Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

DISEÑO DE ARQUITECTURA DE RED SDN / NFV PARA PROVEEDORES DE SERVICIOS

Carlos Daniel Alvarado Velásquez
Asesorado por el Ing. Christian Antonio Orellana López

Guatemala, febrero de 2020

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO DE ARQUITECTURA DE RED SDN / NFV PARA PROVEEDORES DE SERVICIOS

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

CARLOS DANIEL ALVARADO VELÁSQUEZ
ASESORADO POR ING. CHRISTIAN ANTONIO ORELLANA LÓPEZ

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO ELECTRÓNICO

GUATEMALA, FEBRERO DE 2020

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Inga. Aurelia Anabela Córdova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton De León Bran
VOCAL IV	Br. Christian Moisés de la Cruz Leal
VOCAL V	Br. Kevin Armando Cruz Lorente
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

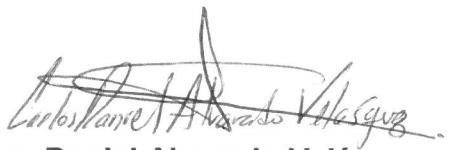
DECANO	Ing. Pedro Antonio Aguilar Polanco
EXAMINADOR	Ing. Marvin Marino Hernández
EXAMINADOR	Ing. Luis Eduardo Durán Córdova
EXAMINADOR	Ing. Helmut Federico Chicol Cabrera
SECRETARIA	Inga. Lesbia Magalí Herrera López

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

DISEÑO DE ARQUITECTURA DE RED SDN / NFV PARA PROVEEDORES DE SERVICIOS

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 7 de junio del 2017.



Carlos Daniel Alvarado Velásquez

Guatemala 12 de junio de 2019

Ingeniero
Julio Solares
Coordinador Área de Electrónica
Facultad de Ingenieria
Presente

Por este medio atentamente me dirijo a usted, para comunicarle que he revisado el trabajo de graduación del estudiante: **Carlos Daniel Alvarado Velásquez**, con número de carne: 200413454, con el título **"DISEÑO DE ARQUITECTURA DE RED SDN / NFV PARA PROVEEDORES DE SERVICIOS"**, luego de realizadas las revisiones correspondientes he encontrado que es satisfactorio, en virtud de lo anterior recomiendo su aprobación.

Sin otro particular me es grato suscribirme.

Atentamente,

Ing. Christian Orellana
Col.11989

Ing. Christian Orellana
Ingeniero Electrónico
Asesor de trabajo de graduación
Área de Ingeniería Mecánica Eléctrica

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

Guatemala, 12 de julio de 2019

Señor Director
Armando Alonso Rivera Carrillo
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC

Estimado Señor Director:

Por este medio me permito dar aprobación al Trabajo de Graduación titulado **DISEÑO DE ARQUITECTURA DE RED SDN / NFV PARA PROVEEDORES DE SERVICIOS**, desarrollado por el estudiante **Carlos Daniel Alvarado Velásquez**, ya que considero que cumple con los requisitos establecidos.

Sin otro particular, aprovecho la oportunidad para saludarlo.

Atentamente,

ID Y ENSEÑAD A TODOS

Ing. Julio Cesar Solares Peñate
Coordinador de Electrónica

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

REF. EIME 45. 2019.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto bueno del Coordinador de Área, al trabajo de Graduación de el estudiante: CARLOS DANIEL ALVARADO VELÁSQUEZ titulado: DISEÑO DE ARQUITECTURA DE RED SDN / NFV PARA PROVEEDORES DE SERVICIOS, procede a la autorización del mismo.

Ing. Armando Alonso Rivera Carrillo

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

GUATEMALA, 18 DE SEPTIEMBRE 2019.

Universidad de San Carlos
De Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.034-2020

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al trabajo de graduación titulado: **DISEÑO DE ARQUITECTURA DE RED SDN/NFV PARA PROVEEDORES DE SERVICIOS,** presentado por el estudiante universitario: **Carlos Daniel Alvarado Velásquez,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, se autoriza la impresión del mismo.

IMPRÍMASE.

Inga. Aurelia Anabela Cordova Estrada
Decana

Guatemala, febrero de 2020

AACE/asga
cc

ACTO QUE DEDICO A:

Dios	Por ser la fuente de la vida, sabiduría y haberme dado la fortaleza para cumplir mis metas.
Mis padres	Carlos Alvarado y Rosa Marina Velásquez, por todo su amor y apoyo incondicional a lo largo de mi vida.
Mi esposa	Evelyn Garrido, por ser una importante influencia en mi carrera personal y profesional, entre otras cosas.
Mi hijo	Carlos Alberto Alvarado, por ser una fuente de motivación para ser mejor persona y buen ejemplo en todo.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por permitirme ser parte de la cultura universitaria y fomentarme los valores para ser una persona de éxito y autosuficiente.
Facultad de Ingeniería	Por brindarme las facilidades de realizar mis estudios en un ambiente agradable.
Mis amigos	Por compartir sus conocimientos y su apoyo durante los años de carrera.
Mi asesor	Ing. Christian Orellana, por haberme guiado en la elaboración de este trabajo y compartir conmigo el amplio conocimiento que posee.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
bps	Bits por segundo
Kbps	Miles de bits por segundo
Gbps	Millones de bits por segundo
%	Porcentaje
Rx	Recepción de datos
5G	Red celular de generación 5
Tx	Transmisión de datos

GLOSARIO

ACL Lista de control de acceso, utilizada para limitar el acceso de direcciones IP o usuarios en un *firewall.*

Ancho de banda Cantidad de información o de datos que se puede enviar a través de una conexión de red en un periodo de tiempo.

AMS Sistema de mitigación de ataques, una solución híbrida de mitigación de ataques que integra detección y mitigación basada en la nube.

API Conjunto de funciones y procedimientos que cumplen una o muchas funciones con el fin de ser utilizadas por otro software.

Backbone Indica las principales conexiones troncales de Internet, compuesta de un gran número de enrutadores interconectados comerciales, gubernamentales, universitarios y entre países.

Big data Conjunto de datos o combinaciones de conjuntos de datos cuyo tamaño, complejidad y velocidad de crecimiento dificulta su captura, gestión, procesamiento o análisis mediante tecnologías y herramientas convencionales.

BGP	Protocolo de puerta de enlace de frontera, protocolo mediante el cual se intercambia información de enrutamiento entre sistemas autónomos.
BRAS	*Broadband remote access server*, parte de la red de núcleo en un proveedor de servicios de Internet que provee sesiones a los usuarios para accesar a la red de datos.
BSC	Elemento de una red de telefonía móvil que gestiona los recursos de asignación y liberación de frecuencias en estaciones base de la red GSM.
CAPEX	Capital de inversión, cubre la parte del despliegue que se deprecia con el tiempo en función de las amortizaciones tanto del equipamiento como de las instalaciones.
CloudNaaS	Plataforma en la nube utilizada en aplicaciones de alto nivel para almacenar datos.
CMTS	Sistema de terminación de cablemodems, equipo que se utiliza para proporcionar servicios de datos de alta velocidad.
Conmutador	Dispositivo digital lógico de interconexiones de equipos que opera en la capa de enlace del modelo OSI, su función es interconectar dos o más *host* a través de la red de datos.

CPE	Equipo local del cliente, equipo utilizado para originar, encaminar o terminar una comunicación.
Data center	Centro de datos, construcción de gran tamaño que alberga los equipos electrónicos necesarios para mantener una rede computadores.
Dirección IP	Identificador numérico de 32 bits para un equipo conectado en una red IP.
Dirección MAC	Identificador numérico de 48 bits para la tarjeta de red de un equipo conectado en una red IP.
DoD/DDoS	Ataque de negación de servicio distribuido, el cual genera un gran flujo de información desde varios puntos de conexión hacia un mismo punto de destino.
Docker	Software utilizado para crear contenedores en los servidores para implementar aplicaciones de forma independiente.
DSLAM	Multiplexor de acceso de línea de abonado digital, proporciona a los suscriptores el acceso a los servicios DSL sobre cable de par trenzado de cobre.
DWDM	Multiplexado denso por división en longitudes de onda, es una técnica de transmisión de señales a través de fibra óptica usando la banda C (1550nm).

Enrutador	Dispositivo que permite interconectar equipos que operen en la capa de red del modelo OSI.
Enrutador de borde	Es un enrutador que se comunica con una red de modo de transferencia asíncrona (ATM).
Ethernet	Estándar de redes de área local para computadores que define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo ISI.
Firewall	Es un dispositivo que permite limitar, cifrar o descifrar el tráfico entre los diferentes ámbitos de una red de datos sobre la base de un conjunto de normas y otros criterios.
GPON	Red óptica pasiva con capacidad de gigabit, es una tecnología de acceso que utiliza fibra óptica para llegar hasta el suscriptor.
GRE	*Generic Routing Encapsultaion,* es un protocolo para el establecimiento de túneles a través de Internet.
Guest	Define al sistema operativo ubicado en la máquina virtual, dentro de un ambiente virtualizado proporcionado por un *host.*
Hardware	Conjunto de elementos físicos o materiales que constituyen un sistema informático.

HFC	Híbrido de fibra coaxial, define una red de fibra óptica que incorpora tanto fibra óptica como cable coaxial para crear una red de banda ancha.
Host	Nombre que recibe un equipo conectado a una red de datos que provee y utiliza servicios de ella.
IBGP	Protocolo de puerta de enlace de frontera interno, se encarga de intercambiar información de encaminamiento entre sistemas autónomos.
Internet	Es el conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP.
IP/MPLS	Conmutación de etiquetas multiprotocolo, opera entre la capa de enlace de datos y la capa de red del modelo OSI para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.
ISP	Proveedor de servicios de Internet, es la empresa que brinda conexiones a Internet a sus clientes a través de diferentes tecnologías.
JAVA	Lenguaje de programación orientado a objetos.
LAN	Red de área local que abarca un área reducida a una casa, un departamento o un edificio.

Linux	Sistema operativo libre tipo Unix, multiplataforma, multiusuario y multitarea.
Máquina virtual	Software que simula un sistema de computación y con el cual pueden ejecutarse programas como si fuese una computadora real.
MSAN	Nodo de acceso multiservicio, es un dispositivo que permite integrar los servicios de telefonía y de banda ancha en un solo equipo.
Módem	Acrónimo para modulador y demodulador, el cual convierte señales digitales en analógicas y viceversa.
Modelo OSI	Sistema de interconexión abierta, el cual es utilizado como modelo de referencia para los protocolos implementados en redes de datos.
Nodo	Dispositivo que se encuentra conectado a la red de datos con capacidad de poder comunicarse con los diferentes dispositivos que se encuentran en la misma.
Nube	Es un paradigma que permite ofrecer servicios de computación a través de una red de datos, que usualmente es Internet.
Nube privada	Ofrece un servicio de computación dedicado a una solo organización.

ONOS	Sistema operativo abierto para redes diseñado como controlador para redes SDN.
OPEX	*Operational expenditures*, es el costo permanente para el funcionamiento de un producto, negocio o sistema.
Paquete de datos	Es cada uno de los bloques en que se divide la información para enviar en el nivel de red.
Peering	Es la interconexión voluntaria de redes de Internet administrativamente independientes con el fin de intercambiar tráfico entre los usuarios de cada red.
QoS	Calidad de servicio, es el rendimiento promedio de una red de telefonía o de computadoras, particularmente el rendimiento visto por los usuarios de la red.
Redes ATM	Tecnología de transmisión a través de una red sin tener que ocupar fragmentos específicos de tiempo en la alineación de paquetes.
Servidor	Es una combinación de hardware y software que permite el acceso remoto a herramientas o información que generalmente residen en una red de dispositivos.

Segment routing	Es una variante de encaminamiento donde un nodo de entrada prepara una cabecera de paquetes que contengan una lista de segmentos, que son instrucciones que se ejecutan en nodos posteriores de la red.
TCP	Protocolo de control de transmisión, utilizado para asegurar la transmisión en redes IP.
Telemetría	Tecnología que permite la medición remota de magnitudes físicas y el posterior envío de la información hacia el operador del sistema.
Virtualización	Es la creación a través de software de una versión virtual de algún recurso tecnológico.
VPN	Red privada virtual, es una tecnología de red de computadoras que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet.
WAN	Es una red de computadoras que une varias redes locales.
Wi-Fi	Tecnología que permite la interconexión inalámbrica de dispositivos electrónicos.

RESUMEN

En la actualidad se está atravesando por una evolución de los modelos estáticos para las redes de telecomunicaciones que implica un cambio a modelos virtualizados para cubrir las necesidades de grandes empresas de telecomunicaciones y ganar mercado optimizando costos y automatizando servicios.

Sin embargo, esta evolución trae consigo la necesidad de adoptar e implementar nuevas tecnologías como SDN y NFV a los modelos para gestionar y administrar las redes de datos de los operadores, por lo que las siguientes preguntas son válidas: ¿cuál es el primer paso para adoptar estas nuevas tecnologías? Y ¿cuáles son las consideraciones a tomar en cuenta?

Este documento de graduación hace un análisis a fondo de las respuestas a estas preguntas, evaluando los factores técnicos para el diseño, control y operación, para que exista una visibilidad completa de las redes del futuro y cómo puede aplicarse este cambio para que la transición de tecnologías sea más simple.

OBJETIVOS

General

Elaborar una propuesta técnica de arquitectura de red utilizando las tecnologías SDN y NFV en redes de datos de proveedores de servicios.

Específicos

1. Dar a conocer los fundamentos básicos para redes SDN y NFV de datos de proveedores de servicio.

2. Presentar las arquitecturas y modelos de control para redes de datos SDN y NFV.

3. Dar a conocer los conceptos de virtualización y su aplicación para redes de datos.

4. Proponer una arquitectura de red moderna, robusta y escalable utilizando SDN y NFV para redes de datos de proveedores de servicio.

INTRODUCCIÓN

La presente investigación se enfoca en hacer la propuesta de una arquitectura SDN / NFV para una red moderna de proveedores de servicio, la estructura del documento se presenta de la siguiente manera:

- Capítulo 1: se dan a conocer los fundamentos básicos de arquitecturas de redes tradicionales en proveedores de servicio, incluyendo el modelo jerárquico de capas, estructura de nodos, así como los conceptos de SDN y NFV, con sus elementos principales.
- Capítulo 2: dar a conocer las distintas arquitecturas y modelos de control que se utilizan en SDN y NFV, así como los elementos de aplicación que se automatizan al integrar esta tecnología.
- Capítulo 3: dar a conocer los elementos básicos de virtualización, así como los esquemas y beneficios que se obtienen al virtualizar los componentes de una red de datos en proveedores de servicio.
- Capítulo 4: planteamiento de una propuesta técnica para SDN / NFV, de forma que puedan ser analizados los aspectos importantes de una implementación, así como un caso de uso para ambas tecnologías con el fin de analizar costos y alcances.

1. SDN: ANTECEDENTES Y MOTIVADORES

Las tecnologías de redes en proveedores de servicios que permiten diseñar, desarrollar, implementar y operar redes complejas modernas incluyen especialmente redes definidas por software (SDN) y virtualización de funciones de red (NFV). Antes de entrar en los detalles de estas tecnologías, es necesaria una visión general del entorno de red actual y los desafíos que trae.

Este capítulo ofrece una visión de los elementos clave de la creación de redes modernas para un proveedor de servicios de Internet, se inicia con la descripción de alto nivel de lo que se considera el típico ecosistema de redes y a los desafíos que se enfrenta. A continuación se examina a detalle el enfoque de las redes definidas por software (SDN), su arquitectura, sus características y estándares relacionados.

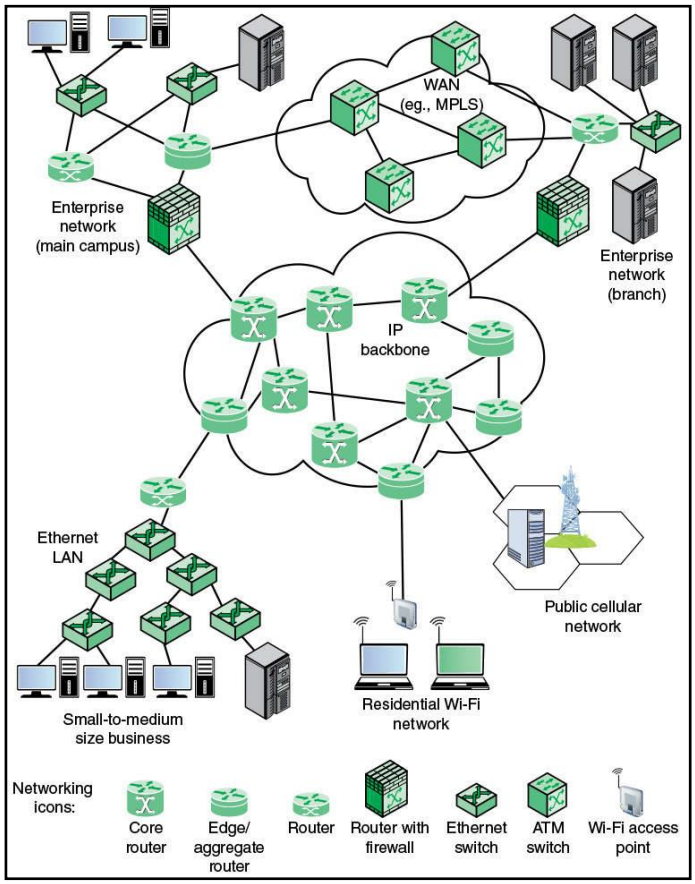
1.1. Arquitectura de red actual

En la figura 1 se ilustran los elementos típicos de comunicaciones que se utilizan en una arquitectura de red, donde:

- En el centro se encuentra una red IP núcleo, que representa una parte de Internet o una red IP de un proveedor de servicios, normalmente, la columna vertebral se compone de enrutadores de alto rendimiento, denominados enrutadores de *backbone*, interconectados con enlaces ópticos de alto volumen, los enlaces ópticos a menudo hacen uso de lo que se conoce como multiplexación compacta por división de longitudes

de onda (DWDM), de manera que cada enlace tiene múltiples canales lógicos que ocupan diferente porciones del ancho de banda óptico.

Figura 1. **Arquitectura de red de proveedor de servicios**



Fuente: Foundations of Modern Networking. *SDN, NFV, QoE, IoT, and Cloud.* Chapter 1. Consulta: marzo de 2019.

- En la frontera de la red de acceso y la de núcleo IP se encuentran enrutadores que proporcionan conectividad a redes externas y usuarios, a estos enrutadores se les llama enrutadores de borde o enrutadores de agregación, la cantidad de los mismos dependerá y variará según cada proveedor de servicios, según las ubicaciones de los nodos, del tamaño

del país al que se intenta dar cobertura y de la cantidad de suscriptores que haya, los enrutadores de agregación también se utilizan dentro de una red empresarial para conectar varios enrutadores y conmutadores de acceso a recursos externos, como un Backbone IP o una WAN de alta velocidad.

- Las velocidades de manejo según el grupo de evaluaciones de ancho de banda Ethernet [XI11] del IEEE indica que para el año 2020 los requerimientos de los enrutadores de agregación estarán en el rango de 200Gbps a 400Gbps por enlace óptico y para los enrutadores principales o de *backbone* estarán en el rango de 400Gbps a 1Tbps por enlace óptico.

- La parte superior representa un enlace de datos a nivel entre dos grandes empresas, utilizando la infraestructura de un proveedor de servicios, con dos secciones de la red conectadas a través de una WAN privada de alta velocidad, con conmutadores interconectados con enlaces ópticos utilizando una red IP/MPLS, los activos empresariales están conectados y protegidos de un Backbone IP o de Internet a través de enrutadores con capacidad de *firewall.*

- La parte inferior izquierda representa un diseño para una pequeña o mediana empresa, donde la conexión a Internet se hace a través de enrutadores y los clientes empresariales se conectan con enlaces dedicados de alta velocidad hacia la red de acceso y agregación del proveedor de servicios.

- La porción inferior también muestra cómo se conectan los usuarios residenciales a un proveedor de servicios de Internet (ISP) a través de una conexión de abonado, como por ejemplo la tecnologías xDSL o HFC,

que proporcionan un enlace de alta velocidad a través de líneas telefónicas que requieren módems especiales, y una instalación de televisión por cable, que requiere un módem por cable, o una conexión inalámbrica.

