

**UNIVERSIDAD NACIONAL DE INGENIERÍA**  
FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA



**DISEÑO E IMPLEMENTACIÓN PARA LA RED DEL CENTRO DE  
SERVICIOS DE UNA EMPRESA OPERADORA MÓVIL  
INFORME DE COMPETENCIA PROFESIONAL  
PARA OPTAR EL TÍTULO PROFESIONAL DE:**

**INGENIERO ELECTRÓNICO**

**PRESENTADO POR:**

**JOSÉ ANDRÉS GAMARRA DEL VALLE**

**PROMOCIÓN**

**2006- II**

**LIMA – PERÚ**

**2013**

**DISEÑO E IMPLEMENTACIÓN PARA LA RED DEL CENTRO DE SERVICIOS DE UNA  
EMPRESA OPERADORA MÓVIL**

Dedico este trabajo a mi querida familia  
quienes son mi constante soporte para  
todos los nuevos retos que emprendo.

## SUMARIO

Actualmente la operadora móvil de telecomunicaciones cuenta con una infraestructura de red para contener sus plataformas, pero esta no tiene las condiciones para ofrecer continuidad y alta disponibilidad de los servicios que brinda; además que no cumple con las condiciones recomendadas de instalación de un centro de datos.

Las plataformas móviles son las que brindan más ingresos económicos a la empresa y ante la pérdida de servicio aunque sea por pocos minutos, se ve traducido en millones de ingresos que deja de percibir la empresa y hasta en penalizaciones por el organismo regulador de telecomunicaciones.

Ante la criticidad de los servicios móviles que se ofrecen, es indispensable tener una infraestructura que permita la continuidad de los mismos, por lo cual se planteó la instalación de nuevos equipos que conformarán el nuevo centro de servicios de la operadora móvil.

Este nuevo centro de servicios será redundante geográficamente, con rápida convergencia ante problemas y alta disponibilidad de los servicios prestados, entre los que destacan Recargas Virtuales, Plataforma Prepago, Servicios de Valor Agregado, Portales Web de Servicios, Mensajería y entre otros muchos.

## INDICE

### CAPÍTULO I

#### PROBLEMÁTICA ACTUAL DE LA RED DE SERVICIOS DE LA EMPRESA OPERADORA MÓVIL

1.1	Composición Actual.....	2
1.1.1	Switches de Servicios.....	2
1.1.2	Firewall de Servicios.....	2
1.1.3	Servicios ofrecidos.....	3
1.2	Problemática actual.....	4
1.2.1	Concentración de Servicios.....	4
1.2.2	Concentración de capas Core, Agregación y Acceso.....	5
1.2.3	Equipos de acceso y servicios de diferentes proveedores.....	6
1.2.4	Falta de virtualización de servicios.....	6
1.2.5	Gestión en Banda (InBand).....	6
1.2.6	No hay equipos de servicios centralizados.....	6
1.2.7	Flujos de tráfico.....	7
1.2.8	Infraestructura fuera de soporte y capacidad excedida.....	8
1.2.9	Capacidad de troncales de red.....	8

### CAPITULO II

#### MARCO TEÓRICO

2.1	Marco Teórico.....	9
2.2	Alternativas de plataformas para la operación de una nueva red de servicios....	10
2.2.1	JUNIPER.....	10
2.2.2	CISCO.....	14
2.2.3	HP.....	19
2.3	Análisis de las alternativas.....	22

### CAPITULO III

#### REDES NECESARIAS PARA LA OPERACIÓN DEL CENTRO DE SERVICIOS

3.1	Red de Networking.....	23
-----	------------------------	----

3.2	Red de Servicios .....	23
3.3	Red de Gestión Fuera de Banda.....	23
3.4	Red de Transmisiones .....	24
3.5	Energía DC y AC.....	25
3.6	Red de Monitoreo .....	25

## **CAPITULO IV**

### **DETERMINACIÓN DE NECESIDADES Y REQUERIMIENTOS DE DISEÑO**

4.1	Especificaciones mínimas requeridas .....	26
4.2	Redundancia Geográfica .....	27
4.3	Fases y tiempos requeridos de implementación.....	27
4.4	Bloques funcionales .....	27
4.5	Arquitectura de equipamiento .....	28
4.6	Dimensionamiento de puertos .....	28
4.7	Consideraciones de Diseño .....	28

## **CAPITULO V**

### **INGENIERIA DEL PROYECTO**

5.1	Diagrama de bloques de la arquitectura .....	29
5.2	Requerimientos de hardware y software.....	32
5.3	Diseño Físico.....	32
5.3.1	Diseño Físico del bloque WAN.....	33
5.3.2	Diseño Físico del bloque Core/Agregación .....	34
5.3.3	Diseño Físico del bloque de Servicio .....	35
5.3.4	Diseño Físico del bloque de Acceso .....	36
5.4	Diseño Lógico.....	37
5.4.1	Diseño Lógico del bloque WAN .....	37
5.4.2	Diseño Lógico del bloque Core/Agregación.....	38
5.4.3	Diseño Lógico del Bloque Servicios .....	40
5.4.4	Diseño Lógico del Bloque de Acceso.....	44
5.5	Especificaciones técnicas del equipamiento .....	45
5.5.1	Cisco ASR 9006 .....	45
5.5.2	Nexus 7010 .....	48
5.5.3	Nexus 5010 .....	51

5.5.4	Nexus 2248 .....	51
5.5.5	Switch Catalyst 6509 .....	52
5.5.6	Módulo de Firewall (FWSM) .....	53
5.5.7	Módulo Balanceador (Application Control Engine 20).....	54
5.5.8	Cisco IPS 4270 (Intrusion Prevention System).....	54
5.5.9	Cisco ASA 5520 (Adaptive Security Appliance) .....	55
5.6	Programa de Implementación.....	56

## **CAPITULO VI**

### **COSTOS DEL PROYECTO**

6.1	Equipamiento.....	59
6.2	Servicios.....	61
6.2.1	Servicios Cisco de Reemplazo.....	61
6.2.2	Servicios Profesionales de Migración del Proveedor .....	62
6.2.3	Servicios Avanzados Cisco.....	62
6.2.4	Training in Job .....	62
6.2.5	AT-Proveedor-1 .....	62
6.3	Costos de inversión (CAPEX).....	62
6.4	Costos de operación (OPEX).....	63

<b>CONCLUSIONES Y RECOMENDACIONES .....</b>	<b>64</b>
---------------------------------------------	-----------

<b>BIBLIOGRAFIA.....</b>	<b>65</b>
--------------------------	-----------

<b>ACRÓNIMOS .....</b>	<b>66</b>
------------------------	-----------

## INTRODUCCIÓN

Este trabajo presenta una propuesta de diseño de un centro de servicios robusto, escalable y redundante para soportar todas las plataformas de la operadora móvil con el fin que esta pueda ofrecer continuidad en sus servicios, mejorar la experiencia del usuario final y aumentar los ingresos económicos de la operadora.

Así mismo busca preparar la infraestructura del centro de servicios para poder soportar las nuevas tendencias del mercado, como la virtualización de plataformas, la cual permite brindar grandes ahorros a la compañía tanto en CAPEX como OPEX con la reducción de espacio, energía y equipos en el centro de servicios.

A lo largo del documento, primero se detallará la cómo está compuesto el data center de la operadora móvil y la problemática que se tiene actualmente. Luego se plantea la propuesta de solución indicando el diseño que debe desplegar la operadora para soportar un crecimiento a gran escala, ordenado y de alta disponibilidad.



# CAPÍTULO I

## PROBLEMÁTICA ACTUAL DE LA RED DE SERVICIOS DE LA EMPRESA OPERADORA MÓVIL

### 1.1 Composición Actual

Actualmente la red de servicios está compuesta de la manera como se muestra en la Figura 1.1

#### 1.1.1 Switches de Servicios

El actual centro de Servicios de la operadora móvil se encuentra distribuido en dos nodos con diferente zona geográfica.

Cada nodo cuenta con un par de switches ubicados en diferentes pisos para brindar mayor disponibilidad a los servicios, pues cada switch es energizado con llaves de energía independiente y se conecta a la red a través de medios de transmisión independientes (diferentes perfiles de ruta de fibra)

Son 4 switches Cisco 7609 formando un cuadrilátero, que permiten distribuir servicios en forma inter-nodal. Ver la Figura 1.2.

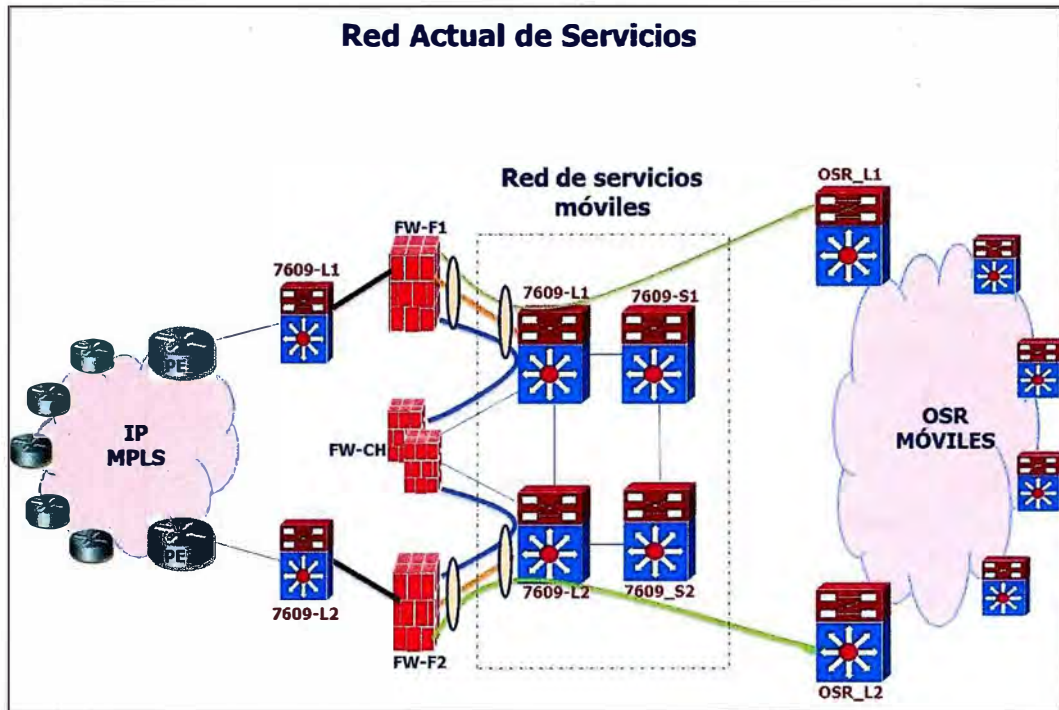
Estos switches son modulares, tienen tarjetas de puertos de fibra (1GE y 10GE) y puertos eléctricos 10/100/1000Mb. Los puertos de fibra son usados para las conexiones inter-nodales y de equipos como firewall, DPI u otros equipos principales; y, los puertos eléctricos para conectar plataformas de servicios (servidores u otros switches que concentran servidores). Ver la Figura 1.3.

Los switches usan el protocolo MST (Multiple Spanning Tree), el cual le permite tener una topología libre de loops y gran capacidad de escalamiento para el manejo de vlans.

#### 1.1.2 Firewall de Servicios

En el nodo 1 se cuentan con 2 firewall Checkpoint redundantes, los cuales fueron con los cuales se iniciaron los servicios y ya se encuentran sobrecargados

En el nodo 1 también tenemos 2 nuevos firewall Fortinet redundantes, en los cuales se provisionan los nuevos servicios y a los cuales se está migrando los servicios provisionados en el firewall Checkpoint



**Figura 1.1 - Conexión Global Centro de Servicios**

En el nodo 2 sólo tenemos 2 firewall Checkpoint redundantes. Si en este nodo se crean nuevos servicios, estos son provisionados extendiendo la Capa 2 hasta los firewall Fortinet de La Victoria

Los switches del nodo 1 adicionalmente tienen 2 firewall Fortinet redundantes que sirven para el servicio de Banda Ancha Móvil (BAM). Ver la Figura 1.4 para referencia.

### 1.1.3 Servicios ofrecidos

Entre los servicios principales tenemos:

Portal web : portal para servicios de Banda Ancha Móvil

Plataformas de control y tarificación

Servicios MMS y SMS

Plataforma de streaming – MobileTV

Plataformas de cache

Plataformas DPI

Gestión de plataformas

Transporte de internet móvil (BAM), conexión de equipo Core de Paquetes (GGSN, SGSN, Router acceso a internet)

Servicios de call center (conexión de PBX, servidores)

Servicios NGN (SBC, gateways)

Servicios de VPN

Otros

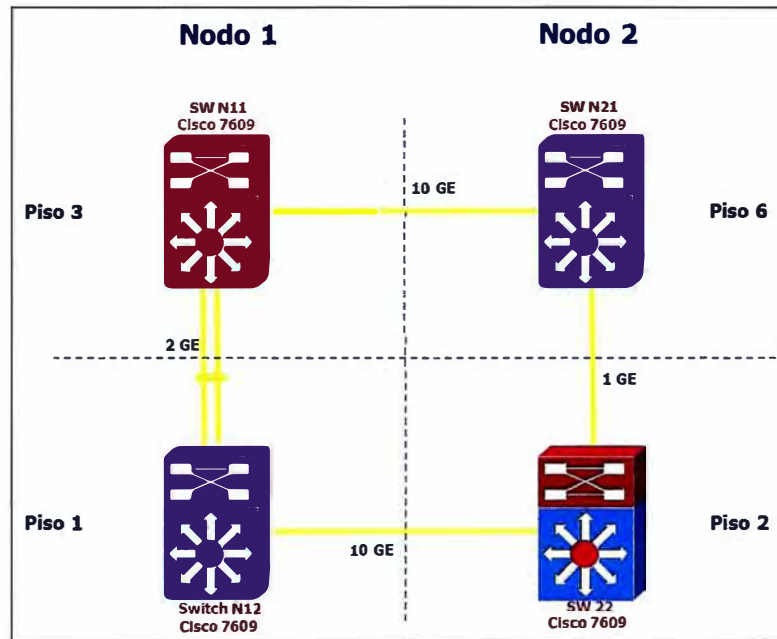


Figura 1.2 Diagrama físico de conexión de switches

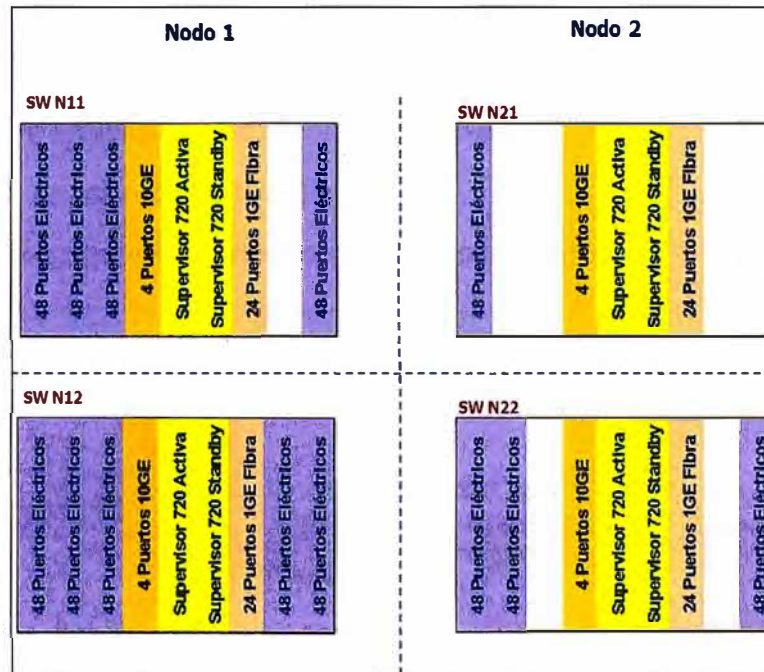


Figura 1.3 Distribución de tarjetas de los switches

## 1.2 Problemática actual

### 1.2.1 Concentración de Servicios

Actualmente el acceso a internet y diferentes servicios que se prestan en la operadora móvil se encuentran concentrados principalmente en 4 switches. Este crecimiento no controlado ocasiona que se presenten los siguientes riesgos:

Puntos de falla único para varios servicios

Problemas en un servicio específico puede concatenar afectación de otros servicios

Aumento de la carga de procesamiento de los equipos.

No está bien definido el perímetro entre el servicio de internet y las plataformas de servicios.

Gestión compartida de la infraestructura. Dos áreas diferentes de la empresa tienen control de la infraestructura, lo cual complica las responsabilidades de los servicios.

### 1.2.2 Concentración de capas Core, Agregación y Acceso

Actualmente no se tiene un modelo jerárquico en la red que divida la infraestructura de red en modelo de 3 capas (Acceso, Agregación, Core), y todo se tiene compactado en switches que hacen la misma función de las 3 capas. Ver la Figura 1.5. Esto presenta las siguientes desventajas:

Red más complicada de mantenimiento

Falta de escalabilidad de la red. En un punto nos encontraremos limitados en disponibilidad de puertos de acceso y troncales.

La implementación de nuevos servicios es más compleja.

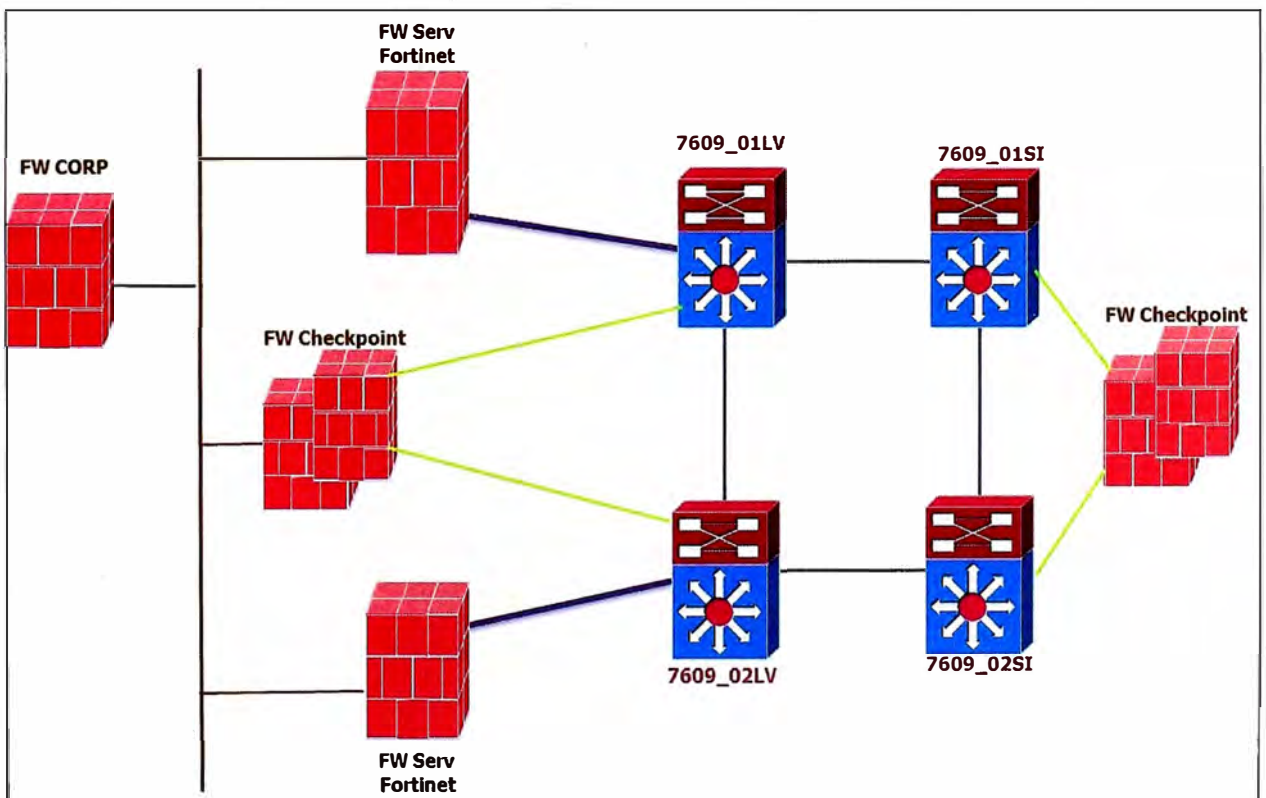
Red sin tener un comportamiento predictivo por capas

Configuraciones de equipos más extensas y complejas

Desventajas en la relación costo/beneficio

Dominio de spanning-tree más extenso y complejo de manejar

Más complicado darle un tratamiento especial a los diferentes tipos de tráfico



**Figura 1.4** Distribución de firewalls

### 1.2.3 Equipos de acceso y servicios de diferentes proveedores

Algunas soluciones que se integran al centro de servicios vienen con sus propios equipos de red, sean switches que concentran sus servidores, balanceadores de carga y en algunos casos equipamiento de firewall. Esto presenta las siguientes desventajas:

Mayores costos de mantenimiento y capacitación en nuevas tecnologías

Problemas con la topología de los switches (spanning-tree)

Dificultad en la operación de equipamiento de diferentes marcas de equipos

Configuraciones básicas desplegadas en los equipos de red dentro de las soluciones integrales de proveedores

Mayores costos de inversión de energía. Ver Figura 1.6 para mayor ilustración.

### 1.2.4 Falta de virtualización de servicios

Las soluciones del área de Ingeniería de Plataformas cuentan con un considerable número de servidores, lo cual es una desventaja por los siguientes puntos:

Mayor inversión en CAPEX (energía, espacio, bastidores)

Falta de optimización en el uso de los recursos en los servidores.

### 1.2.5 Gestión en Banda (InBand)

Las interfaces de gestión (O&M) están ubicadas sobre la misma infraestructura de servicio. Si hubiera algún problema con el equipamiento de servicio, se perdería incluso el control remoto de los equipos.

