UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TEMA:

Características de las Redes Definidas por Software (SDN) para su Implementación en el Ecuador

AUTORA:

Ochoa Brito María Jesús, Ing.

Trabajo de titulación previo a la obtención del grado de

MAGISTER EN TELECOMUNICACIONES

TUTORA:

Romero Amondaray Lídice, Msc.

Guayaquil, a los 22 días del mes de enero del año 2018

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación, fue realizado en su totalidad por Ochoa Brito María Jesús, como requerimiento para la obtención del Título de Magister en Telecomunicaciones.

TUTORA

f. _____
Romero Amondaray Lídice, Msc.

DIRECTOR DEL PROGRAMA

f. _____
Romero Paz Manuel, Msc.

Guayaquil, a los 22 días del mes de enero del año 2018

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, Ochoa Brito María Jesús

DECLARO QUE:

El Trabajo de Titulación, Características de las Redes Definidas por Software (SDN) para su implementación en el Ecuador previo a la obtención del Título de Magíster en Telecomunicaciones, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 22 días del mes de enero del año 2018

LA AUTORA

f. _____
Ochoa Brito María Jesús, Ing.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, Ochoa Brito María Jesús

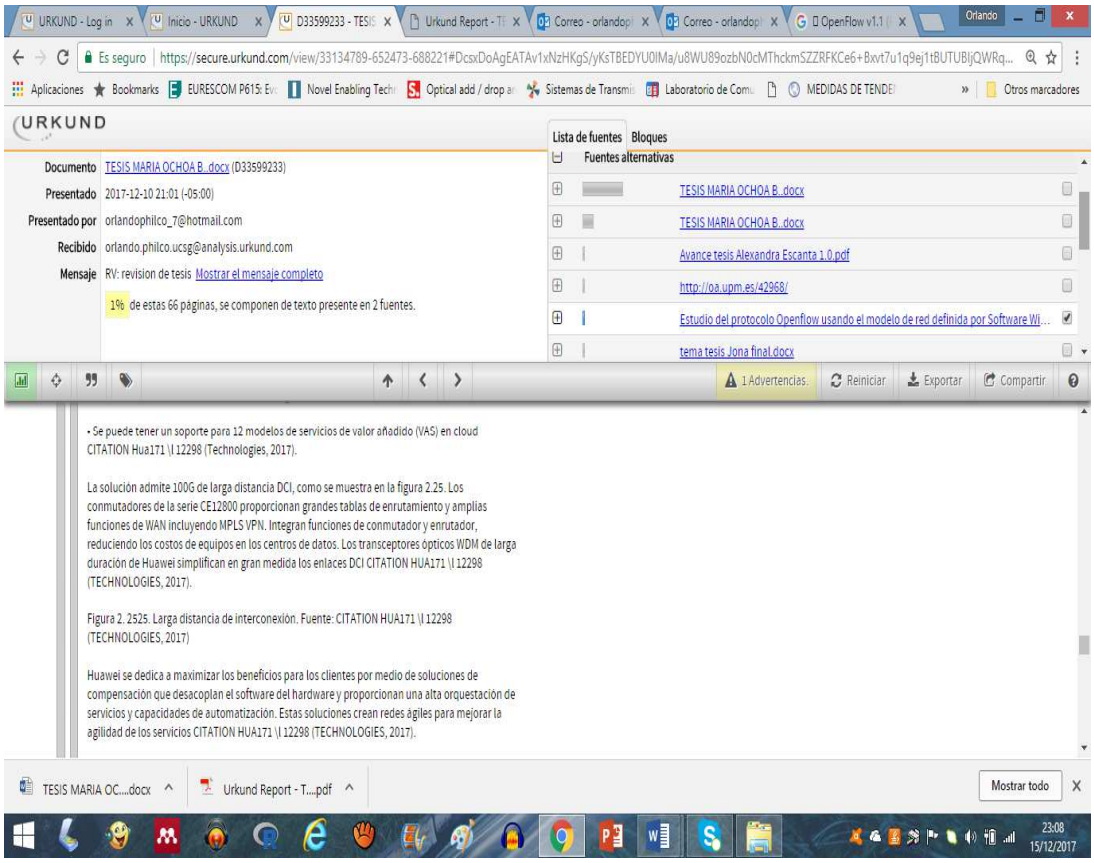
Autorizo a la Universidad Católica de Santiago de Guayaquil a la publicación en la biblioteca de la institución del Trabajo de Titulación, Característica de las Redes Definidas por Software (SDN) para implementación en el Ecuador, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 22 días del mes de enero del año 2018

