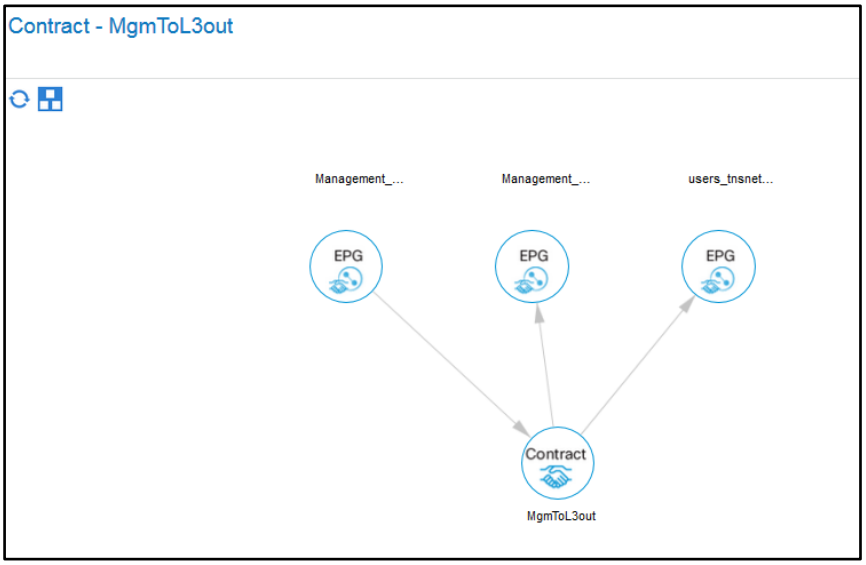


CAPTURA 7: PANTALLA DE UNA DE LAS SALIDAS DE ENRUTAMIENTO

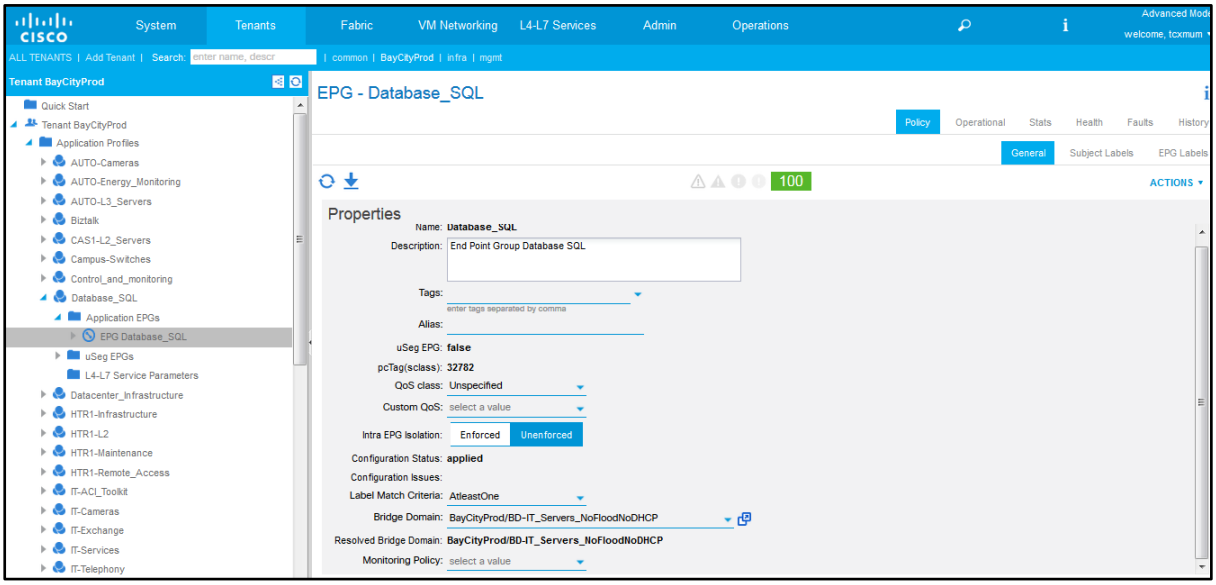
VI. Contratos



CAPTURA 8: VISTA DE LOS CONTRATOS



CAPTURA 9: EJEMPLO DE UN CONTRATO SENCILLO



CAPTURA 10: EJEMPLO DE UN EPG

APÉNDICE II. ESPECIFICACIÓN TÉCNICA PARA LA ORDEN DE COMPRA

La siguiente lista de materiales incluye todos los componentes de networking que finalmente se compraron para la planta. Muchos de ellos no son mencionados en el presente trabajo, ya que no forman parte central de la solución de SDN.