### 1.2.6 No hay equipos de servicios centralizados

Actualmente sólo se cuenta con equipos de firewall, mas no con equipamiento que brinde servicios centralizados de:

Balanceo de carga

IPS/IDS

Anti-DoS



**Figura 1.5** Modelo NO Jerárquico de Campus



### 1.2.7 Flujos de tráfico

Los flujos de tráfico de los servicios son complejos, pasan por varios firewalls y en algunos casos se encuentra tráfico asimétrico. Ver Figura 1.6

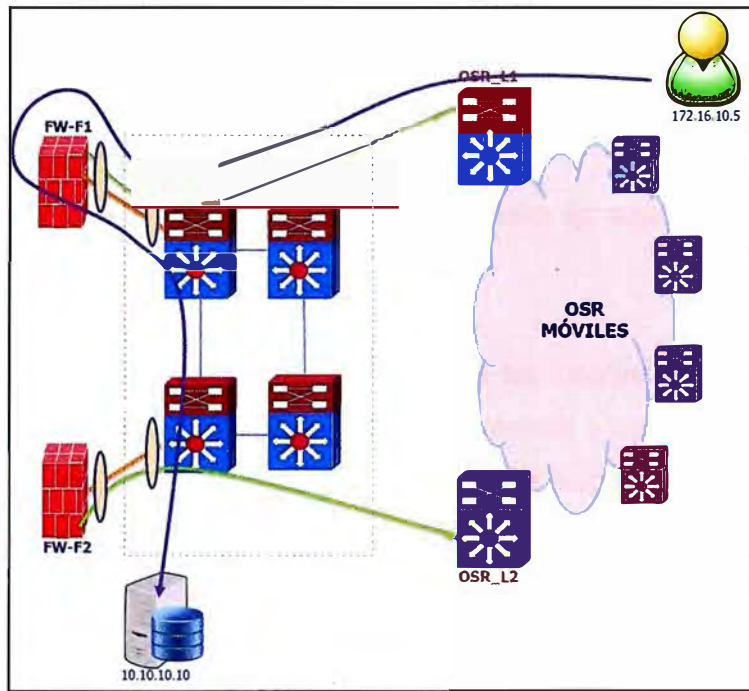


Figura 1.6 Tráfico downstream hacia la aplicación

Por ejemplo, como se muestra en la figura, cuando el usuario accede a la aplicación dentro del servidor 10.10.10.10 ubicado en el centro de servicios de la operadora móvil, el tráfico pasa a través del firewall. Ver Figura 1.7

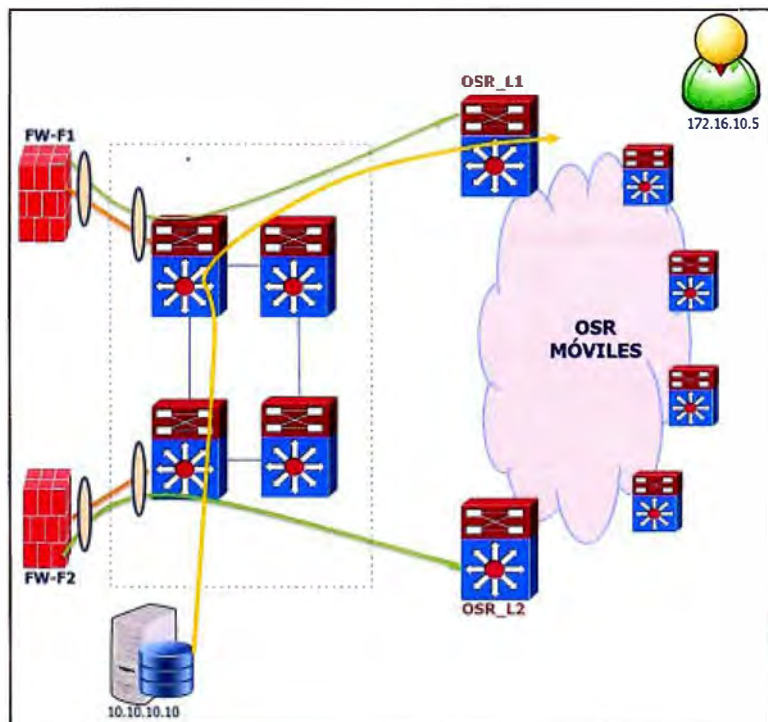


Figura 1.7 Tráfico upstream hacia la aplicación

Sin embargo, el tráfico de retorno al no tener una ruta específica que apunte al firewall y utilizar la ruta default de los switches (0.0.0.0), es enviado hacia el usuario sin pasar por el equipo de seguridad, formándose de esta manera la asimetría en el tráfico. Esto hace que el monitoreo y control de tráfico sea complejo.

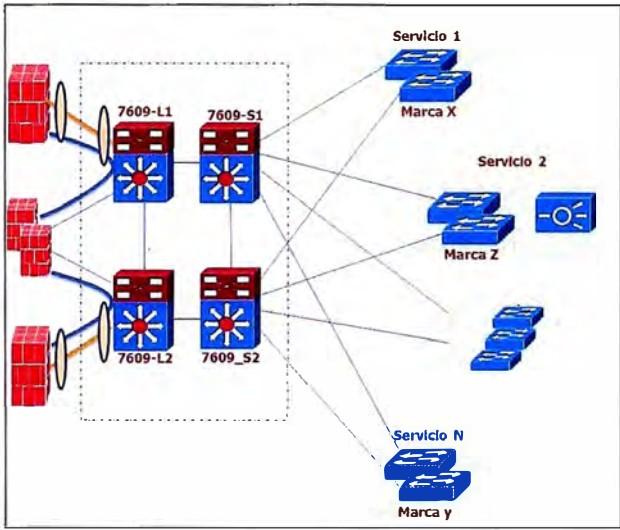
**1.2.8 Infraestructura fuera de soporte y capacidad excedida**

Hay algunos switches antiguos que concentran aún plataformas de servicios, y se agregan en los switches principales

Estos switches (Cisco 4005, Passport8k) ya están fuera de soporte y en el límite de su capacidad.

**1.2.9 Capacidad de troncales de red**

Al concentrar las diferentes plataformas de servicios las interfaces troncales que interconectan los switches, las que conectan la salida de internet y otros equipos de red se encuentran en su gran mayoría por saturarse; lo cual ha ocasionado que se agreguen interfaces de 1GE (port-channel). En algunos casos se tienen hasta 4 interfaces de GE agregadas.



**Figura 1.8** Diferentes proveedores brindan servicios

## **CAPITULO II MARCO TEÓRICO**

### **2.1 Marco Teórico**

La operadora móvil de telecomunicaciones en mención, es uno de los Service Provider líderes del mercado, quien siempre anda buscando generar nuevos servicios para sus clientes, reducir el tiempo de lanzamiento de nuevos productos al mercado, sacar más provecho a su infraestructura propia, preocuparse por la experiencia final del usuario y ser siempre líder en la nueva tecnología que tiene el mercado de las telecomunicaciones.

Sin embargo, el rápido aumento de la demanda de los servicios móviles en los últimos años, ha hecho que el crecimiento en red no se planifique correctamente y simplemente se busque atender las necesidades cuando estas se presentaban. Todo esto ha causado que se tenga una red que no cumpla con las mejores prácticas recomendadas de diseño.

Ante esta problemática, la operadora tiene la necesidad de implementar un Centro de Servicios para su red móvil, la cual cumpla con las mejores prácticas de diseño y le permita tener una infraestructura estable, escalable y altamente disponible. Entre las prácticas de diseño recomendadas listamos las siguientes:

Diseño Jerárquico con bloques funcionales

Despliegue de un bloque de servicios (firewall, balanceadores de carga, detectores de intrusos), para ser brindados a demanda al usuario.

Habilitación de redundancia interna en los equipos (procesadoras redundantes)

Habilitación de redundancia externa (equipos redundantes)

Virtualización de equipos

Utilización de troncales con interfaces de 10GE

Soporte de MPLS VPN para brindar servicio a usuarios en redes IP MPLS

Soporte de enrutamiento IPv4 e IPv6, manejo de colas para aplicar calidad de servicio, soporte de multicast y despliegue de configuraciones para más rápida convergencia de protocolos.



## Eliminación de topologías complejas de spanning-tree

Con el fin de hacer un análisis de las tecnologías y diseños de los principales proveedores, se analizaron 3 marcas que están presentes en el mercado y se detallarán a continuación.

## 2.2 Alternativas de plataformas para la operación de una nueva red de servicios

A continuación se detallará la solución que brinda cada empresa y el detalle de los equipos principales que conforman su solución.

### 2.2.1 JUNIPER

La solución de Juniper busca brindar una solución que brinde cuatro funciones principalmente: simplificar, compartir, asegurar y automatizar.

Las capas del modelo jerárquico son: Acceso, Agregación y Core. Juniper considera este modelo como legado por lo siguiente:

Hace la red más lenta por las capas adicionales que maneja, lo cual añade latencia y saltos de red al tráfico. Ver Figura 2.1.

La solución se hace más cara al requerir puertos de alta capacidad (de altos costos) para la integración altamente disponible entre capas y la conexión a otras redes

Al tener varias capas de red, hace la red mucho más compleja

Juniper ofrece la **Solución 3-2-1**, la cual busca aplanar y simplificar el actual modelo de 3 capas, reduciéndolo de 3 a 2 capas en la actualidad, y en un futuro a una sola capa con el modelo de Q-Fabric

Para eliminar una capa (la capa de agregación), Juniper propone la solución de **“Virtual Chassis” en el Acceso**, la cual consiste en conectar el Acceso directamente al Core.

Con Virtual Chassis, se pueden conectar los switches uno contra otro y administrarlos como una única caja

Virtual Chassis considera los siguientes beneficios:

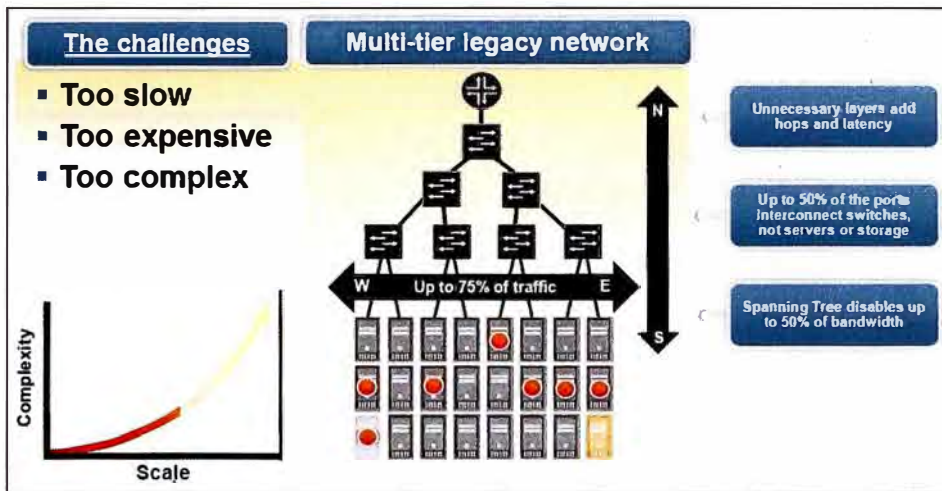
Operación simplificada

Incremento del ancho de banda al eliminar Spanning-tree (STP)

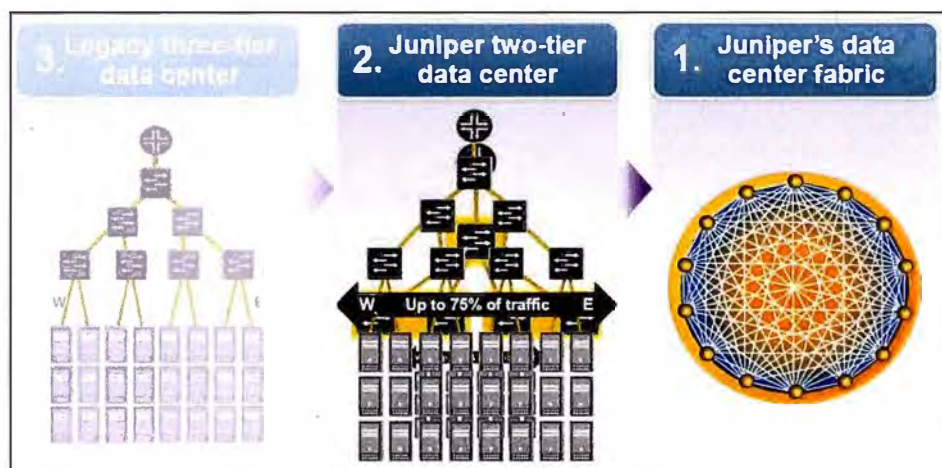
Disminuye la cantidad de equipos, menos enlaces para inter-conectarlos, y menos costos por la no adquisición de los mismos.

Disminuye la latencia hasta en una tercera parte por reducción de capas de equipos.

Luego de mostrar el resumen de las características de la solución de Juniper, su modelo presenta lo siguiente en la Figura 2.2:



*Figura 2.1 Desventajas de los modelos multicapas*



*Figura 2.2 Modelo Juniper 3-2-1*

## EDGE

Para la zona de enrutamiento recomienda sus equipos de la serie MX, los cuales ofrecen capacidades de seguridad y conmutación Ethernet de alto rendimiento. Las características avanzadas de enrutamiento incluyen virtualización de red MPLS, multicast, QoS avanzada y seguridad

## CORE

En la parte de conmutación de alta escalabilidad y rendimiento para redes de centro de datos están presentes los equipos de la serie EX. Revisar Figura 2.3

Los conmutadores modulares de alta densidad y rendimiento EX8208 y EX8216 admiten entornos de informática de nube y centro de datos.

## EX8200 line of modular Ethernet switches

JUNIPER NETWORKS

**High-performance chassis platforms**

- EX8208 – Eight line cards, 960 Mpps
- EX8216 – Sixteen line cards 1.92 Bpps
- 100 GbE ready
- Fully redundant routing engines with N+1 redundant switch fabrics
- Up to 256 wire-speed, non-blocking 10GbE ports in a rack
- 320 Gbps capacity per line card

**Virtual Chassis technology**


- Two-member Virtual Chassis
- External Routing Engine (XRE) required

**Fully redundant power and cooling**

- Redundant, load-sharing PSUs (AC, DC)
- Hot-swap fan tray with redundant fans

**Proven Juniper technology**

- Switch fabrics, control plane
- Packet Forwarding Engine (PFE)
- Junos operating system



JUNOS

Module Description	Max Ports	Interface
48-port 10/100/1000B-T	384 or 768	RJ-45
48-port 100B-FX/1000B-X	384 or 768	SFP
8-port 10GbE	64 or 128	SFP+
40-port GbE/10GbE	320 or 640	SFP/SFP+

*Figura 2.3 Características del equipo Juniper EX8200*

## ACCESO

También recomiendan equipos de la serie EX

La línea EX4500 admite despliegues de agregación en la parte superior del bastidor de 10Gbps de alta densidad, mientras que la línea EX4200 admite despliegues de acceso en la parte superior en Gbits. Ver Figura 2.4.

## EX4200 line of Ethernet switches with Virtual Chassis technology

JUNIPER NETWORKS

**Virtual Chassis technology**

- 128 Gbps virtual backplane
- Manage up to 10 as a single device
- Extend over 10GbE or GbE uplinks
- Master and backup route engines

**Flexible uplink modules**


- 4-port GbE (SFP)
- 2-port 10GbE (XFP)
- Dual-mode 4-port GbE/2-port 10GbE (SFP+)

**Fully redundant power and cooling**

- Dual, hot-swappable AC, DC PSU
- External RPS option
- Fan FRU, multiple blowers
- Full Class 3 PoE (15.4 W)

**LCD display**

Runs Junos operating system with full OSPF and IP multicast in base license




JUNOS

# Ports	Port Type	PoE Ports	Max Power Consumption (Incl. PoE)
24	10/100/1000B-T	8	129 (320) W
24	10/100/1000B-T	24	160 (600) W
24	100B-FX/1000B-X	N/A	108 (N/A) W
48	10/100/1000B-T	8	181 (320) W
48	10/100/1000B-T	48	224 (930) W

*Figura 2.4 Características del equipo Juniper EX4200*

Virtual chassis permite interconectar varios conmutadores EX4200 que funcionen como un único dispositivo. En la Figura 2.5 se pueden observar las características de EX4500:

## EX4500 LINE OF 10GbE DATA CENTER SWITCHES



**10GbE Ethernet switch**

- 2RU, 40x 1/10GbE SFP/SFP+
- Two uplink modules (4 x SFP+/each)
- Available Q210

**Data center-optimized**

- Reversible airflow (2 SKUs - front-to-back; back-to-front)
- Versatile mounting options
- Twinax/DAC support for ToR server access

**10GbE aggregation switch**

- Building/campus distribution and core

**Virtual Chassis enabled<sup>®</sup>**


- 128G Virtual Chassis compatible with EX4200
- High-speed optical Virtual Chassis

**Wire-rate performance on all ports**

**Redundant power & fans**

**Junos operating system**

- L2 and L3 in base



Model	# Ports	Port Type	Uplinks	Air Flow
EX4500-40F-FB	40	1/10GbE	8xSFP+	Front-to-back
EX4500-40F-BF	40	1/10GbE	8xSFP+	Back-to-front

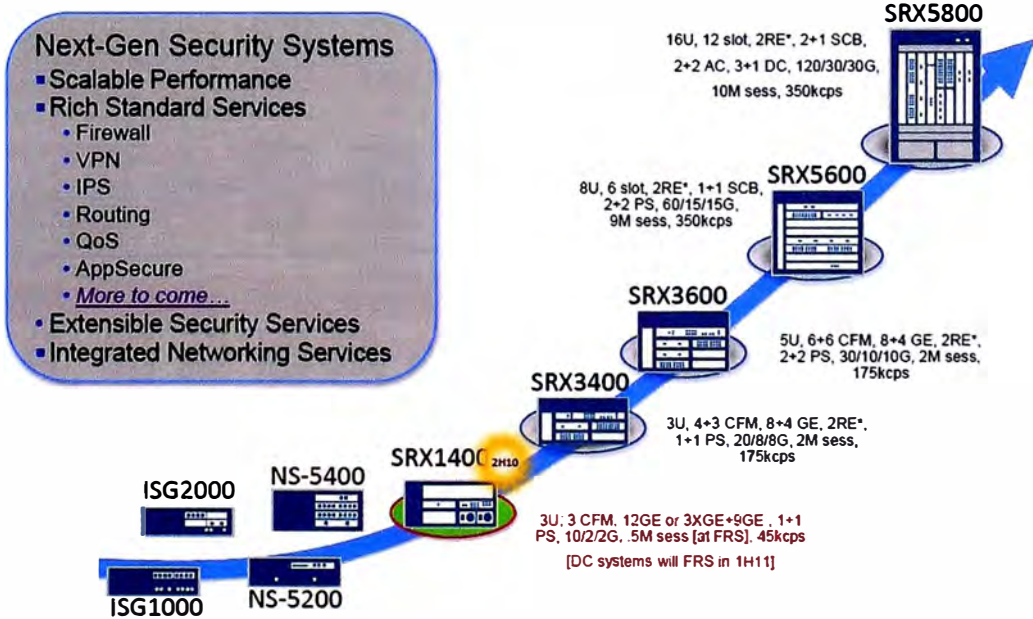
*Figura 2.5 Características del equipo Juniper EX4500*

### SERVICIOS

Para la zona de servicios que combinan funciones de enrutamiento, conmutación y aplicaciones, recomiendan los equipos de la serie SRX

Se ofrecen servicios de Firewall, VPN, IPS; así como funcionalidades de routing, QoS y aplicaciones de seguridad. Observar los modelos en la Figura 2.6.

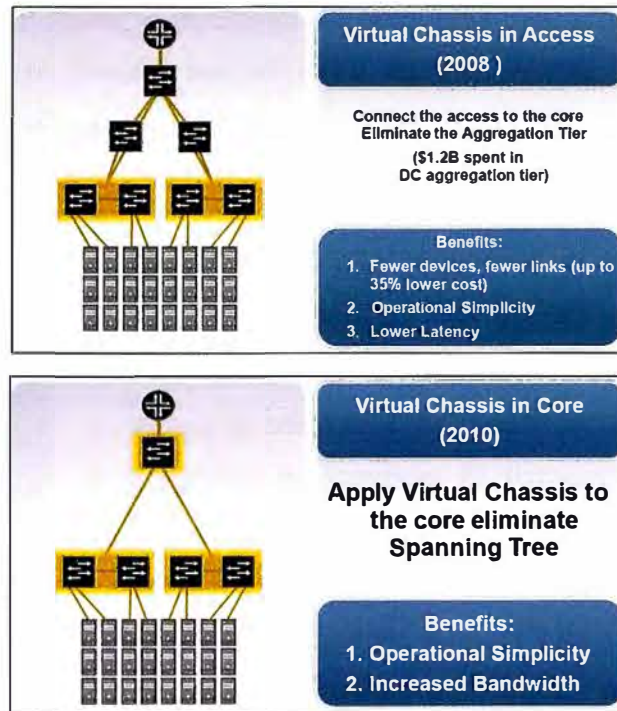
### SRX / DATA CENTER SERVICES PLATFORMS



*Figura 2.6 Equipos de servicios Juniper – Serie SRX*

En la Figura 2.7 se muestra los modelos actuales considerando capa de agregación, y la Figura 2.8 retirando la capa de agregación:





*Figura 2.7 Modelos con y sin la capa de agregación*

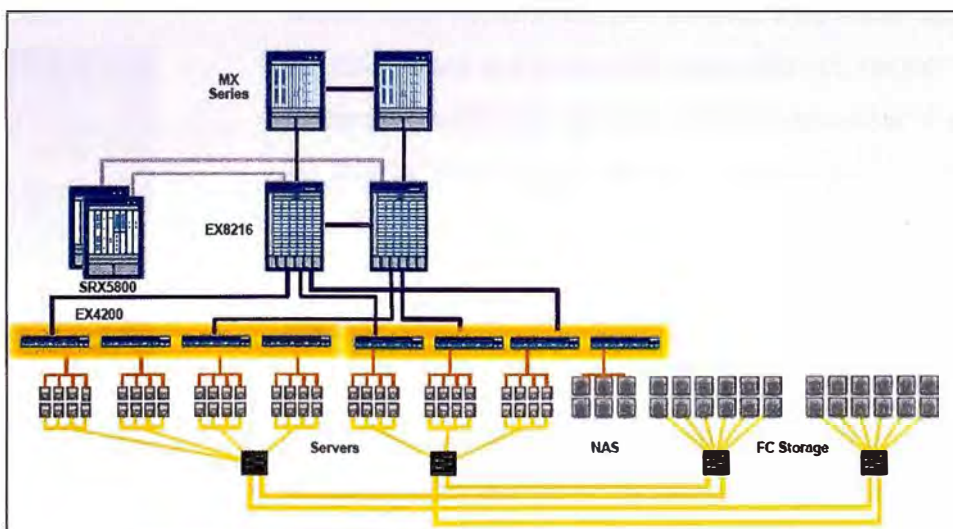
En resumen, se puede observar su solución recomendada con detalle en Figura 2.8

El EDGE formado por los equipos MX

El CORE es un equipo EX8216

El ACCESO en virtual chassis son los EX4200

Los equipos para brindar SERVICIOS son SRX5800



*Figura 2.8 Diseño recomendado de Data Center*

## 2.2.2 CISCO

La solución de Cisco busca incrementar el ahorro de las operadoras y acelerar la entrega de servicios. La virtualización es un elemento principal que permitirá conseguir los nuevos retos, permitiendo la unificación de elementos de red y cómputo, así como el cumplimiento con la seguridad y desempeño en aplicaciones

En el Cuadro 1.1. se muestra el portafolio de productos que propone Cisco para transformar el Data Center en un activo más eficiente, ágil y resistente.