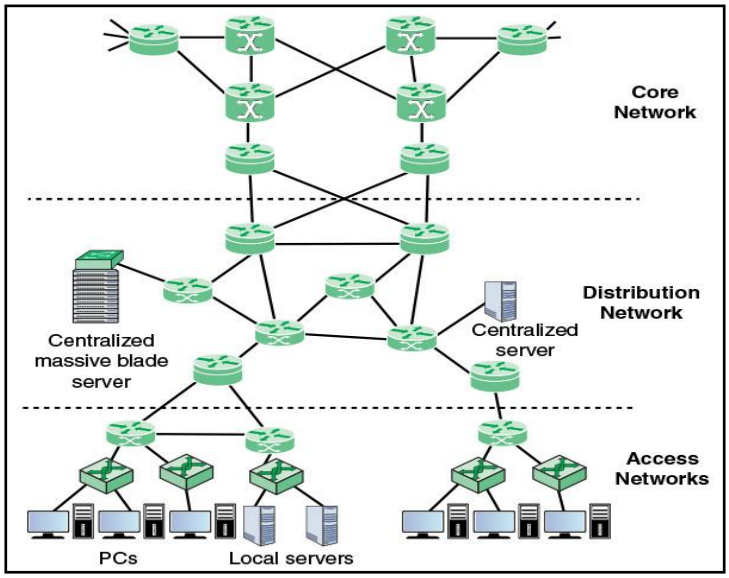
- Por último, se muestran cómo se conectan los usuarios de la red móvil, con dispositivos como los teléfonos inteligentes y las tabletas, estos regularmente pueden conectarse a Internet a través de la red pública de telefonía móvil, que tiene una conexión de alta velocidad, típicamente óptica, hacia Internet.

1.1.1. Una típica arquitectura de red jerárquica

En la figura 2 se ilustra una arquitectura de red IP/MPLS que es común a muchas empresas de proveedores de servicios de datos, la cual está diseñada según una red jerárquica de tres niveles: acceso, distribución y núcleo.

- La red de acceso es una red de área local (LAN) o una red para clientes corporativos, o clientes internos, se conectan a nivel de Ethernet y en algunos casos se utilizan enrutadores IP que proporcionan conectividad entre los conmutadores a nivel de capa 3, un proveedor de servicio soporta equipos de usuarios finales, tales como clientes corporativos (bancos, empresas gubernamentales, empresas comerciales, industrias, entre otros.), además concentra plataformas que se utilizan para dar servicios de Internet a usuarios masivos tanto para la red móvil como para la red fija, ejemplo de estas plataformas son las siguientes: DSLAM, BRAS, CMTS, GPON, MSAN, RNC, BSC, eNB.

Figura 2. **Arquitectura de red jerárquica**



Fuente: Foundations of Modern Networking. *SDN, NFV, QoE, IoT, and Cloud.* Chapter 1. Consulta: marzo de 2019.

- La red de distribución se encarga de conectar redes de acceso entre sí y agregar el tráfico destinado a la red de núcleo a través de enrutadores de borde, el uso de esta red limita el número de enrutadores que establecen relaciones entre los enrutadores de borde en el núcleo, ahorrando memoria, procesamiento y capacidad de transmisión, por lo que esta red también puede conectar directamente servidores aplicativos que son de uso a múltiples a redes de acceso, tales como servidores de bases de datos, servidores de gestión de red y servidores cache.

- La red de núcleo conecta redes de distribución geográficamente dispersas y proporciona acceso a otras redes que no forman parte de su dominio, normalmente esta red también puede conectarse a servidores de alto rendimiento y alta capacidad, como servidores de bases de datos grandes y servicios como nube privada, que desempeñan una función específica,

como por ejemplo el servicio interno de cada proveedor de servicios para facturar el servicio móvil o de la red fija.

Una arquitectura de red jerárquica optimiza las capacidades, características y funcionalidad del equipo de red (enrutadores, conmutadores y servidores de gestión de red), debido al buen diseño modular dentro de la jerarquía dada.

1.1.2. Estructura de un nodo de red actual

Los tres componentes básicos de un nodo de la red jerárquica actual son:

- Hardware con fines específicos: es construido para tareas específicas que el nodo debe realizar, ejemplo de estos nodos son los siguientes:
  - Un nodo de procesamiento de voz: está compuesto por tarjetas con la función incorporada de procesamiento de voz en el hardware.
  - Un nodo para procesamiento de llamadas: es un servidor seleccionado para manejar mensajes que ingresan y salen del nodo con un diseño personalizado para la función que ofrece.

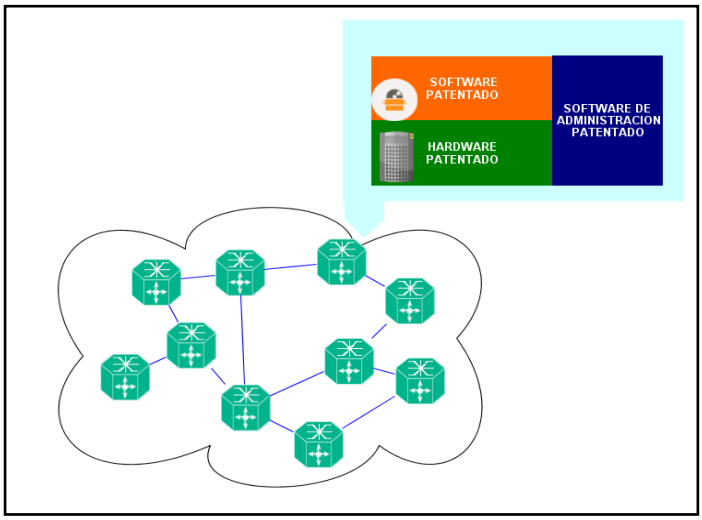
- Software patentado: proporciona un servicio y función específica para el nodo, este software controla y recibe los mensajes de otros nodos, ya sea para facturación o para procesamiento de voz o datos, siempre bajo la misma lógica de diseño de un servicio y función específica.

- Software de administración patentado: dedicado a realizar las siguientes actividades:
  - La correcta ejecución del software
  - El correcto funcionamiento de todos los procesos
  - El tipo de alarmas activadas

- Evaluar los contadores activados
- Evaluar el correcto funcionamiento del hardware específico

Cada uno de los nodos tendrá una estructura similar, como se ve en la figura 3, variando el diseño para cada proveedor y marca, sin embargo en la red se pueden tener muchos proveedores diferentes, por lo que desde la perspectiva del operador se debe tomar ese nodo patentado y obtener información clave con el fin de administrar los elementos de la red como un todo.

Figura 3. **Componentes de un nodo en la red actual**

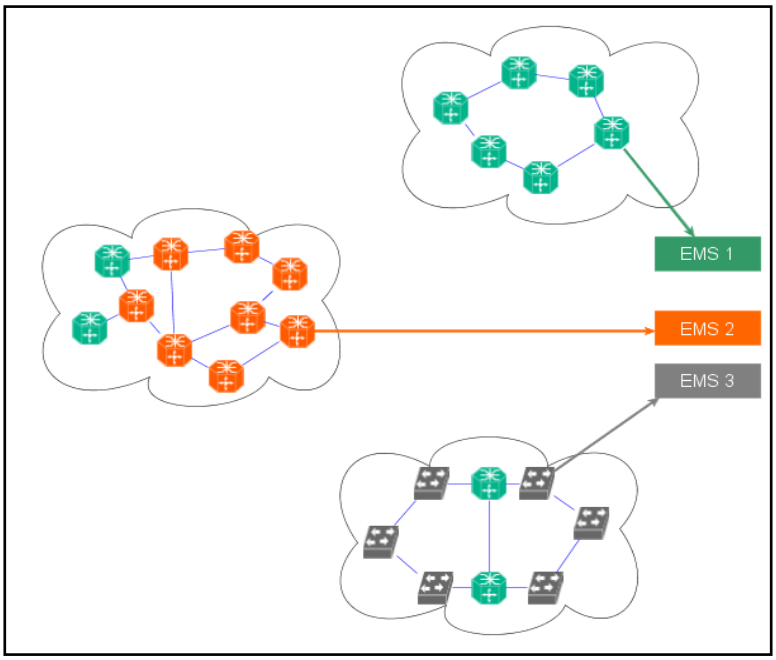


Fuente: elaboración propia.

La información clave necesaria para la administración de la red es obtenida de los nodos mediante el sistema de administración de elementos (EMS, por sus siglas en inglés), el cual se conecta a cada uno de los nodos de la red y los administra de forma que este recibirá la información de alarmas, contadores y registros, sin embargo, dado el diseño independiente de cada proveedor, se tendrá un EMS por cada proveedor.

Por lo tanto, de forma general según la arquitectura de una red IPS descrita, cada nodo tiene un software ligado al hardware, y algún tipo de sistema de administración de elementos patentado que permite integrarlo a la infraestructura, donde si se quiere brindar un nuevo servicio se debe implementar un nuevo elemento de hardware físico, por ejemplo, si en la red hay nodos de tres diferentes proveedores y marcas también se tendrán tres EMS, este concepto se ilustra a continuación en la figura 4.

Figura 4. **Sistema de administración de elementos (EMS)**



Fuente: elaboración propia.

1.2. Desafíos de las redes actuales

Incluso con la mayor capacidad de los esquemas de transmisión y el mayor rendimiento de los dispositivos de red, las arquitecturas de redes tradicionales son cada vez más inadecuadas frente a la creciente complejidad, variabilidad y alto volumen de la carga impuesta por las nuevas funciones y servicios

requeridos por los usuarios, por lo que la *Open Networking Foundation* (ONF) cita cuatro limitaciones generales para las arquitecturas de redes tradicionales:

- Arquitectura estática y compleja: para responder a demandas como niveles diferentes de calidad de servicio (QoS), volúmenes de tráfico muy altos y requisitos de seguridad, la tecnología de redes se ha vuelto más compleja y difícil de gestionar, esto ha dado lugar a una serie de protocolos independientes, cada uno de los cuales se ocupa de una parte de los requisitos de red, los procedimientos manuales como la asignación de recursos, la configuración que se realiza equipo por equipo, según sea su funcionalidad, ya sea para configurar parámetros de seguridad, calidad de servicio o requieran una optimización del flujo de datos.

- Políticas inconsistentes: para implementar una política de seguridad de toda la red, el personal debe realizar cambios en la configuración de miles de dispositivos y mecanismos, por lo tanto una red grande, cuando se activa una nueva máquina virtual, puede tardar horas o incluso días en reconfigurar las ACL en toda la red.

- Escalabilidad limitada: las demandas en las redes están creciendo rápidamente, tanto en volumen como en variedad, esto por los temas de movilidad que permiten nuevas tecnologías como 5G, la adición de más equipos y capacidad de transmisión involucra múltiples equipos de diversas aplicaciones y proveedores, una estrategia de las empresas consiste en utilizar los patrones de tráfico históricos y con estos realizar proyecciones, sin embargo, el uso de la virtualización y la creciente variedad de aplicaciones multimedia vuelve los patrones de tráfico impredecibles.

- Dependencia de los fabricantes: la falta de interfaces estandarizadas limita la adaptación de red, dejando a las empresas dependientes de utilizar los mismos fabricantes.[1]

1.3. Desafío de SDN y su enfoque

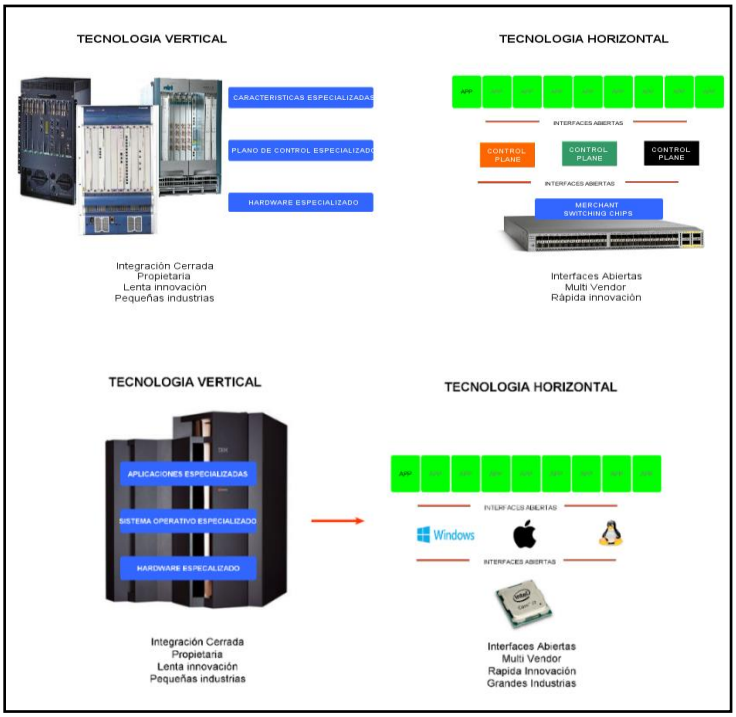
Las redes definidas por software (SDN) representan una manera totalmente nueva de concebir la configuración, el control y el funcionamiento de las redes de datos, SDN automatiza tanto los procesos como el aprovisionamiento de servicios y la configuración correctiva a través de software, de forma general se considera el enfoque de SDN sobre los siguientes puntos:

- Beneficios económicos.
- Programación de red mediante una clara separación del plano de datos y el plano de control.
- Compartimiento de la infraestructura de red proporcionando múltiples funciones.
- Gestión centralizada: la inteligencia de la red está centralizada en un software llamado concentrador SDN, que mantienen una visión global de la red, haciendo parecer por ejemplo una gran red de conmutadores como un único conmutador lógico.
- Programación configurada: SDN permite a los administradores de red configurar, administrar, asegurar y optimizar los recursos de red muy rápidamente a través de los programas de SDN dinámicos, que pueden ser escritos sin depender de software propietario.
- Reemplazar las funciones que tradicionalmente se ejecutan en servidores de productos básicos de forma separada.

[1] ONF12. Open Networking Foundation. *Software-defined networking: the new norm for networks.* ONF White Paper, April 13, 2012.

Para entender de mejor manera los beneficios de SDN, existe una analogía con la industria de computación. Cuando se adquiría un computador IBM, por ejemplo, este traía un hardware especializado, un sistema operativo especializado y aplicaciones especializadas, todo era especializado y único del mismo proveedor, no se podían utilizar los mismos procesadores propietarios en otro computador de otra marca, por ejemplo en alguna Apple MAC, esto se conoce como la tecnología vertical, la cual se caracteriza por ser cerrada, todo es propietario y hay poca innovación, sin embargo la industria de la computación ha cambiado hacia un modelo de tecnología horizontal, que se caracteriza por tener interfaces abiertas, rápida innovación y mayor crecimiento en la industria, estos conceptos se ilustran en la figura 5.

Figura 5. **Tecnología vertical y horizontal (industria de computación)**



Fuente: elaboración propia.

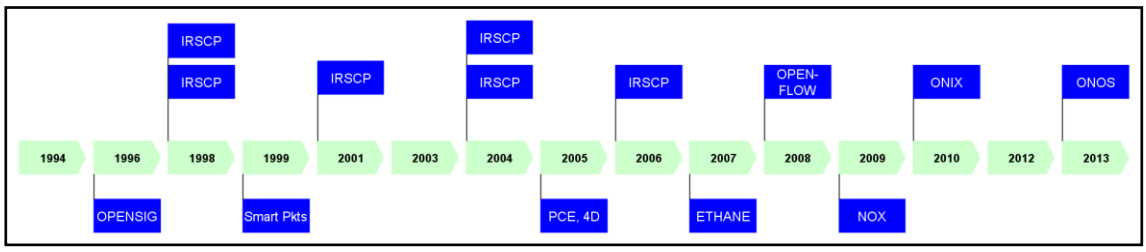
En analogía para la transición de una arquitectura de red tradicional a una arquitectura SDN / NFV, el concepto de la tecnología horizontal y vertical se aplica de la misma forma, dado que se pretende tener interfaces abiertas, múltiples planos de control no importando el proveedor y múltiples aplicaciones, lo cual permite crear rápida innovación.

SDN representa el punto pivote en cómo las redes se construyen y quién las maneja, la tecnología es análoga a la virtualización de los centros de datos y el cambio a SDN es en gran parte un intento de aprovechar al máximo el valor de los centros de datos virtualizados y las nubes con NF.

1.3.1. Antecedentes de SDN

En la figura 6 se proporciona una visión general de los esfuerzos para diseñar redes programables por software y los precursores de las arquitecturas para redes de datos, las cuales fueron diseñadas para simplificar el hardware de red, si bien SDN ha recibido una atención considerable, es importante señalar que la idea de redes “programables” y lógicas de control desacoplado ha existido desde hace muchos años.

Figura 6. **Precursores de SDN**



Fuente: elaboración propia.

En 1995 el grupo de trabajo OPENSIG desarrolló propuestas para proporcionar acceso al hardware de redes ATM, Internet y móviles a través de interfaces abiertas y programables, lo cual proporcionó al grupo de trabajo IETF las pautas para desarrollar el protocolo GSMP que luego, con el diseño de 4D, permitió una separación lógica de enrutamiento y la de los protocolos que rigen la interacción de los elementos de la red.

Posterior a estos protocolos el diseño del proyecto Ethane creó una lógica centralizada y una solución para el control de flujos para el acceso en redes empresariales, el cual preparó el camino para la creación de *OpenFlow*, protocolo que permite a una red LAN como la de un centro de datos ser gestionada como un todo, siendo el servidor el que dice a los conmutadores hacia dónde enviar los paquetes de datos, logrando con esto que las decisiones que implican movimiento o enrutamiento de paquetes estén controladas de forma centralizada.

En el 2011 la ONF (*Open Nerwork Fundation*) se crea con el propósito de estandarizar las tecnologías emergentes impulsando el software a la vanguardia de la gestión de red, estos trabajos solo abordan aplicaciones para el soporte de control de rutas arbitrarias en el contexto estrecho de cálculo de rutas, sin embargo, para soportar aplicaciones de control arbitrarias el controlador ONYX introdujo el concepto de una base de datos de información de red, incluyendo una representación topológica de red y otro estado de control.

Recientemente el sistema operativo de red abierta (ONOS), alojado bajo la fundación de Linux, es un software escrito en un ambiente de desarrollo de programación JAVA para redes definidas por software y para proveedores de servicios, el cual facilita la creación de aplicaciones y servicios.

1.4. Desarrollo de estándares para SDN y NFV

A diferencia de algunas áreas tecnológicas como Wi-Fi, no hay organismo de normas único responsable de desarrollar estándares abiertos para SDN y NFV, sin embargo, existe una gran colección de organizaciones de desarrollo de normas (SDO). En la tabla I se enumeran las principales SDO y los principales resultados obtenidos por cada una de ellas.

Tabla I. **Organizaciones que participan en el desarrollo de SDN y NFV**

Organización	Misión	Esfuerzo relacionado con SDN y NFV
ONF	Un consorcio de la industria dedicado a la promoción y adopción de SDN a través del desarrollo de estándares abiertos.	Desarrollo del protocolo *OpenFlow*.
IETF	El organismo de normas técnicas de Internet, produce los documentos de referencia (RFC) y estándares de Internet.	Desarrollo de interfaz con los sistemas de enrutamiento (I2RS). Encadenamiento de funciones de servicio.
ETSI	Una organización de estándares auspiciada por la UE que produce estándares globales aplicables a las tecnologías de la información y las comunicaciones.	Arquitectura para NFV.
OpenDaylight	Un proyecto colaborativo bajo los auspicios de la Fundación Linux.	Desarrollo de OpenDaylight.
UIT-T	Organismo de las Naciones Unidas que produce recomendaciones con miras a normalizar las telecomunicaciones a nivel mundial.	Requisitos y arquitectura funcional de SDN.

Continuación de la tabla I.