LA AUTORA:

f. _____
Ochoa Brito María Jesús, Ing.

REPORTE URKUND



El análisis Urkund al Trabajo de Titulación “Características de las Redes Definidas por Software (SDN) para su Implementación en el Ecuador” a cargo de la ingeniera María Jesús Ochoa Brito, está al 1% de coincidencias.

DEDICATORIA

Este trabajo se encuentra dedicado en primer lugar a Dios, por haberme dado la fuerza y la salud para poder llegar hasta este momento tan importante de mi vida profesional. A mis padres, que estuvieron junto a mí en cada momento, apoyándome y no dejando que desmaye en ningún instante, a pesar de todos los momentos difíciles que pasamos. A todos mis maestros que aportaron con su granito de arena para poder cumplir con la meta trazada.

Ing. María Jesús Ochoa Brito.

AGRADECIMIENTO

A Dios por la bendición dada, y por la fuerza para poder continuar, a pesar de los obstáculos presentados.

A mi madre por su amor y apoyo incondicional durante toda mi vida, y por las palabras de aliento en momentos duros.

A mi padre por su amor y su eterno apoyo en cada uno de mis logros en mi vida, y por ser el segundo pilar para estar de pie en la vida.

A mis compañeros de aula y amigos Liuva y Pedro, por el apoyo y la complicidad en todo momento.

A todos los profesores de mi vida estudiantil, por sus enseñanzas no solo para la vida profesional sino también para la vida personal. Y en especial a quienes ayudaron a que esta tesis hoy sea posible.

A mi tutora Msc. Lidice Romero, por su guía y asesoramiento durante la elaboración de esta.

Y a todos mis amigos y seres queridos, que de una u otra forma colaboraron y estuvieron pendientes para que esto sea posible.

Ing. María Jesús Ochoa Brito.

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

ROMERO AMONDARAY LIDICE, MSC.

TUTORA

f. _____

PHILCO ASQUI ORLANDO, MSC.

REVISOR

f. _____

BOHORQUEZ ESCOBAR CELSO, MSC.

REVISOR

f. _____

ROMERO PAZ MANUEL, MSC.

DIRECTOR DEL PROGRAMA

RESUMEN

Las redes definidas por software (SDN, por sus siglas en inglés), nacen por la necesidad de contar con una mejor administración, distribución, flexibilidad y sobre todo para tener una mejor administración del ancho de banda. La estrategia de migración para un centro de datos hacia SDN, ayuda a crear una nueva arquitectura que aumentara las posibilidades de crecimiento de la red, sin verse afectados los servicios durante el proceso. En este trabajo se presentan varias estrategias tomando en cuenta el punto de partida de la red, se describen dos ejemplos de migraciones exitosas. Para tomar la decisión de migrar un centro de datos, se deben analizar lo más conveniente, dependiendo del tráfico que maneje este, y así realizarlo ya sea de forma directa o en fases. Esta nueva tecnología, ayuda con la simplificación de los procesos y rapidez al brindar una respuesta de solicitudes, que antes podían demorar más de lo debido. La tesis tiene enfoque cuantitativo, cuyo alcance de la investigación es descriptivo y explicativo. Es descriptivo, porque se revisará información de relevancia de las redes definidas por software (SDN) y es explicativo, porque se pretende caracterizar las SDNs para futuras implementaciones en el Ecuador. Se espera despertar un gran interés en su funcionamiento al igual que en las aplicaciones que se utilizan, lo que conlleve a su implementación en los diferentes centros de datos del país.