**Cuadro 2.1 – Portafolio de Productos Cisco**



Componente	Descripción
<p><b>Cisco UCS</b></p> 	<p>Cisco UCS es una plataforma de siguiente generación que unifica cómputo, red acceso a almacenamiento y virtualización en un sistema cohesivo diseñado para reducir el costo total de propiedad (TCO) e incrementar la agilidad del negocio. El sistema integra un fabric de red unificado de clase empresarial de 10GE con baja latencia y baja pérdida. El sistema en una plataforma integrada, escalable y multi chassis dónde todos los componentes forman parte de un único dominio de administración.</p> <p>El una sucursal, Cisco UCS Express es una infraestructura dónde el cómputo, red y virtualización convergen en un único dispositivo que permite correr aplicaciones que no pueden ser centralizadas.</p>
<p><b>Cisco Nexus Series Switches</b></p> 	<p>La familia Cisco Nexus es la base del Data Center de Cisco. Está compuesta por switches de clase Data Center diseñados para permitir a los clientes migrar a 10GE y fabrics unificados de una manera granular y eficiente en costos como parte de las estrategias de transformación del Data Center.</p> <p>Cisco Nexus 1000V es un switch de acceso de VM diseñado específicamente para cumplir con los desafíos de ambientes virtuales. Es switch Cisco 1000V series es una implementación de software switch para ambientes Vmware vSphere que corren el sistema operativo NX-OS.</p>
<p><b>Cisco MDS 9000 Series Multilayer Switches</b></p>	<p>La serie MDS 9000 elevan el estándar para switches San de clase empresarial. Proveen elementos líderes en la industria en temas de disponibilidad, escalabilidad, seguridad y gestión. Los switches Cisco de la serio 9000 permiten a los negocios desplegar SAN's de alto</p>

Componente	Descripción
	<p>desempeño con bajo costo total de propiedad (TCO). La serie MDS 9000 de Cisco cumple con los requerimientos más exigentes de los ambientes almacenamiento de grandes Data Centers al combinar servicios y red inteligente en un switch fabric de protocolo independiente.</p>
<p><b>Cisco Catalyst Series Switches</b></p> 	<p>Los SW 6500 establecen un Nuevo estándar para comunicación ip y entrega de aplicaciones en redes de campus empresarial y de ISP al maximizar la productividad de usuario y mejor el control operacional mientras se provee protección a la inversión. Entregan servicios seguros y convergentes de extremo a extremo en los niveles de core, Data Center y frontera.</p> <p>Los SW 4900 tienen configuración fija que ofrecen alto desempeño y actúan como SW de servidor de rack optimizado para Data Centers de cualquier tamaño. Estos switches entregan alto rendimiento y baja latencia a velocidad de cable para servicios de capa 2 y 3. Además son ideales para despliegues donde el espacio es una restricción ya que ocupan 1 o 2 unidades de rack.</p>
<p><b>Cisco WAAS</b></p> 	<p>Cisco WASS es una solución integral de optimización de WAN, aceleración de aplicaciones, es componente clave de Borderless Network y arquitecturas virtualizadas de Data Center. Cisco Wass permite a los departamentos de TI consolidar el Data Center, entregar virtualización de escritorios, desplegar nuevas aplicaciones con contenido multimedia enriquecido y entregar aplicaciones basadas en cloud y SaaS.</p>
<p><b>Cisco vWAAS</b></p>	<p>Cisco vWAAS es la primera solución de optimización de WAN lista para la nube de la industria. Cisco vWASS es un dispositivo virtual que acelera las aplicaciones de negocio entregadas desde infraestructuras privadas e infraestructuras privadas en la nube. Cisco vWASS es desplegado sobre VMware Hypervisor y servidores Cisco UCS x86, otorgando un despliegue ágil, y elástico.</p>



Componente	Descripción
<p><b>Cisco Application Control Engine</b></p> 	<p>Cisco ACE es la única solución virtualizada de balanceo de carga y entrega de aplicaciones de la industria. Cisco ACE incluye diversos mecanismos de balanceo de carga, conmutación de contenido, descarga de servidor y optimización de aplicaciones.</p> <p>Cisco ACE ofrece flexibilidad y elección mientras se entrega un aprovisionamiento consistente basado en políticas, además simplifica la operación y la portabilidad de carga de trabajo a lo largo de la red y ambientes de cómputo.</p>
<p><b>Cisco Carrier Routing System</b></p> 	<p>Cisco CRS-1 Carrier Routing System es el único sistema de ruteo completamente modular y distribuido de la industria que permite a los proveedores de servicio entregar una suite completa de data, voz y servicios de video sobre una red Ip de siguiente generación altamente escalable y disponible. Los modelos de Cisco CRS incluyen:</p> <ul style="list-style-type: none"> <li>• Cisco CRS-3: Potenciado por un arreglo QuantumFlow de Cisco, una arquitectura de chipset diseñada en múltiples dimensiones de escalabilidad, servicios y ahorro.</li> <li>• Cisco CRS-1: Construido sobre Cisco Silicon Packet Processor</li> </ul> <p>Los modelos Cisco CRS-3 están contruidos sobre el modelo CRS-1 y son totalmente compatibles.</p>
<p><b>Cisco Data Center Services Node</b></p>	<p>Cisco DSN es un Nuevo producto que complementa los switches de la serie Cisco 7000 en el Data Center. Cisco DSN es la plataforma ideal para albergar servicios específicos integrados de red importantes en el Data Center. Ejemplos de servicios de red son: FWSM y Cisco ACE para balanceo de carga.</p>



Componente	Descripción
<p data-bbox="166 259 528 340"><b>Cisco 7600 Series Internet Routers</b></p> 	<p data-bbox="569 259 1347 663">Con router de internet Cisco 7600 usted puede desplegar características IP/MPLS de alto desempeño al igual que servicios Ip personalizadas en la frontera de la red. Como primer router de clase carrier de la industria ofrece conmutación Ethernet de alta densidad, ruteo IP/MPLS e interfaces de 10GE. El router de internet Cisco 7600 provee una plataforma flexible de agregación que se ajusta a despliegues WAN.</p>
<p data-bbox="166 694 528 775"><b>Cisco Firewall Services Module</b></p> 	<p data-bbox="569 694 1347 987">Cisco FWSM para los switches Cisco Catalyst 6500 and los router Cisco 7600, es un firewall de inspección "stateful", alta performance con un motor de inspección de protocolos y aplicaciones. Este provee un throughput de 5.5 Gbps 100,000 conexiones por Segundo y un millón de conexiones concurrentes.</p>

La Figura 2.9 muestra el diseño recomendado por Cisco; y los equipos recomendados para la infraestructura de red son:

Para la WAN (edge), recomiendan los router Cisco ASR, los cuales pueden ser de la familia 9000 ó 1000 según el dimensionamiento de la solución. En este caso se considerará el modelo 9006, el cual tiene slot para considera crecimiento y permite módulos de servicio (módulo para CGNAT)

Para la parte de CORE y AGREGACIÓN, recomiendan los switches NEXUS 7000, los cuales serán virtualizados (switches virtuales). En este caso se usará el Nexus 7009.

Para la parte de ACCESO recomiendan los NEXUS 5000 y NEXUS 2000. En este caso se usarán los Nexus 5548 y los Nexus 2210

Para la parte de SERVICIOS, recomiendas los switches 6500, los cuales son modulares y pueden contener módulos de firewall, balanceadores de carga, IPS y VSS.

Los principales features que ofrece Cisco para mejorar el rendimiento de la infraestructura de red para un Data Center:

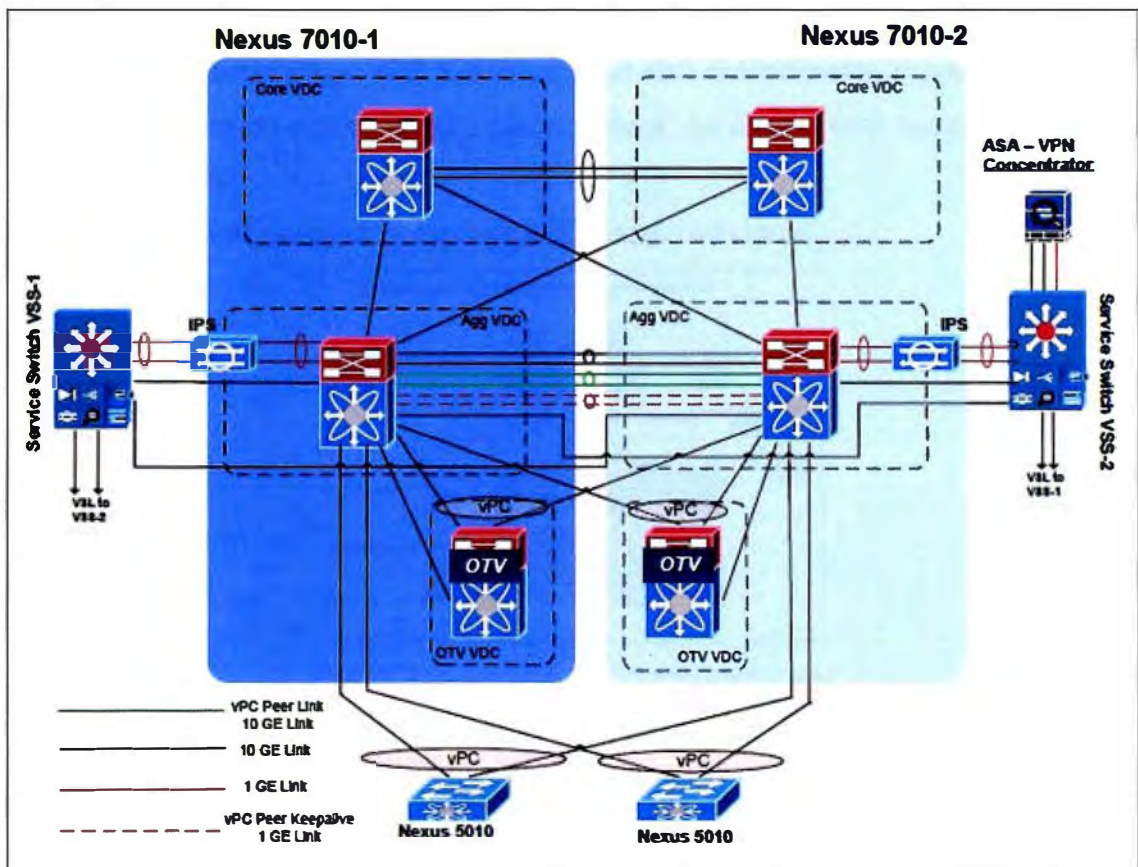
**Fabric Path**, ofrece la estabilidad y el rendimiento del routing de Capa 3 a redes conmutadas de capa 2 para crear una estructura de capa 2 altamente flexible y escalable, haciendo Data Center flexibles y ampliables de forma masiva. Esto elimina el problema de Spanning-tree y elimina los enlaces ociosos redundantes.

**Virtual Device Context (VDC)**, permite la virtualización de hasta 4 switches en los Nexus 7K

**Virtual Port-Channel (VPC)**, permite tener port-channel entre diferentes equipos, eliminando las dificultades del Spanning-tree y mejorando la capacidad throughput (sin enlaces ociosos).

**Overlay Transport Virtualization (OTV)** es una técnica de “MAC en IP” para soportar VLANs sobre cualquier transporte, sin extender el dominio de broadcast

**Virtual Switching System (VSS)**, permite administrar los enlaces redundantes, comportándose externamente con un simple port-channel, manteniendo una topología libre de loops



*Figura 2.9 Solución Cisco/Nexus para Data Center*

### 2.2.3 HP

La solución de HP busca reducir la complejidad de la red, disminuir costos y flexibilidad para brindar servicios.

Las principales características de su solución son: consolidación, simplificación, continuidad de servicio, ahorro de energía, escalabilidad y performance

HP propone las siguientes alternativas para conseguir una infraestructura de data center de siguiente generación:

Intelligent Resilient Framework (IRF) e Intelligent Management Center (IMC)

Virtual Connect / FlexFabric

## HP TippingPoint Secure Virtualization Framework (SVF)

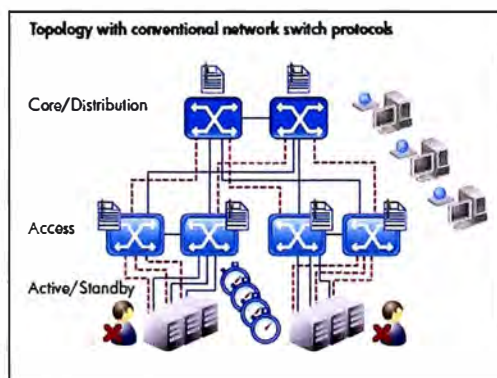
Una tecnología que te permite “aplanar” el data center, eliminando la necesidad de una capa de agregación dedicada y entregando una conexión directa y de alta capacidad entre los usuarios y los recursos de red.

IRF extiende el control de red sobre múltiples switches activos. Este grupo es administrado con una sola IP, la cual simplifica la configuración de red y operación. Bajo esta modalidad, puedes formar un “virtual switch fabric” de hasta 9 switches.

Este grupo IRF puede estar formado por switches que están separados hasta 70Km, potenciando la ventaja de “disaster recovery”.

Un switch miembro del grupo IRF actúa como el sistema primario, manteniendo el plano de control y el plano de datos. Si este switch fallara, se elegirá otro nuevo switch primario dentro del grupo IRF

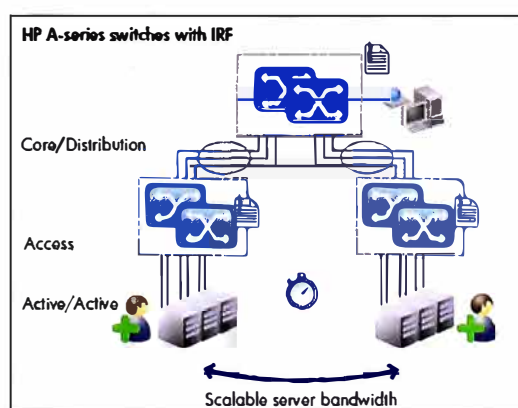
En la Figura 2.10, HP muestra el modelo jerárquico tradicional:



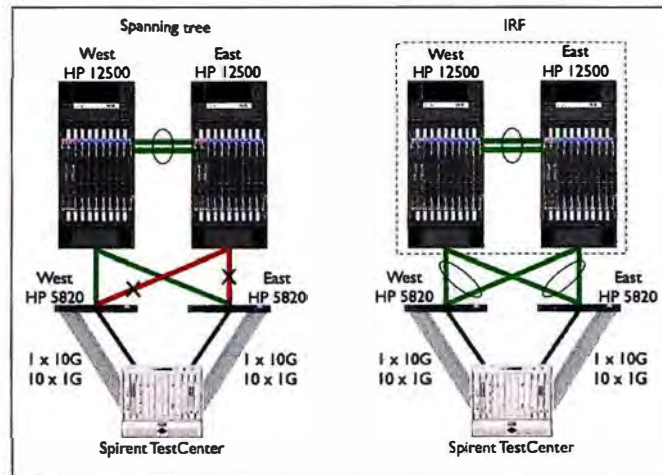
**Figura 2.10** Modelo Jerárquico tradicional

En la Figura 2.11, se ve a los switches de Acceso formando un solo grupo IRF, así como los switches de Core forman otro grupo IRF.

Entre estas capas se verán como una sola unidad, eliminando la necesidad de tecnologías de convergencia lenta como Spanning-Tree (STP). Así mismo, disminuyen la cantidad de equipos a usarse, las interfaces de red, los enlaces troncales y los protocolos a configurar y administrar. Ver Figura 2.12.



**Figura 2.11** Modelo recomendado por HP

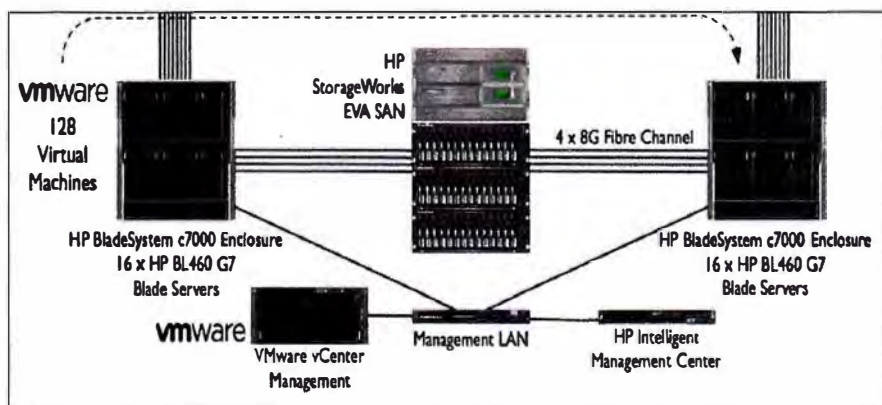


**Figura 2.12** Conexiones tradicionales y las recomendadas por HP

### Virtual Connect / Flex Fabric

La actual distribución y uso de servidores en los DC no es óptima, por lo cual HP recomienda la virtualización y el uso de blades.

FlexFabric brinda inteligencia en el acceso combinando una gestión centralizada que permitirá la virtualización de redes/servidores, impulsando el rendimiento predecible y un rápido aprovisionamiento de nuevos servicios



**Figura 2.13** Uso de blades y FlexFabric en el Data Center

### Intelligent Management Center

Permitirá unificar la administración de las redes físicas y virtuales, y ayudará a sobrellevar los nuevos desafíos de administrar el nuevo borde de servidores virtuales.

La solución proveerá una única vista de la infraestructura física y virtual, acelerando la entrega de aplicaciones y servicios, simplificando operación y mejorando la disponibilidad.

### HP TippingPoint Secure Virtualization Framework (SVF)

Provee una solución que se integra con las máquinas virtual (VMware) y diseñada para habilitar una segmentación de zonas seguras (firewall) y zonas de inspección (IPS) entre zonas seguras de todo el data center



Para lograr lo expuesto, HP recomienda el siguiente equipamiento:

**Equipo Core:** Se recomiendan los switches 12500. Estos equipos tienen capacidad de enrutamiento de 6,66Tb y está preparado para 13,32Tb. Brinda interfaces de Acceso de 10GbE de alta densidad con 128 1:1 y 512 4:1. Contemplan acceso futuro de 40GbE/100GbE. Manejan una estructura redundante (fuente y bandeja de ventilador).

**Equipos de Acceso:** Se recomiendan los equipos 5830 GbE y 5820 10 GbE. Son equipos "Top-of-Rack" (situados en la parte superior del bastidor) que ofrecen una combinación de puertos Ethernet GbE y 10GbE de alta densidad y funciones completas IPv4 e IPv6 de doble pila de nivel 2 y 3. Adicionalmente a su gran densidad de puertos, ofrecen compatibilidad con IPv4 e IPv6, así como convergencia con FCoE.

### 2.3 Análisis de las alternativas

Luego de revisar las soluciones encontradas en el mercado, se observó la conclusión que las tendencias de los proveedores son similares:

- Solución de bloques funcionales
- Conexiones en interfaces de 10GE
- Operación simplificada con la reducción de equipos y el uso de funciones de virtualización lógica de equipos.
- Bloque de servicios con servicios de valor agregado como firewall, balanceadores e IPS
- Consolidación de equipos

Por tal motivo se analizaron otras variables como la presencia de soluciones similares en el mercado y conocimiento de la solución por el equipo operativo de la empresa, lo cual permitirá disminuir los riesgos y costos de operación. En el Cuadro 2.2 se muestra el comparativo de las 3 marcas propuestas.

**Cuadro 2.2 – Cuadro Comparativo de marcas propuestas**

MARCA	JUNIPER	CISCO	HP
Presencia en el mercado peruano	Posicionados como equipos Toll Gate y CORE de la red	Posicionado como equipo de Data Center y Centro de Servicios de los principales ISP	Posicionado como solución de servidores
Despliegues en la operadora móvil	Despliegues en el Core de la red fija de la operadora móvil	La red fija de la operadora ya tiene un Centro de Servicios con la marca Cisco	Despliegue en servidores para aplicaciones
Experiencia del equipo operativo	Experiencia en configuración de router Juniper	Experiencia en configuración de Router, Switches, Firewall, Balanceadores y equipos IPS Cisco	Experiencia sólo en configuración de servidores

Con estas variables se optó por la opción de darle continuidad a la tecnología Cisco en el despliegue del nuevo centro de servicios móviles para la operadora.

## **CAPITULO III**

### **REDES NECESARIAS PARA LA OPERACIÓN DEL CENTRO DE SERVICIOS**

Se necesita la siguiente infraestructura para cumplir con requerimientos de la operadora:

#### **3.1 Red de Networking**

Se requiere una infraestructura de switches/routers robustos que cumplan con las siguientes características:

Gran escalabilidad

Reducción de costos de adquisición

Disminución del exceso requerido de energía, refrigeración y espacio adicional

Gran capacidad de throughput y performance

Disminución de la capacidad no utilizada

Elimine la problemática ocasionada con Spanning-Tree

Alta disponibilidad y redundancia

Flexibilidad para la creación de nuevos servicios

#### **3.2 Red de Servicios**

Se necesita una infraestructura que permita atender los diferentes servicios requeridos por las plataformas que se instalarán en Centro de Servicios.

Estos servicios deben tener la capacidad de escalables, virtualizables y modulares, lo cual permitirá armar el set de servicios según los requerimientos de la plataforma a atender. Como referencia de los servicios brindados ver los PODs en la Figura 3.1.

Los servicios que se deben atender son:

Servicios de Firewall

Servicios de Balanceo de Carga

Servicios de inspección de tráfico (IPS)

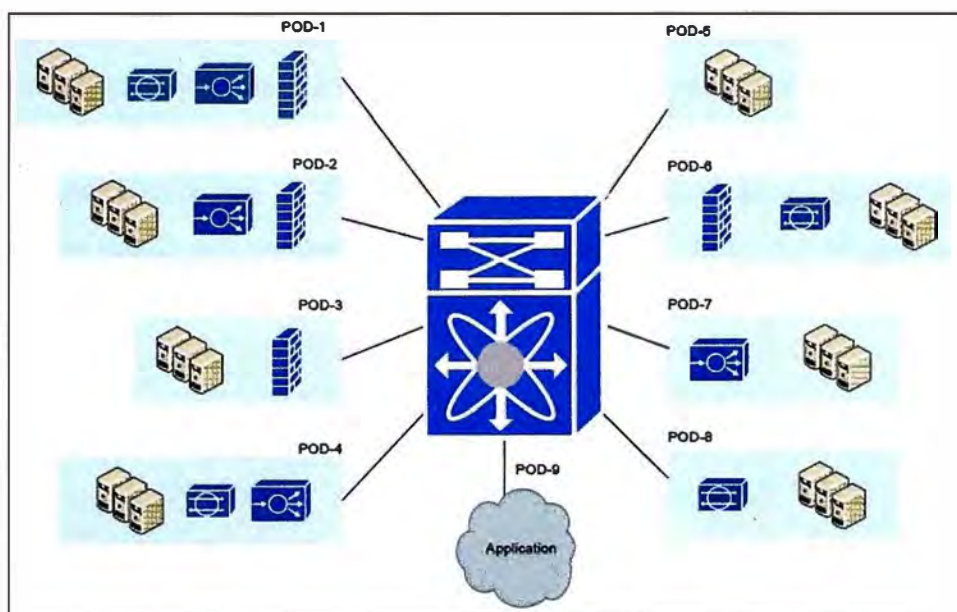
Servicios de VPN

#### **3.3 Red de Gestión Fuera de Banda**

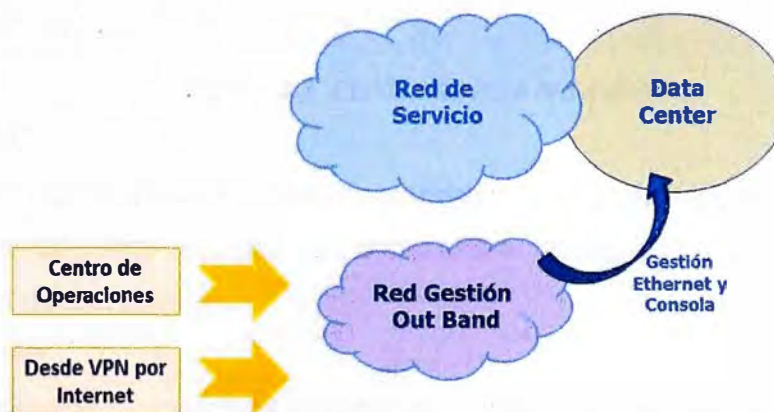
Se necesita una red paralela a la red de Servicio, que nos permita siempre tener gestión remota de los equipos. Ver Figura 3.2.

Esta gestión fuera de banda podrá ser accedida a través del Centro de Gestión de la Operadora, así como desde una VPN de usuario

Esta gestión tiene que poder realizarse a través del puerto de Management (IP), así como a través de los puertos de consola de los equipos de Centro de Servicios y equipos remotos que se comuniquen con la red de Centro de Servicios



**Figura 3.1** PODs de Servicios



**Figura 3.2** Modelo de Gestión OB

Si hubiera algún problema con la Gestión Fuera de Banda, el equipo automáticamente se debería gestionar en banda a través de la red de Servicio.

La infraestructura de esta red deberá tener cabeceras redundantes para darle alta disponibilidad

### 3.4 Red de Transmisiones

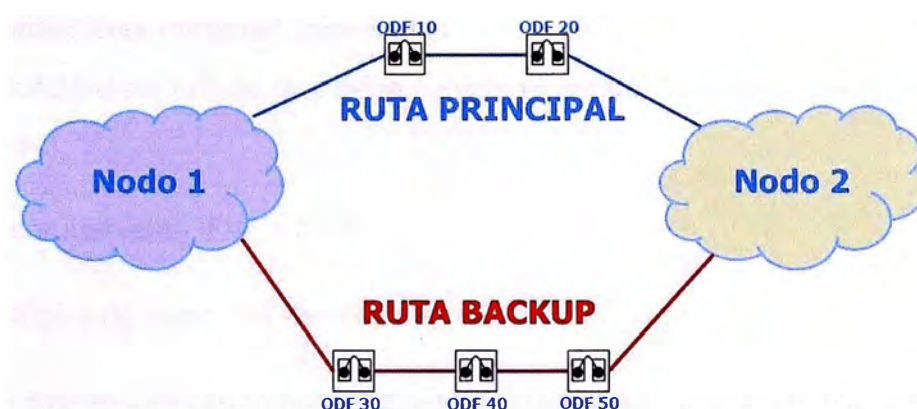
Se plantea tener el Centro de Servicios distribuido entre dos nodos con diferente ubicación geográfica

La conexión entre ellos será redundante mediante enlaces de 10GE.