ODCA	Consorcio de las principales organizaciones de tecnologías de la información que desarrollan soluciones y servicios interoperables para la computación en la nube.	Modelo de uso SDN.
IRTF / SDNRG	Grupo de investigación dentro de IRTF que produce documentos de referencia (RFC) relacionados con SDN.	Arquitectura para SDN.
MEF	Consorcio industrial que promueve el uso de Ethernet para aplicaciones metropolitanas y de área amplia.	Definición de API para orquestación de servicios sobre SDN y NFV.
OIF	Consorcio de la industria que promueve el desarrollo y el despliegue de soluciones interoperables del establecimiento de una red y servicios para los productos ópticos de la red.	Requisitos en redes de transporte en arquitecturas SDN.
BBF	Consorcio de la industria que desarrolla especificaciones de red de paquetes de banda ancha.	Requisitos y marco para SDN en las redes de banda ancha de telecomunicaciones.
IEEE 802	Un comité de IEEE responsable de desarrollar estándares para LANs.	Estandarizar las capacidades de SDN en las redes de acceso.
ATIS	Organización que desarrolla estándares para la industria de comunicaciones unificadas (UC).	Oportunidades operativas y desafíos de la infraestructura programable SDN / NFV.
OPNFV	Un proyecto de código abierto enfocado a acelerar la evolución del NFV.	Infraestructura NFV.

Fuente: elaboración propia, empleando Microsoft Office Word 2013.

Los documentos creados por las organizaciones proporcionan requisitos, especificaciones, directrices o características que se utilizan de manera consistente para asegurar que los materiales, productos, procesos y servicios sean los adecuados para su propósito, los estándares se establecen por

consenso entre los participantes de organizaciones y la elaboración de normas es aprobada por un órgano generalmente reconocido.

1.4.1. Consorcios de la industria

Debido al lento proceso de las organizaciones de desarrollo de normas para proporcionar normas útiles en el acelerado mundo de la tecnología, varios consorcios se han involucrado en el desarrollo de normas para SDN y NVF, dentro de los principales están:

- *Open Networkin Foundation* (ONF): se dedica a la promoción y adopción de SDN a través del desarrollo de estándares abiertos, su contribución más importante hasta la fecha es el protocolo *OpenFlow* y API.

- Open Data Center Alliance (ODCA): dedicados a celebrar la adopción de soluciones interoperables y de servicios en la nube, mediante el desarrollo de modelos que definen los requisitos para el despliegue de nubes SDN y NFV.

- Alianza para Soluciones de la Industria de Telecomunicaciones (ATIS): proporciona las herramientas necesarias para que la industria identifique estándares, directrices y procedimientos operativos que hacen posible la interoperabilidad de productos y servicios de telecomunicaciones existes y emergentes.

- Iniciativas de desarrollo abierto: las cuales con creadas por los usuarios y tienen un enfoque particular siempre con el objetivo de desarrollar estándares abiertos o software de código abierto.

- Plataforma abierta para NFV (OPNFV): es un proyecto de código abierto dedicado a acelerar la adopción de elementos NFV estandarizados, estableciendo una plataforma de referencia de código abierto, integrada, de clase operadora, que los pares de la industria construirán de forma conjunta para avanzar en la evolución del NFV y asegurar la consistencia, el rendimiento y la interoperabilidad entre múltiples componentes de código abierto.

2. SDN ARQUITECTURA Y MODELOS DE CONTROL

El uso de redes definidas por software (SDN) implica la utilización de la arquitectura y protocolos adecuados para lograr la gestión de los elementos de la red, por lo tanto el diseño consiste en definir funciones y protocolos para el plano de datos y métodos que aseguren el re-direccionamiento de los paquetes de datos de forma correcta.

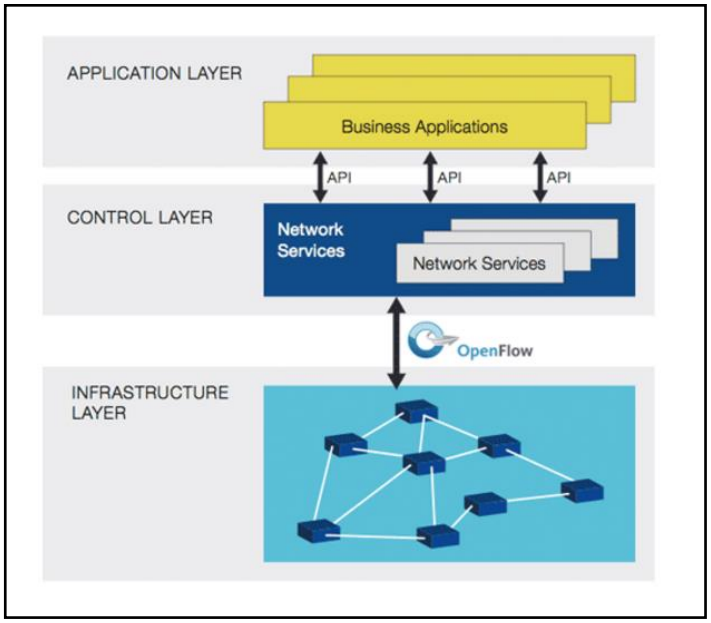
El protocolo *OpenFlow* es la primera interfaz estándar diseñada específicamente para SDN que puede aplicarse tanto en hardware como en software, permitiendo que las redes de datos evolucionen por medio de un software de control lógico, centralizando la capacidad de modificar el comportamiento de los dispositivos a través de un conjunto de instrucciones de reenvío bien definido.

2.1. Arquitectura de SDN

La arquitectura SDN se basa en el desacoplamiento entre el plano de datos y el plano de control de la red, para lograrlo se crea una capa de infraestructura en la que se encuentran todos los dispositivos de red y una capa de control donde se ubicará el controlador SDN.

En la figura 7 se ilustra la arquitectura de SDN especificada por la ONF. donde se muestra a un alto nivel los puntos de referencia e interfaces al controlador, considerando las siguientes capas: capa de aplicación, capa de control y capa de infraestructura.

Figura 7. **Arquitectura SDN especificada por ONF**



Fuente: Open Networking Foundation. *Capas de SDN.* https://opennetworking.org. Consulta: abril de 2019.

2.2. SDN, capa de infraestructura y *OpenFlow*

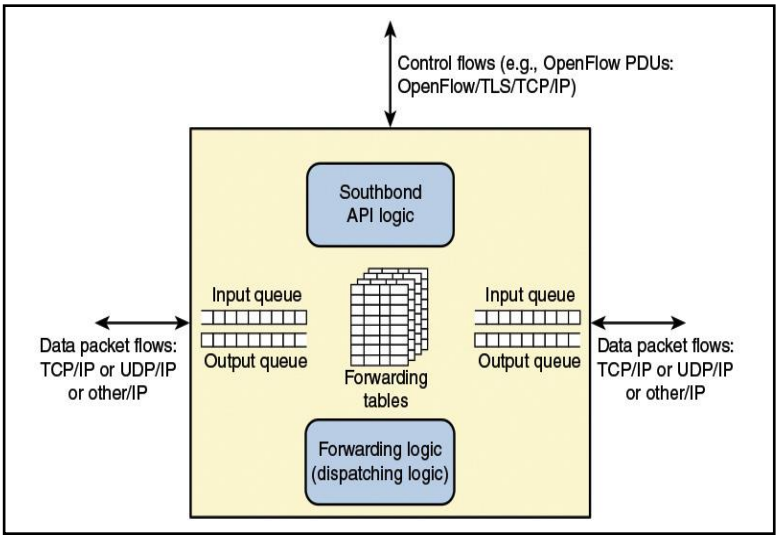
La implementación más utilizada en la capa de infraestructura de datos SDN es *OpenFlow*, ya que define tanto una especificación de la estructura lógica para la funcionalidad de la capa de infraestructura, como un protocolo ente los controladores SDN y los dispositivos de red, por lo tanto se distinguen dos procesos diferentes para el plano de datos: funciones y protocolos.

2.2.1. Funciones del plano de datos

El plano de datos SDN, denominado capa de recursos en ITU-T Y.3300, también denominada a menudo capa de infraestructura, es donde los dispositivos

de red realizan el reenvío, el transporte y procesamiento de datos de acuerdo con las decisiones tomadas por el plano de control SDN, la característica más importante de los dispositivos de red en una arquitectura SDN es que estos dispositivos realizan la simple función de reenvío de paquetes de datos, sin un software incorporado para tomar decisiones autónomas.

Figura 8. **Plano de datos en un dispositivo de red**



Fuente: Open Networking Foundation. *Plano de datos.* https://opennetworking.org. Consulta: abril de 2019.

En la figura 8 se ilustra las funciones realizadas por los dispositivos de red del plano de datos (también llamados elementos de red del plano de datos o conmutadores), donde las funciones principales del dispositivo de red son las siguientes:

- Función de soporte de control: interactúa con la capa de control SDN para soportar la programación a través de interfaces de control, donde el

conmutador se comunica con el controlador y el controlador gestiona el conmutador a través del protocolo de conmutación *OpenFlow*.

- Función de reenvío de datos: acepta los flujos de datos entrantes de otros dispositivos de red y sistemas finales y los reenvía a lo largo de las rutas de reenvío de datos que se han calculado y establecido de acuerdo con las reglas previamente definidas por las aplicaciones SDN.

Las reglas de reenvío utilizadas por el dispositivo de red están incorporadas internamente en sus tablas de reenvío gracias al protocolo *OpenFlow* en SDN, las cuales trabajan según una determinada categoría de paquetes especificando cuál debería ser el salto siguiente en la ruta determinada. Además del simple reenvío de un paquete, el dispositivo de red puede alterar el encabezado antes de reenviarlo o descartarlo, dado que estos paquetes se colocan en una cola de entrada, esperando el procesamiento y posteriormente los paquetes reenviados se colocan en una cola de salida, esperando la transmisión.

De forma básica un dispositivo de red cuenta con tres puertos de entrada y salida, de los cuales el primero proporciona la comunicación con el controlador SDN mientras que los demás proporcionan una entrada y salida para los paquetes de datos, sin embargo de forma general un dispositivo de red puede tener varios puertos para comunicarse con varios controladores SDN y puede tener más de dos puertos de entrada y salida para el flujo de paquetes hacia y desde el dispositivo.

2.2.2. Protocolo del plano de datos

Para aplicar el concepto de SDN en una implementación práctica se deben cumplir dos requisitos:

- Una arquitectura lógica común en todos los conmutadores, enrutadores y otros dispositivos de red para ser administrados por un controlador SDN, esta arquitectura lógica debería poderse implementar en diferentes equipos de proveedores y en diferentes tipos de dispositivos de red, siempre que el controlador SDN vea una funcionalidad común de conmutación.

- Un protocolo estándar que provea seguridad entre el controlador SDN y los dispositivos de red.

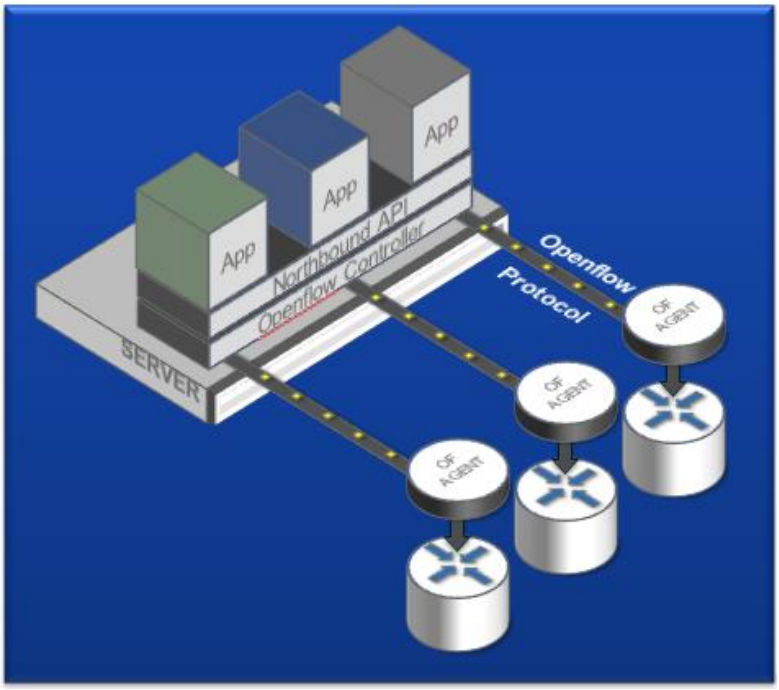
El protocolo que cumple con estos requisitos es *OpenFlow*, dado que puede ser utilizado entre los controladores SDN y los dispositivos de red, definiendo una estructura de red como un protocolo de conmutación, los elementos principales de *OpenFlow* son:

- Controlador SDN: es el elemento donde reside el software que proporciona la función del plano de control para la red.
- API superior: diseñada para escucha e iniciar la comunicación hacia las aplicaciones, clientes, bases de datos, entre otros.
- Agentes de dispositivo: es una porción pequeña de software que reside en cada conmutador o componente de la red, que tiene la inteligencia para comunicarse con el controlador de *OpenFlow.*
- Protocolo *OpenFlow*: encargado de establecer sesiones TCP entre el controlador SDN y los agentes de dispositivo de cada conmutador utilizando el puerto TCP 6653 para establecer dichas conexiones e intercambio de información.

El intercambio de paquetes en el protocolo *OpenFlow* es completamente IP, dado que la tabla de reenvió define entradas basadas en los campos de los

encabezados de protocolo de nivel superior como TCP, UDP u otro protocolo de transporte de aplicación, por lo tanto el dispositivo de red examina la cabecera IP y otros encabezados según sea considerado necesario para cada paquete y toma una decisión de reenvío, en la figura 9 se ilustran los elementos principales de *OpenFlow*.

Figura 9. **Elementos principales de *OpenFlow***



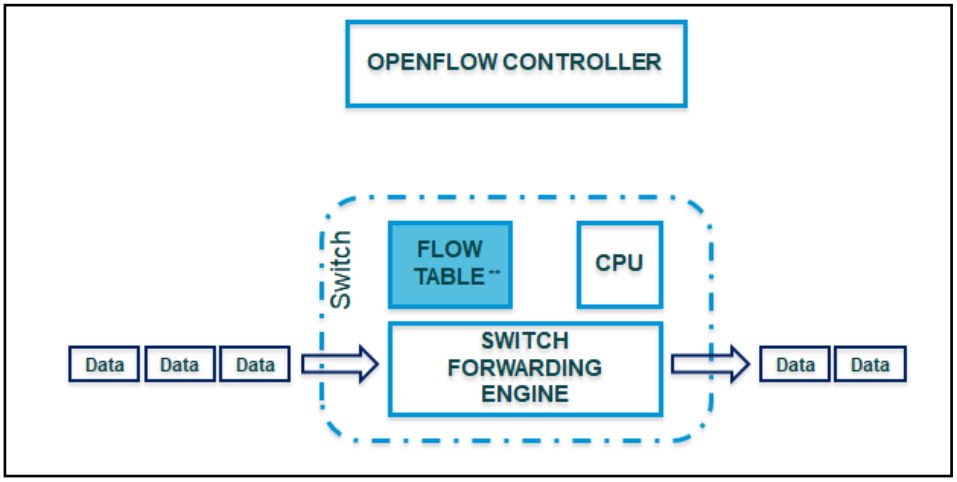
Fuente: Elementos de *OpenFlow*. http://www.himawan.nu/2015/08/. Consulta: abril de 2019.

2.2.2.1. Modelo de reenvío de OpenFlow

Cada conmutador de *OpenFlow* tiene una tabla de flujo, la cual ha sido descargada previamente y programada desde el controlador SDN, para proveer el control de ruta que cada paquete debe tomar, adicional cada conmutador tiene un CPU que se encarga del procesamiento.

La figura 10 ilustra el modelo de reenvío de paquetes, donde la información que entra ingresa a un conmutador con el agente de dispositivo de *OpenFlow*, el dispositivo busca y compara con la tabla de enrutamiento y, si dentro de las instrucciones está realizar un envío, se reenvían los datos, de lo contrario los paquetes se descartan.

Figura 10. **Modelo de reenvío en *OpenFlow***



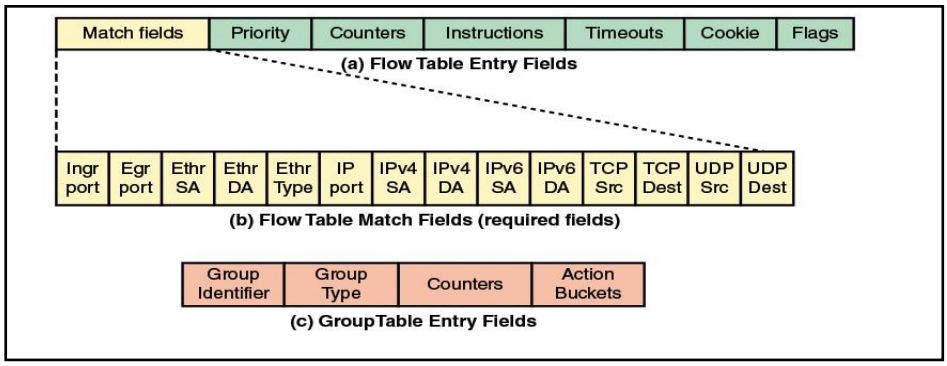
Fuente: *Modelo de reenvío en Openflow.* https://s3f.iti.illinois.edu. Consulta: abril de 2019.

Cada paquete de datos entra al conmutador integrado a la arquitectura SDN y pasa a través de una tabla de control de flujo, esta tabla consta de filas llamadas entradas con los siguientes campos:

- Campos de igualdad
- Prioridad
- Contadores
- Instrucciones
- Tiempo vencido
- *Cookie*

La cabecera de campos de igualdad contiene 14 elementos, los cuales son utilizados por el conmutador para comparar la información de cada paquete con la tabla de flujos previamente descargada y programada por el controlador SDN, estos campos se ven en la figura 11.

Figura 11. **Componentes de tabla de flujo *OpenFlow***



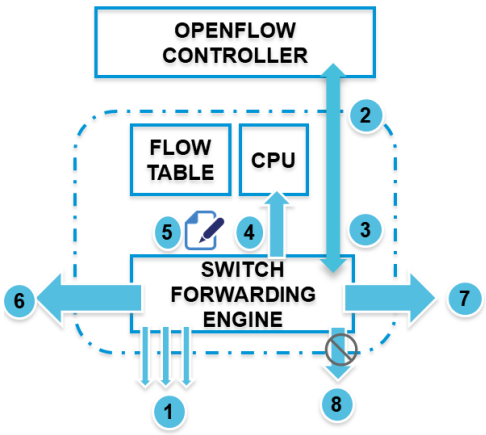
Fuente: *Tabla de flujo Openflow.* https://s3f.iti.illinois.edu/. Consulta: abril de 2019.

En la figura 12 se ilustran las principales acciones que los conmutadores integrados a la arquitectura SDN pueden llevar a cabo con los resultados de la comparación de los campos, entre estas acciones están:

- Reenvía a todos los puertos en excepción al puerto que recibe
- Redirecciona al controlador
- Sacar del controlador
- Reenviar al CPU local
- Reescribir la cabecera del paquete
- Reenviar hacia el puerto que lo recibe
- Reenviar al puerto destino
- Descartar paquete

Figura 12. **Acciones principales de *OpenFlow***

1	Re enviar a todos los puerto en excepción al puerto que lo recibe
2	Re direccionar al controlador
3	Sacar del controlador
4	Re enviar al CPU local
5	Re escribir en la cabecera del paquete
6	Re enviar hacia el puerto que lo recibe
7	Re enviar al puerto de destino
8	Descartar paquete



Fuente: *Acciones principales de Openflow.* https://s3f.iti.illinois.edu/. Consulta: abril de 2019.

2.3. SDN: capa de control

Esta capa incluye las funciones de control, configuración de recursos y dirección de flujos de tráfico, ya que la arquitectura SDN define la abstracción de la capa física hasta la capa de aplicación en contraste de las redes que siguen el modelo OSI donde las primeras tres capas cuentan con ese control (físico, enlace de datos y red).

En SDN se cuenta con una entidad controladora por software, agnóstica a los protocolos y multivendor, esta entidad es la encargada de eliminar la inteligencia de conmutación y encaminamiento de los nodos independientes permitiendo interoperabilidad y simplificación. Dentro de las principales funciones que tiene la capa de control se pueden mencionar:

- Selección de la ruta más corta: utiliza la información de enrutamiento recopilada de los enrutadores para establecer rutas preferidas.
- Administración de notificaciones: recibe, procesa y envía eventos, como notificaciones de alarmas y cambios de estado.
- Proporciona mecanismos de seguridad entre aplicaciones y servicios.
- Crea y mantiene información de topología de interconexión de los dispositivos de red.
- Recopila datos sobre el tráfico a través de los conmutadores.
- Realiza configuración de los parámetros y atributos de los equipos de red y gestiona las tablas de flujo.