Palabras Claves: *SDN, OpenFlow, OpenStack, NETCOF, Migración, Centro de datos.*

ABSTRACT

Software-defined networks (SDNs) are born out of the need for better management, distribution, flexibility and, above all, better bandwidth management. The migration strategy for a data center towards SDN helps to create a new architecture that will increase the possibilities of growth of the network, without being affected the services during the process. In this thesis we present several strategies taking into account the starting point of the network, in which we mention two examples of successful migrations. In order to make the decision to migrate a data center, it is necessary to analyze the most convenient, depending on the traffic that manages this, and to do so either directly or in phases. This new technology helps with the simplification of processes and speed by providing a response of requests, which before could take longer than due. The thesis has a quantitative approach, whose scope of the research is descriptive and explanatory. It is descriptive, because it will review relevant information of the networks defined by software (SDN) and it is explanatory, because it is intended to characterize the SDNs for future implementations in Ecuador. It is expected to arouse great interest in its operation as well as in the applications used, leading to its implementation in the different data centers of the country.

Key Words: *SDN, OpenFlow, OpenStack, NETCOF, Migration, Data Center*

ÍNDICE

ÍNDICE DE FIGURAS

Capítulo 1: MARCO TEÓRICO.

Capítulo 2: MIGRACIÓN DE UN CENTRO DE DATOS A SDN

ÍNDICE DE TABLAS

INTRODUCCIÓN

Justificación.

Las redes definidas por software (SDN por sus siglas en inglés) son usadas para la creación de redes que serán administradas y serán gestionadas mediante un controlador, de una manera ágil y efectiva. Este nuevo paradigma de redes ayuda a un crecimiento acelerado de los centros de datos, al no tener que adquirir un mayor equipamiento, sino con solo crear más aplicaciones relacionadas con lo que se esté por implementar o utilizar para mejoras en la red.

Con este estudio se quiere mostrar los beneficios que se tendrán al no depender de equipos físicos, la flexibilidad que brinda tanto en la administración como en las soluciones siendo más rápidas y eficaces que en los diferentes escenarios que se puedan presentar, esto es posible al poder realizar el trabajo de manera remota sin tener que dirigirse hasta el equipo que presenta la afectación.

Mediante las SDN, por la flexibilidad que estas brindan frente a los centros de datos tradicionales con hardware, es factible crecer de una manera más acelerada y con una menor inversión.

También se pretende demostrar que las limitantes de las redes actuales, como la escalabilidad, las complicaciones para crear reglas de seguridad, entre otras, con esta tecnología no se tendrán, ya que al ser mediante programas el manejo de la misma, se pueden crear aplicaciones que sirvan para mejorar la calidad del servicio y aumentar la seguridad.

Antecedentes

SDN es una tecnología relativamente nueva que al momento en el país no se encuentra desarrollada. Empieza a aplicarse en el 2013 virtualizando de la red WAN o los equipos usados en los centros de datos. Desde sus inicios se tienen previstas tres etapas de aplicación (Colt Technology Services Group Limited., 2015)

- **Automatización de redes:** en la actualidad, el control de software de las redes se realiza en la propia empresa y, con frecuencia, por medios rudimentarios. Al liberar el código fuente de las API, es cuando se produce la rapidez que se busca.
- **Virtualización de las redes:** cuando se disponga de la automatización básica, se puede iniciar realmente el proceso de separación de la capa 2 y 3 de la red y la capa física. Se utilizan controladores y un nuevo protocolo SDN, para la programación de controladores virtuales.
- **Aplicación de SDN en las redes WAN:** no solo los centros de datos tendrán grandes ventajas, ya que las redes WAN también pueden ser administradas.

En las redes tradicionales los enrutadores y conmutadores utilizan softwares propietarios, en SDN al emplear el protocolo OpenFlow, de estándar abierto, une todos los parámetros de los controladores individuales de los diferentes fabricantes, para poder obtener una infraestructura de fácil administración (Tilves., 2013).