Estos enlaces deben tener perfiles (rutas) diferentes de fibra oscura o enlaces a través de Transmisiones con el fin de garantizar la alta disponibilidad de los servicios brindados por el Centro de Servicios. Ver Figura 3.3.

Localmente en cada nodo también se necesita tener equipos redundantes en diferentes pisos. Para la interconexión de los mismos se utilizarán pares de fibra de las bandejas de ODF de cada piso.

Para la redundancia de la red de Gestión fuera de Banda también se necesitará fibra internodal. En este caso será suficiente contar con fibras de 1GE, por lo cual se utilizará fibra oscura o Transmisiones, según la disponibilidad.



**Figura 3.3** Perfiles de fibra redundantes

### 3.5 Energía DC y AC

En cada piso de los nodos se deben tener bastidores de energía redundantes. Esto es necesario porque se requerirán equipos con doble fuente de energía, y así se garantizará la alta disponibilidad del servicio.

### 3.6 Red de Monitoreo

Se debe tener un sistema que permita monitorear el nuevo equipamiento, así como herramientas que den flexibilidad para la operación de los equipos.



## CAPITULO IV

### DETERMINACION DE NECESIDADES Y REQUERIMIENTOS DE DISEÑO

El proyecto para cumplir con las expectativas de la operadora móvil debe enmarcarse y cumplir lo detallado a continuación.

#### **4.1 Especificaciones mínimas requeridas**

Las especificaciones mínimas que debe cumplir el centro de servicios a implementar son las siguientes:

Soporte de enrutamiento IPv4 e IPv6

Separación lógica de tráfico de clientes

Tratamiento diferenciado de tráfico mediante calidad de servicio y priorización

Implementación de servicios de valor agregado como firewall, balanceadores de carga y equipos detectores de intrusos

Conexiones de alta velocidad y capacidad (10GE)

Alta densidad de puertos de acceso para conexión de plataformas

Capa de acceso en alta disponibilidad y eliminación de topologías complejas de Spanning-tree

Soporte de soluciones de consolidación de servidores (conexión de chassis/blades en interfaces de 10GE)

Soporte de soluciones de virtualización de plataformas

Soporte de soluciones de almacenamiento SAN/NAS

Diseño basado en capas funcionales.

## 4.2 Redundancia Geográfica

La mayoría de las plataformas de la operadora móvil se encuentran distribuidas en 2 nodos ubicados en Lima. Actualmente esta demanda es atendida con el esquema descrito en el capítulo inicial, el cual no asegura los niveles de disponibilidad mínimos requeridos. Por tal motivo, estos dos nodos serán los seleccionados para el despliegue inicial del centro de servicios redundante.

Posteriormente por distribución de la demanda se ubicará una extensión del centro de servicios en un tercer nodo de la ciudad y se ampliará la redundancia geográfica desplegando centro de servicios en otras ciudades del país.

Lima, es la ciudad principal de ubicación de los nodos de la operadora. Las otras ciudades que se utilizarán posteriormente como nodos redundantes serán Arequipa y Trujillo.

## 4.3 Fases y tiempos requeridos de implementación

El proyecto inicial abarca la implementación del centro de servicios redundante en Lima. Esta fase del proyecto necesita ser implementada en 3 meses como máximo luego de puesta la orden de compra del equipamiento necesitado.

Luego se realizarán las ampliaciones en Lima y en Provincias según la Tabla 4.1:

**Tabla 4.1 – Fases de Implementación**

Centro de Servicios	Año 1	Año 2	Año 3
Lima - Nodo 1 y 2	Adjudicación Implementación Operación	Operación Ampliación	Operación
Lima - Nodo 3	-	Adjudicación Implementación Operación	Operación
Provincia - Arequipa	-	Adjudicación Implementación	Operación
Provincia - Trujillo	-	Adjudicación Implementación	Operación

## 4.4 Bloques funcionales

El diseño de la solución debe estar basado en bloques funcionales según la Figura 4.1

WAN, CORE/AGREGACION, SERVICIOS DE VALOR AGREGADO y ACCESO

**Figura 4.1 – Bloques Funcionales**



#### 4.5 Arquitectura de equipamiento

Los equipos considerados deben tener las siguientes consideraciones:

- Los equipos deben ser modulares, de tal manera que puedan escalar en capacidad y puertos con aumento de módulos y no sea necesario cambiar de equipo para ampliaciones futuras.
- Los equipos deben tener una arquitectura que separe el plano de control (procesamiento) y el plano de forwarding (datos) .
- Para mayor disponibilidad, los equipos deben considerar redundancia interna, es decir, deben procesadoras, fuentes de energía y módulos de línea (puertos de red) duplicados.
- Los equipos deben manejar interfaces de 10GE

#### 4.6 Dimensionamiento de puertos

- El bloque WAN de cada nodo del Centro de Servicios Móviles debe conectarse en forma redundante al CORE de la operadora móvil. Estos puertos de conexión debe ser en 10GE.
- El bloque de acceso debe tener los siguientes requerimientos según la Tabla 4.2

**Tabla 4.2 – Tabla de Puerto de switches**

Nodos	Switches de Acceso Puertos 10GE		
	Año 1	Año 2	Año 3
Lima - Nodo 1	2	6	8
Lima - Nodo 2	2	6	8
Lima - Nodo 3	-	2	4
Provincia - Arequipa	-	2	2
Provincia - Trujillo	-	2	2

#### 4.7 Consideraciones de Diseño

- Los equipos deben mantener su procesamiento y manejo de tráfico como máximo al 75% de su capacidad total

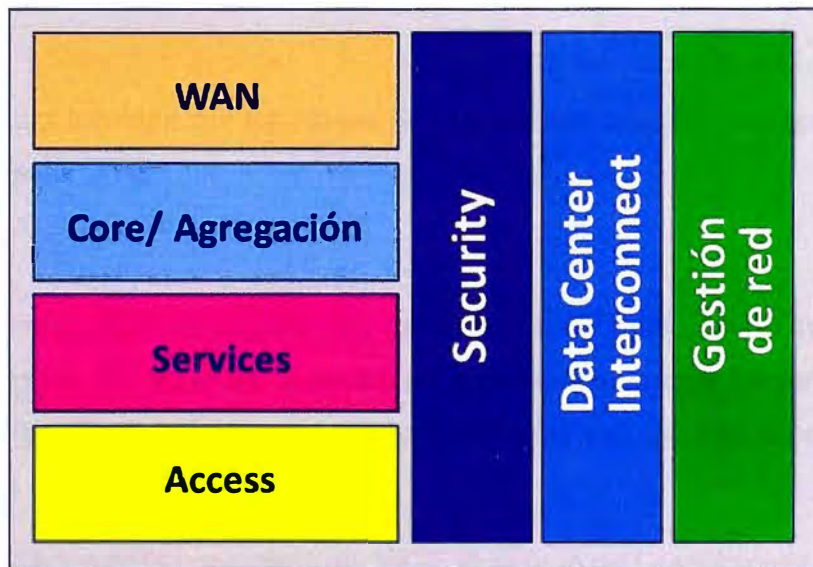
## CAPITULO V INGENIERÍA DEL PROYECTO

Considerando los requerimientos de diseño se planteará la arquitectura descrita en los bloques funcionales.

### 5.1 Diagrama de bloques de la arquitectura

Este diagrama de bloques permite un diseño modular y escalable para un mejor entendimiento de los vínculos y dependencias de cada parte de la red.

Los bloques que comprenden el diseño son: WAN, Core/Agregación, Servicios, Acceso, Seguridad, Data Center Interconnect y Gestión de Red. Ver Figura 5.1



*Figura 5.1 Diagrama de bloques del Centro de Servicios*

#### **WAN**

Este bloque provee la conectividad entre el centro de servicios a implementar y la red IP MPLS del ISP.

Este bloque estará formado por los router ASR quienes cumplirán la función de CE, con conexión tanto a la red Móvil como la red Fija del ISP.

#### **Core/Agregación**

Este bloque concentrará la conectividad entre todos los elementos internos del centro de servicios. Para un mejor escalamiento y por recomendación de diseño las capas de Core y Agregación han sido colapsadas en una sola.

Este bloque concentrará las conexiones uplink de todos los switches que conforman el bloque de acceso y proveerá la conectividad al bloque WAN de todas las aplicaciones ubicadas en el centro de servicios.

Además proveerá la conexión al bloque de servicios según la demanda de las aplicaciones del centro de servicios.

Este bloque estará formado por un switch virtual en el Nexus 7010.

### **Acceso**

El bloque de acceso brinda la conexión física a los servidores del centro de servicios y opera en Capa 2. Este bloque juega un rol importante en encontrar todos los requerimientos de servidores tales como NIC teaming y clustering. Este bloque es el primer punto de “oversubscription” en el centro de servicios porque agrega el tráfico de servidores en interfaces uplink de 10GE hacia el bloque de Core/Agregación.

La interconexión entre el bloque de acceso y el bloque de Core/Agregación se realizará con port-channels (convencionales y virtual Port-channel vPC) para brindar alta redundancia.

Este bloque estará formado por los Nexus 5010 junto con sus extensiones (Fabric EXtender FEX), los Nexus 2048.

### **Servicios**

El bloque de servicios brinda seguridad y servicios de optimización de aplicaciones a todas las aplicaciones ubicadas en el centro de servicios, mediante firewalls, IPS y balanceadores de carga. También provee servicios VPN punto a punto para conectar el centro de servicios con proveedores externos.

El bloque de servicios está conectado en 10GE al bloque de Core/Agregación.

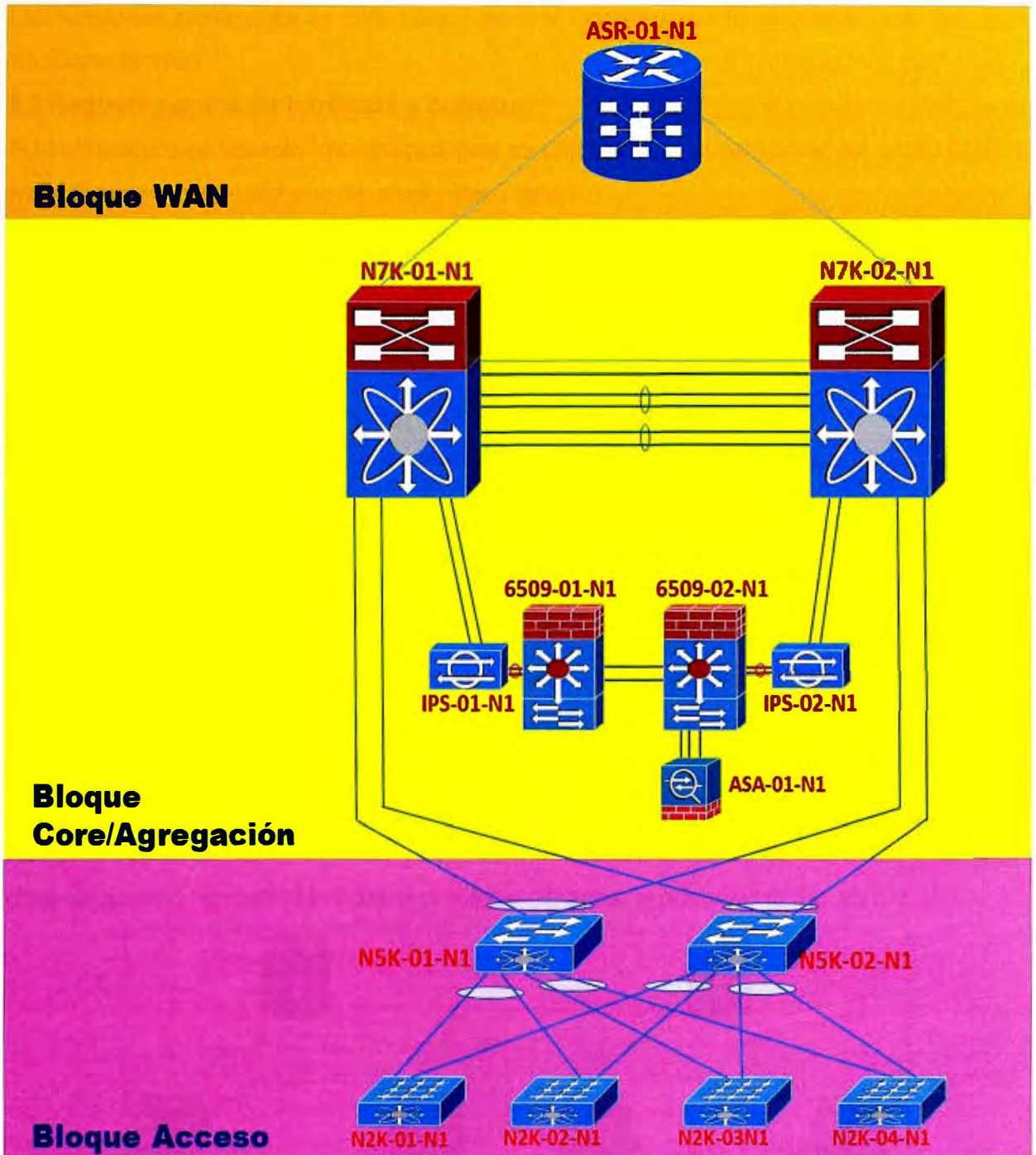
Este bloque estará conformado por el switch modular 6500, el cual cuenta con los módulos de firewall (FWSM), módulos de balanceadores de carga (ACE), equipos IPS y concentrador de vpn (ASA).

### **Seguridad**

Este bloque refiere a los features que habilitan la seguridad E2E de toda la red de Centro de Servicios. Esta seguridad va más allá de los elementos de seguridad como firewall o IPS, sino se refiere a las políticas de seguridad que se alinean con los objetivos del negocio. Estas políticas incluyen las mejores prácticas recomendadas por el proveedor. La seguridad debe ser considerada como un componente integrado en la arquitectura de la solución.

La Figura 5.2 muestra el esquema de bloques de la solución de Cisco.





*Figura 5.2 Centro de servicios dividido en bloques*

### Data Center Interconnect (DCI)

Este bloque es el encargado de extender los límites del centro de servicios, con el fin de proveer la habilidad de virtualizar o poner en cluster servidores entre los dos nodos.

Este bloque también puede proveer la habilidad de implementar redundancia inter-nodal teniendo datos replicados entre los nodos.

### Gestión de red

Este bloque contendrá todas las aplicaciones de gestión de red, por lo cual tendrá conectividad a todos los elementos de red en el centro de servicios.

Las funciones principales de este bloque será el monitoreo de la red, gestión de cambios y soporte técnico.

### 5.2 Requerimientos de hardware y software

A continuación se listarán los equipos que se utilizarán en el proyecto, así como el software requerido por cada uno de ellos. Ver Tabla 5.1

**Tabla 5.1 – Lista de requerimientos de hardware y software**

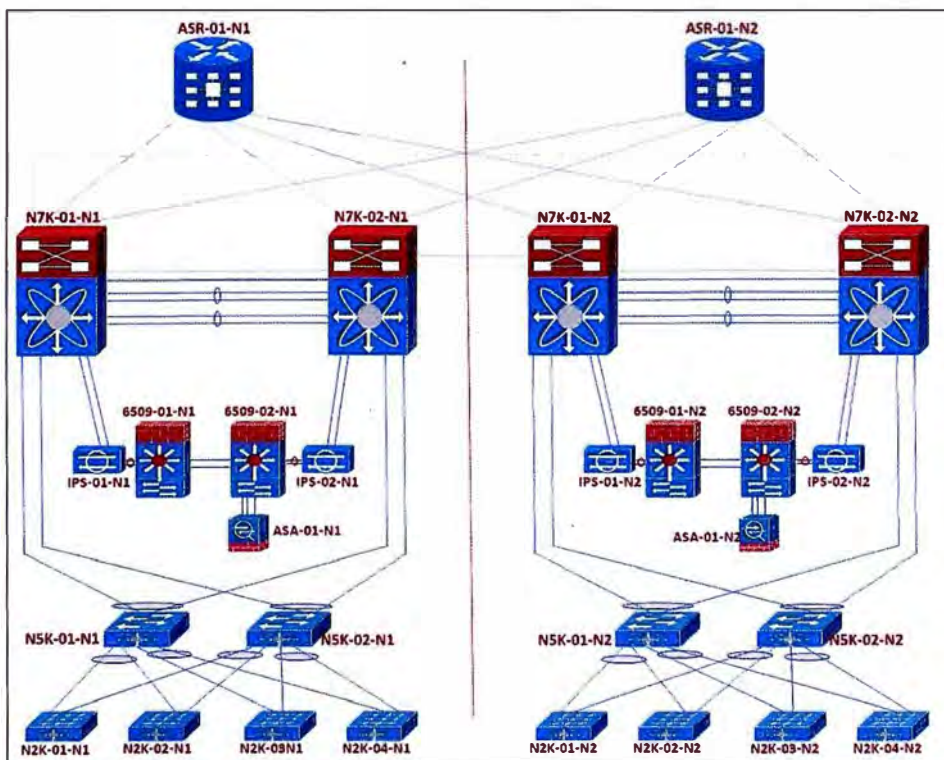
Equipo	Cantidad	Bloque	Software	Descripción
ASR 9006	2 (1 x nodo)	WAN	XR 4.0.3	Interconexión con la red del ISP
Nexus 7010	4 (2 x nodo)	Core/Agregación	5.1.3	Conexión a todos los elementos de CS
Nexus 5010	4 (2 x nodo)	Acceso	5.0(2)N1(1)	Complementado con los N2K (FEX)
Catalyst 6509	4 (2 x nodo)	Servicio	12.2(33)SX14	Switch modular para brindar servicios
ACE 20	4 (2 x nodo)	Servicio	A2(3.4)	Módulo balanceador de carga
FWSM	4 (2 x nodo)	Servicio	4.1.4	Módulo de firewall
IPS 4270	4 (2 x nodo)	Servicio	7.0.2	Equipo detector de intrusos
ASA 5520	2 (1 x nodo)	Servicio	8.4(1)	Concentrador de VPNs
DCNM	1	Gestión	5.1.3u	Servidor para gestión de red

### 5.3 Diseño Físico

Tenemos dos ramas idénticas de equipos redundantes geográficamente e interconectadas a través de fibra óptica.

Como cabecera de cada nodo tenemos un router ASR, los cuales estarán conectados en interfaces de 10GE con los Nexus 7010 locales e inter-nodales, con el fin de tener un esquema altamente redundado.

Los Nexus 7K también están conectados entre ellos localmente e inter-nodalmente. Los Nexus 7K también tienen conexión en 10GE contra los switches de Servicios y los switches de acceso Nexus5010. Para una referencia general observar la Figura 5.3.



**Figura 5.3 Diagrama físico del Centro de Servicios**

Los switches 6509 contienen los módulos de firewall y de balanceo de carga, y están conectados en 10GE a sus Nexus 7K locales. A los switches 6509 también están conectados los equipos de prevención de intrusos (IPS) y el equipo que permitirá establecer las vpn (Asa 5520).

Los Nexus 5K permiten la agregación de los Nexus 2K, quienes estarán en la parte superior de cada bastidor concentrando todas las conexiones de servidores y/o aplicaciones. Los Nexus 5k conectan al core y a los Nexus 2K en interfaces 10GE.

Para la nomenclatura de los nombres de los equipos se consideró lo siguiente: **“Tipo de Equipo-Número-Nodo”**

Como primera parte se considera el tipo de equipo

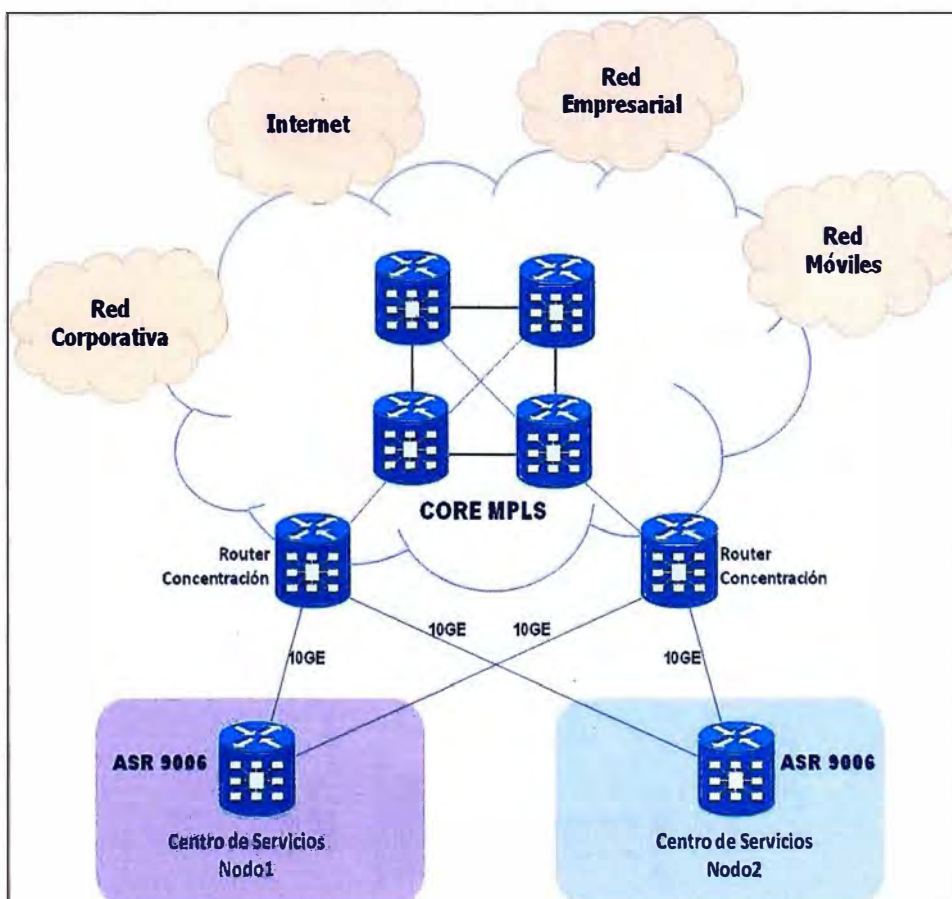
Como segunda parte se considera el número de equipo en el nodo

Como tercera parte se considera el nodo donde está ubicado el equipo (Nodo 1 = N1 y Nodo 2 = N2)

### 5.3.1 Diseño Físico del bloque WAN

Está conformado por los dos ASR quienes se conectan al Core del ISP a través de Router de concentración y por el cual tendrán conectividad a todas las redes externas

Las conexiones son en 10GE y redundantes. Se utiliza fibra oscura para las cuatro conexiones requeridas. Ver Figura 5.4



**Figura 5.4** Conexiones en el bloque WAN



### 5.3.2 Diseño Físico del bloque Core/Agregación

El bloque de Core/Agregación está conformado por 2 Nexus 7010 en cada nodo los cuales están conectados entre sí para brindar alta redundancia.

Los Nexus 7K inter-nodales se conectan por fibra oscura para conectar los centros de servicios de ambos nodos y brindar redundancia geográfica.

Todas las conexiones troncales de los switches N7K son interfaces de 10GE.

Las Figuras 5.5 y 5.6 muestran las conexiones físicas tanto en el nodo 1 como en el nodo 2 respectivamente.