2.3.1. Modelos de control SDN

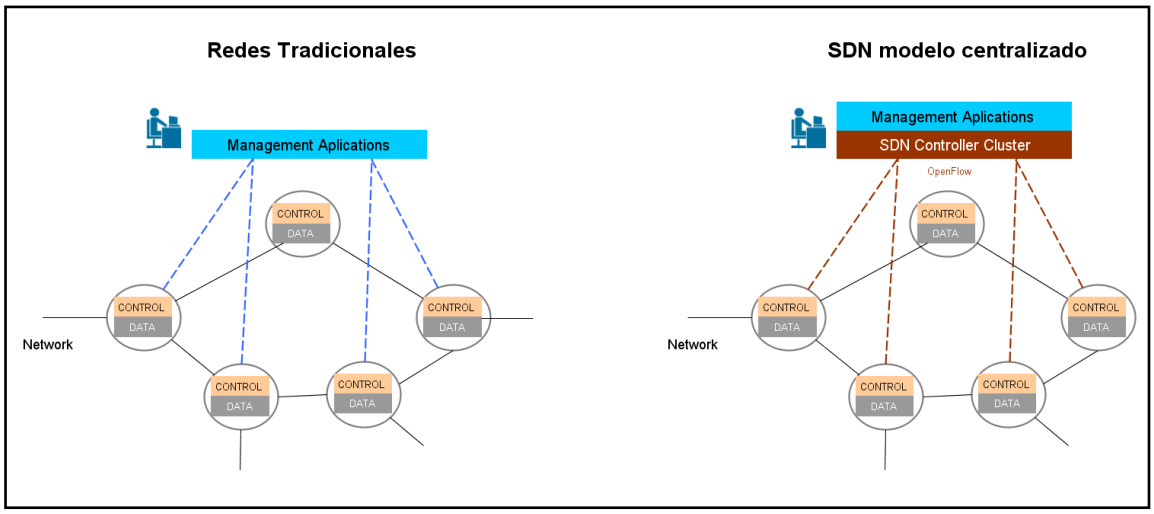
La implementación de redes con una arquitectura SDN puede realizarse sobre un modelo basado en una arquitectura centralizada o una arquitectura distribuida, cada uno debe ser considerada con sus diferentes requisitos y elementos, sin embargo un despliegue exitoso requiere un análisis previo para elegir la arquitectura correcta, para posteriormente realizar la homologación para realizar las pruebas en los diferentes contextos de red y servicios

2.3.1.1. Arquitectura SDN centralizada

En esta arquitectura, un proceso de software central (o controlador SDN centralizado) mantiene completa la topología, conectividad, estados de red, entendimiento de la red y el direccionamiento desde la perspectiva del usuario, los procesos del núcleo corren en el controlador por algoritmos y políticas de red para definir rutas a través de la red para cada flujo, las rutas son creadas por direccionamiento hacia todos los dispositivos a lo largo de la ruta para actualizar

la tabla de reenvío y para que los paquetes pasen a través de la ruta trazada. En la figura 13 se ilustra esta arquitectura.

Figura 13. **Arquitectura SDN centralizada**



Fuente: elaboración propia, empleando programa yED Graphic Editor.

El protocolo *OpenFlow* fue diseñado para soportar este modelo donde existe un controlador centralizado para comunicar la tabla de reenvío hacia los dispositivos de red, esta comunicación podría ocurrir de una forma proactiva, basada en un mapa de toda la red, o reactivamente, en respuesta a una solicitud del dispositivo, a continuación se describen las ventajas y desventajas de una arquitectura SDN centralizada:

- Ventajas:
  - El controlador tiene la visión completa de la red, por lo que es más simple asegurar la consistencia de la red y optimización en la configuración.
  - Provee una administración estándar y simple.

- Fácil integración con equipos legados, cualquiera y todas las aplicaciones son soportadas directamente por el controlador centralizado no importando la marca de los dispositivos que conforman la red.

- Desventajas:
  - Agrega latencia para establecer los flujos de datos.
  - Se crea dependencia con el controlador, por lo que este debe ser escalable y estar siempre disponible.
  - Todos los servicios avanzados se manejan centralmente, en lugar de localmente, perpetuando un cuello de botella a medida que se crece a gran escala.

2.3.1.2. Arquitectura SDN distribuida

La arquitectura SDN distribuida agrega mecanismos de control para redes basadas en software de las redes IP y Ethernet tradicionales, el objetivo es lograr un comportamiento más controlable al tomar los protocolos ya existentes como MPLS (Multiprotocol Label Switching), GRE (Generic Routing Encapsulation) y protocolos basados en políticas como parte de SDN.

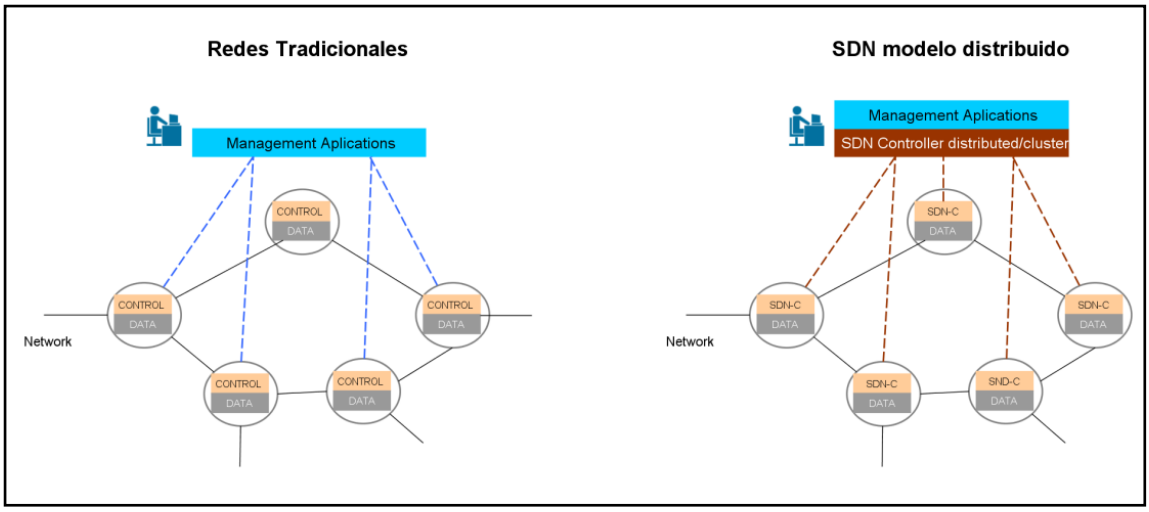
El modelo distribuido se caracteriza por dejar cierta parte del control en los diferentes dispositivos y una gran mayoría de las funciones de control, así como permitir que una gran cantidad de funciones esté localizada en la capa de control, principalmente las funciones de creación y tablas de rutas para reenvío.

- Desventajas:
  - La sincronización de la topología de red puede ser lenta mientras la cantidad de nodos aumenta.

- Si se tienen equipos heredados como conmutadores antiguos, se necesita tener un controlador centralizado que los conecte al plano de control distribuido.

En la figura 14 se ilustra la arquitectura SDN en modo distribuido.

Figura 14. **Arquitectura SDN distribuida**



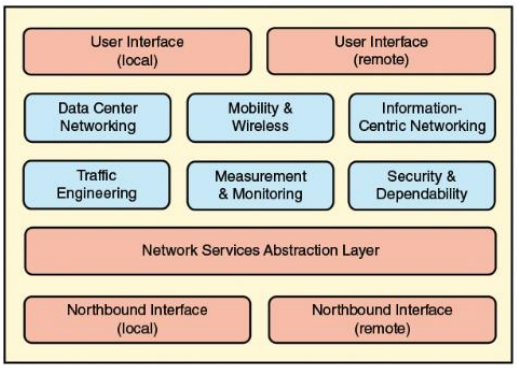
Fuente: elaboración propia, empleando programa yED Graphic Editor.

2.4. SDN: capa de aplicación

La ventaja que provee el enfoque de las redes SDN está en que permite supervisar y administrar el comportamiento de los dispositivos de la red, proporcionando funciones y servicios que facilitan el rápido desarrollo y despliegue de aplicaciones. Dentro del grupo de aplicaciones utilizada en los servicios de comunicación de SDN a través de APIs están las siguientes: REST, JSON, HTML, entre otras, todas estas aplicaciones permiten automatizar tareas como aprovisionamiento, configuración y gestión de servicios de red.

Las interfaces superiores permiten a las aplicaciones acceder a funciones y servicios del plano de control sin necesidad de conocer los detalles de los elementos de red subyacentes, esta funcionalidad es similar a la de un monitor de hipervisor o máquina virtual que desacopla las aplicaciones del sistema operativo subyacente del hardware.

Figura 15. **Elementos en plano de aplicaciones SDN**



Fuente: Foundations of Modern Networking. *SDN, NFV, QoE, IoT, and Cloud.* Chapter 6. Consulta: abril de 2019.

En la figura 15 se describen los elementos principales del plano de aplicaciones en SDN, donde las principales son:

- Ingeniería de control de tráfico
- Redes para centros de datos
- Medición y monitoreo
- Seguridad
- Redes centradas en la información

2.4.1. Ingeniería de tráfico

Analiza dinámicamente, regula y predice el comportamiento de los datos que fluyen en redes con el objetivo de optimizar el rendimiento para cumplir con los acuerdos de nivel de servicio aplicando políticas de enrutamiento, en una arquitectura SDN la tarea de ingeniera de tráfico se simplifica en gran medida debido que se cuenta con una visión global y uniforme de los equipos heterogéneos en la red, así como herramientas para configurar y gestionar los conmutadores de red

En una arquitectura SDN se pueden implementar las siguientes aplicaciones:

- Redes privadas virtuales bajo demanda
- Balanceo de carga
- Enrutamiento energético
- Calidad de servicio (QoS) para redes de acceso de banda ancha
- Programación y optimización
- Ingeniería de tráfico con gastos mínimos
- Enrutamiento dinámico de QoS para aplicaciones multimedia
- Recuperación rápida a través de grupos de conmutación rápida
- Marco de gestión de políticas de QoS
- Aplicación de la QoS sobre redes heterogéneas
- Gestión de colas para la aplicación de QoS
- División y difusión de tablas de reenvío

2.4.2. Redes para centros de datos

La computación en la nube (c*loud computing* en inglés), los macro de datos (b*ig data* en inglés), las grandes redes empresariales y, en muchos casos, las redes empresariales más pequeñas dependen fuertemente de centros de datos altamente escalables y eficientes, un caso de uso para el plano de aplicaciones en el Data Center Networking es el servicio de Cloud Network as a Service (CloudNaaS), el cual es un sistema de red en la nube que explota las capacidades de SDN y *OpenFlow*, para proporcionar un mayor grado de control sobre las funciones de red por parte del cliente, CloudNaaS permite implementar aplicaciones que incluyen varias funcionalidades de red como:

- Aislamiento virtual.
- Diferenciación de servicios con políticas de calidad QoS.
- Direccionamiento personalizado y la interposición flexible de varios dispositivos de red como balanceadores de carga.

2.4.3. Medición y monitoreo

El área de aplicaciones de medición y monitoreo se divide en las siguientes categorías:

- Aplicaciones que brindan nuevas funcionalidades para otros servicios de red, como el caso de las conexiones de área doméstica de banda ancha, donde una red basada en SDN agrega nuevas funciones a la medición del tráfico y la demanda de la red doméstica, permitiendo que el sistema reaccione a condiciones cambiantes.

- Aplicaciones que agregan valor a las redes SDN basadas en *OpenFlow*, implica el uso de diferentes tipos de muestreo y técnicas de estimación para reducir la carga del plano de control en la recopilación de estadísticas del plano de datos.

2.4.4. Seguridad

Dado que SDN implica una arquitectura en tres capas (aplicación, control y datos), así como un enfoque para un control distribuido y la encapsulación de datos, se introducen potenciales nuevos vectores de ataque en la red, por lo que las aplicaciones en el área de seguridad tienen como objetivo abordar todas las medidas de seguridad relacionadas con SDN y utilizar las funcionalidades de SDN para mejorar la seguridad de la red.

Las amenazas de seguridad pueden ocurrir en cualquiera de las tres capas o en la comunicación entre capas, por lo que es necesario proveer un uso seguro de cada uno de las etapas, sin embargo estos nuevos desafíos de seguridad también proporcionan una plataforma para implementar políticas de seguridad y mecanismos coherentes y centralizados para la red, permitiendo el desarrollo de controladores de seguridad que pueden aprovisionar y organizar servicios.

Un ejemplo de una aplicación de seguridad SDN es *OppenDaylight DDDoS*, que ofrece a los operadores y proveedores de servicios en la nube la detección y mitigación de denegación de servicio (DDoS) distribuidas como un servicio de red nativo, permitiendo a los operadores aprovisionar un servicio de protección DoS/DDoS por segmento de red virtual o por cliente, este consta de los siguientes elementos:

- Recopilación de estadísticas de tráfico y aprendizaje del comportamiento estadístico de los objetos protegidos en tiempos de paz, creando a partir de estos resultados las líneas de base de tráfico normales de los objetos protegidos.

- Detección de patrones de ataque DDoS como anomalías de tráfico que se desvían de las líneas de base normales.

- Desvío de tráfico sospechoso de su ruta normal a sistemas de mitigación de ataques (AMS) para depuración de tráfico, bloqueo selectivo de fuente y otras acciones pertinentes, el tráfico analizado que sale de los centros de depuración se vuelve a inyectar en el destino original del paquete.

2.4.5. Redes centradas en la información

Dado que la distribución y manipulación de la información se ha convertido en la principal función de Internet, las redes centradas en la información tienen como objetivo proporcionar primitivas de red nativas para la recuperación de información eficiente, nombrando y operando directamente en objetos de información, en contraste con la red tradicional que se enfoca en el *host,* donde la información se obtiene contactando *hosts* específicos.

Las redes centradas en la información realizan una distinción entre ubicación e identidad, desacoplando información para sus fuentes, donde el enfoque es que las fuentes pueden colocar y los usuarios pueden encontrar información en cualquier parte de la red, porque la información se nombra, se dirige y se empareja independiente de su ubicación.

Para las redes centradas en la información, en lugar de especificar un par de *host* de origen y destino para la comunicación, se nombra una pieza de información, ya que después de que se envía una solicitud, la red es responsable de localizar la mejor fuente que puede proporcionar la información deseada**.**

3. NFV: VIRTUALIZACIÓN DE FUNCIONES DE RED

La virtualización, que normalmente se utiliza en el ámbito de la informática, se refiere a la virtualización de servidores, sin embargo, cuando se utiliza como una frase independiente se refiere a la abstracción de la aplicación y el sistema operativo desde el hardware, enfocándose en el software y la verdadera esencia de los servicios del proveedor de servicios para ejecutar ese software en una infraestructura de nube, sin considerar el hardware patentado.

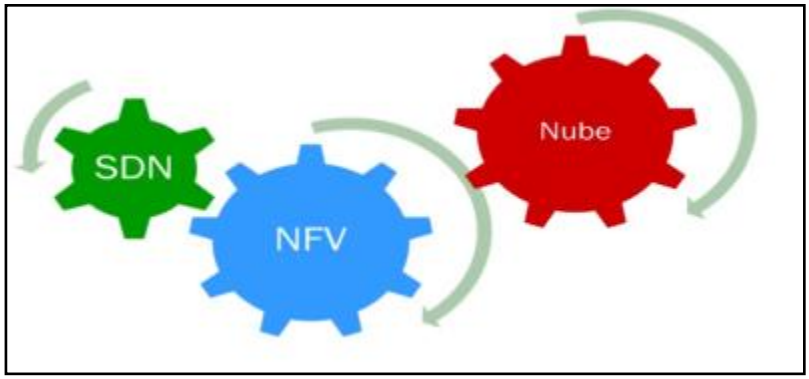
3.1. Concepto de NVF y su relación con otras tecnologías

La virtualización de red o NFV (Network Function Virtualization por sus siglas en inglés) es la abstracción de las funcionalidades de la red de la parte física o del hardware, NFV diferencia el hardware del software tomando un software patentado para mantenerlo y ejecutarlo en una infraestructura de nube.

Derivado del hecho de tomar funciones de red y convertirlas en software se obtiene varias ventajas, entre las cuales una de ellas es la movilidad del software, considérese el caso de un software que se está ejecutando en el servidor 15 del centro de datos 1, pero debido a una falla, o una demanda del servicio o al crecimiento de la red, se mueve al servidor 20 del centro de datos 2, ya que el software puede moverse de un servidor a otro sin problemas en una infraestructura de nube, aun es necesario que la red pueda enviarle paquetes de datos a ese elemento de software donde quiera que esté ubicado físicamente, es decir, brindar conectividad, ahí es donde la red definida por software brinda el soporte necesario.

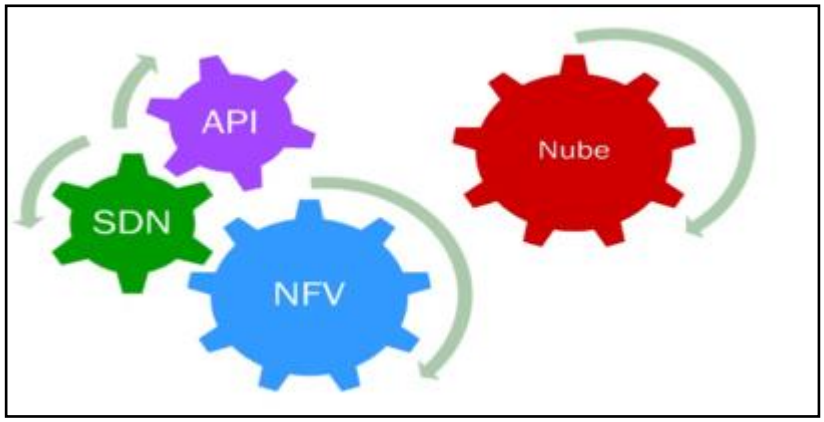
Las redes definidas por software ofrecen un transporte flexible para la red en un esquema donde la infraestructura de la nube actúa como el hardware, SDN como un transporte flexible y NFV como el software que se encarga de las funciones, este concepto se ilustra en la figura 16.

Figura 16. **Relación entre SDN – NFV – Nube**



Fuente: elaboración propia.

Figura 17. **Relación entre SDN – API – NFV – Nube**

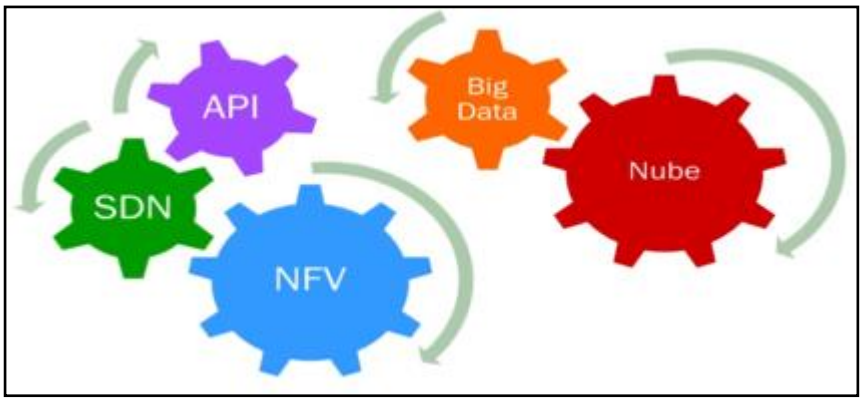


Fuente: elaboración propia.

En la figura 17 se ilustra la ubicación de las interfaces de programación de aplicaciones (API), las cuales permiten la comunicación de las entidades de software entre sí, resolviendo los mecanismos de comunicación de manera que varios componentes del software tendrán interfaces de programación de aplicaciones publicadas de manera que las entidades de software puedan hacer cambios en la red según sea necesario, ejemplo de estos cambios es mover la funcionalidad hacia otro hardware físico.