I. Centro de datos

Número de parte	Descripción	Duración	Cant.
DC - 2Spines/3APIC			
ACI-C9336-APIC-B1	ACI Bundle with 2 9336 and APIC	---	1
N9K-C9336PQ	Nexus 9K ACI Spine, 36p 40G QSFP+	---	2
CON-3SNT-9336PQ	3YR SMARTNET 8X5XNBD Nexus 9336 ACI Spine switchw/36p 40G QS	36	2
ACI-N9KDK9-11.1	Nexus 9K ACI Base Software NX-OS Rel 11.1	---	2
N9K-C9300-ACK	Nexus 9300 Accessory Kit	---	2
CAB-N5K6A-NA	Power Cord, 200/240V 6A North America	---	4
N9K-C9300-RMK	Nexus 9300 Rack Mount Kit	---	2
N9K-C9300-FAN3-B	Nexus 9300 Fan 3, Port-side Exhaust	---	4
N9K-PAC-1200W-B	Nexus 9300 1200W AC PS, Port-side Exhaust	---	4
APIC-CLUSTER-M2	APIC Cluster - Medium Configurations (Up to 1000 Edge Ports)	---	1
CON-SSSNT-APIC3M2	SOLN SUPP 8X5XNBD APIC Cluster - Medium Configurations (Up	36	1
APIC-SERVER-M2	APIC Appliance - Medium Configuration (Upto 1000 Edge Ports)	---	1
APIC-A03-D600GA2	2.5" 600GB, 10K RPM, SAS 6Gb	---	2
APIC-MRAID12G	Avila Cisco 12G SAS Modular Raid Controller (Raid 0/1)	---	1
APIC-PSU1-770W	770W power supply for USC C-Series	---	1
APIC-USBFLSHB-16GB	UCS Servers 16GB Flash USB Drive	---	1
APIC-TPM2-001	Trusted Platform Module	---	1
APIC-MR-1X162RU-A	16GB DDR4-2133-MHz RDIMM/PC4-17000/dual rank/x4/1.2v	---	4
APIC-SD120G0KS2-EV	120 GB 2.5 inch Enterprise Value 6G SATA SSD	---	1
APIC-CPU-E52609D	1.90 GHz E5-2609 v3/85W 6C/15MB Cache/DDR4 1600MHz	---	2
R2XX-RAID0	Enable RAID 0 Setting	---	1
APIC-PSU1-770W	770W power supply for USC C-Series	---	1
APIC-PCIE-CSC-02	Cisco VIC 1225 Dual Port 10Gb SFP+ CNA	---	1
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	---	2
APIC-DK9-1.1	APIC Base Software Release 1.1	---	1
APIC-SERVER-M2	APIC Appliance - Medium Configuration (Upto 1000 Edge Ports)	---	1
APIC-A03-D600GA2	2.5" 600GB, 10K RPM, SAS 6Gb	---	2