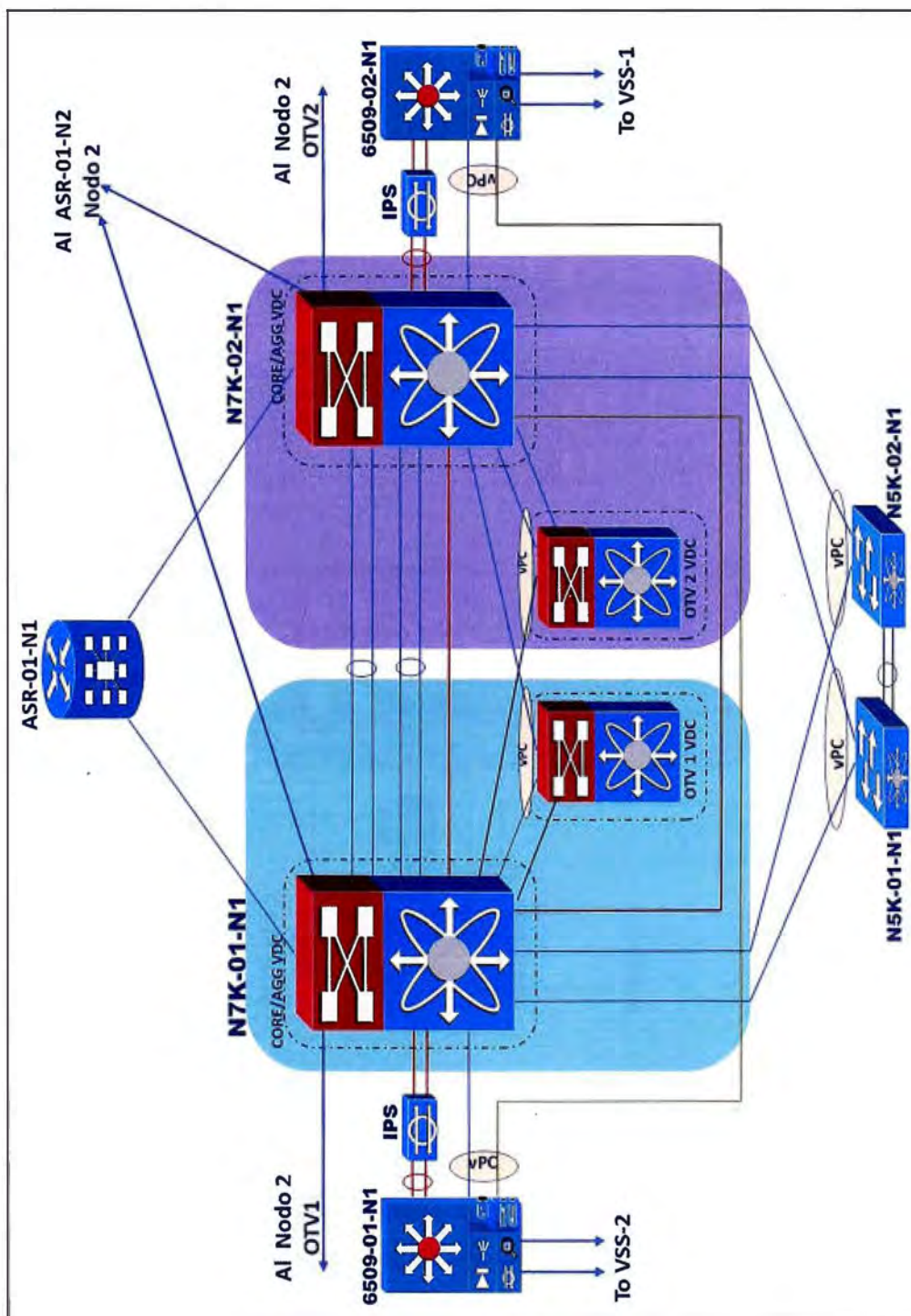


Figura 5.5 Conexiones en el bloque Core/Agregación – Nodo 1

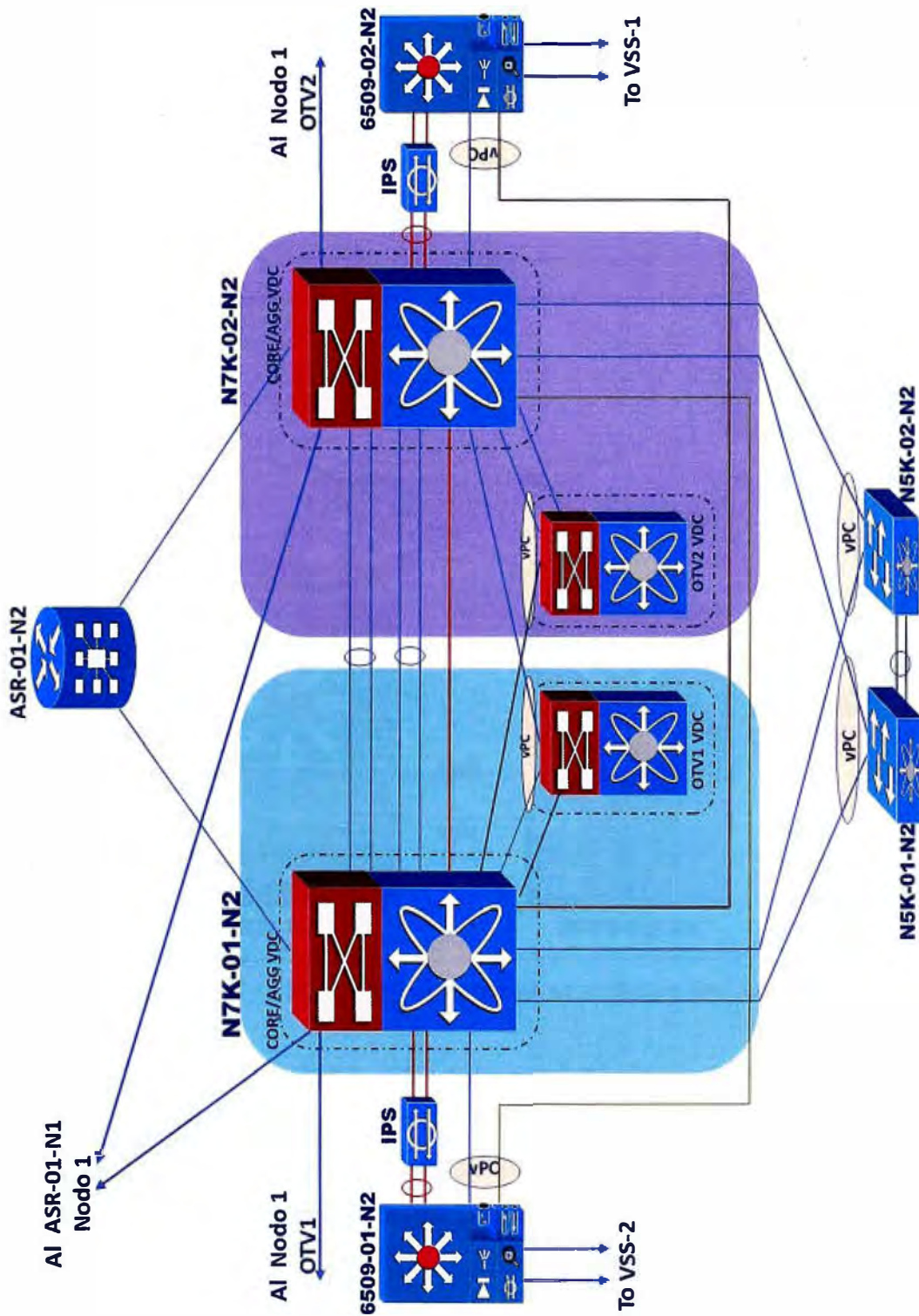
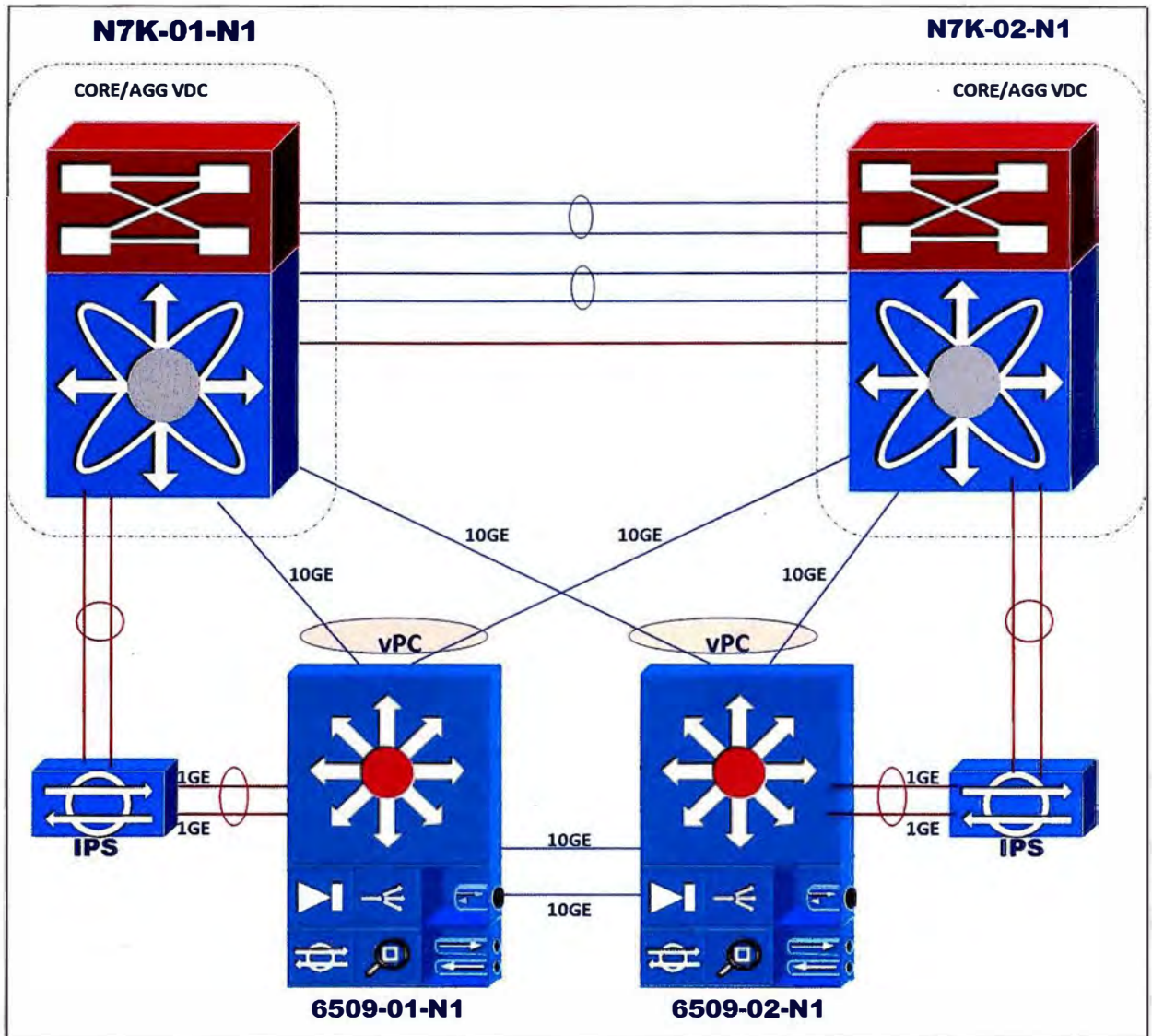


Figura 5.6 Conexiones en el bloque Core/Agregación – Nodo 2

### 5.3.3 Diseño Físico del bloque de Servicio

El bloque de servicio está conformado por los switches modulares 6509, los cuales contienen los módulos de firewall y balanceadores de carga como servicio. Y adicionalmente se tiene el equipo IPS para servicios que lo requieran. Ver Figura .5.7



*Figura 5.7 Conexiones en el bloque Servicios*

Los switches 6509 están conectados entre ellos con 2 interfaces de 10GE.

Los switches 6509 están conectados al bloque Core/Agregación con interfaces de 10GE.

Los IPS están conectados con 2 interfaces de 1GE a los N7K haciendo un port-channel. Así mismo, el IPS se conecta al bloque de Core/Agregación también con 2 interfaces de 1GE.

Este esquema es replicado para ambos nodos.

#### **5.3.4 Diseño Físico del bloque de Acceso**

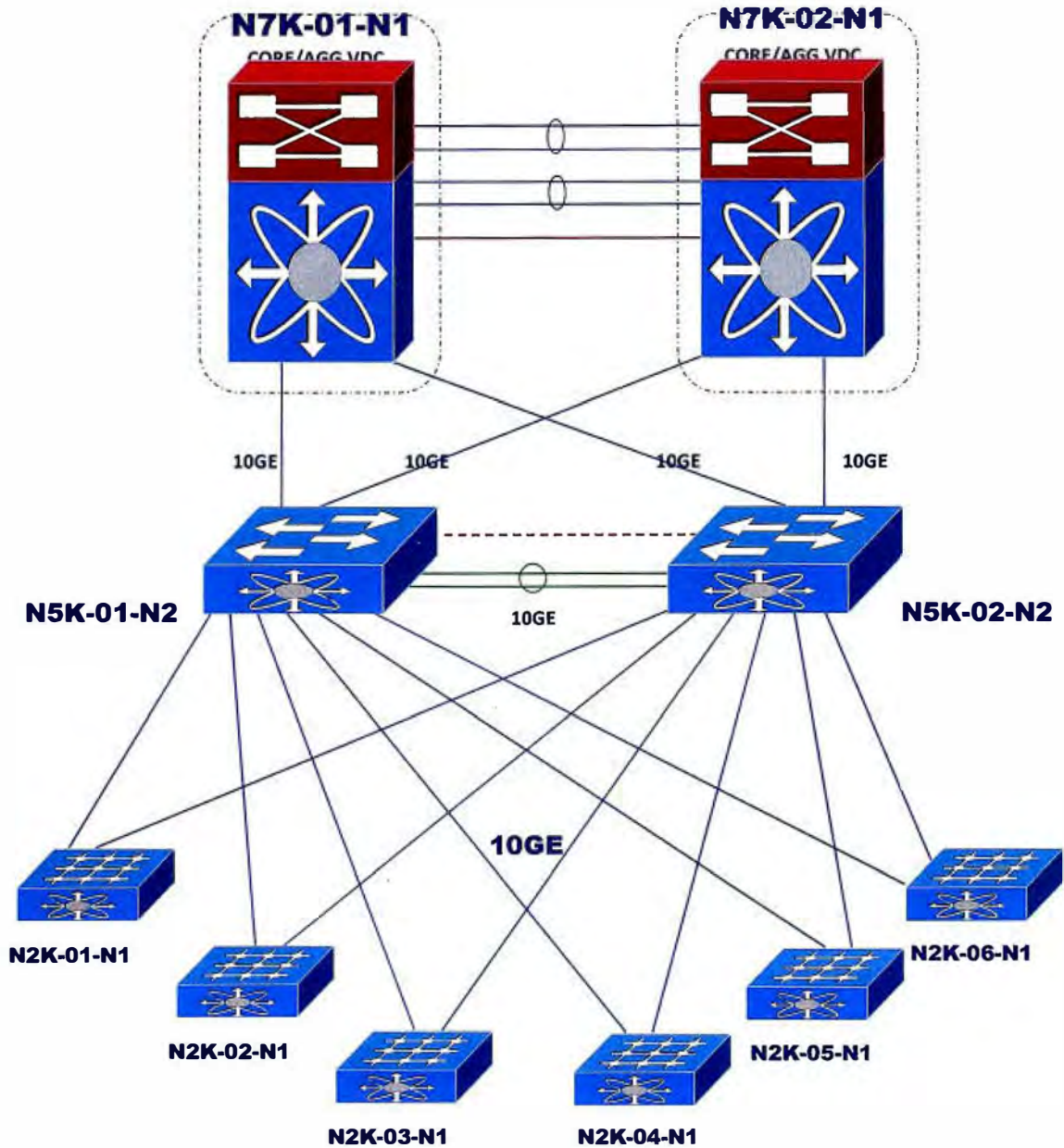
El bloque de acceso es construido usando la combinación de switches Nexus 5010 y Nexus 2248 (Fabric Extender FEX).

Los switches N5K se conectan al bloque superior con interfaces de 10GE, así mismo conectan a los switches N2K Fabric Extender (FEX) con interfaces de 10GE.

Finalmente, los FEX proveen de interfaces 100/1000 Mbps para la conexión de servidores en el centro de Servicios



Este esquema es replicado para ambos nodos. Ver Figura 5.8



*Figura 5.8 Conexiones en el bloque Acceso*

## 5.4 Diseño Lógico

En esta parte del documento se explicará el diseño lógico de cada bloque funcional, y se describirán las principales funcionalidades y features que se habilitarán en los equipos involucrados.

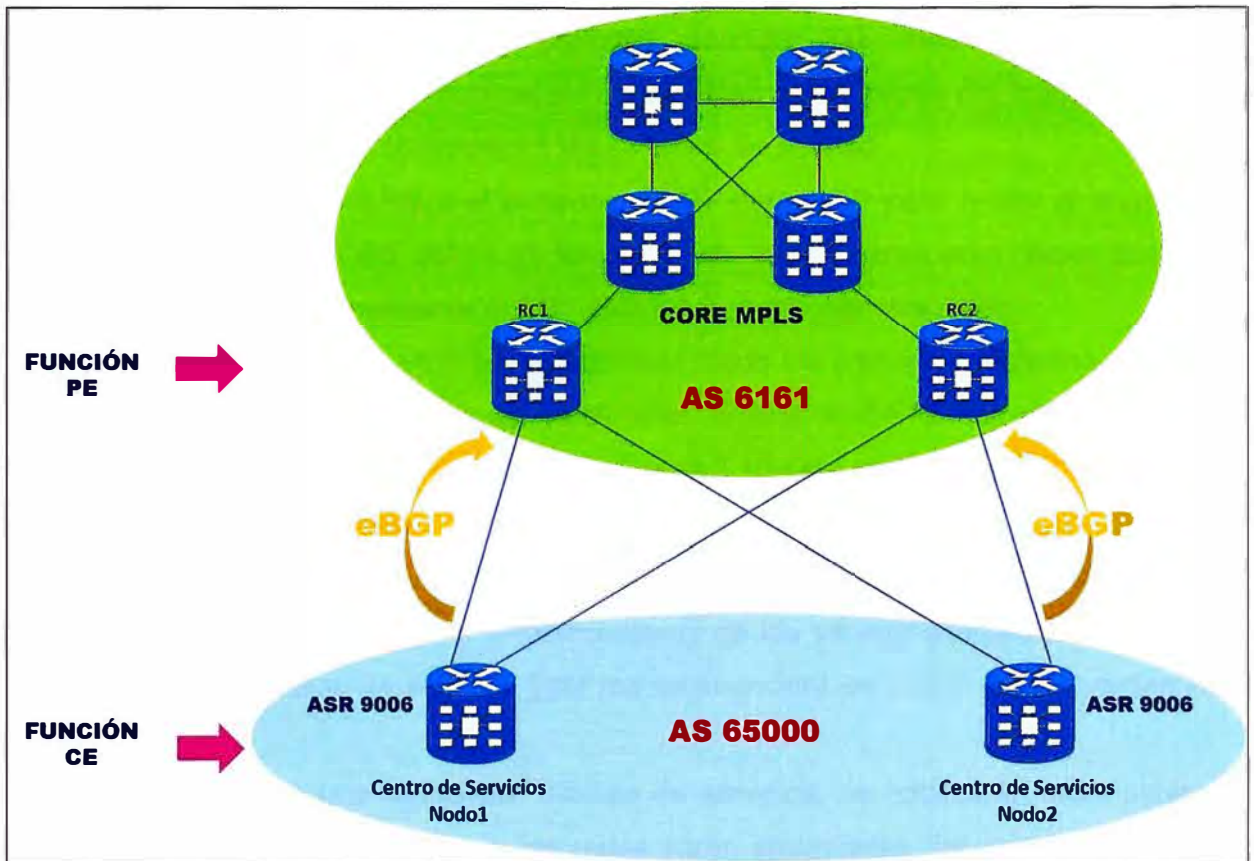
### 5.4.1 Diseño Lógico del bloque WAN

Ya sabemos que las conexiones físicas entre los ASR y el Core serán en 10GE.

Los ASR cumplirán la función de CE (Customer Edge), con el fin de tener conexión al Core Fijo y al Core Móvil sin mezclar los planos de control de ambas redes.

Los router de concentración, los cuales reciben las conexiones 10GE de los ASR, tendrán la función de PE (Provider Edge).

Entre estos PE y CE se configurará el protocolo eBGP como protocolo de ruteo externo para intercambio de rutas entre el centro de servicios y las demás redes. Por seguridad, las sesiones eBGP serán autenticadas. Ver Figura 5.9



*Figura 5.9 Esquema lógico en el bloque WAN*

Los PE tendrán configuradas las familias IPv4, VPNv4, MDT e IPv6 para brindar los servicios y conectividad al centro de servicios según los requerimientos de las aplicaciones. En los ASR también se habilitará QoS, con el fin que ellos marquen a los paquetes según cómo se requiera sean tratados a través del Core.

#### **5.4.2 Diseño Lógico del bloque Core/Agregación**

Los switches Nexus 7000 tienen la habilidad de dividir un solo switch físico en hasta 4 switches virtuales. Estos switches virtuales toman el nombre de VDC (Virtual Device Context), donde cada VDC opera como un switch independiente con un diferente archivo de configuración, puertos únicos para cada contexto y con protocolos de plano de control también independientes.

El bloque de Core/Agregación está conformado por un VDC dedicado para esta función, el cual tiene asignado las interfaces de 10GE para conectar a los ASR, los switches 6500 de servicios y los switches de acceso Nexus 5010.

En cada N7K se habilitará un VDC que funcionará como VDC Core/Agregación.

## OSPF

IGP con buena performance, escalabilidad y compatibilidad con diversos proveedores.

El protocolo OSPF se habilitará en las interfaces que conectan con los ASR y las interfaces que interconectan con los VDC locales e inter-nodales. El área a utilizar será la "0".

Mediante el protocolo OSPF se permitirá anunciar las redes de los servidores/aplicaciones internas de centro de servicios, estén estas detrás del módulo de servicios, o sean conectadas directamente a los switches de acceso.

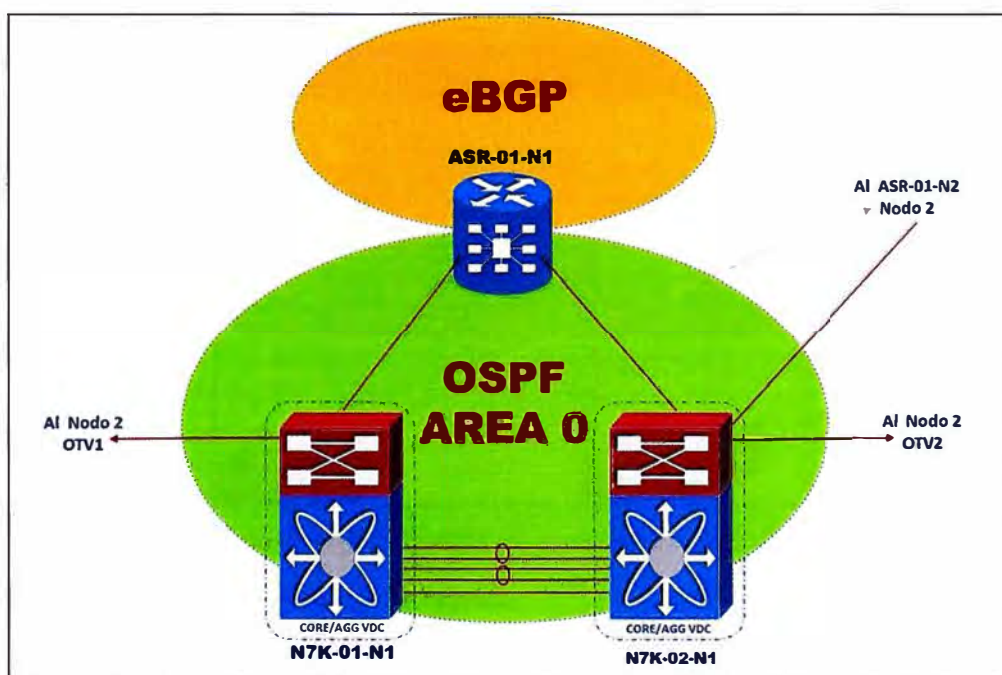
En el ASR también se habilitará el protocolo OSPF como IGP para recibir el anuncio de todas las redes internas del centro de servicios, las cuales serán anunciadas posteriormente al mundo externo mediante el EGP (eBGP) que manejan los ASR.