En las redes de proveedores de servicio es necesario recopilar la mayor cantidad posible de datos sobre la red, ya que esos datos pueden ser registros, contadores, alarmas, incluso medios de comunicación social, gente hablando sobre la red, *tickets* de incidencia, personas que llaman y clientes que presentan sus quejas y toda esta información sobre la red es colocada en un motor de *big data,* para que sean analizados todos los datos para elaborar medidas o métricas aceptables, análisis comerciales que permitirán conocer y modificar la red, esto se ilustra en la figura 18.

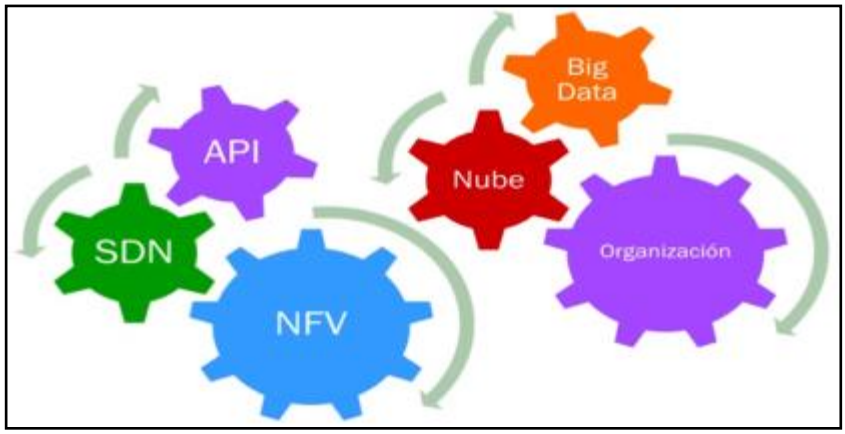
Figura 18. **Relación entre SDN – API – NFV – *Big data* – Nube**



Fuente: elaboración propia.

El último elemento de NFV es el organizador, este elemento es muy importante ya que es el que unirá todas las tecnologías de virtualización entre sí para determinado servicio, este se centra en la automatización de servicios extremo a extremo y la adaptación de la red, según sea necesario, además crea el vínculo que une todas las tecnologías y está enfocado a los servicios, este concepto se ilustra en la figura 19.

Figura 19. **SDN – API – NFV – *Big data* – Nube – Organizador**



Fuente: elaboración propia.

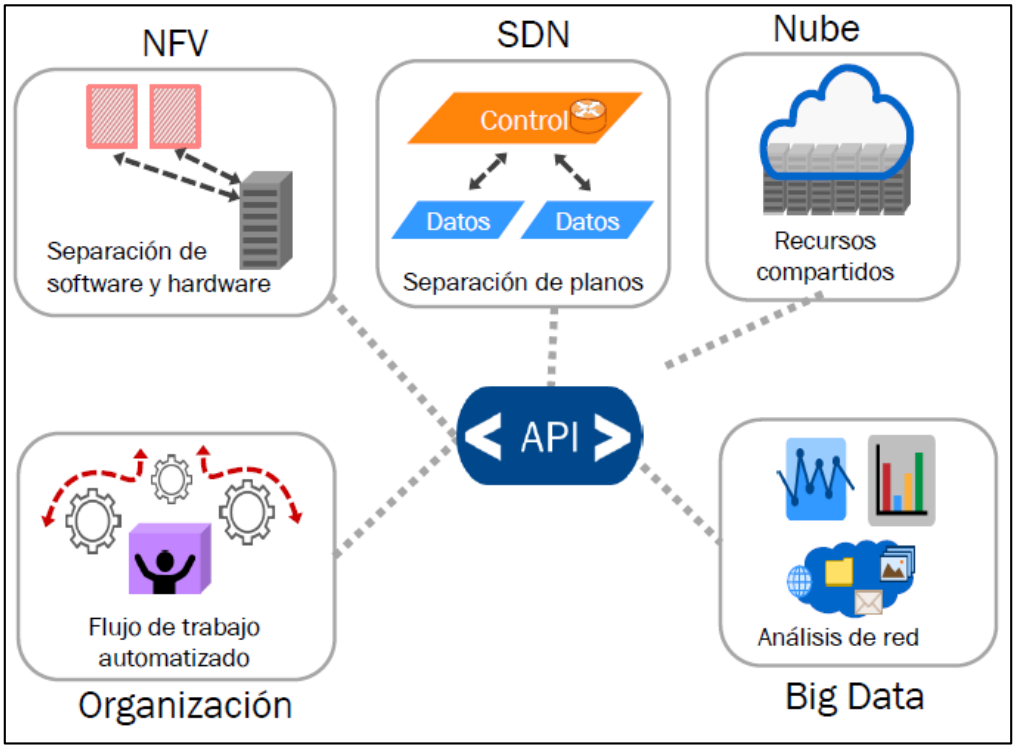
En la figura 20 se ilustra el análisis de comparación y contraste sobre la relación de NFV con otras tecnologías, de este se obtiene lo siguiente:

- La nube se trata de recursos y hardware compartido, se implementa para dar soporte a otras cosas y se puede compartir esa nube para dar otros servicios.
- La NFV es la disociación del software y hardware, la separación del software y hardware patentado se refiere a la virtualización de los servicios de la capa 4 a 7 del modelo OSI, como por ejemplo funciones como balanceadores de carga y *firewalls,* básicamente, esto convierte

dispositivos de diversas funcionalidades en una red de máquinas virtuales, que luego pueden desplegarse rápida y fácilmente donde se necesiten.

- La SDN se trata del trasporte flexible y la separación de los elementos de transporte de algún tipo de entidad de control.
- La organización es la automatización de la red, la cual se asegura que todo funcione correctamente, según sea necesario.
- El motor de *big data* es el encargado del análisis, recopila información, toma decisiones y posterior transmite esas decisiones a las API para realizar alguna acción o cambios en la propia red.

Figura 20. **NFV y su relación con otras tecnologías**

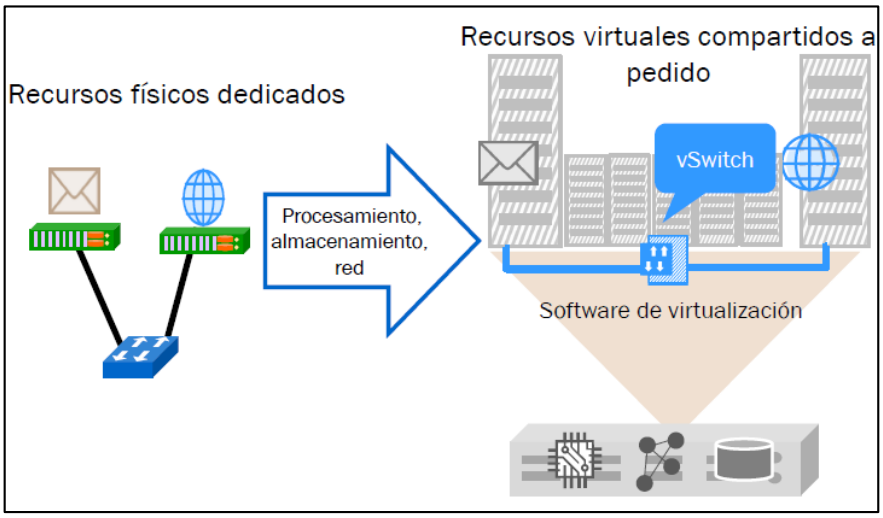


Fuente: *NFV y otras tecnologías.* https://builders.intel.com/university/networkbuilders/course. Consulta: abril de 2019.

3.2. Máquinas virtuales y su aplicación para infraestructuras en la nube

En la figura 21 se muestran dos servidores y un conmutador de datos conectados entre sí a través de un conmutador, uno de los servidores está ejecutando un servicio de correo electrónico y el otro un servicio web, todos los equipos ejecutan su propia función y es posible que no utilicen el máximo de sus capacidades, sin embargo son considerados como equipos dedicados, utilizando un software adicional de virtualización es posible unir las tres funcionalidades en un solo hardware tomando varios servicios y compartirlos en un servidor virtual.

Figura 21. **Recursos físicos dedicados vs recursos virtuales compartidos**

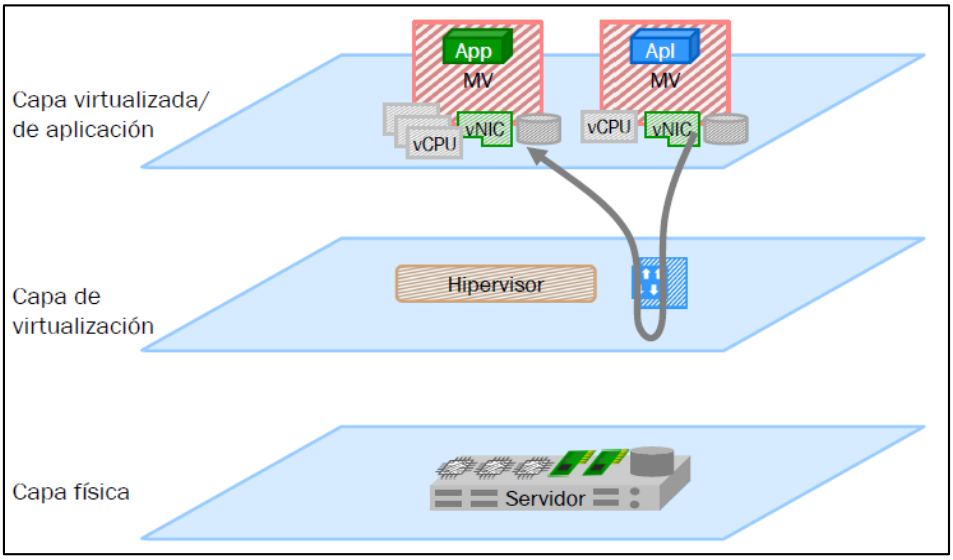


Fuente: *Físicos versus virtuales.* https://builders.intel.com/university/networkbuilders/course. Consulta: abril de 2019.

Una vez activado este software de virtualización se podrán tomar varios servicios, moverlos al software y compartirlos en un servidor individual, de hecho, se puede hacer esto con más de dos elementos, permitiendo una mayor agrupación. En la figura 22 se ilustra el esquema utilizado para la virtualización, el cual es descrito a continuación:

- Capa física: define al servidor físico según sus las características de sus recursos informáticos, así como de su sistema operativo.
- Capa de virtualización: es implementada por medio del hipervisor y el vSwitch, de forma posterior al completar el montaje de un sistema operativo en el servidor físico.
- Capa de virtualización de aplicación: considerada la capa donde se implementan las máquinas virtuales con todos sus complementos para su correcto funcionamiento.

Figura 22. **Esquema de redes virtualizadas**



Fuente: elaboración propia.

3.2.1. Capa física

El servidor físico debe poseer los recursos informáticos fundamentales para un proceso de virtualización, dado que estos serán distribuidos entre las máquinas virtuales que sean configuradas, estos recursos informáticos son:

- Procesador: el cual debe poseer la velocidad de procesamiento, la cantidad de núcleos y la disposición para soportar tecnología de virtualización.
- Memoria RAM: la cual debe seleccionarse según el sistema operativo y aplicación que se desplegará en las máquinas virtuales, dado que la correcta distribución de este recurso define el funcionamiento óptimo de las funciones requeridas.
- Almacenamiento: dado que las máquinas virtuales utilizan archivos que tienen la función de contenedor, estos archivos requieren el mismo espacio de almacenamiento en el disco duro físico que el que se asigna al configurar la máquina virtual.
- Recursos de red: describe la cantidad de interfaces de red físicas y funciones configurables para manejar el acceso a las máquinas virtuales a través de redes IP.

El proceso de virtualización permite implementar cualquier tipo de sistema operativo que se necesite, sin embargo debe considerarse los siguientes términos:

- Sistema operativo *host,* el cual define el sistema operativo aplicado al servidor físico que albergará las máquinas virtuales.
- Sistema operativo *guest,* el cual define el sistema operativo aplicado a las máquinas virtuales que se van a implementar sobre el servidor físico.

Tanto para el sistema operativo *host* como *guest* la principal característica es el aislamiento de sus funciones, donde cada máquina virtual pasa a considerarse de forma completamente independiente, por lo que la aplicación del sistema operativo tanto en el *host* como en el *guest* es determinada por la aplicación que deba implementarse en la máquina virtual.

3.2.2. Capa de virtualización

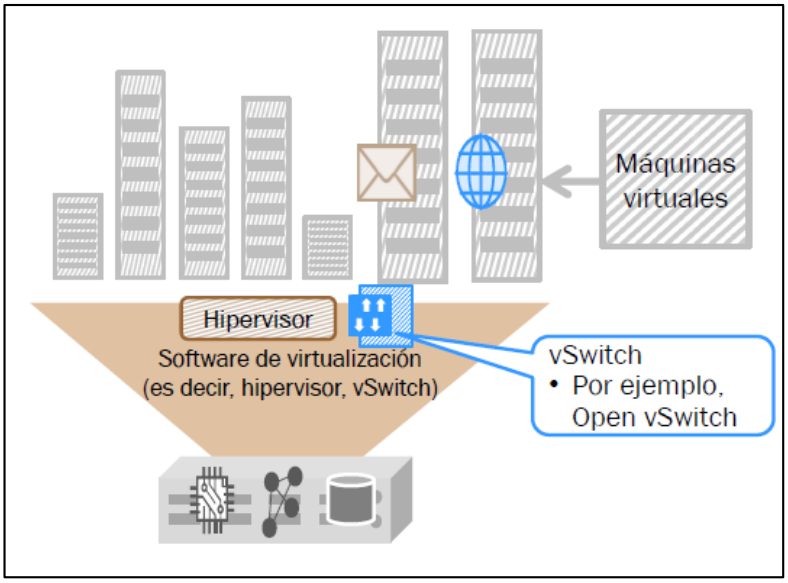
La capa de virtualización consta de dos componentes clave, los cuales son:

- Hipervisor, el cual trata al servidor físico como un recurso agrupado para proporcionar al administrador la libertad de gestionar y compartir el total de recursos con las máquinas virtuales implementadas.

- vSwitch, el cual permite la conectividad entre las máquinas virtuales y con el servidor físico y desde las máquinas virtuales hacia fuera del servidor físico.

En la figura 23 pueden verse las características de un proceso de virtualización.

Figura 23. **Virtualización (Hipervisor + vSwicht)**



Fuente: Virtualización. https://builders.intel.com/university/networkbuilders/course. Consulta: abril de 2019.

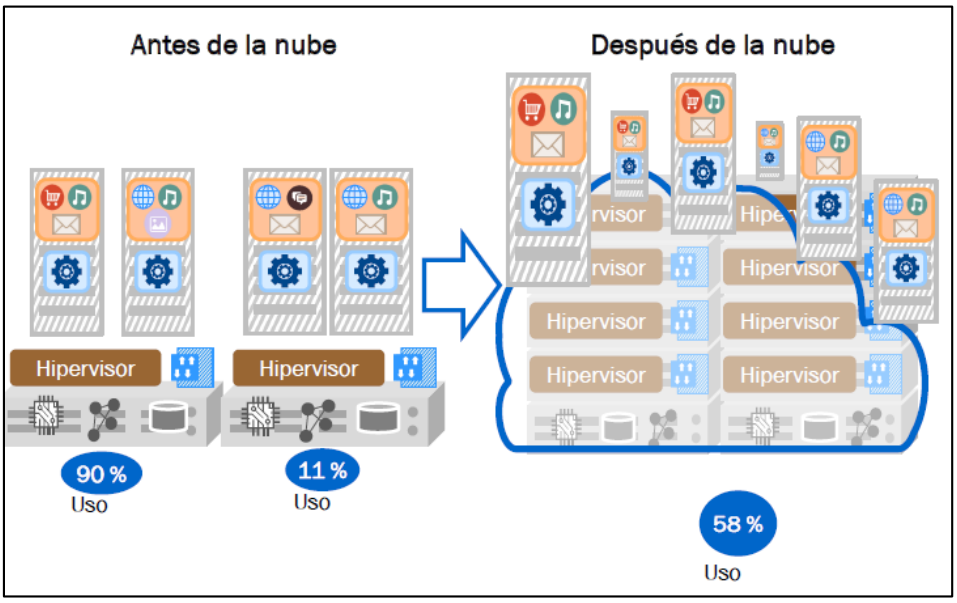
El hardware posee una interfaz de red física por la que ingresan los paquetes destinados a las máquinas virtuales, los cuales son procesados por la interfaz de red del vSwitch que posteriormente decidirá en qué máquina virtual es necesario que se reciba, este vSwitch puede considerarse como una versión actualizad de un conmutador físico, en contraste el hipervisior se implementa en cada servidor físico de tal manera que pueda compartirse entre varias máquinas virtuales.

Por lo tanto, el proceso de virtualización proporciona a las máquinas virtuales una unidad de procesamiento virtual conocida como VCPU con una cantidad de recursos asignados en la capa de virtualización por el hipervisor desde la unidad central de procesamiento del servidor físico, de forma análoga también es asignado el almacenamiento y la cantidad de memoria RAM para la máquina virtual, de forma adicional se asocia una interfaz de red virtual conocida como vNIC proporcionando una comunicación mediante el direccionamiento IP o con conectividad de capa 2.

3.2.3. Funcionalidades en una infraestructura de nube

Las funciones del hipervisor en una arquitectura de nube incluyen la de asignar recursos como CPU y almacenamiento, además de supervisar el estado de las máquinas virtuales, por lo tanto, este puede tomar decisiones en caso de fallas, bloqueos o excesivo uso de recursos, así como en la migración de máquinas virtuales dentro del sistema, estas actividades realizadas por el hipervisor son muy importantes dado que proporciona los mecanismos para administrar los servicios en una nube.

Figura 24. **Virtualización y nube**



Fuente: elaboración propia.

En la figura 24 se tiene un servidor con un 90 % de utilización y otro con 11% de uso, lo cual representa un inconveniente para la distribución de recursos, por lo que virtualizar resolvería el problema, sin embargo un proceso manual para 10, 50, 100, 500 servidores se convierte en una tarea difícil de completar, por lo tanto herramientas como el hipervisor y vSwitch agrupan los recursos en una pila de recursos permitiendo que de forma dinámica se realice la asignación de una máquina virtual y equilibrando la utilización media de toda la red.

3.3. Otras técnicas de virtualización y su aplicación para infraestructuras en la nube

El modelo de virtualización con máquinas virtuales implementadas sobre un servidor físico es considerado como la técnica tradicional para la virtualización de aplicaciones, dado que la aplicación se ejecuta en un sistema operativo

virtualizado donde convive con otros aplicativos, sin embargo también es posible utilizar métodos conocidos como virtualización liviana o contenedor, el cual crea la percepción de un ambiente aislado exclusivo para la aplicación de forma que exista un único sistema operativo para varios contenedores.

3.3.1. Contenedores virtuales

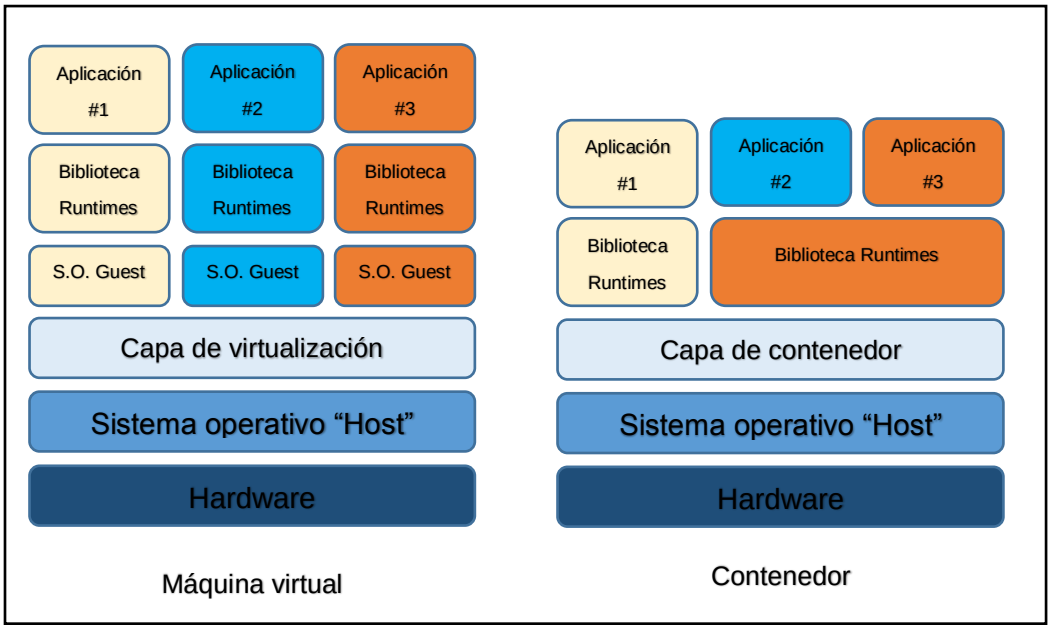
En comparación con las máquinas virtuales tradicionales, brindan mayor nivel de portabilidad y menos exigencias a nivel de recursos para el servidor físico, ya que desde el punto de vista del sistema operativo su funcionalidad simplemente es como un proceso que almacena la aplicación a ejecutarse y todas sus dependencias, proporcionando el acceso únicamente al sistema de ficheros virtuales del contenedor. En la figura 25 se ilustra la comparación entre el esquema de virtualización por medio de máquinas virtuales y el utilizado por contenedores virtuales, el cual consta de lo siguiente:

- Capa física: define al servidor físico según las características de sus recursos informáticos, así como de su sistema operativo.