Se sabe que las marcas fabricantes de equipos (enrutadores y conmutadores) como son Brocade, Arista, Juniper, Extreme Networks, HP, Huawei, IBM, NEC e incluso Cisco, entre otras, promueven el trabajo con OpenFlow (Tilves., 2013).

Definición del problema

La necesidad de gestionar en los centros de datos grandes volúmenes de tráfico de información, implica que se tenga que invertir en adquirir equipos nuevos e incluso la ampliación de espacio físico para su instalación.

El Ecuador no cuenta con estadísticas de la cantidad de centros de datos que existen dentro de él país, porque cada empresa sea esta

mediana o grande puede tener uno. Se procederá a brindar tanto recomendaciones y directrices para realizar el cambio de redes físicas a virtuales y su desarrollo, las cuales pueden ser aplicadas en cualquier centro de datos en el país.

Se tomará en cuenta la forma del equipamiento a nivel general, para proponer una estrategia de cambio efectiva. Se hará mención de las especificaciones técnicas que existen en el mercado, para que sean tomadas en consideración al momento de realizar el paso a la nueva tecnología.

Objetivos

Objetivo General

Proponer una estrategia para viabilizar la migración en los centros de datos sin afectaciones al servicio, así como la seguridad que se tendrá de no perder información en caso de existir alguna afectación en el controlador principal.

Objetivos Específicos

- ✓ Establecer los motivos por los cuales es necesaria una migración a SDN.
- ✓ Describir el funcionamiento e implementación de este sistema.
- ✓ Proponer una estrategia para la migración a SDN.

Hipótesis

Un centro de datos al migrar a SDN podrá optimizar recursos al igual que empezar a crecer de una manera más acelerada.

Metodología.

El trabajo final de maestría tiene enfoque cuantitativo, cuyo alcance de la investigación es descriptivo y explicativo. Es descriptivo, porque se revisará información de relevancia de las redes definidas por software (SDN) y es explicativo, porque se pretende caracterizar las SDNs para futuras implementaciones en el Ecuador.

Con este trabajo se espera despertar un gran interés en su funcionamiento al igual que en las aplicaciones que se utilizan, lo que conlleve a su implementación en los diferentes centros de datos del país y estar a la par con los avances tecnológicos a nivel mundial.

A continuación se detallará todo lo concerniente a la información teórica técnica para las consideraciones necesarias para ser implementada en nuestro país.

CAPÍTULO 1: MARCO TEÓRICO

1.1 Introducción.

Las SDN, nacen en base a la necesidad de tener una mejor administración, distribución, flexibilidad y sobre todo para una asignación eficiente del ancho de banda dependiendo de las diferentes necesidades de los centros de datos.

Las redes actuales se encuentran limitadas a medida que crece la demanda de aplicaciones para los diferentes tipos de requerimientos de los usuarios finales, quienes no se sienten a gusto atados a un escritorio. Al aplicar SDN se les puede brindar la opción de la libertad de movilidad y la facilidad de acceso a la información en cualquier lugar y hora que esta sea requerida.

SDN se encuentran en pleno crecimiento, a nivel mundial, por las bondades de sus características en programación que brindan una mayor garantía en lo referente a seguridad; permite además redundancia, que es posible implementar, sin olvidar los beneficios que anteriormente se mencionaron para los administradores y clientes.