El protocolo OSPF utilizará MD5 para autenticar todos los paquetes recibidos de las redes en todas sus interfaces. También se afinarán "timers" de OSPF con el fin de mejorar los tiempos de convergencia del IGP. Ver la Figura 5.10 para revisar enrutamiento.

## SVI (Switch Virtual Interface)

Se puede definir a una SVI como una vlan con IP (L3). En el VDC Core/Agregación se crearán SVIs, las cuales serán el default-gateway de los servidores/aplicaciones que no requieran ningún módulo de servicio. Esta red se anunciará en OSPF como directamente conectada.

Para las aplicaciones que necesiten módulo de servicios, se habilitarán rutas estáticas apuntando al switch de servicios, y las redes serán anunciadas distribuyendo las rutas estáticas en OSPF.



**Figura 5.10** Protocolos de ruteo en el bloque Core/Agregación



### HSRP (Hot Standby Routing Protocol)

Para habilitar la redundancia local de los VDC locales, se habilitará HSRP con el cual se tendrá un VDC como activo y el otro como standby. Ver la Figura 5.11.

### STP (Spanning-Tree) / vPC (Virtual Port-Channel)

Este switch virtual tendrá conectado switches de Acceso (Nexus 5000). Para evitar los posibles loops no será necesario habilitar el protocolo Spanning-tree, lo cual es una gran ventaja pues esto suele ser un dolor de cabeza en la operación y mantenimiento de las redes de switches. STP sólo se usará como backup si fallara el nuevo feature que hace prescindir de Spanning-Tree, el cual se llama vPC (virtual Port-Channel). VPC hace ver a ambos VDC locales como un solo switch, lo cual evita los posibles loops mencionados en la topología. Ver Figura 5.12.

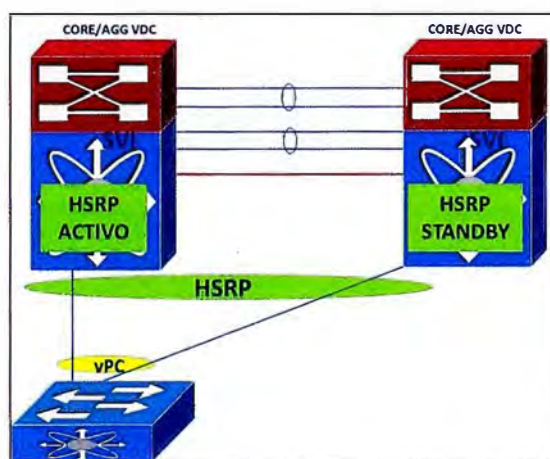


Figura 5.11 Redundancia con protocolo HSRP

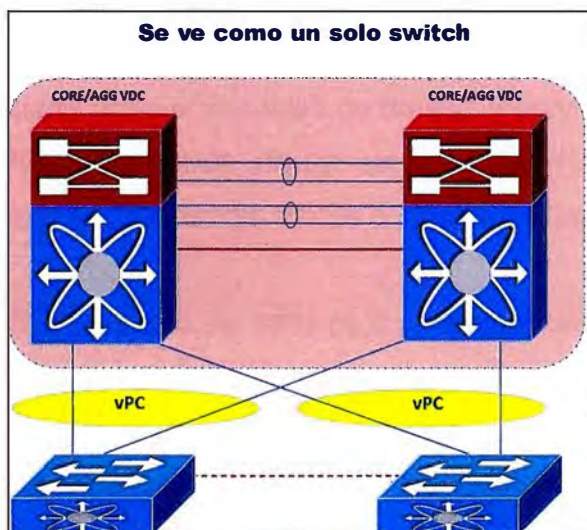


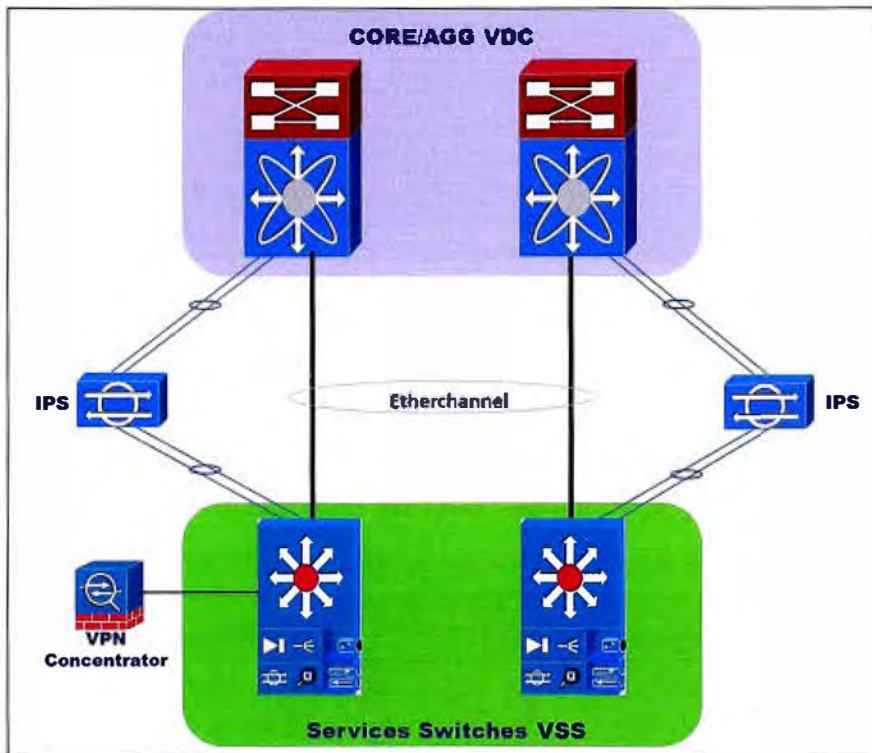
Figura 5.12 Esquema de switches usando vPC

### 5.4.3 Diseño Lógico del Bloque Servicios

Sabemos que el bloque de servicios está conformado por un par de switches 6500 que proveen conectividad en Capa 2 a los módulos de firewall y balanceadores de carga. Es-

tos switches de servicio también proveerán conectividad Capa 2 hacia los equipos IPS y hacia el concentrador de vpn (ASA 5520). Ver Figura 5.13

El módulo de servicio es muy flexible, quiere decir que todos los módulos y equipos instalados en el módulo de servicios serán configurados para proveer diferentes tipos de servicios en demanda. Por ejemplo si algún servicio requiere que el tráfico sea inspeccionado por el IPS será así, y si no es requerido, el tráfico no será inspeccionado.



*Figura 5.13 Esquema lógico del bloque de servicios*

La flexibilidad puede ser alcanzada usando el concepto de PODS. Un POD es una instancia lógica que contendrá los diferentes tipos de servicios que la aplicación necesite. Por ejemplo, un POD puede proveer servicios de firewall y servicios de balanceo de carga mientras que otro POD sólo puede ofrecer servicios de IPS. Con este concepto, el POD puede ser compuesto por elementos físicos o lógicos de firewall, balanceo de carga, IPS, etc.

Adicionalmente se brindan servicios de VPN punto a punto, las cuales serán atendidas por el firewall ASA 5520.

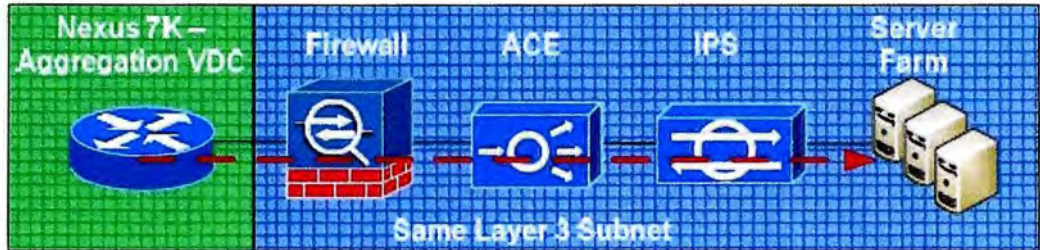
Ya hemos visto la funcionalidad de vPC que es utilizada por los equipos Nexus y que permite ver a ambos equipos como uno solo entidad y evita los problemas de Spanning-tree. Para que los switches de servicios, los Catalyst 6500, tengan la misma funcionalidad, se les incorpora unas tarjetas VSS las cuales harán ver a los 6500 como un solo equipo.

A continuación mostraremos las opciones de POD que tenemos en el Centro de Servicios:



### Si el POD tiene Firewall, IPS y ACE

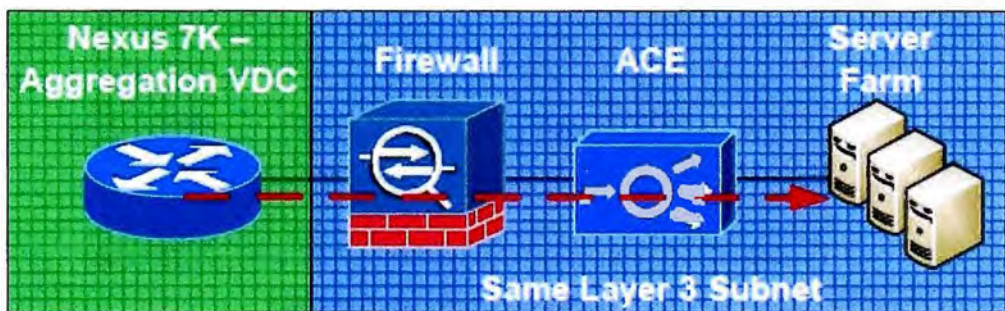
El tráfico que ingresa a centro de servicios a través de los ASR es enviado hacia el VDC de Core/Agregación. De aquí el tráfico será enviado al firewall quien analizará si el tráfico es permitido o no. Si es permitido será enviado hacia el balanceador de carga, para luego pasar al IPS, quien verificará si es tráfico malicioso o no; si no lo es será enviado finalmente a los servidores de aplicación. Ver Figura 5.14



*Figura 5.14* POD Firewall + ACE + IPS

### Si el POD tiene Firewall y ACE

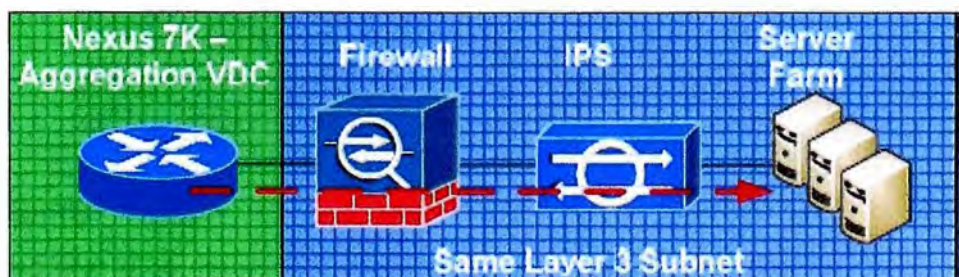
El tráfico que ingresa a centro de servicios a través de los ASR es enviado hacia el VDC de Core/Agregación. De aquí el tráfico será enviado al firewall quien analizará si el tráfico es permitido o no. Si es permitido será enviado hacia el ACE para aplicar las políticas de balanceo y finalmente enviar el tráfico hacia los servidores de aplicación. Ver Figura 5.15



*Figura 5.15* POD Firewall + ACE

### Si el POD tiene Firewall e IPS

El tráfico que ingresa a los servicios alojados en el centro de servicios a través de los ASR es enviado hacia el VDC de Core/Agregación. De aquí el tráfico será enviado al firewall quien analizará si el tráfico es permitido o no. Si es permitido será enviado hacia el IPS, quien verificará si es tráfico malicioso o no; si no lo es será enviado finalmente a los servidores de aplicación. Ver Figura 5.16



*Figura 5.16* POD Firewall + IPS

### Si el POD tiene ACE e IPS

El tráfico que ingresa a centro de servicios a través de los ASR es enviado hacia el VDC de Core/Agregación. De aquí el tráfico es enviado hacia el ACE quien aplicará las políticas de balanceo, para posteriormente enviarlo al IPS, quien verificará si es tráfico malicioso o no; si no lo es será enviado finalmente a los servidores de aplicación. Si el tráfico fuera malicioso, este será descartado. Ver Figura 5.17

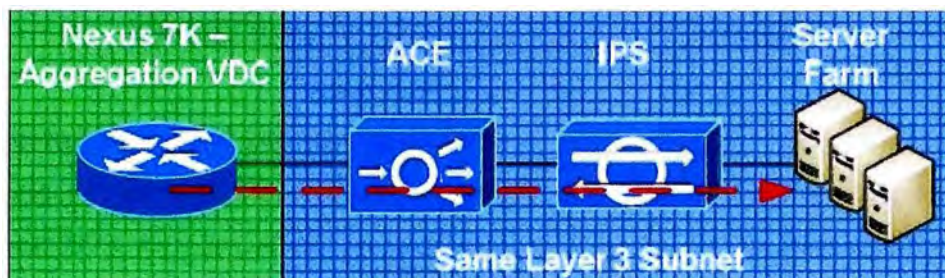


Figura 5.17 POD ACE + IPS

### Si el POD tiene Firewall

El tráfico que ingresa a centro de servicios es enviado hacia el VDC de Core/Agregación. De aquí el tráfico será enviado al firewall quien analizará si el tráfico es permitido o no. Si es permitido será enviado finalmente a los servidores de aplicación. Ver Figura 5.18

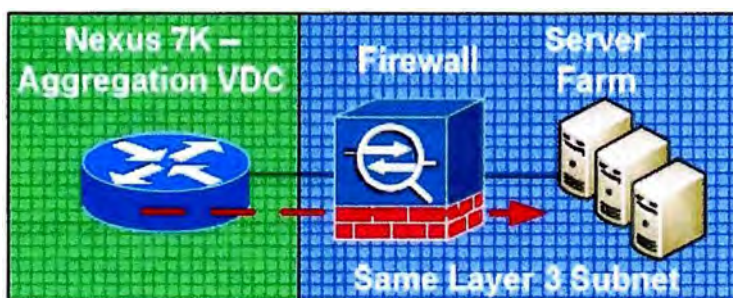


Figura 5.18 POD Firewall

### Si el POD tiene ACE

El tráfico que ingresa a centro de servicios es enviado hacia el VDC de Core/Agregación. De aquí el tráfico es enviado hacia el ACE quien aplicará las políticas de balanceo, para finalmente repartir el tráfico entre los servidores de aplicación. Ver Figura 5.19

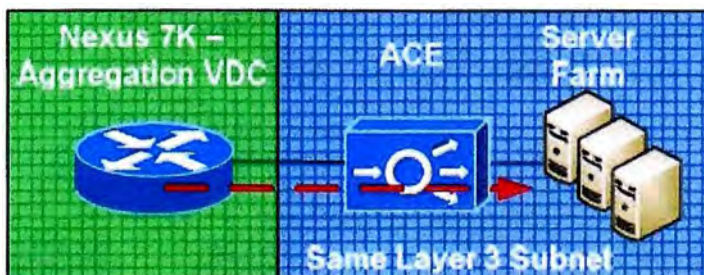


Figura 5.19 POD ACE

### Si el POD tiene IPS

El tráfico que ingresa a centro de servicios a través de los ASR es enviado hacia el VDC de Core/Agregación. De aquí el tráfico es enviado directamente hacia el IPS, quien verifi-



cará si es tráfico malicioso o no; si no lo es será enviado finalmente a los servidores de aplicación. Si el tráfico fuera malicioso, este será descartado. Ver Figura 5.20

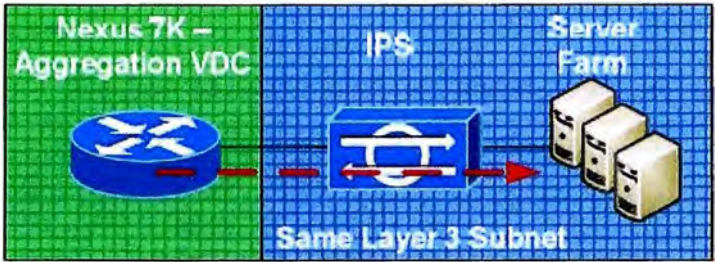


Figura 5.20 POD IPS

5.4.4 Diseño Lógico del Bloque de Acceso

Está formado por los switches Nexus 5k junto con los Nexus 2K Fabric Extender (FEX). Los switches N2K se convierten en una extensión física de los Nexus 5K. Cuando un Nexus 2K se conecta a dos Nexus 5K, se usará el feature vPC para que el N2K vea a ambos N5K como uno solo, lo cual es una ventaja porque evita tener links sin usar debido al spanning-tree y tener los problemas de convergencia del protocolo. Se tendrá configurado spanning-tree en los switches pero sólo como contingencia si fallara el vPC configurado en los equipos. Ver Figura 5.21

Los switches N5K y N2K sólo funcionarán en Capa 2, no se habilitará ningún tipo de enrutamiento a través de estos equipos.

Los switches N2000 son gestionados a través de los N5000. En la consola de los N5k aparecerán la lista de puerto adicionales correspondiente a los N2K y desde allí se realizarán las configuraciones. A los N2K sólo se conectarán hosts, no se conectarán switches.

Los switches N2K se colocarán en la parte superior de los racks, en la forma "Top of the rack".

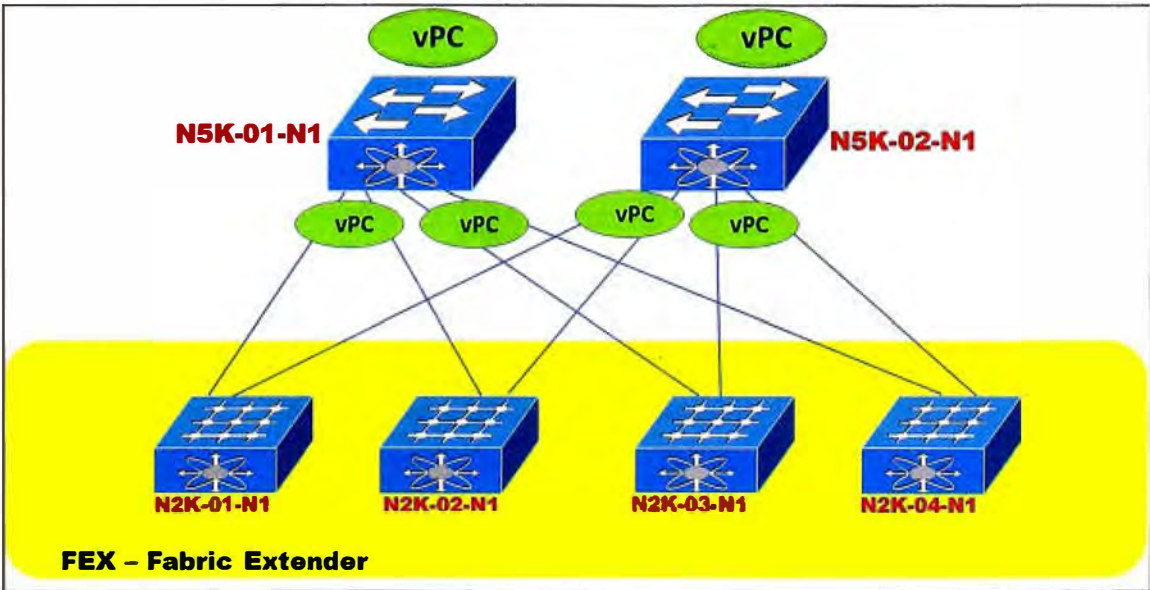


Figura 5.21 Esquema lógico en el bloque de acceso - vPC

## 5.5 Especificaciones técnicas del equipamiento

### 5.5.1 Cisco ASR 9006

Hardware del proyecto

Cada equipo contiene la siguiente distribución de tarjetas según la Tabla 5.1

Slot	Module	Comment
FT0	ASR-9006-FAN	ASR-9006 Fan Tray 0
FT1	ASR-9006-FAN	ASR-9006 Fan Tray 1
RSP0	A9K-RSP-4G	ASR9K Route Switch Processor & Fabric 0
RSP1	A9K-RSP-4G	ASR9K Route Switch Processor & Fabric 1
0	A9kK-4T-B	4-Port 10GE Line Card
1	A9K-LC-FILR	ASR-9K Line Card Filler
2	A9K-4T-L	4-Port 10GE Low Queue Line Card
3	A9K-LC-FILR	ASR-9K Line Card Filler

**Tabla 5.1** – Componentes del Cisco ASR 9006

Chassis

El chassis del ASR-9006 es un componente que sirve de contenedor para módulos y tarjetas, sus principales características son:

Tiene dos slots reservados para tener un par de procesadoras redundantes y 4 slots disponibles para tarjetas de línea (linecards). Ver Figura 5.22

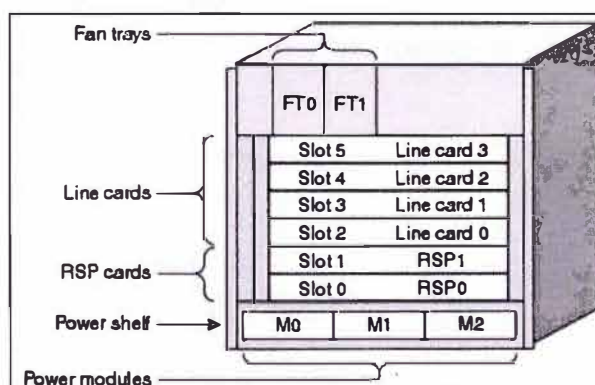
Soporta hasta 400 Gbps por slot y 3.2 Terabits por chassis

Tiene disponibles tarjetas de línea de puertos de 1Gbps o 10Gbps

Switch Fabric redundante contenido en las tarjetas procesadoras (RSP)

Consta de una plataforma de energía y hasta 3 llaves de fuentes de alimentación AC o DC, dependiendo de la cantidad de energía y redundancia deseada

Optimiza el sistema de enfriamiento, estando formado por dos módulos de ventilación, los cuales incluye 6 ventiladores internos.



**Figura 5.22** Distribución de tarjetas en el ASR

Switch Fabric

El "Switch Fabric" es el principal componente para el envío de paquetes en el ASR y es implementado con tarjetas "fabric" internas integradas a cada procesadora (RSP)

Route Switch Processor (RSP)

Proveen la inteligencia al sistema, trabajando como controlador y como inyector de información de forwarding a las tarjetas de línea. Ver Figura 5.23

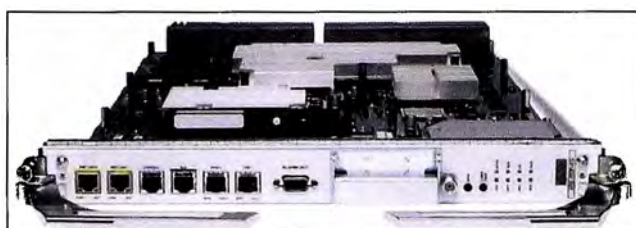
Sólo una RSP es activa a la vez, la otra actúa como backup.

La RSP también se encarga del monitoreo de alarmas y el sistema de enfriamiento. Las principales características de A9K-RSP-4G son:

Contiene módulos de *Switch Fabric*, permitiendo el forwarding full dúplex de 180Gbps/slot

Procesadores Dual-Core de alta performance

Memoria interna DRAM de 4GB. Disco duro de 40GB. Compact Flash de 1GB (externa).