APIC-MRAID12G	Avila Cisco 12G SAS Modular Raid Controller (Raid 0/1)	---	1
APIC-PSU1-770W	770W power supply for USC C-Series	---	1
APIC-USBFLSHB-16GB	UCS Servers 16GB Flash USB Drive	---	1
APIC-TPM2-001	Trusted Platform Module	---	1
APIC-MR-1X162RU-A	16GB DDR4-2133-MHz RDIMM/PC4-17000/dual rank/x4/1.2v	---	4
APIC-SD120G0KS2-EV	120 GB 2.5 inch Enterprise Value 6G SATA SSD	---	1
APIC-CPU-E52609D	1.90 GHz E5-2609 v3/85W 6C/15MB Cache/DDR4 1600MHz	---	2
R2XX-RAID0	Enable RAID 0 Setting	---	1
APIC-PSU1-770W	770W power supply for USC C-Series	---	1
APIC-PCIE-CSC-02	Cisco VIC 1225 Dual Port 10Gb SFP+ CNA	---	1
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	---	2
APIC-DK9-1.1	APIC Base Software Release 1.1	---	1
APIC-SERVER-M2	APIC Appliance - Medium Configuration (Upto 1000 Edge Ports)	---	1
APIC-A03-D600GA2	2.5" 600GB, 10K RPM, SAS 6Gb	---	2
APIC-MRAID12G	Avila Cisco 12G SAS Modular Raid Controller (Raid 0/1)	---	1
APIC-PSU1-770W	770W power supply for USC C-Series	---	1
APIC-USBFLSHB-16GB	UCS Servers 16GB Flash USB Drive	---	1
APIC-TPM2-001	Trusted Platform Module	---	1
APIC-MR-1X162RU-A	16GB DDR4-2133-MHz RDIMM/PC4-17000/dual rank/x4/1.2v	---	4
APIC-SD120G0KS2-EV	120 GB 2.5 inch Enterprise Value 6G SATA SSD	---	1
APIC-CPU-E52609D	1.90 GHz E5-2609 v3/85W 6C/15MB Cache/DDR4 1600MHz	---	2
R2XX-RAID0	Enable RAID 0 Setting	---	1
APIC-PSU1-770W	770W power supply for USC C-Series	---	1
APIC-PCIE-CSC-02	Cisco VIC 1225 Dual Port 10Gb SFP+ CNA	---	1
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	---	2
APIC-DK9-1.1	APIC Base Software Release 1.1	---	1
DC - APIC Extra			
APIC-M1	APIC Appliance - Medium Configuration(Upto 1000 EdgePorts)	---	1
CON-SSSNT-APICM1	SOLN SUPP 8X5XNBD APIC Appliance - Medium Configuration(Up	36	1
APIC-SERVER-M1	APIC Appliance - Medium Configuration (Upto 1000 Edge Ports)	---	1
APIC-TPM1-001	Trusted Platform Module	---	1
APIC-USBFLSH-S-4GB	4G USB small form factor	---	1
APIC-RAID-11-C220	Cisco UCS RAID SAS 2008M-8i Mezz Card for C220 (0/1/10/5/50)	---	1
APIC-CPU-E52620B	2.10 GHz E5-2620 v2/80W 6C/15MB Cache/DDR3 1600MHz	---	2
APIC-SD120G0KS2-EV	120 GB 2.5 inch Enterprise Value 6G SATA SSD	---	1
APIC-A03-D500GC3	500GB 6Gb SATA 7.2K RPM SFF hot plug/drive sled mounted	---	2
R2XX-RAID0	Enable RAID 0 Setting	---	1
APIC-PSU-650W	650W power supply for C-series rack servers	---	1