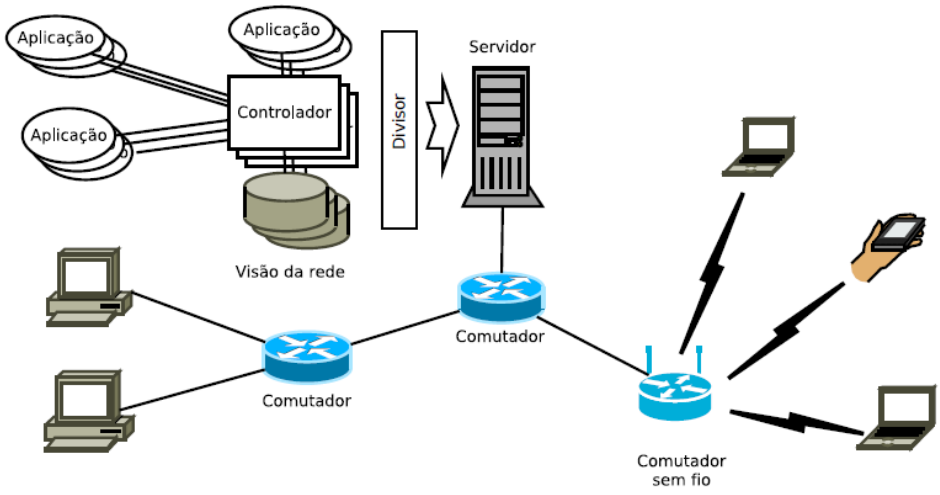


Figura 1. 1 Diagrama de una Red Definida por Software.

Fuente: (Guedes, Vieira, Vieira, Rodrigues, & Nunes, 2014)

Según un reporte del crecimiento de SDN se calcula que su impacto para el año 2018 superará los 25 billones por año, por tanto se piensa que SDN será el cambio que sucede una vez por generación (Barona, 2013).

1.2 Objetivos de SDN.

Los objetivos para SDN establecidos por la ITU son los siguientes:

- Ciclos de red más económicos y rápidos. Reduce el tiempo de respuestas de las solicitudes por parte de los proveedores comerciales a la red.
- Rápida innovación. Acelera la innovación técnica a través de una mayor flexibilidad en las operaciones de la red, para hacerlo más fácil.
- Acelerada adaptación a las demandas del usuario. Facilita el alojamiento de los requisitos de conectividad de los usuarios por medio de negociación dinámica de las características del servicio de la red y de los recursos que esta tenga.
- Mejora de la disponibilidad de recursos y la eficiencia de uso. Se encuentra destinado a mejorar los recursos y la eficiencia de la red, de manera particular cuando es combinado con la virtualización, todo esto debido al alto nivel de automatización en los procedimientos generales de prestación de servicios y operación.
- Personalización de los recursos de la red que incluye la creación de redes de servicio-cuenta. Permite la personalización de la red para los diferentes requisitos, a través de la programación de las operaciones de los recursos de red, incluyendo el de aplicación de la dinámica de conjunto de políticas de calidad de servicio (ITU, 2014).

1.3 Capacidades de alto nivel.

La ITU da las siguientes capacidades de alto nivel:

- Programación. El comportamiento de los recursos de red se puede personalizar mediante una interfaz de programación estándar para la gestión de la red. Los usuarios de la interfaz pueden ser proveedores, de red o de servicios, y clientes incluidos los usuarios finales. Esto permite que las aplicaciones puedan automatizar las operaciones de los recursos de red de acuerdo con las necesidades.
- Abstracción de recursos. La propiedad y el comportamiento de los recursos de las redes adyacentes pueden ser apropiadamente controladas y/o gestionadas gracias a la estandarización de los modelos de información y de datos. Estos modelos proporcionan una vista detallada y abstraída de los recursos de la red sea esta física o virtual (ITU, 2014).

1.4 Requerimientos.

Los requisitos que brinda la ITU para SDN son descritos de la siguiente manera:

- SDN se requiere para:
  - Apoyar la programabilidad de los recursos de la red.
  - Organizar los recursos de la red y aplicaciones SDN.
  - Proporcionar una interfaz de control de aplicaciones para personalizar el comportamiento de los recursos de la red.
  - Proporcionar una interfaz de control de recursos para el controlador de los recursos de la red.
  - Proporcionar un control lógico centralizado de los recursos de la red.
  - Separar el control SDN de los recursos de red.
  - Para apoyar la abstracción de los recursos de red subyacentes, por medio de modelos de información y de datos estándar.
  - Apoyar la gestión de los recursos físicos de red.

- Para apoyar la gestión de los recursos de redes virtuales (ITU, 2014).