- Capa de contenedor: es implementada por medio del software llamado Docker, el cual gestiona los contenedores con las aplicaciones requeridas.

- Capa de virtualización de aplicaciones: elimina la necesidad de un sistema operativo *guest* dado que la capa de contenedores genera imágenes que se reutilizan para que las aplicaciones puedan compartir recursos.

Figura 25. **Esquema para máquinas virtuales y contenedores virtuales**



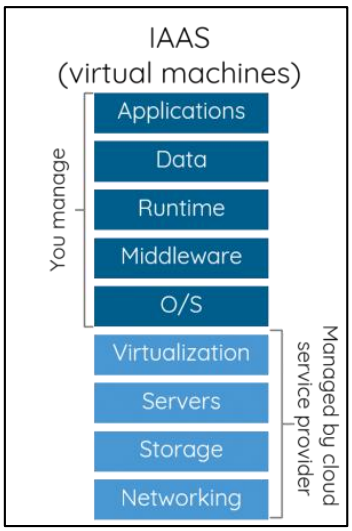
Fuente: elaboración propia, empleando programa Microsoft Office, con base en: ALARCÓN, José Manuel. *¿Qué diferencia hay entre Docker y máquinas virtuales?* Consulta: abril de 2019.

La compatibilidad de aplicaciones que pueden implementarse en los contenedores virtuales depende del sistema operativo *host,* por ejemplo, no es posible ejecutar un contenedor con aplicación para Linux en Windows y viceversa.

3.3.2. OpenStack

Es una solución orientada a la nube del tipo infraestructura como un servicio en la nube IaaS, el cual utiliza un conjunto uniforme de interfaces de programación de aplicaciones (API) para extraer recursos virtuales y dividirlos en conjuntos separados que se utilizan para potenciar las herramientas de computación en la nube estándar con las cuales los administradores y los usuarios interactuarán directamente, en la figura 26 se ilustra el modelo IaaS.

Figura 26. **Modelo IaaS para computación en la nube**



Fuente: *Modelo IaaS.* http://cloudonmove.com/iaas-paas-saas-what-do-they-mean/. Consulta: abril de 2019.

El esquema de funcionamiento utilizado por *OpenStack* utiliza los siguientes componentes básicos:

- *Horizon dashboard*, provee la interfaz a los usuarios finales y a los administradores de los servicios aplicados.
- *Nova compute*, es el componente encargado de transformar imágenes y metadatos en máquinas virtuales según las solicitudes de los usuarios.
- *Neutron network*, provee redes virtuales como servicios entre dispositivos administrados por *OpenStack*, así como máquinas virtuales creadas por Nova.
- *Cinder block storage*, provee el almacenamiento para las máquinas virtuales alojadas en la nube.
- *Glance image*, provee un repositorio para las imágenes.
- *Swift object store*, provee almacenamiento de objetos.

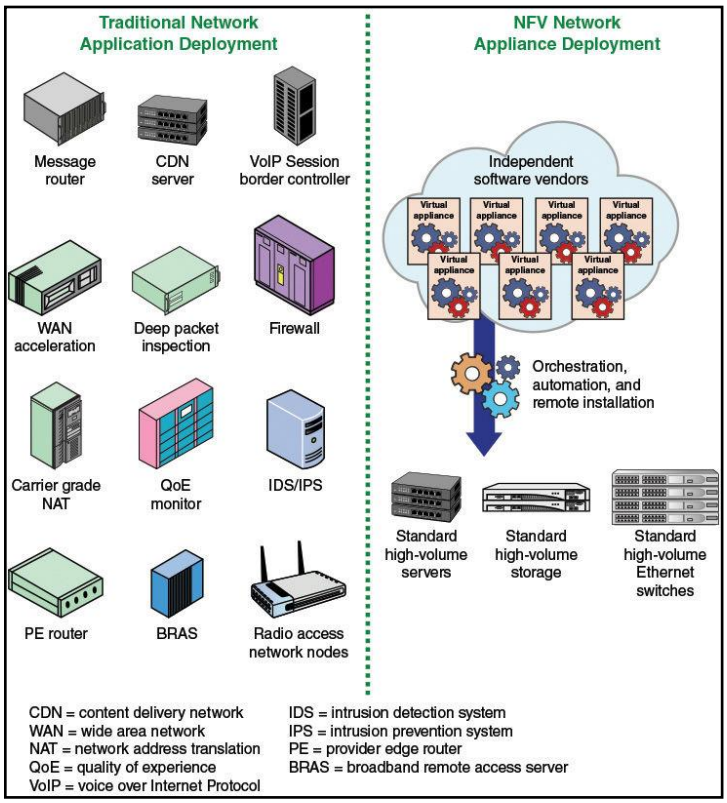
- *Keystone identity*, provee autenticación y autorización para todos los servicios de *OpenStack*.

3.4. NFV: despliegue de principales funciones de red

Los dispositivos de red que el servidor de productos y el software buscan reemplazar pueden variar desde *firewall,* BRAS, conmutadores e inclusive enrutadores, sin embargo el enfoque para NFV incluye elementos de *switching,* dispositivos de red, servicios de red y aplicaciones. Teniendo en cuenta la descripción del libro blanco, a continuación se listan algunas funciones de red que pueden considerarse para NFV:

- Elementos de *switching* como Broadband Remote Access Server (BRAS) o Broadband Network Gateway (BNG), Carrier Grade NAT y *routers.*
- Elementos de la red móvil, como (HLR/HSS), (SGSN/MME), (GGSN/PDN-GW), RNC, NodeB y eNB.
- Elementos finales de casa, como CPE y Set Top Boxes.
- Elementos de análisis de tráfico como DPI.
- Elementos de monitoreo y de diagnóstico, como SLA.
- Elementos de señalización de nueva generación como IMS y SBC.
- Funciones convergentes de la red como servidores de AAA.
- Optimización a nivel de aplicación, incluyendo CDN, servidores cachés, balanceadores de carga y acelerador de aplicaciones.
- Funciones de seguridad, como *firewalls,* IPS y SPAM.

Figura 27. **Despliegue de principales funciones de red en NFV**



Fuente: Foundations of Modern Networking. *SDN, NFV, QoE, IoT, and Cloud.Chapter 7. Network Functions Virtualization.* Consulta: abril de 2019.

En la figura 27 se ilustran las funciones principales que pueden ejecutarse en hardware de informática estándar de una manera virtualizada, ya que además de reducir los costos mediante el uso de equipos genéricos (cargados con las compilaciones específicas del proveedor) y la automatización, los proveedores de servicios también obtienen la elasticidad de los recursos de la nube, garantizando que la capacidad de red necesaria esté disponible para el uso de aplicaciones.

Teniendo en cuenta la lista anterior, los casos de uso de NFV pueden cubrir la red Core / Edge para una red IP/MPLS de un proveedor se servicio, abarcando

el entorno doméstico, redes de distribución de contenido, estación base móvil, controladores LAN inalámbricos, equipos para clientes (CPE) y sistemas de servicios operativos (OSS).

4. APLICACIÓN DE ARQUITECTURA SDN Y NFV PARA PROVEEDORES DE SERVICIO

Dado que el ritmo de los servicios solicitados por los usuarios de la red cambia con mucha rapidez, una de las principales necesidades de un proveedor de servicios es cubrir con agilidad los cambios que la red requiera para obtener un mayor beneficio económico, esta agilidad que demanda el mercado se logra utilizando arquitecturas basadas en SDN y NFV que proporcionan la flexibilidad y agilidad deseadas, sin embargo debe tenerse en cuenta que la implementación de estas arquitecturas requiere un análisis que reduzca y optimice los costos, dado que los de las plataformas que se utilizan para brindar el transporte de los datos en una red de un proveedor de servicios suelen ser muy elevados.

4.1. Consideraciones importantes para implementación de SDN y NFV

Para una implementación de una arquitectura de red SDN / NFV se deben tener en cuenta los siguientes aspectos:

- Reducción de costos durante la ejecución e incrementar los ingresos a través del servicio prestado a los usuarios.

- Interoperabilidad que permita a la red existente una correcta operación con redes SDN / NFV, de forma que puedan ser aprovechadas todas las ventajas del servicio, dado que no es posible remplazar todos los equipos con los que una red puede contar en el momento de la implementación.

- La escalabilidad y el desempeño que los controladores de SDN deben poseer para prestar la disponibilidad necesaria a la red en caso de problemas para que la comunicación y el control no se pierdan.

- El formato de instalación de nuevos equipos, dado que de forma tradicional un operador implementa un enrutador físico y lo configura iniciando sesión de forma remota, mientras que en redes SDN / NFV basta con conectarse al controlador para tener acceso total a la configuración de los equipos.

4.1.1. Adaptación de SDN en el mercado

Las implementaciones de SDN en redes WAN presentan una mayor aceleración para el año 2018 y se considera que existirá un crecimiento más significativo para el año 2020, estas implementaciones se adaptan al mercado de la siguiente manera:

- Tipo WAN: la cual permite hacer configuraciones de servicios en un ambiente multi-vendor en un mismo dominio, por ejemplo, en un ambiente MPLS, configura y orquesta servicios L2/L3 VPN, automatizando las configuraciones, minimizando errores humanos en dichas configuraciones y servicios, siendo esta una de las primeras implementaciones o versiones de SDN que se están implementando en la red a partir del año 2017.

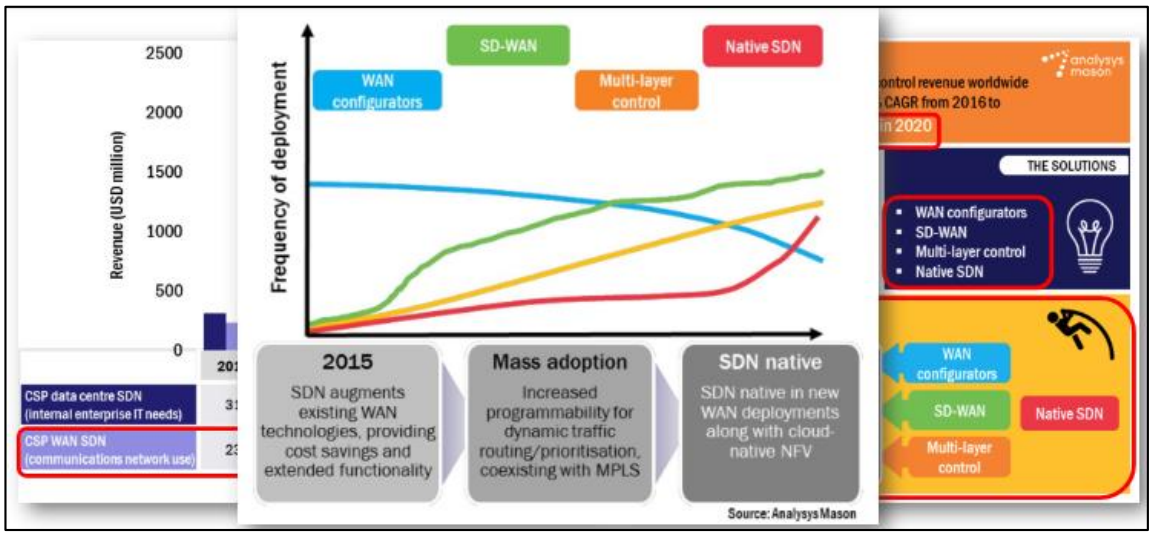
- Tipo SDN-WAN: la cual permite extender la red de paquetes a sitios donde el cliente / operador no tiene infraestructura propia, se basa en el uso de Internet para llegar a sus distintos sitios remotos y optimizar la entrega de aplicaciones a través de la red.

- Tipo control multicapas: donde se logra una integración entre la capa de control y la capa óptica para optimizar el Capex de la red.

- Tipo SDN nativo: la cual describe una red con equipos en hardware básico y abierto, donde todas las funcionalidades están en la nube.

Dado que estas implementaciones no se realizan en un ambiente homogéneo ideal, cualquier nueva red SDN / NFV debe coexistir con la infraestructura y arquitectura actual de la red, en la figura 28 se ilustra la adaptación de estas implementaciones SDN / NFV al mercado.

Figura 28. **Adaptación de SDN al mercado de las telecomunicaciones**



Fuente: Maison. *Adopción de la tecnología* . http://www.analysysmason.com/. Consulta: abril de 2019.

4.2. Propuesta de solución SDN / NFV

Según los requisitos solicitados por los proveedores de servicios se establecieron las siguientes características para el diseño de una arquitectura SDN / NFV:

- Innovación y economía: ahorros sustanciales de CAPEX y OPEX, dimensionando las capacidades de hardware de por lo menos cinco años a futuro, reemplazando solo aquellas plataformas que no soporten SDN / NFV.
- Estabilidad y agilidad de ejecución: continuidad de procesos IP existentes y migración transparente.
- Escalabilidad: capacidades de transporte, planificación automatizada de crecimiento y premisas de diseño basadas en KPI.
- Red inteligente: automatización y orquestación de procesos multicapa (IP + óptica), monitoreo analítico en tiempo real (telemetría).

Adicional un diseño innovador de la red IP contempla las siguientes premisas de diseño:

- Plataformas y sistemas operativos de última generación.
- Simplificación de red a niveles de capas, topologías y protocolos.
- Gestión unificada IP y óptica.
- Interfaces programáticas abiertas.
- Cumplimiento de estándares de la industria de los protocolos y modelo de datos.
- Diseño basado en patrones de tráfico y optimización de la red en tiempo real.

4.2.1. Arquitectura y plataformas propuestas

Para el cumplimiento de las premisas de diseño evaluadas, es necesario que la solución SDN / NFV contemple una renovación tecnológica con alcances que logren cumplir dichos requisitos, dado que a todo nivel de red se requiere realizar cambios, a continuación se muestran los principales alcances que se deben tomar en cuenta para una renovación tecnológica para cada nivel de red:

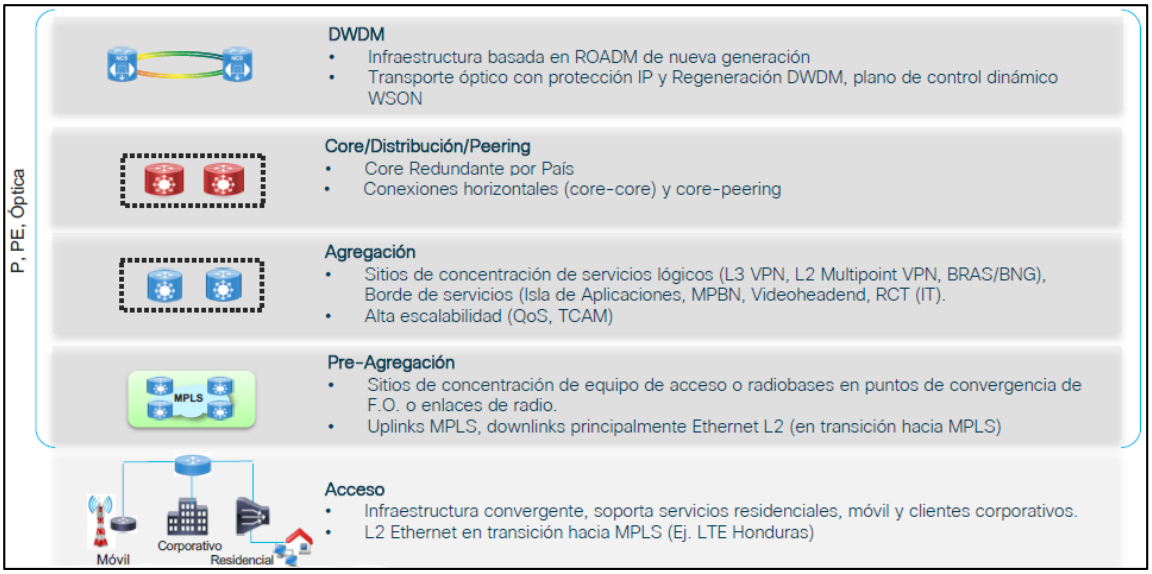
- Capa física para enlace de larga distancia (DWDM): proporciona redes de gran capacidad en fibra óptica, lo cual permite una evolución flexible y económica para responder a las demandas de mayor ancho de banda por parte de los nuevos servicios multimedia, para el presente diseño se propone una infraestructura DWDM para el área rural de la cobertura del proveedor de servicios, con infraestructura basada en ROADM de nueva generación, lo cual significa que un nodo puede concentrar varias direcciones a través de demandas, utilizando un par de hilos de fibra óptica puede direccionarse a varios lados, permitiendo formar una topología de red IP, optimizando el medio físico.

- Núcleo y distribución: conecta redes de distribución geográficamente dispersas y proporciona acceso a otras redes que no forman parte de su dominio, hacia Internet o Peering.

- Acceso: típicamente una red de acceso es una red de área local (LAN) o una red para clientes corporativos, o clientes internos, típicamente se conectan a nivel de Ethernet y en algunos casos se utilizan enrutadores IP que proporcionan conectividad entre conmutadores a nivel de capa 3.

En la figura 29 se muestran los alcances a diferentes niveles de capas de red, que manejan los proveedores de servicios:

Figura 29. **Alcances de arquitectura por capas de red**

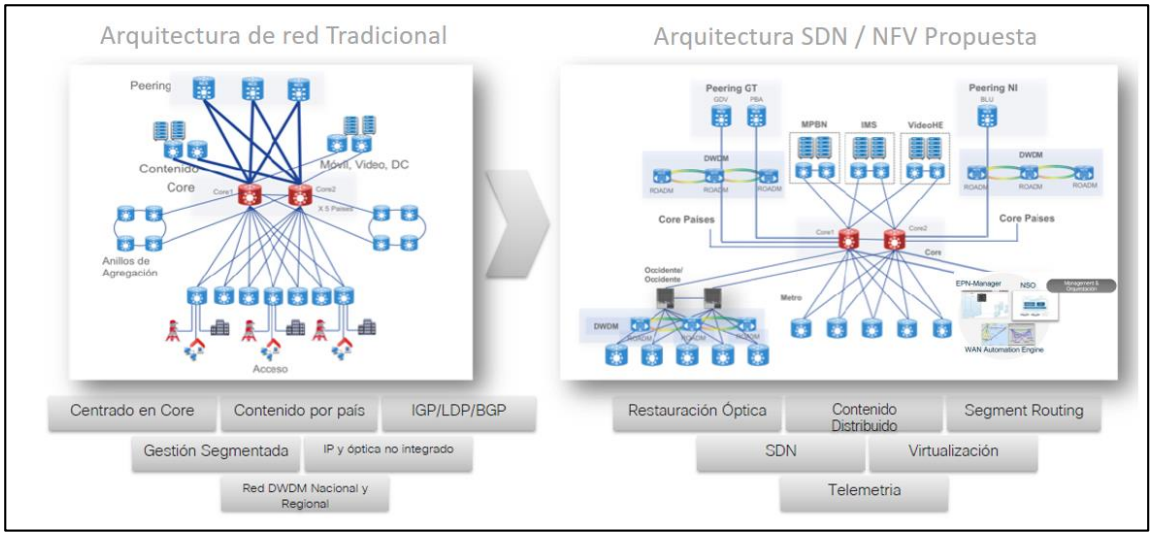


Fuente: elaboración propia.