**Figura 5.23** Tarjeta procesadora del ASR

#### Linecards

Las linecards proveen el sistema de interfaces a través del cual se envía y se recibe el tráfico del usuario. Ver Figura 5.24. Tienen las siguientes características:

Servicios L2/L3 integrados

QoS jerárquico (HQoS)

Plano de control distribuido de alta performance

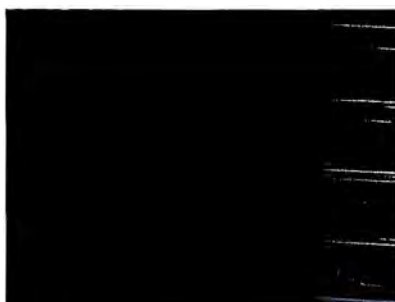
Plano de datos distribuido y flexible

Procesamiento distribuido OA&M

Netflow distribuido

OIR ( Inserción y retiro en línea)

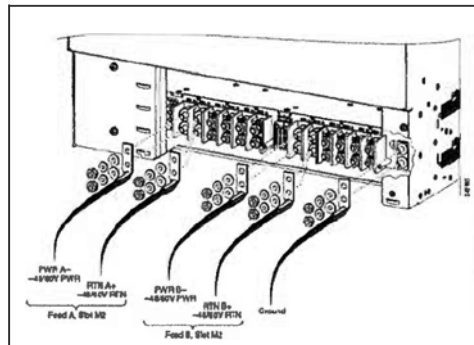
Las tarjetas ASR9K-4T-L/B tienen 4 puertos de 10Gbps y usan conectores XFP. Estos incluyen Network Processors (NP)



**Figura 5.24** Tarjetas de línea en el ASR

#### Sistema de energía

Cuenta con un sistema de energía que alimenta a 3 fuentes. Cada fuente requiere de 4 cables como se muestra en la Figura 5.25 y 5.26



**Figura 5.25** Forma de conexión de fuentes de alimentación



**Figura 5.26** Fuentes de poder - ASR

El sistema no es dividido por zonas, cada fuente de alimentación de 2100W distribuye energía equitativamente a los módulos instalados. La cantidad recomendada de alimentación debe cubrir los requerimientos de energía para los módulos instalados más una fuente adicional (redundancia N+1)

La prioridad de asignación de energía es la siguiente:

1. Módulos de energía
2. Sistemas de ventilación
3. Tarjetas procesadoras (RSP)
4. Linecards empezando desde el slot 0

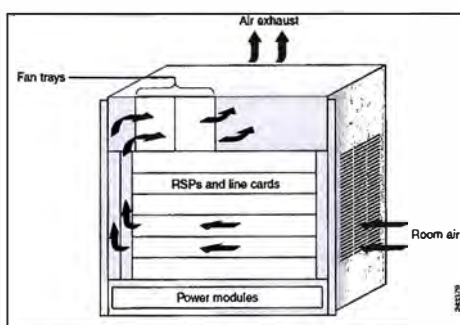
Sistema de ventilación

Está formado por dos sistemas de ventilación, cada uno con 6 ventiladores

Ambos sistemas tienen la habilidad de modificar su velocidad (rpm), en caso de que un ventilador falle, el sistema puede incrementar la velocidad del ventilador y continuar trabajando apropiadamente, sin embargo es recomendable que el reemplazo no exceda las 24 horas

El flujo de aire del ASR 9000 entra por el lado lateral y sale por la parte superior. Es importante considerar esto para colocar el equipo correctamente según los pasillos fríos y calientes del data center. Ver Figura 5.27





**Figura 5.27** Flujo de aire en el ASR

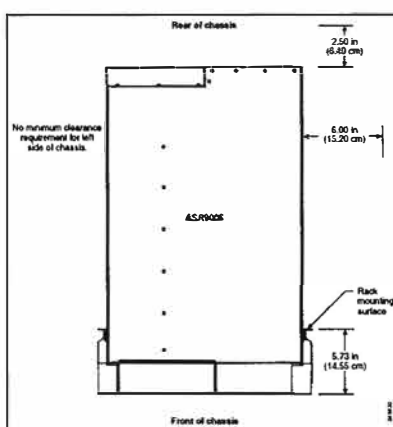
### Consideraciones de instalación

La altura del ASR 9006 es de 44.45 cm, por lo cual la mayoría de bastidores puede contener hasta 4 de estos equipos. Ver Figura 5.28

El ASR con todos sus slots ocupados puede pesar más de 100kg, por lo cual el rack debe poder soportar este peso.

### Software

Tienen el nuevo software Cisco IOS XR, el cual es el mismo de los equipos líderes en la industria (Carrier Class)



**Figura 5.28** Dimensiones del ASR

## 5.5.2 Nexus 7010

### Hardware del proyecto

Cada equipo Nexus 7010 del proyecto contiene la siguiente distribución de tarjetas:

Slot	Module	Comment
1	N7K-M108X2-12L	Nexus 7000 - 8 port 10GbE with XL option
2	N7K-M108X2-12L	Nexus 7000 - 8 port 10GbE with XL option
3	N7K-M108X2-12L	Nexus 7000 - 8 port 10GbE with XL option
4	N7K-M108GS-11L	Nexus 7000 - 48 port GE Module with XL option
5	A9K-4T-B	Nexus 7000 - Supervisor
6	A9K-LC-FILR	Nexus 7000 - Supervisor
7	Empty	Empty
8	Empty	Empty
9	Empty	Empty
10	Empty	Empty

## Chassis

El chassis del Nexus 7010 junto con el software Cisco NX-OS, permite una operación sin interrupciones. Algunas de las características son las siguientes:

El flujo de aire entra por la parte delantera y sale por la parte trasera. Está formado por 10 slots de posición vertical y un sistema de administración de cables integrado que facilita la instalación, operación y enfriamiento de las nuevas y existentes instalaciones.

Diseñado para confiabilidad y máxima disponibilidad, todos los módulos de interfaces y supervisoras son accesibles desde la parte frontal; y las fuentes de alimentación redundantes, sistemas de ventilación y módulos “fabric” son accesibles desde la parte trasera para asegurar que el cableado no sea interrumpido durante una tarea de mantenimiento.

El sistema usa dos módulos dedicados para supervisoras, una arquitectura de “fabric” distribuida compuesta de hasta 5 módulos. Esta distribución puede brindar hasta 230 Gbps por slot para 4.1 Tbps de forwarding

Tiene hasta 8 slots para módulos I/O, los cuales soportan hasta 256 puertos de 10 GB Ethernet o 384 puertos de 1GB Ethernet. Ver Figura 5.29

## Supervisora

La supervisora de la serie Nexus 7000 está diseñada para entregar funciones de administración y plano de control escalables. Está basada en un procesador dual.



**Figura 5.29** Chassis del Nexus 7010

La supervisora controla servicios de Capa 2 y 3, capacidades de redundancia, configuración de administración, monitoreo de estatus, administración de energía y medio ambiente, y más. Esta posee un sistema de fabric centralizado para todas las tarjetas de línea

(linecards). La supervisora incorpora un procesador de administración dedicado (CMP) para soportar administración remota y troubleshooting del sistema. Ver Figura 5.30



**Figura 5.30** Tarjeta supervisora del Nexus 7010

#### Fabric Module

Cisco Nexus 7010 tiene módulos fabric separados que proveen canales fabric paralelos hacia los módulos I/O. Hasta 5 módulos fabric activos simultáneamente trabajan juntos entregando hasta 290 Gbps por slot. El módulo de fabric provee el elemento central de switching para un forwarding distribuido en los módulos I/O. Cada fabric provee de 46 Gbps por slot.

#### - Módulo 10 Gigabit Ethernet

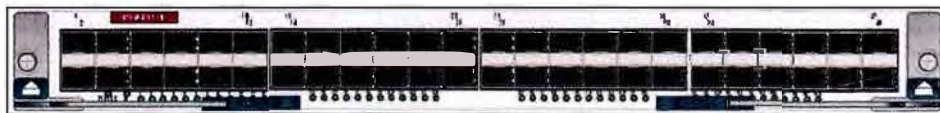
El módulo N7K-M108X2-12L será usado para enlaces de 10GB, el cual provee 8 puertos de 10GB. Ver Figura 5.31



**Figura 5.31** Tarjeta 10GE del Nexus 7010

#### Módulo Gigabit Ethernet

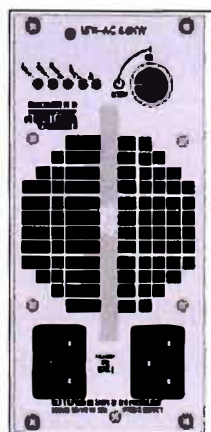
El módulo N7K-M148GS-11L provee 48 puertos de fibra (SFP). El conector SFP debe ser seleccionado de acuerdo a los requerimientos de distancia y específicos del enlace (10Km ó 40 Km). Ver Figura 5.32



**Figura 5.32** Tarjeta de puertos 1GE en Nexus 7010

#### Sistema de Energía

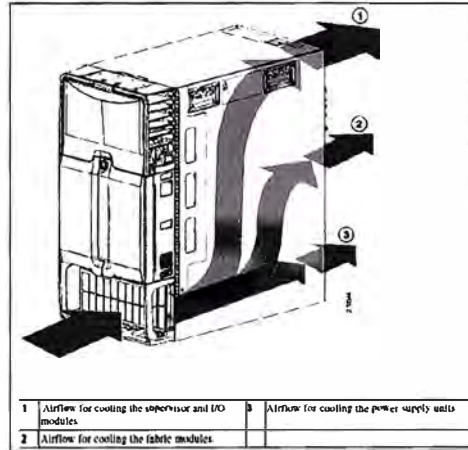
Cada Nexus será energizado con dos fuentes de poder de 6 KW AC. Ver Figura 5.33



**Figura 5.33** Fuente de alimentación del Nexus 7010

## Sistema de enfriamiento

Los switches Nexus 7000 disipan considerable energía que genera mucho calor. El Cisco Nexus 7010 disipa hasta 35,172 BTUs por hora. Respecto al flujo de aire, este entra por la parte delantera y sale por la parte trasera. Ver Figura 5.34



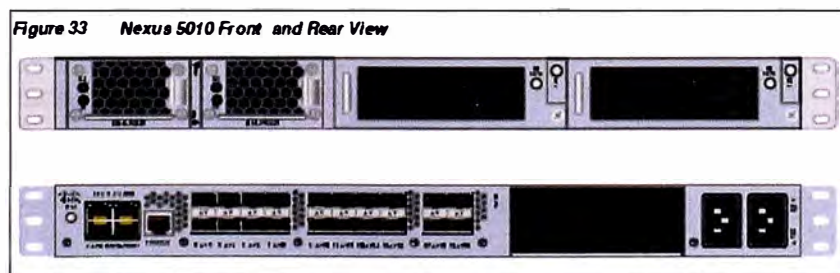
**Figura 5.34** Flujo de aire en Nexus 7010

### 5.5.3 Nexus 5010

- Hardware del proyecto

Nexus 5010 es un switch de 1 unidad de rack (1 RU), 10 Gigabit Ethernet, FCoE y Fibre Channel que provee más de 520 Gbps de capacidad con muy baja latencia. Este equipo tiene 20 puertos de 10 Gigabit Ethernet y puertos FCoE SPF+. Ver Figura 5.35

El switch tiene un puerto de consola serial y un puerto de gestión fuera de banda de 10/100/1000 Mbps. El switch es energizado con redundancia 1+1, con fuentes de poder "hot-pluggable" y redundancia 1+1. Los módulos de ventilación "hot-pluggable" proveen un sistema de enfriamiento confiable, el flujo de ventilación es de adelante hacia atrás.



**Figura 5.35** Equipos Nexus 5010

### 5.5.4 Nexus 2248

- Hardware del proyecto

Nexus 2248 es un extensión de fabric de 1 unidad de rack (1 RU) que soporta hasta 48 puertos 1000-TX para hosts y 4 puertos 10GB SFP+ para conexión a la red. El equipo Nexus 2248 es configurado y administrado completamente por su equipo superior Nexus 5010. El equipo N2K descarga la imagen de software desde el switch Nexus 5K en la



misma forma que un módulo descargaría el software desde la supervisora en un chassis modular.

Como se muestra en la Figura 5.36, las fuentes de poder y los ventiladores están en la parte frontal, los 48 puertos 100/1000 BASE-T y 4 puertos 10GE en la parte trasera.

Sus 2 fuentes de poder de 400W pueden ser intercambiadas en caliente.

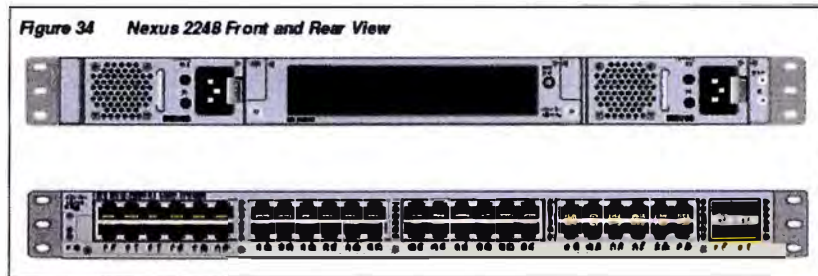


Figura 5.36 Equipos Nexus 2248

### 5.5.5 Switch Catalyst 6509

- Hardware del proyecto

Cada equipo Nexus 7010 del proyecto contiene la siguiente distribución de tarjetas:

Slot	Module	Comment
1	WS-X6704-10GE	Cat6500 4-port 10 Gigabit Ethernet Module
2	WS-6724-SFP	Catalyst 6500 24-port GigE Mod
3	WS-6748-GE-TX	Cat6500 48-port 10/100/1000 GE Mod
4	Empty	Empty
5	VS-S720-10G-3C	Cat 6500 Supervisor 7200 with MSFC3 PFC3C
6	Empty	Empty
7	Empty	Empty
8	ACE20-MOD-K9	Application Control Engine 20 Hardware
9	WS-SVC-FWM-1-K9	Firewall blade

Se usarán 4 conectores XENPAK-10GB-LR+, 6 conectores GLC-LH-SM y 1 conector X2-10GB-SR por cada Catalyst 6509. Ver Figura 5.37



Figura 5.37 Chassis del equipo Cisco 6509



## Chassis

Flujo aire de lado a lado con 8 módulos de slots horizontales accesibles desde la parte central.

Diseñado para confiabilidad y máxima disponibilidad, todas las interfaces, las supervisoras y las fuentes de poder redundantes son accesibles por la parte frontal

### - Módulo 10 Gigabit Ethernet

El módulo WS-X6704-10GE brindará los enlaces 10GB. Este provee cuatros puertos Ethernet dedicados de 10GB, y soporta una variedad de XENPAK ópticos. Ver Figura 5.38



**Figura 5.38** Tarjeta de puertos 10GE para el switch 6509

### Módulo Gigabit Ethernet

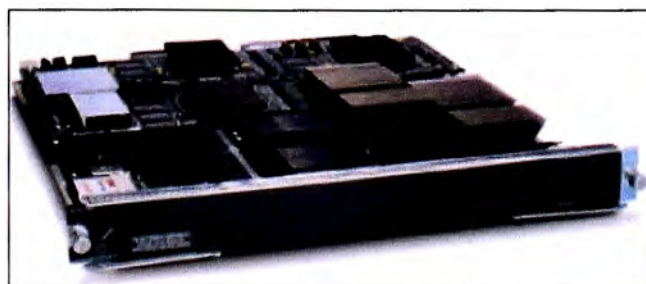
El módulo WS-X6724-SFP provee 24 puertos Gigabit Ethernet ópticos (SFP). El conector SFP debe ser seleccionado de acuerdo a los requerimientos de la distancia y el enlace.

## 5.5.6 Módulo de Firewall (FWSM)

El módulo de firewall para los switches Catalyst 6500 es un firewall de inspección de estados de alta performance con motor de inspección de aplicaciones y protocolos. Este provee un throughput de 5.5 Gbps, 100 mil nuevas conexiones por segundo, un millón de conexiones concurrentes o 256 mil traslaciones NAT, hasta 80 mil entradas de control de acceso (acl), hasta 1000 vlans en total por módulo. Hasta 4 FWSM pueden ser instalados en un solo chassis, proveyendo una escalabilidad de hasta 20Gbps por chassis.

Además de proteger el perímetro de la red corporativa de ataques, el FWSM instalado en el chassis del switch Cisco 6500 o Router Cisco 7600, inspecciona los flujos de tráfico y previene a usuarios no autorizados de acceder a redes particulares, redes de trabajo o redes LAN en la red corporativa.

La integración de redes inteligentes permite al FWSM proveer una mejor inversión en protección y un más bajo costo total de compra. Cualquier puerto físico en el switch puede ser configurado para operar con la protección y políticas de firewall, permitiendo un fácil despliegue sin cableado y configuración adicional, y provee seguridad de firewall dentro de la infraestructura de red. Ver Figura 5.39



**Figura 5.39** Tarjeta de firewall para switches 6509

### 5.5.7 Módulo Balanceador (Application Control Engine 20)

El módulo ACE20 para switches 6500 o router 6500 es un motor de control aplicaciones. Estos módulos incrementan la disponibilidad, aceleración y seguridad de las aplicaciones del data center.

El módulo Cisco ACE permite:

Incrementa disponibilidad de aplicaciones

Acelera la performance de las aplicaciones

Protege las aplicaciones del data center y críticas del negocio

Facilita la consolidación del data center a través del uso de pocos servidores, balanceadores de carga y firewalls.

El módulo ACE consigue estos objetivos a través de su amplio conjunto de balanceo de carga inteligente de Capa 4 y tecnologías de content-switching de capa 7 integrado con capacidades de aceleración y seguridad. Un elemento de diseño diferenciado de Cisco con las otras soluciones del mercado, es su habilidad para tener una arquitectura virtualizada y capacidad de administración basada en roles que racionalizan y reducen los costos de operación envueltos en despliegue, escalamiento, aceleración y protección de aplicaciones. Ver Figura 5.40



**Figura 5.40** Tarjeta de balanceo de carga - ACE

Sus características principales son las siguientes:

**Performance.** Hasta 4 Gbps por módulo de servicio ( hasta 8 Gbps y 16 Gbps con un upgrade de licencia)

Hasta 4 ACE por chassis y 350 mil syslogs por segundo

**Vlans.** Hasta 4000 vlans (total de vlans de cliente y de servidores)

**SSL.** Hasta 3.3 Gbps de tráfico y entre 1000 a 15000 TPS según licencia

**Contextos.** Hasta 250 contextos de acuerdo a la licencia

### 5.5.8 Cisco IPS 4270 (Intrusion Prevention System)

Hoy en día, la continuidad de los negocios recae en una prevención de intrusos en la red para detener ataques maliciosos, y abuso de aplicaciones antes que ellas afecten los datos y recursos de red. Además estos requerimientos normalmente son solicitados por la empresas certificadoras de calidad (ISO).

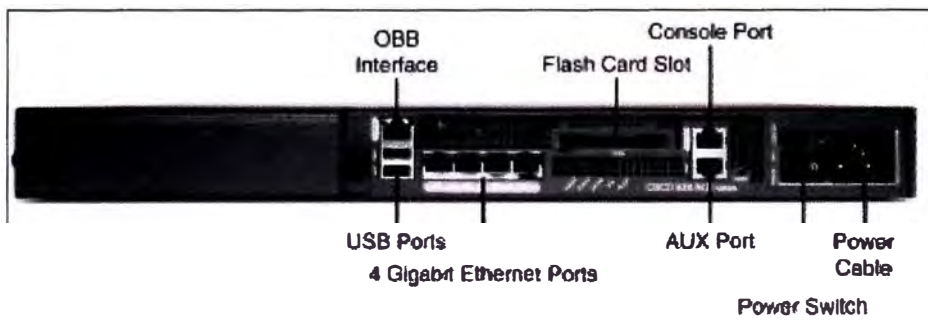
Cisco IPS 4200 detectan, clasifican y detienen tráfico malicioso mientras entrega continuidad y protección a una red asegurada. Ver Figura 5.41



*Figura 5.41* Equipo IPS 4270

### 5.5.9 Cisco ASA 5520 (Adaptive Security Appliance)

Cisco ASA 5520 entrega Servicios de seguridad con alta disponibilidad activo/activo y conectividad 1GB Ethernet para redes empresariales de tamaño mediano en un equipo de alta performance y modular. Con 4 interfaces Gigabit Ethernet y soporte de hasta 100 Vlans, puede desplegar fácilmente múltiples zonas en la red. Ver Figura 5.42



*Figura 5.42* Parte posterior del firewall ASA 5520

#### Performance

La avanzada seguridad en capa de aplicación y seguridad de contenidos proveído por Cisco ASA 5520 puede ser extendido con el despliegue del uso de la prevención de intrusos y capacidad de mitigación de gusanos del módulo AIP SSM, o la protección contra malware del módulo CSC SSM. Usando las capacidades de contextos de seguridad del equipo, el negocio puede desplegar hasta 20 firewall virtuales para tener políticas de control de seguridad en nivel de departamentos. Esta virtualización fortalece la seguridad y reduce los costos de administración y soporte mientras consolida elementos múltiples de seguridad en un solo equipo.

Su performance en número es la siguiente:

Hasta de 450 Mbps de capacidad de firewall y 225 Mbps de capacidad de VPN.

Hasta 280 mil sesiones concurrentes y 750 peers de VPN IPsec

Hasta 150 vlans

## 5.6 Programa de Implementación

### Planificación de la solución

En esta etapa el área de Planificación presentará la propuesta de diseño que busca cumplir todos los requerimientos de un centro de servicios convergente y altamente disponible

### Gestión de Compra

Se elegirá al proveedor que cumpla de la mejor manera con los requerimientos del proyecto y será a quién se le adjudicará el proyecto. El cronograma del proyecto es:

Actividades	Mes 1-4				Mes 5				Mes 6				Mes 7			
	Mes1	Mes2	Mes3	Mes4	Sem1	Sem2	Sem3	Sem4	Sem1	Sem2	Sem3	Sem4	Sem1	Sem2	Sem3	Sem4
Planificación de la solución	■															
Gestión de Compra	■															
Entrega de Equipos		■	■	■												
Site Survey		■														
Entrega Recursos de Energía		■	■	■												
Entrega Recursos de Tx (fibra óptica)		■	■	■												
Elaboración Documentos Diseño alto y bajo nivel		■	■	■												
Elaboración Documento Plan de Implementación					■	■	■	■								
Instalación de Equipos					■	■	■	■								
Energización de Equipos						■	■	■								
Revisión de equipamiento							■	■								
Tendido de cableados								■	■	■						
Configuración de equipos									■	■	■	■				
Integración con red en producción											■	■				
Pruebas de funcionalidad y alta disponibilidad													■	■		
Migración de servicios													■	■	■	■
Transferencia de conocimientos																■
Entrega a Operaciones																■

### Entrega de Equipos

Luego de la gestión de la Orden de Compra, el proveedor deberá entregar el equipamiento hasta en los 90 días posteriores a la misma.

### Site Survey

Se visitará en forma previa a la instalación de los equipos en los nodos elegidos con el fin de obtener la siguiente información:

Ubicación de espacio requerido para instalación de los bastidores que contendrán a los equipos

Revisión de la ruta para el tendido de cableado de energía hacia los bastidores de energía y revisión de la ruta de fibra óptica hacia los ODFs del nodo. Sino existieran se deberán realizar los trabajos para la instalación de canaletas.

### Entrega de Recursos de Energía

Realizar la solicitud de llaves de energía para los nuevos equipos del proyecto. Luego de recibir la asignación de llaves, se deberá ir al nodo para revisar que todo esté conforme para el momento de la instalación.

### **Entrega de Recursos de Tx**

Realizar la solicitud de los perfiles de fibra para las interconexiones inter-nodales. Luego de tener la asignación de perfiles, se deberá probar la conectividad de punto a punto con equipos especiales de medición de potencia. Es necesario que los valores de potencia obtenidos satisfagan los valores que no demuestren atenuación en el medio.

### **Elaboración de Documentos de Diseño de Alto y Bajo Nivel**

Se deberán obtener dos documentos:

High Level Design (HLD): se elaborará el documento de alto nivel, donde se plantearán a grandes rasgos todos los requerimientos del proyectos y la forma de cómo se atenderán.

Low Level Design (LLD): se elaborará el documento de bajo nivel, donde se explicará a detalle cómo se atenderán los requerimientos del proyecto. Es importante un completo levantamiento de información de la red en producción para su posterior integración a la red de producción.