1.5 Arquitectura de SDN.

En la figura 1.2 se muestra la arquitectura de una SDN. Esta arquitectura se compone de tres capas: aplicación, control e infraestructura. A continuación se procederá a describir cada una de ellas:

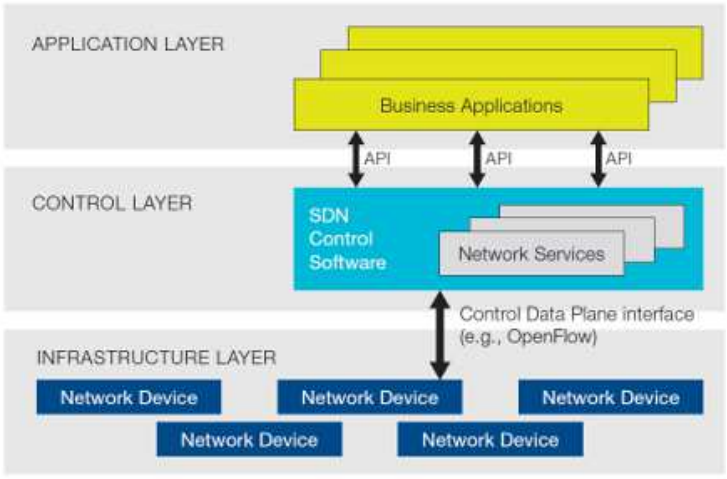


Figura 1. 2. Arquitectura de una SDN.

Fuente: (Bautista, 2015)

1.5.1 Capa de Aplicación

Admite establecer aplicaciones para de forma automática ejecutar las configuraciones, abastecimiento y extender los nuevos servicios en la red (Maldonado, 2014).

Las capas de aplicación y control se comunican mediante una API, para conocer el estado general de la red, esto ayuda a mejor la forma de transmitir los datos porque los nodos podrán administrar el tráfico de flujos de las redes individuales para aplicaciones específicas, como sus plataformas de control serán distribuidas (Maldonado, 2014).

La capa de aplicaciones permite relacionar las funciones de los centros de datos para obtener seguridad en la red mientras se está

trabajando a la vez que mejora de forma constante la automatización (Maldonado, 2014).

Las aplicaciones utilizadas bajo la arquitectura OpenFlow son: (Maldonado, 2014)

- **Visor de flujo (FlowVisor):** permite ver el flujo de datos sobre una topología de red, filtrando datos con características específicas como tipo de datos, destino y remitente. Esta aplicación utiliza por defecto los puertos 8080 y 6633 para OpenFlow v1.0 (Moreno, 2015).
- **Aster'X:** en una topología de red dedicada principalmente a voz IP, se realiza de manera dinámica un balanceo de cargas, mejorando la calidad de servicio y bajando el porcentaje de utilización de cada elemento de red.
- **Usando toda la red inalámbrica que me rodea (Using all wireless Network Around me):** se implementa un proceso de traspaso sobre una red SDN. La implementación se realiza bajo una aplicación streaming utilizando una red WiFi y una red WiMAX.
- **ElasticTree:** caracteriza de un centro de datos y evalúa el consumo de energía con y sin la arquitectura SDN.
- **Canales abiertos (Open Pipes):** es una plataforma para la construcción de sistemas de hardware distribuidos en módulos y conectados en diferentes puertos físicos en una red OpenFlow (Maldonado, 2014).

1.5.2 Capa de Control

Esta capa es responsable de establecer el trato de los flujos de los datos, con la ayuda del controlador SDN. Aunque existen varios protocolos, se utiliza OpenFlow (Pinilla, 2015).

1.5.3 Capa de Infraestructura

Se encuentra conformada por enrutadores y conmutadores físicos, encargados de la administración de las tablas de flujo mediante el controlador, encargada de cambiar o agregar dispositivos. Capa enlazada con el plano de datos (Barona, 2013) (Icaza, 2016).

Las solicitudes que se ejecutan entre la capa de infraestructura y la capa de control son realizadas mediante la Interfaz Southbound. La comunicación entre la capa de control y las aplicaciones es realizada con la Interfaz NorthBound (Icaza, 2016).