En la figura 30 se ve la arquitectura SDN / NFV propuesta, con las siguientes características:

- Topología Hub & Spoke, con plano de control simplificado utilizando SDN.
- Red unificada con capacidad dimensionada para 5 años.
- Automatización y orquestación de procesos multicapa IP y óptica.
- Reemplazo de plataformas obsoletas.
- Reducción en tiempo de aprovisionamiento y cambios para configuración de servicios L3VPN.
- Simplificación de enrutamiento por medio de tecnología Segment Routing.

Figura 30. **Diagrama de arquitectura SDN / NFV propuesta**



Fuente: elaboración propia.

4.3. Caso práctico de aplicación NFV y estimación económica

Los proveedores de servicios y las empresas de todo el mundo confían en el Border Gateway Protocol (BGP) como parte integral en el despliegue de servicios para ofrecer Internet a los usuarios, así como Internet Peering, servicios VPN de capa 2 / capa 3, MVPN, entre otros. BGP ofrece la robustez, estabilidad y flexibilidad que otras tecnologías futuras utilizan para el transporte *loop-free* de información dentro del sistema autónomo (AS) y a través de otros AS.

El despliegue de BGP tiene algunas implicaciones y consideraciones importantes, ya que es necesario un *full-mesh* de vecinos iBGP para asegurar una red estable y operando apropiadamente, permitiendo el conocimiento de todos los caminos en el plano de control, esto plantea un problema de escalabilidad significativo especialmente cuando el número de nodos iBGP aumenta.

Para abordar este problema de escalabilidad, el uso de *route reflectors* (RR) (RFC 4456) en la red es una de las soluciones que se pueden utilizar para reducir el número total de sesiones BGP en la red, donde el despliegue de un *route reflector* puede hacerse utilizando enrutadores dedicados o no dedicados, sin embargo la utilización de un RR dedicado tiene una mejor estabilidad, escalabilidad y convergencia.

Los RR dedicados, a menudo también llamados RR *off-path* o RR *on-a-stick*, requieren alta demanda de recursos de CPU para el cálculo de rutas y una memoria amplia para almacenar todas las rutas aprendidas, el ancho de banda es un factor clave para la comunicación de las actualizaciones de la ruta BGP, sin embargo el rendimiento en los nodos RR en este caso no es considerado crítico, ya que no están en la ruta de reenvío.

4.3.1. Virtualización de router reflector

Un *virtual route reflector* (vRR) es una excelente solución para aplicaciones dedicadas de RR *off-path*, con el fin de poder cumplir con los altos requerimientos de CPU y memoria, estos recursos pueden ser asignados y manejados de una forma muy flexible al momento de la creación de las máquinas virtuales asociadas a los servicios de *virtual route reflectors* (vRR).

Una consideración importante en los centros de datos es el consumo de energía y recursos de refrigeración, la implementación de NFV logra ahorrar y optimizar el consumo de estos recursos, ya que al aumentar el número de instancias vRR no aumenta el consumo de energía de forma significativa, ya que los componentes físicos comunes como los ventiladores o procesadores siguen siendo los mismos, posicionar el vRR dentro de un centro de datos o nodo centralizado con alto nivel de disponibilidad aún permite una ubicación lógica en

aquellas localidades que se consideran más útiles para la arquitectura de enrutamiento del cliente.

La solución propuesta consiste en la instalación de dos servidores Cisco UCS Blade Server 5108 que serán conectados a los equipos del núcleo del proveedor de servicio utilizando enlaces de 10G, donde cada uno de los UCS Blade Server 5108 cuentan con un UCSB B200 M4 en el cual se virtualizan dos enrutadores ASR 9001-S con las siguientes funciones:

- El primero realizará las funciones de un vRR de IPv6
- El segundo realizará las funciones de un vRR de VPNv6

Se toman dos nodos en distintas ubicaciones para una implementación redundante y se considera el despliegue de NFV de vRR para los servicios de 6PE/6vPE, en cada una de las localidades es necesario implementar dos máquinas virtuales con el software IOS XRv 9000 soportando los servicios de VRR para 6PE y 6vPE, en la tabla II se muestra una estimación económica para la implementación de un vRR IPv6 y un vRR VPNv6 para el sitio A.

Tabla II. **Estimación económica para implementar vRR IPv6 / VPNv6 en sitio A**

No. parte	Descripción	Precio de lista por unidad (Q)	Cantidad	Precio neto por unidad (Q)	% descuento	Precio total (Q)
R-IOSXRV9000-IMG	Cisco IOS XRv 9000 Software	0,00	2	0,00	74,00	0,00
R-VROUTER-IMG	IOS XRv 9000 Software Production Images	0,00	2	0,00	74,00	0,00

Continuación de la tabla II.

R-XRV9000-5.4.0	**IOS XRv 9000 Software Production Images for v5.4.0**	**0,00**	**2**	**0,00**	**74,00**	**0,00**
S-XRV9000-VRR-1M	IOS XRv 9000 License for vRR functionality with 1m Route	10 000,00	2	2 600,00	74,00	5 200,00
S-XRV-ROUTE-T1	IOS XRv 9000 vRR scale license for upto 4m Route	10 000,00	2	2 600,00	74,00	5 200,00
UCS-MINI-Z0001	Cisco Unified Computing System	0,00	1	0,00	60,00	0,00
UCSB-5108-DC2	UCS 5108 Blade Server DC2 Chassis/0 PSU/8 fans/0 FEX	6 999,00	1	2 799,60	60,00	2 799,60
N20-CBLKP	Power supply unit blanking panel for UCS 5108	0,00	2	0,00	60,00	0,00
N20-FW014	UCS 5108 Blade Chassis FW Package 3.1	0,00	1	0,00	60,00	0,00
UCSB-PWRM-DC48	48V DC Power Input Module for UCS 5108	0,00	1	0,00	60,00	0,00
N20-FAN5	**Fan module for UCS 5108**	**0,00**	**8**	**0,00**	**60,00**	**0,00**
N20-CBLKB1	Blade slot blanking panel for UCS 5108/single slot	0,00	7	0,00	60,00	0,00
UCSB-5108-PKG-HW	**UCS 5108 Packaging for chassis with half width blades.**	**0,00**	**1**	**0,00**	**60,00**	**0,00**
N20-CAK	Accessory kit for UCS 5108 Blade Server Chassis	0,00	1	0,00	60,00	0,00
N20-CBLKI	Fabric extender slot blanking panel for UCS 5108	0,00	1	0,00	60,00	0,00
UCSB-B200-M4	UCS B200 M4 w/o CPU, mem, drive bays, HDD, mezz	2 995,00	1	1 198,00	60,00	1 198,00

Continuación de la tabla II.

UCS-CPU-E52683E	**2.10 GHz E5-2683 v4/120W 16C/40MB Cache/DDR4 2400MHz**	**5 559,00**	**2**	**2 223,60**	**60,00**	**4 447,20**
UCS-MR-1X322RV-A	32GB DDR4-2400-MHz RDIMM/PC4-19200/dual rank/x4/1.2v	1 100,00	4	440,00	60,00	1 760,00
UCSB-MRAID12G	Cisco FlexStorage 12G SAS RAID controller with Drive bays	749,00	1	299,60	60,00	299,60
UCS-HD900G10K12G	900GB 12G SAS 10K RPM SFF HDD	1 367,00	2	546,80	60,00	1 093,60
UCSB-MLOM-40G-01	Cisco UCS VIC 1240 modular LOM for blade servers	1 499,00	1	599,60	60,00	599,60
UCS-M4-V4-LBL	Cisco M4 - v4 CPU asset tab ID label (Auto-Expand)	0,00	1	0,00	60,00	0,00
UCSB-HS-EP-M4-R	CPU Heat Sink for UCS B200 M4/B420 M4 (Rear)	0,00	1	0,00	60,00	0,00
UCSB-HS-EP-M4-F	**CPU Heat Sink for UCS B200 M4/B420 M4 (Front)**	**0,00**	**1**	**0,00**	**60,00**	**0,00**
C1UCS-OPT-OUT	Cisco ONE Data Center Compute Opt Out Option	0,00	1	0,00	60,00	0,00
VMW-VSP-EPL-1A	**VMware vSphere 6 Ent Plus (1 CPU), 1-yr, Support Required**	**5 825,00**	**2**	**2 330,00**	**60,00**	**4 660,00**
UCSB-PSU-2500DC48	2500W -48V DC Power Supply for UCS 5108	2 999,00	2	1 199,60	60,00	2 399,20
UCS-FI-M-6324	UCS 6324 In-Chassis FI with 4 UP, 1x40G Exp Port, 16 10Gb	22 000,00	1	8 800,00	60,00	8 800,00
N10-MGT014	UCS Manager v3.1	0,00	1	0,00	60,00	0,00
SFP-GE-T	1000BASE-T SFP (NEBS 3 ESD)	440,00	1	114,40	74,00	114,40

Continuación de la tabla II.

SFP-10G-LR-X=	10GBASE-LR SFP Module for Extended Temp range	4 195,00	2	1 090,70	74,00	2 181,40
					TOTAL	40 752,60

Fuente: elaboración propia.

En la tabla III se muestra una estimación económica para la implementación de un vRR IPv6 y un vRR VPNv6 para el sitio B.

Tabla III. **Estimación económica para implementar vRR IPv6 / VPNv6 en sitio B**

No. parte	Descripción	Precio de lista por unidad (Q)	Cantidad	Precio neto por unidad (Q)	% descuento	Precio total (Q)
R-IOSXRV9000-IMG	Cisco IOS XRv 9000 Software	0,00	2	0,00	74,00	0,00
R-VROUTER-IMG	IOS XRv 9000 Software Production Images	0,00	2	0,00	74,00	0,00
R-XRV9000-5.4.0	**IOS XRv 9000 Software Production Images for v5.4.0**	**0,00**	**2**	**0,00**	**74,00**	**0,00**
S-XRV9000-VRR-1M	IOS XRv 9000 License for vRR functionality witth 1m Route	10 000,00	2	2 600,00	74,00	5 200,00
S-XRV-ROUTE-T1	IOS XRv 9000 vRR scale license for upto 4m Route	10 000,00	2	2 600,00	74,00	5 200,00
UCS-MINI-Z0001	Cisco Unified Computing System	0,00	1	0,00	60,00	0,00
UCSB-5108-DC2	UCS 5108 Blade Server DC2 Chassis/0 PSU/8 fans/0 FEX	6 999,00	1	2 799,60	60,00	2 799,60

Continuación de la tabla III.

N20-CBLKP	Power supply unit blanking panel for UCS 5108	0,00	2	0,00	60,00	0,00
N20-FW014	UCS 5108 Blade Chassis FW Package 3.1	0,00	1	0,00	60,00	0,00
UCSB-PWRM-DC48	48V DC Power Input Module for UCS 5108	0,00	1	0,00	60,00	0,00
N20-FAN5	Fan module for UCS 5108	0,00	8	0,00	60,00	0,00
N20-CBLKB1	Blade slot blanking panel for UCS 5108/single slot	0,00	7	0,00	60,00	0,00
UCSB-5108-PKG-HW	**UCS 5108 Packaging for chassis with half width blades.**	**0,00**	**1**	**0,00**	**60,00**	**0,00**
N20-CAK	Accessory kit for UCS 5108 Blade Server Chassis	0,00	1	0,00	60,00	0,00
N20-CBLKI	Fabric extender slot blanking panel for UCS 5108	0,00	1	0,00	60,00	0,00
UCSB-B200-M4	UCS B200 M4 w/o CPU, mem, drive bays, HDD, mezz	2 995,00	1	1 198,00	60,00	1 198,00
UCS-CPU-E52683E	**2.10 GHz E5-2683 v4/120W 16C/40MB Cache/DDR4 2400MHz**	**5 559,00**	**2**	**2 223,60**	**60,00**	**4 447,20**
UCS-MR-1X322RV-A	32GB DDR4-2400-MHz RDIMM/PC4-19200/dual rank/x4/1.2v	1 100,00	4	440,00	60,00	1 760,00
UCSB-MRAID12G	Cisco FlexStorage 12G SAS RAID controller with Drive bays	749,00	1	299,60	60,00	299,60
UCS-HD900G10K12G	900GB 12G SAS 10K RPM SFF HDD	1 367,00	2	546,80	60,00	1 093,60
UCSB-MLOM-40G-01	Cisco UCS VIC 1240 modular LOM for blade servers	1 499,00	1	599,60	60,00	599,60

Continuación de la tabla III.

UCS-M4-V4-LBL	Cisco M4 - v4 CPU asset tab ID label (Auto-Expand)	0,00	1	0,00	60,00	0,00
UCSB-HS-EP-M4-R	CPU Heat Sink for UCS B200 M4/B420 M4 (Rear)	0,00	1	0,00	60,00	0,00
UCSB-HS-EP-M4-F	CPU Heat Sink for UCS B200 M4/B420 M4 (Front)	0,00	1	0,00	60,00	0,00
C1UCS-OPT-OUT	Cisco ONE Data Center Compute Opt Out Option	0,00	1	0,00	60,00	0,00
VMW-VSP-EPL-1A	**VMware vSphere 6 Ent Plus (1 CPU), 1-yr, Support Required**	**5 825,00**	**2**	**2 330,00**	**60,00**	**4 660,00**
UCSB-PSU-2500DC48	2500W -48V DC Power Supply for UCS 5108	2 999,00	2	1 199,60	60,00	2 399,20
UCS-FI-M-6324	UCS 6324 In-Chassis FI with 4 UP, 1x40G Exp Port, 16 10Gb	22 000,00	1	8 800,00	60,00	8 800,00
N10-MGT014	UCS Manager v3.1	0,00	1	0,00	60,00	0,00
SFP-GE-T	1000BASE-T SFP (NEBS 3 ESD)	440,00	1	114,40	74,00	114,40
SFP-10G-LR-X=	**10GBASE-LR SFP Module for Extended Temp range**	**4 195,00**	**2**	**1 090,70**	**74,00**	**2 181,40**
					TOTAL	40 752,60

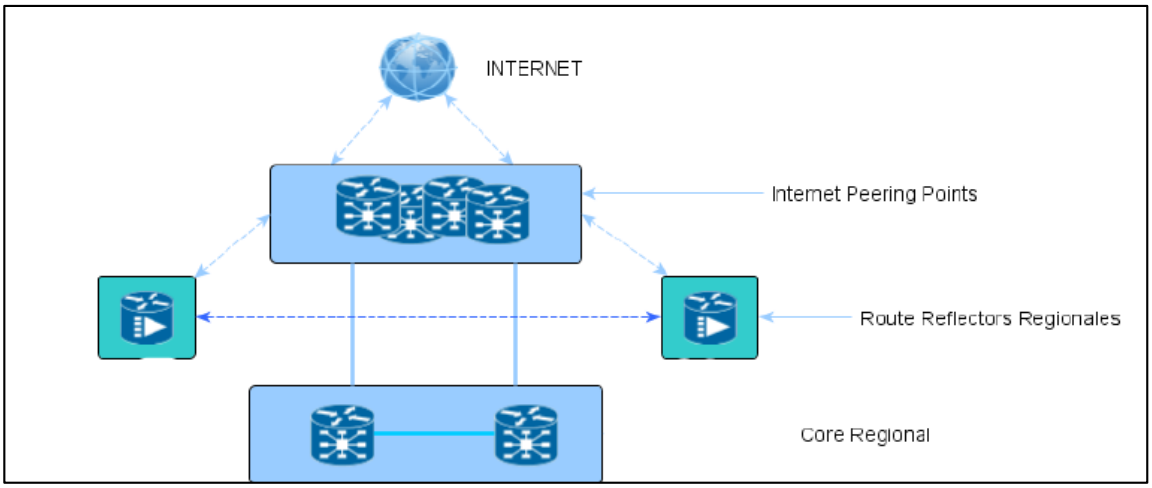
Fuente: elaboración propia.

Cada uno de los vRR tiene funciones específicas para soportar diferentes servicios, en el caso de los vRR de IPv6 intercambian información de enrutamiento IPv6 con los RR regionales de IPv6 y los equipos locales que tengan el requerimiento de establecer soluciones de 6PE.

Los vRR que se implementan para VPNv6 estarán a cargo del intercambio de información de enrutamiento VPNv6 con los RR regionales VPNv6 y los equipos locales que tengan el requerimiento de establecer soluciones de 6VPE, además tiene sesiones iBGP IPv6 Labeled Unicast con los equipos regionales RR IPv6 ubicados en el núcleo del proveedor de servicios, por lo tanto, se cuenta con redundancia lógica por medio de dos sesiones hacia equipos ubicados en diferentes localidades.

En la figura 31 se observa el esquema lógico de conectividad de los vRR regionales y los Internet Peering Point (IPP) que a su vez tienen conectividad hacia la tabla Global de BGP de Internet.

Figura 31. **Esquema de conectividad lógica vRR IPv6**



Fuente: elaboración propia.

4.4. Caso práctico de aplicación SDN en la WAN y estimación económica

Utilizando la plataforma EPN que está diseñada para sistemas de gestión de elementos y redes, se puede proporcionar la gestión de elementos, resolución de fallas, monitoreo, métricas de desempeño, umbrales, alertas, activación y aprovisionamiento gráfico de servicios, topología multicapa (IP + óptica), además brinda seguridad para el acceso controlado basado en roles. En las tablas IV a VII se presenta la estimación económica para la implementación de SDN en la WAN utilizando la plataforma EPN.

Tabla IV. **Estimación económica para EPN Manager (EMS)**

No. parte	Descripción	Precio de lista por unidad (Q)	Cantidad	Precio neto por unidad (Q)	% descuento	Precio total (Q)
R-CISCO-2-EPNM-K9	Cisco Evolved Programmable Network Manager 2.X - Electronic	0,00	1	0,00	70,00	0,00
EPNM-2.1-PAK	Cisco Evolved Programmable Network Manager 2.1 Base App Lic	0,00	1	0,00	70,00	0,00
EPNM-2.1-K9	Cisco Evolved Programmable Network Manager 2.0 Base App	10 000,00	1	3 000,00	70,00	3 000,00
L-EPNM-2-SBY	Cisco EPN Manager 2.X - RedundancyLicense (LocalHA or GeoDR)	9 000,00	1	2 700,00	70,00	2 700,00
L-ASR9006-EPNM2RTM	Cisco EPN Manager 2 - Cisco ASR 9006 Right to Manage	8 800,00	76	2 640,00	70,00	200 640,00

Continuación de la tabla IV.

L-ASR9010-EPNM2RTM	Cisco EPN Manager 2 - Cisco ASR 9010 Right to Manage	20 800,00	0	6 240,00	70,00	0,00
L-NCS6008-EPNM2RTM	Cisco EPN Manager 2 - Cisco NCS 6008 Right to Manage	61 200,00	2	18 360,00	70,00	36 720,00
L-NCS2015-EPNM2RTM	Cisco EPN Manager 2 - Cisco NCS 2015 Right to Manage	29 900,00	76	8 970,00	70,00	681 720,00
L-NCS2006-EPNM2RTM	Cisco EPN Manager 2-Cisco NCS 2006/ONS1545-M6 RighttoManage	12 900,00	0	3 870,00	70,00	0,00
L-EPNM-2-NBI	Cisco EPN Manager 2.X - Northbound Interface	**50 000,00**	**1**	**15 000,00**	**70,00**	**15 000,00**
UCSC-C240-M4S2	UCS C240 M4 SFF 16 HD w/o CPU,mem,HD,PCIe,PS,railkt w/expndr	3 665,00	2	1 649,25	55,00	3 298,50
UCS-CPU-E52667D	3.20 GHz E5-2667 v3/135W 8C/20MB Cache/DDR4 2133MHz	6 264,00	4	2 818,80	55,00	11 275,20
UCS-ML-1X324RU-A	32GB DDR4-2133-MHz LRDIMM/PC4-17000/quad rank/x4/1.2v	2 200,00	8	990,00	55,00	7 920,00
UCS-HD2T7K12G	2 TB 12G SAS 7.2K RPM SFF HDD	2 379,00	2	1 070,55	55,00	2 141,10
UCS-SD960GBKS4-EV	960GB 2.5 inch Enterprise Value 6G SATA SSD	3 334,00	2	1 500,30	55,00	3 000,60

Continuación de la tabla IV.