APIC-MR-1X162RZ-A	16GB DDR3-1866-MHz RDIMM/PC3-14900/dual rank/x4/1.5v	---	4
APIC-PSU-650W	650W power supply for C-series rack servers	---	1
APIC-PCIE-CSC-02	Cisco VIC 1225 Dual Port 10Gb SFP+ CNA	---	1
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	---	2
APIC-DK9-1.1	APIC Base Software Release 1.1	---	1
DC - 2Spines			
N9K-C9336PQ	Nexus 9K ACI Spine, 36p 40G QSFP+	---	2
CON-3SNT-9336PQ	3YR SMARTNET 8X5XNBD Nexus 9336 ACI Spine switchw/36p 40G QS	36	2
ACI-N9KDK9-11.1	Nexus 9K ACI Base Software NX-OS Rel 11.1	---	2
N9K-C9300-ACK	Nexus 9300 Accessory Kit	---	2
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	---	4
N9K-C9300-RMK	Nexus 9300 Rack Mount Kit	---	2
N9K-C9300-FAN3-B	Nexus 9300 Fan 3, Port-side Exhaust	---	4
N9K-PAC-1200W-B	Nexus 9300 1200W AC PS, Port-side Exhaust	---	4
DC - 6Leafs			
N9K-C9372PX-E-B18Q	2 Nexus 9372PX-E with 8 QSFP-40G-SR-BD	---	3
CON-3SNT-72PEB18Q	3YR SNTC 8X5XNBD 2 Nexus 9372PX-E with 8 QSFP-40G-SR-BD	36	3
N9K-C9372PX-E-BUN	Nexus 9372PX-E bundle PID	---	3
CON-3SNT-372PXEBN	3YR SNTC 8X5XNBD Nexus 9372PX-E bundle PID	36	3
N3K-C3064-ACC-KIT	Nexus 3064PQ Accessory Kit	---	3
QSFP-40G-SR-BD	QSFP40G BiDi Short-reach Transceiver	---	12
ACI-N9KDK9-11.1	Nexus 9K ACI Base Software NX-OS Rel 11.1	---	3
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	---	6
NXOS-703I2.1	Nexus 9500, 9300, 3000 Base NX-OS Software Rel 7.0(3)I2(1)	---	3
ACI-LIC-PAK	ACI Software License PAK Expansion	---	3
ACI-N9K-48X	ACI SW license for a 48p 1/10G Nexus 9K	---	3
N9K-C9372PX-E-BUN	Nexus 9372PX-E bundle PID	---	3
CON-3SNT-372PXEBN	3YR SNTC 8X5XNBD Nexus 9372PX-E bundle PID	36	3
N3K-C3064-ACC-KIT	Nexus 3064PQ Accessory Kit	---	3
QSFP-40G-SR-BD	QSFP40G BiDi Short-reach Transceiver	---	12
ACI-N9KDK9-11.1	Nexus 9K ACI Base Software NX-OS Rel 11.1	---	3
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	---	6
NXOS-703I2.1	Nexus 9500, 9300, 3000 Base NX-OS Software Rel 7.0(3)I2(1)	---	3
ACI-LIC-PAK	ACI Software License PAK Expansion	---	3
ACI-N9K-48X	ACI SW license for a 48p 1/10G Nexus 9K	---	3
NXA-FAN-30CFM-F	Nexus 2K/3K/9K Single Fan, port side exhaust airflow	---	12
N9K-PAC-650W-B	Nexus 9300 650W AC PS, Port-side Exhaust	---	6
NXA-FAN-30CFM-F	Nexus 2K/3K/9K Single Fan, port side exhaust airflow	---	12

N9K-PAC-650W-B	Nexus 9300 650W AC PS, Port-side Exhaust	---	6
DC - Twinax40G Spines/Leafs different rows			
QSFP-H40G-AOC15M=	40GBASE Active Optical Cable, 15m	---	8
DC - Twinax40G Spines/Leafs same row			
QSFP-H40G-AOC2M=	40GBASE Active Optical Cable, 2m	---	4
QSFP-H40G-AOC3M=	40GBASE Active Optical Cable, 3m	---	4
DC - SFP40G LR			
QSFP-40GE-LR4=	QSFP 40GBASE-LR4 Transceiver Module, LC, 10KM	---	24
DC - Twinax10G for APIC			
SFP-10G-AOC3M=	10GBASE Active Optical SFP+ Cable, 3M	---	8
SFP-10G-AOC5M=	10GBASE Active Optical SFP+ Cable, 5M	---	8
DC - FEX			
N2K-C2248TP-E	N2K-C2248TP-E-1GE (48x100/1000-T+4x10GE), airflow/PS option	---	4
CON-3SNT-C2248TPE	3YR SMARTNET 8X5XNBD Null SKU-No line item services included	36	4
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	---	8
N2248TP-E-FA-BUN	Standard Airflow pack:N2K-C2248TP-E-1GE, 2 AC PS, 1Fan	---	4
CON-3SNT-2248EFA	3YR SMARTNET 8X5XNBD Standard Airflow pack:N2K-C2248TP-E-1GE	36	4
DC - FEX Twinax to Leaf			
SFP-10G-AOC10M=	10GBASE Active Optical SFP+ Cable, 10M	---	8
DC - Deployment service ACI			
ASF-DCV1-G-ACI-BUN	Cisco DC Deployment Service for ACI Starter Kit	---	1