1.5.3.1 Northbound API (NB API)

Se trata de una interfaz que va hacia la parte externa. Es heterogénea: REST, RPC, OSGI, etc. Mediante a estas interfaces se pueden comunicar entre aplicaciones y controladores, para realizar configuraciones de red con las solicitudes de las aplicaciones. Si se desea tener un nivel de seguridad alto, el administrador puede controlar las peticiones que se realicen, mediante reglas sobre el uso del tráfico o sobre permisos de accesos (Moreno, 2015).

1.5.3.2 Southbound API (SB API)

En el plano de control, es el lugar en el que se realizan las configuraciones de los controladores. Mediante SB API, son enviadas las reglas de flujos de tráficos a todos los dispositivos de la red (Moreno, 2015).

También es posible la colocación de capas intermedias a manera de proxy, entre el controlador y los dispositivos de la red, para poder ser usados para la administración en distintos controladores o NB APIS (Moreno, 2015).

1.6 Protocolos de Comunicación SDN.

En la actualidad existen tres protocolos de comunicación para SDN son OpenFlow, OpenStack y NETCONF, los que se describen a continuación:

1.6.1 OpenFlow

OpenFlow es una tecnología de conmutación abierta que se inició en el año 2008 como un proyecto de investigación de la Universidad de Stanford para no afectar el tráfico normal. Bajo esta tecnología, una red puede ser gestionada como un todo y no como una serie de dispositivos individuales (Jacobs, 2012) (Park & Baack, 2012).

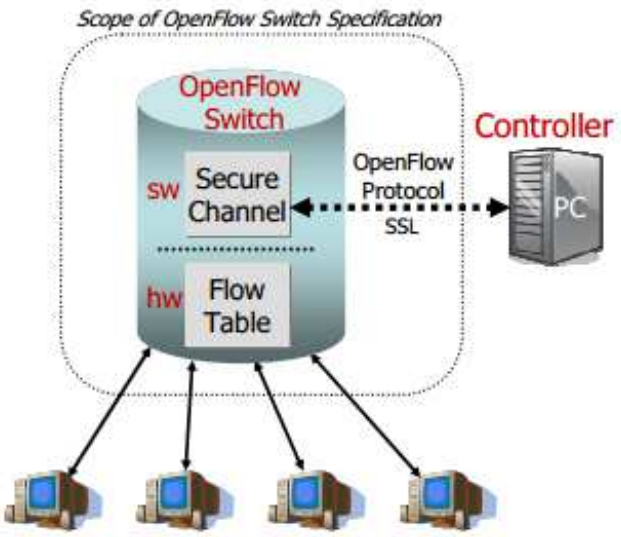


Figura 1. 3. OpenFlow Conmutador.

Fuente: (McKeown, y otros, 2008)

Luego de su primera aparición, OpenFlow cambió a la comunidad académica ONF en el 2011. Actualmente cuenta con más de 90 miembros que impulsaron el desarrollo de este protocolo. Este protocolo cuenta ya con cinco versiones adicionales, que se muestran a continuación:

- **OpenFlow v1.1 (Feb, 2011)**
  - **Agrega el uso de múltiples tablas:** la versión 1.0 tenía solamente una tabla lo que restringía las capacidades del hardware. Actualmente, con la implementación de múltiples tablas, es posible organizar cada una para aumentar el rendimiento y la escalabilidad.
  - **Grupos:** se pueden adicionar grupos de puertos para realizar acciones como la redundancia.

- **Soporte de etiquetas MPLS y VLAN:** estas capacidades adicionan flexibilidad en la programación del plano de reenvio, ya que los paquetes proveen de más información al controlador.
- **Puertos virtuales:** permite la virtualización de la red para varios clientes a escala.
- **Fallo en la conexión del controlador:** la versión 1.0 ofrecía un flujo de emergencia que en la práctica era difícil implementar. En la versión 1.1 se añade dos modos en caso de la desconexión de la red:
    - El modo seguro en la cual el conmutador sigue trabajando con los flujos que tienen establecidos.
    - El modo de falla en el cual el conmutador desactiva a OpenFlow.