### **Elaboración de Documentos del Plan de Implementación**

El entregable de esta fase deberá ser la NIP (Network Implementation Plan), el cual es el documento donde se detallan todas las configuraciones a desplegar sobre los equipos de red, así como el procedimiento y plan para realizar la configuración, integración y migración de servicios.

### **Instalación de Equipos**

Se realizará el traslado seguro de los equipos e instalación en los bastidores de ambos nodos.

### **Energización de Equipos**

Se realizará el tendido de cableado de energía así como la energización de los equipos en ventanas de mantenimiento.

### **Revisión de Equipamiento**

Luego de energizado los equipos, se revisará que los equipos no tengan ningún problema a nivel de hardware y software. Si hubiera algún problema se procederá a realizar el RMA (cambio de equipo) con el proveedor.

### **Tendido de cableados**

Se realizará la instalación de patch-panels para cableado utp y de fibra óptica, así como el tendido de cableados según diseño de la solución. Es importante el tendido de fibras hacia los ODF así como la prueba de conectividad entre los nodos remotos. Será necesari-



rio tener personal en cada nodo para hacer pruebas de conectividad física (loops) con los ODF.

### **Configuración de equipos**

Se realizarán las configuraciones de los equipos basados en el documento NIP entregado anteriormente.

### **Integración con la red de producción**

Luego de tener los equipos del proyecto con las configuraciones desplegadas, se programará una ventana de mantenimiento donde se realizará la integración de los equipos con la red de producción.

### **Pruebas de funcionalidad y alta disponibilidad**

Ya integrado los equipos a la red, se deberá probar las diversas funcionalidades ofrecidas por el centro de servicios, sea firewall, balanceo de carga, IPS; así como la alta disponibilidad y los mínimos tiempos de convergencia requeridos.

### **Migración de Servicios**

Luego de haber probado la nueva infraestructura y haber corrido un ATP (plan de pruebas de aceptación por el cliente), se procederán a migrar los servicios que se encuentran bajo el antiguo centro de servicios, así como la puesta en producción de nuevos servicios. Se requerirá que todos estos trabajos se realicen en una ventana de mantenimiento para minimizar los riesgos de afectación de usuarios finales. Se coordinará con el cliente un plan de ventanas de mantenimientos, para que el cliente solicite y/o anuncie los trabajos a la empresa reguladora y sus usuarios.

### **Transferencia de conocimientos**

Se realizarán charlas sobre la nueva tecnología y la forma de funcionamiento del proyecto al equipo de operaciones. Junto con los entregables del proyecto, se dejarán manuales que servirán de modelo para la provisión de nuevos servicios. Luego de puesto en producción, el cliente dispondrá de un servicio de Helpdesk para absolver cualquier consulta sobre el equipamiento entregado.

### **Entrega a Operaciones**

Se realizará la entrega de información del proyecto y se formalizará la recepción del proyecto por parte del equipo de operaciones.

## CAPITULO VI

### COSTOS DEL PROYECTO

#### 6.1 Equipamiento

Los costos del proyecto incluyen todo el equipamiento necesario para la implementación del centro de servicios en ambos nodos. El detalle del equipo (BOM) para todos los bloques considerados en el diseño se detallará en la Tabla 6.1

*Tabla 6.1 – Detalle de equipos adquiridos por el cliente*

<b>NEXUS 7010 - BLOQUE CORE Y AGREGACIÓN</b>		
<b>Producto</b>	<b>Descripcion</b>	<b>Cantidad</b>
N7K-C7010-BUN	Nexus 7010 Bundle (Chassis,SUP1,(3)FAB1,(2)AC-6KW PSU)	4
N7KS1K9-50	Cisco NX-OS Release 5.0	4
DCNM-N7K-K9	DCNM LAN Enterprise License for one Nexus 7000 Chassis	4
N7K-ADV1K9	Nexus 7000 Advanced LAN Enterprise License (VDC, CTS ONLY)	4
N7K-LAN1K9	Nexus 7000 LAN Enterprise License (L3 protocols)	4
N7K-TRS-P1	Limited Time Promotion for Transport Services license (OTV)	4
N7K-M108X2-12L	Nexus 7000 - 8 Port 10GbE with XL option (req. X2)	4
X2-10GB-ER	10GBASE-ER X2 Module	4
X2-10GB-LR	10GBASE-LR X2 Module	28
N7K-M108X2-12L	Nexus 7000 - 8 Port 10GbE with XL option (req. X2)	4
X2-10GB-ER	10GBASE-ER X2 Module	4
X2-10GB-LR	10GBASE-LR X2 Module	28
N7K-M148GS-11L	Nexus 7000 - 48 Port GE Module with XL Option (req. SFP)	4
SFP-GE-L	1000BASE-LX/LH SFP (DOM)	48
SFP-GE-S	1000BASE-SX SFP (DOM)	48
N7K-M108X2-12L=	Nexus 7000 - 8 Port 10GbE with XL option (req. X2)	4
X2-10GB-LR	10GBASE-LR X2 Module	16
SFP-GE-T	1000BASE-T SFP	4
SFP-GE-T	1000BASE-T SFP	4
N7K-CPF-2GB	Nexus Compact Flash Memory 2GB (Expansion Flash - Slot 0)	4
N7K-SUP1	Nexus 7000 - Supervisor, Includes External 8GB Log Flash	4
N7K-CPF-2GB	Nexus Compact Flash Memory 2GB (Expansion Flash - Slot 0)	4
CAB-AC-2500W-US1	Power Cord, 250Vac 16A, straight blade NEMA 6-20 plug, US	16
N7K-C7010-AFLT	Nexus 7010 Air Filter	4
N7K-TRS1K9	Nexus 7000 Transport Services License (OTV)	4
N7K-SUP1-BUN	Nexus 7000 - Supervisor 1, Includes External 8GB Flash	4
N7K-C7010-FAB1-BUN	Nexus 7000 - 10 Slot Chassis - 46Gbps/Slot Fabric Module	12
N7K-AC-6.0KW	Nexus 7000 - 6.0KW AC Power Supply Module	8
N7K-C7010-FD-MB	Nexus 7010 Front Door Kit	4

**ASR 9006 - BLOQUE WAN**

Producto	Descripcion	Cantidad
ASR-9006-DC	ASR-9006 DC Chassis	2
ASR-9006-FAN	ASR-9006 Fan Tray	4
A9K-2KW-DC	2kW DC Power Module	6
A9K-RSP-4G	ASR9K Fabric, Controller 4G memory	4
A9K-K9-03.09	Cisco IOS XR IP/MPLS Core Software 3DES	2
A9K-4T-B	4-Port 10GE Line Card, Requires XFPs	2
XFP-10GLR-OC192SR	Multirate XFP module for 10GBASE-LR and OC192 SR-1	8
A9K-4T-L	4-Port 10GE Low Queue Line Card, Requires XFPs	2
XFP-10GER-192IR+	Cisco Multirate 10GBASE-ER and OC-192/STM-64 IR-2 XFP Module	4
XFP-10GLR-OC192SR	Multirate XFP module for 10GBASE-LR and OC192 SR-1	4
A9K-AIP-LIC-B	L3VPN Line Card License, for use with -B or -L Line Cards	2
A9K-LC-FILR	ASR-9K Line Card Filler	4

**NEXUS 5010 - BLOQUE DE ACCESO**

Producto	Descripcion	Cantidad
N5010P-N2248TP-BE	Nexus 5010/4x2248TP/20xSR Bundle	4
CAB-N5K6A-NA	Power Cord, 200/240V 6A North America	8
CAB-N5K6A-NA	Power Cord, 200/240V 6A North America	32
N2K-C2248TP-BUN	Nexus 2248TP for N5K/N2K Bundle	16
N5K-C5010P-BUN-E	Nexus 5010P in N5010P-N2K Bundle	4
N5010-ACC-KIT	Nexus 5010 Accessory Kit, Option	4
N5K-M1-BLNK	N5000 1000 Series Expansion Module Blank	4
N5K-PAC-550W	Nexus 5010 PSU module, 100-240VAC 550W	8
N5KUK9-421N1.1	Nexus 5000 Base OS Software Rel 4.2(1)N1(1)	4
SFP-10G-SR	10GBASE-SR SFP Module	80
SFP-10G-LR=	10GBASE-LR SFP Module	8

**IPS 4270 - BLOQUE DE SERVICIO**

Producto	Descripcion	Cantidad
IPS4270-2X10GE-K9	IPS 4270-20 bundled with 2-port 10GE NIC	4
CAB-US515P-C19-US	NEMA 5-15 to IEC-C19 13ft US	8
IPS-SW-7.0	Cisco IPS software version 7.0	4
IPS-4GE-BP-INT	4-Port Copper NIC with bypass for the IPS 4260 and 4270	4
IPS-2X10GE-SR-INC	2X10GE interface card included in 10GE 4270 bundle	4

**ASA5520 - BLOQUE DE SERVICIO**

Producto	Descripcion	Cantidad
ASA5520-BUN-K9	ASA 5520 Appliance with SW, HA, 4GE+1FE, 3DES/AES	2
CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	2
SF-ASA-8.3-K8	ASA 5500 Series Software v8.3	2
ASA-VPN-CLNT-K9	Cisco VPN Client Software (Windows, Solaris, Linux, Mac)	2
ASA5520-VPN-PL	ASA 5520 VPN Plus 750 IPsec User License (7.0 Only)	2
ASA5500-ENCR-K9	ASA 5500 Strong Encryption License (3DES/AES)	2
SSM-BLANK	ASA/IPS SSM Slot Cover	2
ASA-180W-PWR-AC	ASA 180W AC Power Supply	2
ASA-ANYCONN-CSD-K9	ASA 5500 AnyConnect Client + Cisco Security Desktop Software	2

**SWITCH 6509E - BLOQUE DE SERVICIO**

<b>Part Number</b>	<b>Part Description</b>	<b>Quantity</b>
VS-C6509E-S720-10G	Catalyst Chassis+Fan Tray+Sup720-10G; IP Base ONLY incl. VSS	4
SV33IBK9L-12233SXI	Cisco CAT6000-VSS720 IOS IP BASE SSH LAN ONLY	4
CF-ADAPTER-SP	SP adapter for SUP720 and SUP720-10G	4
MEM-C6K-CPTFL1GB	Catalyst 6500 Compact Flash Memory 1GB	4
X2-10GB-SR	10GBASE-SR X2 Module	4
WS-X6724-SFP	Catalyst 6500 24-port GigE Mod: fabric-enabled (Req. SFPs)	4
GLC-LH-SM	GE SFP, LC connector LH transceiver	21
WS-X6748-GE-TX	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45	8
PWR-6000-DC	6000W DC PS for CISCO7609/7609-S/13, Cat6506/09/13 chassis	8
WS-X6704-10GE=	Cat6500 4-port 10 Gigabit Ethernet Module (req. XENPAKs)	4
MEM-XCEF720-256M	Catalyst 6500 256MB DDR, xCEF720 (67xx interface, DFC3A)	4
WS-F6700-CFC	Catalyst 6500 Central Fwd Card for WS-X67xx modules	4
WS-F6K-XENBLNKCVR	Catalyst 6500 Xenpak Blank Covers for WS-X6704-10GE	16
XENPAK-10GB-LR+=	10GBASE-LR XENPAK Module with DOM support	16
WS-SVC-FWM-1-K9=	Firewall blade for 6500 and 7600, VFW License Separate	4
SC-SVC-FWM-4.0-K9	Firewall Module Software 4.0 for 6500 and 7600, 2 free VFW	4
FR-SVC-FWM-VC-T2	Catalyst 6500 and 7600 virtual FW licensing for 50 VF	4
SF-FWM-ASDM-6.1F	Device Manager for FWSM 4.0 for Catalyst 6500 and 7600	4
ACE20-MOD-K9=	Application Control Engine 20 Hardware	4
SC6K-A21-ACE	ACE A2(1) Software Release	4
ACE-04G-LIC	Application Control Engine (ACE) 4Gbps License	4
ACE-VIRT-050	Application Control Engine Virtualization 50 Contexts	4
VS-S720-10G-3C	Cat 6500 Supervisor 720 with 2 ports 10GbE and MSFC3 PFC3C	4
VS-F6K-MSFC3	Catalyst 6500 Multilayer Switch Feature Card (MSFC) III	4
VS-F6K-PFC3C	Catalyst 6500 Sup 720-10G Policy Feature Card 3C	4
VS-S720-10G	Catalyst 6500 Supervisor 720 with 2 10GbE ports	4
MEM-C6K-CPTFL1GB	Catalyst 6500 Compact Flash Memory 1GB	4
BF-S720-64MB-RP	Bootflash for SUP720-64MB-RP	4
MEM-XCEF720-256M	Catalyst 6500 256MB DDR, xCEF720 (67xx interface, DFC3A)	4
WS-F6700-CFC	Catalyst 6500 Central Fwd Card for WS-X67xx modules	4
SF-FWM-ASDM-6.1F	Device Manager for FWSM 4.0 for Catalyst 6500 and 7600	4
MEM-XCEF720-256M	Catalyst 6500 256MB DDR, xCEF720 (67xx interface, DFC3A)	4
WS-F6700-CFC	Catalyst 6500 Central Fwd Card for WS-X67xx modules	4
WS-C6509-E-FAN	Catalyst 6509-E Chassis Fan Tray	4

**6.2 Servicios****6.2.1 Servicios Cisco de Reemplazo**

Si hubiera alguna falla con algún equipamiento adquirido, este podrá ser reemplazado por uno nuevo. Este servicio es brindado hasta por 1 año luego de la compra.

El reemplazo de partes contemplado es 8x5xNBD. Esto significa que el cambio de partes se efectuará durante las 8 horas laborales del día, los 5 días a la semana y al día siguiente laborable.

### 6.2.2 Servicios Profesionales de Migración del Proveedor

Incluye los servicios profesionales del proveedor para realizar los trabajos de configuración y migración de los servicios. Se especificaron la migración de 8 servicios.

### 6.2.3 Servicios Avanzados Cisco

Incluye el soporte de Cisco para la elaboración de los documentos de diseño de bajo y alto nivel, así como el documento del plan de implementación. En este caso, también está incluido la migración de los 2 primeros servicios a la nueva infraestructura.

### 6.2.4 Training in Job

Incluye capacitación sobre la nueva tecnología a usar en el centro de servicios. Habrá una capacitación en fábrica y otra capacitación local.

### 6.2.5 AT-Proveedor-1

Incluye la asistencia técnica por parte del proveedor. Esta asistencia será por 1 año a partir de que los equipos entren en producción

## 6.3 Costos de inversión (CAPEX)

El CAPEX total considerado según se describe en la Tabla 6.1 será de \$2,650,309.00

Producto	Descripción	Precio
<b>Equipamiento</b>	Infraestructura de Red	\$1,972,309.00
<b>Servicios Cisco de Reemplazo</b>	Reemplazo de partes 8x5xNBD (01 año)	\$138,000.00
<b>Servicios Profesionales de Migración del Proveedor</b>	Servicios Profesionales Avanzados DEL PROVEEDOR para la migración de los Servicios Móviles	\$200,000.00
<b>Servicios Avanzados Cisco</b>	Servicios Profesionales Avanzados	\$200,000.00
<b>Training in Job</b>	Entrenamiento en Fábrica para 05 personas DCNI-2 y Entrenamiento Local para 05 personas MPLS	\$50,000.00
<b>AT-Proveedor-1</b>	Asistencia Técnica del Proveedor Anual 365x24x7 (01 año)	\$90,000.00
		<b>\$2,650,309.00</b>

**Tabla 6.2 – Costos de Inversión**



#### 6.4 Costos de operación (OPEX)

Es importante la renovación de “Servicios Cisco de Reemplazo” así como la “Asistencia Técnica” para la operación del centro de servicios.

Considerando esos puntos, el OPEX requerido será de \$228,000.00 según muestra la Tabla 6.2

Producto	Descripción	Precio
<b>Servicios Cisco de Reemplazo</b>	Reemplazo de partes 8x5xNBD (01 año)	\$138,000.00
<b>AT-Proveedor-1</b>	Asistencia Técnica del Proveedor Anual 365x24x7 (01 año)	\$90,000.00
		<b>\$228,000.00</b>

**Tabla 6.3 – Costos de Operación**

## CONCLUSIONES Y RECOMENDACIONES

1. Los Centro de Servicios serán ubicados en dos nodos de distinta ubicación geográfica, con el fin de brindar mayor redundancia a los servicios de la operadora móvil.
2. Como fase inicial los centros de servicios se conectarán al CORE MPLS de la operadora móvil, permitiendo la comunicación con las diferentes redes que brindan los servicios móviles. Posteriormente los centro de servicios se conectarán al core mpls de la red fija, con el fin de hacer sinergia con servicios de uso compartido.
3. Toda las interfaces troncales son de 10GE, lo cual permitirá entregar gran capacidad de forwarding y soportar los crecimientos como mínimo a un plazo de 5 años.
4. El diseño se ha hecho basado en bloques (WAN + Core/Agregación + Acceso + Servicios), lo cual permitirá su escalabilidad y fácil crecimiento.
5. La modularidad del Centro de Servicios permitirá ofrecer servicios de firewall, balanceo de carga e IPS según sea el requerimiento de los servicios.
6. El uso de nuevas funcionalidades tales como Fabric Extender (FEX) y Virtual Port-Channel (vPC) permitirá usar la capacidad de los enlaces al 100% sin tener enlaces “ociosos” ni la problemática que suelen traer Spanning-tree en las redes switcheadas.
7. El uso de switches Nexus 2K Fabric Extender como “Top of the Rack” permitirá tener un mayor orden en los cableados, gestión de equipamiento concentrada en los switches N5K y un rápido despliegue para crecimiento de la red.
8. Ambos Centro de Servicios estarán inter-conectados entre sí a través de un nueva funcionalidad llamada OTV, el cual permitirá ofrecer servicios redundantes geográficamente sin extender el dominio de broadcast entre nodos.
9. Se deberá gestionar con los proveedores de las diversas plataformas a adquirir, que no incluyan switches, firewall ni balanceadores de carga en sus soluciones, pues son servicios que ya serán ofrecidos centralizadamente por el centro de servicios.
10. Luego de implantar el nuevo Centro de Servicios, uno de los siguientes pasos será implantar la virtualización de servidores con el fin de disminuir el uso de espacio y energía que actualmente consumen la gran cantidad de servidores que se usan para las aplicaciones de red.

## BIBLIOGRAFIA

### [1] Libros Cisco

Implementing Cisco Data Center Networking Infraestructure 1 - Student Guide Volumen 1

Implementing Cisco Data Center Networking Infraestructure 1 - Student Guide Volumen 2

Implementing Cisco Data Center Networking Infraestructure 2 - Student Guide Volumen 1

Implementing Cisco Data Center Networking Infraestructure 2 - Student Guide Volumen 2

Designing Cisco Data Center Network Infrastructure - Student Guide Volumen 1

Designing Cisco Data Center Network Infrastructure - Student Guide Volumen 2

### [2] Página Web Cisco

[http://www.cisco.com/en/US/docs/solutions/Enterprise/Data\\_Center/DC\\_3\\_0/DC-3\\_0\\_IPInfra.html](http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_3_0/DC-3_0_IPInfra.html)

[http://www.cisco.com/en/US/netsol/ns743/networking\\_solutions\\_program\\_home.html](http://www.cisco.com/en/US/netsol/ns743/networking_solutions_program_home.html)

### [3] Página Web Juniper

<http://www.juniper.net/es/es/solutions/enterprise/data-center/simplify/#overview>

### [4] Página Web HP

<http://h17007.www1.hp.com/tw/en/solutions/datacenter/index.aspx>

## ACRÓNIMOS

<b>AC</b>	Alternating Current
<b>ACE</b>	Application Control Engine
<b>AIP</b>	Advanced Inspection and Prevention
<b>ASA</b>	Adaptive Security Appliances
<b>ASR</b>	Aggregation Services Routers
<b>ATP</b>	Acceptance Test Plan
<b>BGP</b>	Border Gateway Protocol
<b>BTU</b>	British Thermal Unit
<b>CAPEX</b>	Capital Expenditure
<b>CE</b>	Customer Edge
<b>CRS</b>	Carrier Routing System
<b>CSC</b>	Content Security and Control
<b>CMP</b>	Connectivity Management Processor
<b>DCI</b>	Data Center Interconnect
<b>DPI</b>	Deep Packet Inspection
<b>DoS</b>	Denial of Service
<b>EBGP</b>	External Border Gateway Protocol
<b>EGP</b>	External Gateway Protocol
<b>E2E</b>	End-to-End
<b>FCoE</b>	Fibre Channel over Ethernet
<b>FEX</b>	Fabric Extender Technology
<b>FWSM</b>	Firewall Service Module
<b>GE</b>	GigaEthernet
<b>GGSN</b>	Gateway GPRS Support Node
<b>HLD</b>	High Level Design

<b>HP</b>	Hewlett-Packard
<b>HSRP</b>	Hot Standby Router Protocol
<b>IDS</b>	Intrusion Detection System
<b>IMC</b>	Intelligent Management Center
<b>IPS</b>	Intrusion Prevention System
<b>IPv4</b>	Internet Protocol Version 4
<b>IPv6</b>	Internet Protocol Version 6
<b>IPSEC</b>	Internet Protocol Security
<b>IRF</b>	Intelligent Resilient Framework
<b>ISO</b>	International Organization for Standardization
<b>ISP</b>	Internet Service Provider
<b>KW</b>	Kilowatt
<b>LAN</b>	Local Area Network
<b>LLD</b>	Low level design
<b>MD5</b>	Message-Digest Algorithm 5
<b>MDS</b>	Multilayer Director Switch
<b>MDT</b>	Multicast Distribution Tree
<b>MMS</b>	Multimedia Messaging Service
<b>MPLS</b>	Multiprotocol Label Switching
<b>MST</b>	Multiple Spanning Tree
<b>NAS</b>	Network Attached Storage
<b>NAT</b>	Network Address Translation
<b>NBD</b>	Next-Business Day
<b>NX-OS</b>	Nexus Operation System
<b>NGN</b>	Next-Generation Network
<b>NIC</b>	Network interface controller
<b>NIP</b>	Network Implementation Plan
<b>NP</b>	Network Processor
<b>N5K</b>	Nexus 5548
<b>N7K</b>	Nexus 7009



<b>ODF</b>	Optical Distribution Frame
<b>OIR</b>	Online Insertion and Removal
<b>OPEX</b>	Operational Expenditure
<b>OSPF</b>	Open Shortest Path First
<b>OTV</b>	Overlay Transport Virtualization
<b>O&amp;M</b>	Operations y Maintenance
<b>PBX</b>	Private Branch Exchange
<b>PE</b>	Provider Edge
<b>POD</b>	Pool of devices on Demand
<b>QoS</b>	Quality of service
<b>RMA</b>	Return Material Authorization
<b>RSP</b>	Route Switch Processor
<b>RU</b>	Rack Unit
<b>SAN</b>	Storage Area Network
<b>SBC</b>	Session Border Controller
<b>SFP</b>	Small Form-Factor Pluggable
<b>SGSN</b>	Serving GPRS Support Node
<b>SMS</b>	Short Message Service
<b>SSL</b>	Secure Sockets Layer
<b>SSM</b>	Security Services Module
<b>STP</b>	Spanning Tree Protocol
<b>SVF</b>	Secure Virtual Framework
<b>SVI</b>	Switch Virtual Interface
<b>SW</b>	Switch
<b>TCO</b>	Total cost of ownership
<b>ToR</b>	Top of Rack
<b>TPS</b>	Transactions per second
<b>TX</b>	Transmisiones
<b>UCS</b>	Unified Computing System
<b>VDC</b>	Virtual device context

<b>VLAN</b>	Virtual LAN
<b>VM</b>	Virtual machine
<b>VPC</b>	Virtual Port-channel
<b>VPN</b>	Virtual Private Network
<b>VSS</b>	Virtual Switching System
<b>WAAS</b>	Wide Area Application Services
<b>WAN</b>	Wide Area Network