II. Distribución

Número de parte	Descripción	Duración	Cant.
DISTR - Leaf 9372			
N9K-C9372PX-E-B18Q	2 Nexus 9372PX-E with 8 QSFP-40G-SR-BD	---	4
CON-3SNT-72PEB18Q	3YR SNTC 8X5XNBD 2 Nexus 9372PX-E with 8 QSFP-40G-SR-BD	36	4
N9K-C9372PX-E-BUN	Nexus 9372PX-E bundle PID	---	4
CON-3SNT-372PXEBN	3YR SNTC 8X5XNBD Nexus 9372PX-E bundle PID	36	4
N3K-C3064-ACC-KIT	Nexus 3064PQ Accessory Kit	---	4
QSFP-40G-SR-BD	QSFP40G BiDi Short-reach Transceiver	---	16
ACI-N9KDK9-11.1	Nexus 9K ACI Base Software NX-OS Rel 11.1	---	4
NXA-FAN-30CFM-B	Nexus 2K/3K/9K Single Fan, port side intake airflow	---	16
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	---	8
N9K-PAC-650W	Nexus 9300 650W AC PS, Port-side Intake	---	8
NXOS-703I2.1	Nexus 9500, 9300, 3000 Base NX-OS Software Rel 7.0(3)I2(1)	---	4
ACI-LIC-PAK	ACI Software License PAK Expansion	---	4

ACI-N9K-48X	ACI SW license for a 48p 1/10G Nexus 9K	---	4
N9K-C9372PX-E-BUN	Nexus 9372PX-E bundle PID	---	4
CON-3SNT-372PXEBN	3YR SNTC 8X5XNBD Nexus 9372PX-E bundle PID	36	4
N3K-C3064-ACC-KIT	Nexus 3064PQ Accessory Kit	---	4
QSFP-40G-SR-BD	QSFP40G BiDi Short-reach Transceiver	---	16
ACI-N9KDK9-11.1	Nexus 9K ACI Base Software NX-OS Rel 11.1	---	4
NXA-FAN-30CFM-B	Nexus 2K/3K/9K Single Fan, port side intake airflow	---	16
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	---	8
N9K-PAC-650W	Nexus 9300 650W AC PS, Port-side Intake	---	8
NXOS-703I2.1	Nexus 9500, 9300, 3000 Base NX-OS Software Rel 7.0(3)I2(1)	---	4
ACI-LIC-PAK	ACI Software License PAK Expansion	---	4
ACI-N9K-48X	ACI SW license for a 48p 1/10G Nexus 9K	---	4
DISTR - 1 Uplink from each 9372 to each DC room			
QSFP-40G-LR4=	QSFP 40GBASE-LR4 OTN Transceiver, LC, 10KM	---	32

III. Acceso

Número de parte	Descripción	Duración	Cant.
Access - 3650			
WS-C3650-24PD-L	Cisco Catalyst 3650 24 Port PoE 2x10G Uplink LAN Base	---	100
CON-SNT-WSC364DL	SNTC-8X5XNBD Cisco Catalyst 3650 24 Port PoE 2x10G Up	12	100
S3650UK9-33SE	CAT3650 Universal k9 image	---	100
PWR-C2-640WAC	640W AC Config 2 Power Supply	---	100
CAB-TA-NA	North America AC Type A Power Cable	---	100
PWR-C2-BLANK	Config 2 Power Supply Blank	---	100
C3650-STACK-KIT	Cisco Catalyst 3650 Stack Module	---	100
C3650-STACK	Cisco Catalyst 3650 Stack Module	---	200
STACK-T2-50CM	50CM Type 2 Stacking Cable	---	100
Access - 3650 stack long cable			
STACK-T2-1M=	1M Type 2 Stacking Cable Spare	---	20
Access - SFP Uplink 1G from 3650 to Leafs			
GLC-LH-SMD=	1000BASE-LX/LH SFP transceiver module, MMF/SMF, 1310nm, DOM	---	140
Access - SFP Uplink 10G from 3650 to Leafs			
SFP-10G-LR=	10GBASE-LR SFP Module	---	50
Access - SFP Uplink local from 3650 to 9372			
SFP-10G-AOC3M=	10GBASE Active Optical SFP+ Cable, 3M	---	24
Access - Industrial switch			
IE-4000-8GT8GP4G-E	IE 4000 8 x RJ45 10/100/1000 with 8 x 1G PoE, 4 x 1G Combo ,	---	15
Access - SFP Uplink for IE-4000			
GLC-LH-SMD=	1000BASE-LX/LH SFP transceiver module, MMF/SMF, 1310nm, DOM	---	30