UCSC-PSU2V2-1200W	1200W / 800W V2 AC Power Supply for 2U C-Series Servers	749,00	4	337,05	55,00	1 348,20
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	0,00	4	0,00	55,00	0,00
UCSC-RAILB-M4	Ball Bearing Rail Kit for C220 & C240 M4 & M5 rack servers	220,00	2	99,00	55,00	198,00
CIMC-LATEST	IMC SW (Recommended) latest release for C-Series Servers.	0,00	2	0,00	55,00	0,00
UCSC-HS-C240M4	**Heat sink for UCS C240 M4 rack servers**	**0,00**	**4**	**0,00**	**55,00**	**0,00**
UCSC-SCCBL240	Supercap cable 250mm	0,00	2	0,00	55,00	0,00
N20-BBLKD	UCS 2.5 inch HDD blanking panel	0,00	28	0,00	55,00	0,00
UCSC-MLOM-BLK	MLOM Blanking Panel	0,00	2	0,00	55,00	0,00
UCSC-MRAID12G-4GB	Cisco 12Gbps SAS 4GB FBWC Cache module (Raid 0/1/5/6)	1 967,00	2	885,15	55,00	1 770,30
UCSC-MRAID12G	Cisco 12G SAS Modular Raid Controller	656,00	2	295,20	55,00	590,40
C1UCS-OPT-OUT	Cisco ONE Data Center Compute Opt Out Option	0,00	2	0,00	55,00	0,00

Continuación de la tabla IV.

RHEL-2S2V-1A	Red Hat Enterprise Linux (1-2 CPU,1-2 VN); 1-Yr Support Req	0,00	2	0,00	55,00	0,00
					TOTAL	971 322,30

Fuente: elaboración propia.

Tabla V. **Estimación económica para WAN Automation (Controlador SDN)**

No. parte	Descripción	Precio de lista por unidad (Q)	Cantidad	Precio neto por unidad (Q)	% descuento	Precio total (Q)
WAN-AUTOMATION-E	WAN Automation Software, Perpetual Suite, Single Network	0,00	1	0,00	70,00	0,00
WAE-64-SW-K9	WAN Automation Software Package, Release 6.4	0,00	1	0,00	70,00	0,00
WAE-PP-SIM-PAKL	WAE Planning Premium Design 10 User Licenses, Perpetual	0,00	1	0,00	70,00	0,00
WAE-USERS-P	WAE Planning User PAK Licenses, Perpetual	0,00	1	0,00	70,00	0,00
WAE-SDN-PRM-T2	WAE Premium SDN Bundle, 500 - 999 nodes, Perpetual	11 614,00	154	3 484,20	70,00	536 566,80

Continuación de la tabla V.

UCSC-C240-M4S2	UCS C240 M4 SFF 16 HD w/o CPU,mem,HD,PCIe,PS,railkt w/expndr	3 665,00	2	1 649,25	55,00	3 298,50
UCS-CPU-E52667D	3.20 GHz E5-2667 v3/135W 8C/20MB Cache/DDR4 2133MHz	6 264,00	4	2 818,80	55,00	11 275,20
UCS-ML-1X324RU-A	32GB DDR4-2133-MHz LRDIMM/PC4-17000/quad rank/x4/1.2v	2 200,00	8	990,00	55,00	7 920,00
UCS-HD2T7K12G	2 TB 12G SAS 7.2K RPM SFF HDD	2 379,00	2	1 070,55	55,00	2 141,10
UCS-SD960GBKS4-EV	960GB 2.5 inch Enterprise Value 6G SATA SSD	3 334,00	2	1 500,30	55,00	3 000,60
UCSC-PSU2V2-1200W	1200W / 800W V2 AC Power Supply for 2U C-Series	749,00	4	337,05	55,00	1 348,20
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	0,00	4	0,00	55,00	0,00
UCSC-RAILB-M4	Ball Bearing Rail Kit for C220 & C240 M4 & M5 rack servers	220,00	2	99,00	55,00	198,00
CIMC-LATEST	IMC SW latest release for C-Series Servers.	0,00	2	0,00	55,00	0,00
UCSC-HS-C240M4	Heat sink for UCS C240 M4 rack servers	0,00	4	0,00	55,00	0,00
UCSC-SCCBL240	Supercap cable 250mm	0,00	2	0,00	55,00	0,00
N20-BBLKD	UCS 2.5 inch HDD blanking panel	0,00	28	0,00	55,00	0,00

Continuación de la tabla V.

UCSC-MLOM-BLK	MLOM Blanking Panel	0,00	2	0,00	55,00	0,00
UCSC-MRAID12G-4GB	Cisco 12Gbps SAS 4GB FBWC Cache module (Raid 0/1/5/6)	1 967,00	2	885,15	55,00	1 770,30
UCSC-MRAID12G	Cisco 12G SAS Modular Raid	656,00	2	295,20	55,00	590,40
C1UCS-OPT-OUT	Cisco ONE Data Center Compute Opt Out Option	0,00	2	0,00	55,00	0,00
RHEL-2S2V-1A	Red Hat Enterprise Linux (1-2 CPU,1-2 VN); 1	0,00	2	0,00	55,00	0,00
					TOTAL	568 109,10

Fuente: elaboración propia.

Tabla VI. **Estimación económica para orquestación de servicios**

No. parte	Descripción	Precio de lista por unidad (Q)	Cantidad	Precio neto por unidad (Q)	% descuento	Precio total (Q)
R-NSO-K9	Network Services Orchestrator 4.x (Top Level Ordering)	0,00	1	0,00	0,00	0,00
NSO-HA-LIC-P	NSO Standby Server license for Production Network	45 000,00	1	45 000,00	0,00	45 000,00
NSO-PNF-XL-SLIC-P	NSO RTM license for One XLarge Physical Network Element PNF	13 200,00	2	13 200,00	0,00	26 400,00
NSO-PNF-L-SLIC-P	NSO RTM license for One Large Physical Network Element PNF	3 600,00	0	3 600,00	0,00	0,00

Continuación de la tabla VI.

NSO-PNF-M-SLIC-P	NSO RTM license for One Medium Physical Network Element PNF	960,00	76	960,00	0,00	72 960,00
NED-IOSX-P	NSO NED Cisco IOSXR: 1 Active Prod Netw Srvr Lic Perp	40 000,00	1	40 000,00	0,00	40 000,00
NSO-DEV-45-P-K9	NSO 4.5 Lab Server software	9 000,00	1	9 000,00	0,00	9 000,00
NSO-45-P-K9	NSO 4.5 Active Server software	90 000,00	1	90 000,00	0,00	90 000,00
UCSC-C240-M4S2	UCS C240 M4 SFF 16 HD w/o CPU,mem,HD,PCIe,PS,railkt w/expndr	3 665,00	2	1 649,25	55,00	3 298,50
UCS-CPU-E52667D	3.20 GHz E5-2667 v3/135W 8C/20MB Cache/DDR4 2133MHz	6 264,00	4	2 818,80	55,00	11 275,20
UCS-ML-1X324RU-A	32GB DDR4-2133-MHz LRDIMM/PC4-17000/quad rank/x4/1.2v	**2 200,00**	**8**	**990,00**	**55,00**	**7 920,00**
UCS-HD2T7K12G	2 TB 12G SAS 7.2K RPM SFF HDD	2 379,00	2	1 070,55	55,00	2 141,10
UCS-SD960GBKS4-EV	960GB 2.5 inch Enterprise Value 6G SATA SSD	3 334,00	2	1 500,30	55,00	3 000,60
UCSC-PSU2V2-1200W	1200W / 800W V2 AC Power Supply for 2U C-Series Servers	749,00	4	337,05	55,00	1 348,20
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	0,00	4	0,00	55,00	0,00

Continuación de la tabla VI.

UCSC-RAILB-M4	Ball Bearing Rail Kit for C220 & C240 M4 & M5 rack servers	220,00	2	99,00	55,00	198,00
CIMC-LATEST	IMC SW (Recommended) latest release for C-Series Servers.	0,00	2	0,00	55,00	0,00
UCSC-HS-C240M4	Heat sink for UCS C240 M4 rack servers	0,00	4	0,00	55,00	0,00
UCSC-SCCBL240	Supercap cable 250mm	0,00	2	0,00	55,00	0,00
N20-BBLKD	UCS 2.5 inch HDD blanking panel	0,00	28	0,00	55,00	0,00
UCSC-MLOM-BLK	MLOM Blanking Panel	0,00	2	0,00	55,00	0,00
UCSC-MRAID12G-4GB	Cisco 12Gbps SAS 4GB FBWC Cache module (Raid 0/1/5/6)	1 967,00	2	885,15	55,00	1 770,30
UCSC-MRAID12G	**Cisco 12G SAS Modular Raid Controller**	**656,00**	**2**	**295,20**	**55,00**	**590,40**
C1UCS-OPT-OUT	Cisco ONE Data Center Compute Opt Out Option	0,00	2	0,00	55,00	0,00
RHEL-2S2V-1A	Red Hat Enterprise Linux (1-2 CPU,1-2 VN); 1-Yr Support Req	0,00	2	0,00	55,00	0,00
					TOTAL	224 902,30

Fuente: elaboración propia.

Tabla VII. **Estimación económica para servicios de soporte de software**

No. parte	Descripción	Precio de lista por unidad (Q)	Cantidad	Precio neto por unidad (Q)	% descuento	Precio total (Q)
CON-ECMU-RCISCO2K	SWSS UPGRADES Cisco Evolved Programmable Network Manag	0,00	1	0,00	55,00	0,00
CON-ECMU-EPNM9K21	SWSS UPGRADES Cisco Evolved Programmable Network Manag	2 300,00	1	1 035,00	55,00	1 035,00
CON-ECMU-EPNMBY2L	SWSS UPGRADES Cisco EPN Manager 2.X - RedundancyLicens	2 070,00	1	931,50	55,00	931,50
CON-ECMU-ASR906MT	SWSS UPGRADES Cisco EPN Manager 2	2 024,00	154	910,80	55,00	140 263,20
CON-ECMU-ASR90MTP	**SWSS UPGRADES Cisco EPN Manager 2 - Cisco ASR 9010 Rig**	**4 784,00**	**0**	**2 152,80**	**55,00**	**0,00**
CON-ECMU-LNCS60RT	SWSS UPGRADES Cisco EPN Manager 2 - Cisco NCS 6008 Rig	14 076,00	2	6 334,20	55,00	12 668,40
CON-ECMU-LCS201RT	SWSS UPGRADES Cisco EPN Manager 2 - Cisco NCS 2015 Rig	6 877,00	76	3 094,65	55,00	235 193,40

Continuación de la tabla VII.

CON-SNT-C240M4S2	SNTC-8X5XNBD UCS C240 M4 SFF 16 HD w/o CPU,mem,HD	583,00	2	262,35	55,00	524,70
CON-ISV1-EL2S2V1A	ISV 24X7 RHEL Server 2Socket-OR-2Virtual; ANNUAL List Price	1 428,90	2	643,01	55,00	1 286,02
CON-ECMU-WANAUTOE	SWSS UPGRADES WAN Automation Software, Perpetual Suite	0,00	1	0,00	55,00	0,00
CON-ECMU-WASDNPT2	SWSS UPGRADES WAE Premium SDN Bundle, 500 - 999 nodes,	2 938,25	154	1 322,21	55,00	203 620,34
CON-SNT-C240M4S2	SNTC-8X5XNBD UCS C240 M4 SFF 16 HD w/o CPU,mem,HD	583,00	2	262,35	55,00	524,70
CON-ISV1-EL2S2V1A	ISV 24X7 RHEL Server 2Socket-OR-2Virtual; ANNUAL List Price	1 428,90	2	643,01	55,00	1 286,02
CON-ECMN-RNSOK9	**SWSS NET-Netw Services Orchestrator 4.x**	**0,00**	**1**	**0,00**	**55,00**	**0,00**
CON-ECMN-NSOHALIP	SWSS NET-NSO Standby Server	10 350,00	1	4 657,50	55,00	4 657,50
CON-ECMN-NSOPXLSI	SWSS NET-NSO RTM Lic for One XLarge Phy Nwk Element PNF	3 036,00	2	1 366,20	55,00	2 732,40
CON-ECMN-NSOPNFLS	SWSS NET-NSO RTM Lic for One Large Physical Netw Element PNF	828,00	0	372,60	55,00	0,00

Continuación de la tabla VII.

CON-ECMN-NSOPNFMI	**SWSS NET-NSO RTM Lic for One Medium Phy Nwk Element PNF**	**221,00**	**76**	**99,45**	**55,00**	**7 558,20**
CON-ECMN-NEDIOSPN	SWSS NET NSO NED Cisco IOS/IOSXE: 1 Active Prod N	9 200,00	1	4 140,00	55,00	4 140,00
CON-ECMN-NEDIOSXP	SWSS NET-NSO NED Cisco IOSXR: 1 Active Prod Netw Svr LC Perp	9 200,00	1	4 140,00	55,00	4 140,00
CON-ECMN-NSODEV4P	SWSS NET NSO 4.5 Lab Server software media	2 070,00	1	931,50	55,00	931,50
CON-ECMN-NSO-45-PK	SWSS NET NSO 4.5 Active Serve	20 700,00	1	9 315,00	55,00	9 315,00
CON-SNT-C240M4S2	SNTC-8X5XNBD UCS C240 M4 SFF 16 HD w/o CPU,mem,HD	583,00	2	262,35	55,00	524,70
CON-ISV1-EL2S2V1A	ISV 24X7 RHEL Server 2Socket-OR-2Virtual.	1 428,90	2	643,01	55,00	1 286,02
					TOTAL	**632 618,60**

Fuente: elaboración propia.

La estimación económica se realizó para proporcionar los componentes necesarios a una infraestructura regional de 76 *routers* con las siguientes funciones:

- Automatización automática de servicios L2/L3 VPN
- Redundancia geográfica de controladores SDN
- Optimización de flujo de tráfico MPLS
- Restauración automática multicapa

CONCLUSIONES

1. La propuesta técnica de una arquitectura de red utilizando las tecnologías SDN y NFV en redes de datos de proveedores de servicios evidencia que hay claras ventajas en la virtualización de máquinas para proporcionar los recursos necesarios a las aplicaciones como enrutadores y controladores requeridos en una arquitectura SDN, dado que proporciona una escalabilidad y disponibilidad dentro de la red de datos que mejora el servicio que un proveedor de servicio brinda.

2. El modelo que utiliza SDN para la administración y control de los dispositivos dentro de la red se presenta como una solución que elimina el problema de homogeneidad de la red, dado que el uso de interfaces abiertas en cada uno de los dispositivos de la red para la administración a través de integraciones estándar como el protocolo *OpenFlow* simplifica de manera considerable los esfuerzos para la gestión de configuraciones y soporte dentro de la red.

3. Una implementación SDN basada en el modelo centralizado demuestra que al tener un panorama completo de la red de datos es posible mejorar el enrutamiento del flujo de paquetes, dado que se tiene un control total sobre todos los elementos que componen la red, así como de las rutas más eficientes para cada servicio o aplicación que un proveedor de servicios preste a los usuarios.

4. Una arquitectura NFV permite compartir recursos, eliminando la necesidad de tener una gran cantidad de nodos individuales dentro de la red que desaprovechan el total de sus capacidades, este tipo de arquitectura disminuirá la cantidad de equipos, permitiendo una mejor distribución y manejo de los recursos, y automatizando los servicios para ahorrar tiempo y dinero en la implementación de nuevos servicios.

RECOMENDACIONES

1. Aplicar los métodos descritos para la implementación de una arquitectura de red utilizando las tecnologías SDN y NFV en redes de datos de proveedores de servicios proporcionará los criterios para justificar la compra de equipos más robustos y enlaces con mayor capacidad de ancho de banda, de manera que primero pueda ser optimizado el recurso actual y solo si aún es necesario realizar una ampliación.

2. Elaborar una planificación para la implementación de una arquitectura de red utilizando las tecnologías SDN y NFV en redes de datos de proveedores de servicios que deben cubrirse para cumplir con los requerimientos de capacidad y de evaluación de la red, de forma que se identifiquen los posibles puntos críticos en el marco de aplicación.

3. Dimensionar de forma correcta las capacidades de los equipos físicos que servirán de host para la virtualización de aplicaciones con NFV, dado que de ello depende la capacidad total que las máquinas guest o virtualizadas pueden proporcionar a la red en una arquitectura SDN.

BIBLIOGRAFÍA

1. Academia de Networking de Cisco Systems. Guía del primer año. CCNA 1 y 2. Cisco Systems, Inc. 3a ed. Madrid: Pearson Educación, S. A. 2004. 1008 p.

2. ALARCON, José Manuel. ¿Qué diferencia hay entre *Docker* (contenedores) y Máquinas virtuales (*VMWare, VirtualBox*…)?. [en línea]. <https://www.campusmvp.es/recursos/post/que-diferencia-hay-entre-docker-contenedores-y-maquinas-virtuales.aspx>. [Consulta: junio 2018].

3. ENSI, Maria. *IaaS, PaaS, SaaS – What do they mean*?. [en línea]. <http://cloudonmove.com/iaas-paas-saas-what-do-they-mean/>. [Consulta: septiembre 2019].

4. *Intel Network Bulders*. *Network Transformation*. [en línea]. <https://builders.intel.com/university/networkbuilders/coursescategory/basic-training#network-transformation>. [Consulta: abril de 2018].

5. _____. *NFV Technologies*. [en línea]. <https://builders.intel.com/university/networkbuilders/coursescategory/basic-training#nfv-technologies>. [Consulta: mayo de 2018].

6. _____. *NFV SDN Differences*. [en línea]. <https://builders.intel.com/university/networkbuilders/coursescategory/basic-training#nfv-sdn-differences>. [Consulta: junio de 2018]

7. KUMAR KATTA, Naga Praveen. "*Building efficient and reliable software-defined networks*". Universidad de Princeton, Departamento de ciencias de la computación, noviembre 2016.

8. MAINI, Elisa. "*Orchestration of Logical resources in software defined infrastructures*". Universidad de Napoles Federico II, Facultad de Ingeniería, marzo 2015.

9. MARTÍNEZ DE LA CRUZ, Victoria. En pocas palabras: ¿Cómo funciona *OpenStack*?. [en línea]. <http://vmartinezdelacruz.com/en-pocas-palabras-como-funciona-openstack/>. [Consulta: agosto 2018].

10. MORILLO FUELTALA, Diana Gabriela. "Implementación de un prototipo de una red definida por software (SDN) empleando una solución basada en software". Escuela politécnica nacional de Ecuador, Facultad de ingeniería eléctrica y electrónica. mayo 2014.

11. NUGROHO, Himawan. *How to Bring SDN/NFV into Reality*. [en línea]. <http://www.himawan.nu/2015/08/>. [Consulta: septiembre 2018].

12. OLMO, Lara. Qué son y cómo funcionan los contenedores virtuales. [en línea]. <https://www.ticbeat.com/tecnologias/que-son-y-como-funcionan-los-contenedores-virtuales-infografia/>. [Consulta: agosto 2018].

13. ONF12. *Open Networking Foundation. Software-defined networking: the new norm for networks*. ONF White Paper, abril 2018.

14. SUBHARTHI, Paul. "*Sofware defined application delivery networking*". Universidad Waxhington St. Louis, Departamento de ingeniería y ciencias de la computación, agosto 2018.

15. STALLINGS, William. *Foundations of modern Networking*: SDN, NFV, QoE, IoT, *and Cloud*. 1a ed. Estados unidos: Pearson education, Inc., 2015, 442p. ISBN-13:978-0-13-417539-3.

16. UNDERDAHL, Brian. Redes definidas por software (SDN) para *dummies*, edición especial de cisco. Estados unidos de américa: Jhon wiley & Sons, Inc., 2015. 48p. ISBN: 978-1-119-16445-6.

17. VERIZON. *Network Ingrastructure Plannig*. SDN-NFV reference architecture. Version 1.0, Febrero 2018.

18. XIN, Jin. "Dynamic Control of software-defined networks". Universidad de Princeton, Departamento de ciencias de la computación, septiembre 2018.