IV. Wireless

Número de parte	Descripción	Duración	Cant.
WLAN - Indoor office AP			
AIR-CAP3702I-A-K9	802.11ac Ctrlr AP 4x4:3SS w/CleanAir; Int Ant; A Reg Domain	---	160
CON-SNT-3702IA	SNTC-8X5XNBD 802.11ac Ctrlr AP 4x	12	160
SWAP3700-RCOVRY-K9	Cisco 3700 Series IOS WIRELESS LAN RECOVERY	---	160
AIR-AP-BRACKET-1	802.11n AP Low Profile Mounting Bracket (Default)	---	160
AIR-AP-T-RAIL-R	Ceiling Grid Clip for Aironet APs - Recessed Mount (Default)	---	160
WLAN - Indoor Mill AP Industrial			
IW3702-2E-UXK9	Industrial Wireless AP 3702, 4 antenna ports on top/bottom	---	40
CON-SNT-IW37022E	SNTC-8X5XNBD Industrial Wireless	12	40
S3G3K9W7-15303JA	Cisco 3700 Series IOS WIRELESS LAN	---	40
SWIW3702-RCOVRY-K9	IW3700 Series IOS Wireless LAN Recovery	---	40
WLAN - Mounting for IW3702			
AIR-ACCPMK3700=	IW3700 Series Pole-Mount Kit	---	40
WLAN - Antenna for IW3702-2E-UXK9 (4 antennas per AP)			
AIR-ANT2547V-N=	2.4 GHz 4dBi/5 GHz 7dBi Dual Band Omni Antenna, N connector	---	160
WLAN - Outdoor AP			
AIR-AP1572EAC-B-K9	802.11ac Outdoor AP, External-Ant, AC-power, Reg. Domain-B	---	20
CON-SNT-AIA157BK	SNTC-8X5XNBD 802.11ac Outdoor AP, External-Ant, AC-po	12	20
SW1570-UM01A01-K9	SW Cisco AP1570: Unified Mesh(8.0.TBD)	---	20
AIR-ANT2547VG-N	2.4 GHz 4dBi/5 GHz 7dBi Dual Band Omni Ant., Gray, N conn.	---	80
WLAN - Directional antenna			
AIR-ANT5114P2M-N=	5 GHz 14 dBi Directional Antenna , 2 port , N connectors	---	6
WLAN - Mount Outdoor			
AIR-ACCPMK1570-2=	1570 Series Pole-Mount Kit (Type-2)	---	20
WLAN - SFP Rugged for outdoor AP			
GLC-LX-SM-RGD=	1000Mbps Single Mode Rugged SFP	---	20
WLAN - SFP protector for outdoor AP			
AIR-ACC15-SFP-GLD=	Outdoor-AP1570, SFP Port Gland, Bag of 5 units	---	20
WLAN - SFP1G for distribution switches			

GLC-LH-SMD=	1000BASE-LX/LH SFP transceiver module, MMF/SMF, 1310nm, DOM	---	20
WLAN - PWR Injector for outdoor AP			
AIR-PWRINJ1500-2=	1520 Series Power Injector	---	20
AIR-PWR-CORD-NA	AIR Line Cord North America	---	20
WLAN - WLC licenses x300			
LIC-CT5520-UPG	Top Level SKU for 5520 AP Adder Licenses	---	1
LIC-CT5520-1A	Cisco 5520 Wireless Controller 1 AP Adder License	---	300
WLAN - WLC			
AIR-CT5520-K9	Cisco 5520 Wireless Controller w/rack mounting kit	---	4
CON-3SNT-AIRT5520	3YR SMARTNET 8X5XNBD Cisco 5520 Wireless Controller	36	4
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	---	4
AIR-CT5520-SW-8.1	Cisco 5520 Wireless Controller SW Rel. 8.1	---	4
AIR-PSU1-770W	770W AC Hot-Plug Power Supply for 5520 Controller	---	4
AIR-BZL-C220M4	Cisco 5520 Wireless Controller Security Bezel	---	4
AIR-CPU-E52609D	1.90 GHz E5-2609 v3/85W 6C/15MB Cache/DDR4 1600MHz	---	4
AIR-CT6870-NIC-K9	PCIe Network Interface 20G	---	4
AIR-MR-1X081RU-A	8GB DDR4-2133-MHz RDIMM/PC4-17000/single rank/x4/1.2v	---	16
AIR-SD-32G-S	32GB SD Card for UCS servers	---	4
AIR-SD240G0KS2-EV	240GB 2.5 inch Enterprise Value 6G SATA SSD	---	4
AIR-TPM2-001	Trusted Platform Module 1.2 for UCS (SPI-based)	---	4
WLAN - Twinax for WLC			
SFP-10G-AOC10M=	10GBASE Active Optical SFP+ Cable, 10M	---	4
WLAN - Prime			
R-PI2X-N-K9	Cisco Prime Infrastructure 2.x - No Node Lock	---	1
L-PILMS42-KIT	Prime Infrastructure - LMS License Kit	---	1
L-PI2X-LF-N-500	Prime Infrastructure 2.x - Lifecycle - 500 Device Lic-NNL	---	1
L-PILMS42A-500	Prime Infrastructure LMS 4.2A - 500 Device Base Lic	---	1
WLAN - ISE base lic			
L-ISE-BSE-1K=	Cisco Identity Services Engine 1000 EndPoint Base License	---	1
WLAN - ISE Advance			

L-ISE-ADV-S-1K=	Cisco ISE 1K EndPoint Advanced Subscription License	---	1
ISE-ADV-3YR-1K	Cisco ISE 3-Yr 1K EndPoint Advanced License	36	1
WLAN - ISE server			
R-ISE-VM-K9=	Cisco Identity Services Engine VM (eDelivery)	---	1

V. WAN

Número de parte	Descripción	Duración	Cant.
WAN - Router			
ISR4451-X-V/K9	Cisco ISR 4451 UC Bundle, PVDM4-64, UC Lic,CUBE25	---	2
CON-3SNT-ISR4451-X	3YR SMARTNET 8X5XNBD Cisco ISR 4451 UC Bu	36	2
SL-44-IPB-K9	IP Base License for Cisco ISR 4400 Series	---	2
MEM-4400-4GU16G	4G to 16G DRAM Upgrade (8G+8G) for Cisco ISR 4400	---	2
MEM-FLASH-8U32G	8G to 32G Compact Flash Memory Upgrade for Cisco ISR 4450	---	2
PWR-4450-AC	AC Power Supply for Cisco ISR 4450 and ISR4350	---	2
CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	---	2
MEM-4400-DP-2G	2G DRAM (1 DIMM) for Cisco ISR 4400 Data Plane	---	2
PWR-COVER-4450	Cover for empty 2nd Power Supply slot on Cisco ISR 4450	---	2
SL-44-UC-K9	Unified Communication License for Cisco ISR 4400 Series	---	2
NIM-BLANK	Blank faceplate for NIM slot on Cisco ISR 4400	---	4
PVDM4-64	64-channel DSP module	---	2
SM-S-BLANK	Removable faceplate for SM slot on Cisco 2900,3900,4400 ISR	---	4
POE-COVER-4450	Cover for empty POE slot on Cisco ISR 4450	---	4
FL-CUBEE-25	Unified Border Element Enterprise License - 25 sessions	---	2
SISR4400UK9-315S	Cisco ISR 4400 Series IOS XE Universal	---	2
NIM-1MFT-T1/E1	1 port Multiflex Trunk Voice/Clear-channel Data T1/E1 Module	---	2
PVDM4-64	64-channel DSP module	---	2
WAN - WAAS			
WAVE-694-K9	Wide Area Virtualization Engine 694	---	2
CON-3SNT-WAVE694K	3YR SMARTNET 8X5XNBD Wide Area Virtualization Engine 694	36	2
CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	---	2
SF-WAAS-5.5-WAV-K9	WAAS 5.5 SW image for WAVE 294, 594, 694, 75xx, 85xx	---	2
WAAS-VB-LIC	WAAS Virtual Blade License	---	2
MEM-694-24GB	WAVE 694 24GB memory upgrade	---	2
CVR-WAVE-IOM	WAVE IOM blank cover	---	2
CVR-WAVE-PS	WAVE power supply blank cover	---	2
WAAS-ENT-APL	Cisco WAAS Enterprise License for 1 WAE Appliance	---	2
CON-SAU-WAASENAP	SW APP SUPP + UPGR Cisco WAAS Enterprise Lic for 1 WAE	36	2
SSD-694-600GB	600GB SSD drive for WAVE 694	---	4