➢ **OpenFlow v1.2 (Dic., 2011)**

- **Extensión de soporte de coincidencia:** elimina el tamaño fijo que tenía las coincidencias y agrega nuevos campos.
- **Soporte básico IPv6:** con los campos adicionados en la coincidencia, da soporte para IPv6.
- **Cambia mecanismo de conexión del controlador:** los conmutadores se podrán conectar a más de un controlador.

➢ **OpenFlow v1.3 (Abril., 2013)**

- **Expande el soporte sobre IPv6:** adiciona más campos de coincidencia.
- **Estadísticas de los flujos:** cuando se establece el flujo, es posible agregar la opción de medición y control de la tasa de paquetes.

- **Tunnel-ID meta data:** agrega el campo en el de coincidencia que expone el proceso de encolamiento de meta data a un puerto lógico (Hidalgo I. D., 2014).

➢ **OpenFlow v1.4 (Agosto, 2013)**

- **Ampliación de escalabilidad:** la tabla de flujo se expande mediante una nueva "tabla sincronizada", estas trabajan de forma bidireccional, que permite que se muestre en la tabla origen.
- **Incluye nueva función:** se introduce "Bundle" por la necesidad de agrupar las modificaciones de un grupo transacción. Además, también puede utilizarse para restauración y pre validación de mensajes OpenFlow aplicados a varios conmutadores.
- **Extensibilidad adicional del protocolo:** permite agregar, de una manera más fácil, nuevas características al protocolo en el futuro y ampliar la API de extensión de prueba.
    - **Estructura de puertos:** agrega propiedades de descripción, mod y de stats de puertos.
    - **Estructuras de tablas:** agrega propiedades de mod, descripciones de tabla multipart y añade mensaje asincrónico del estado de la tabla.
    - **Estructuras de encolados:** migrar la descripción de encolamiento de varias partes, convierte propiedades de descripción de encolamiento a TLV estandarizados, agrega propiedades de encolamiento de estadísticas.
    - **Estructuras set-async:** convierte set-async a configuración TLVs, agrega la propiedad experimental set-async.
    - **Estructuras de instrucción:** instrucciones clarificadas TLVs.

        - **Estructuras de acciones:** clarificar acciones TLVs.
        - **Estructuras experimentadas:** aclarar experimentador TLVs.
        - **Errores de propiedades:** agrega un conjunto de códigos de error unificado para todas las propiedades.
    - **Cambiar el puerto TCP por defecto a 6653:** IANA asignó a ONF el número de puerto TCP 6653 para ser utilizado por el protocolo de conmutador OpenFlow. Todos los usos de los números de puerto anteriores, 6633 y 976, se deben descontinuar. Los conmutadores OpenFlow y los controladores OpenFlow deben usar 6653 por defecto (cuando no se usa un número de puerto especificado por el usuario) (FOUNDATION, 2014).

- **OpenFlow v1.5 (Diciembre, 2014)**
    - **Tabla de salida:** esta versión introduce las tablas para que el procesamiento se realice en el contexto del puerto, procesa en la primera tabla de salida para definir y redirigir el paquete a otras tablas.
    - **Campo OMX:** habilita la entrada de flujo de salida para que coincida con el puerto saliente, OXM_OF_ACTSET_OUTPUT.
        - El paquete enviado a un puerto de salida es procesado por la primera tabla de salida.
        - El procesamiento de grupo y la sustitución de puertos reservados ocurren antes de las tablas de salida.
        - Defina el comportamiento de las entradas de las tablas de salida y de egreso, principalmente que sean similares a la entrada.

- El nuevo campo de coincidencia OXM_OF_ACTSET_OUTPUT, usado para coincidir con el valor de salida del conjunto de acciones, es obligatorio para las tablas de salida, pero es opcional para las tablas de ingreso.
- Prohíbe agregar o acción de grupo en el conjunto de acciones de salida para evitar que cambie el puerto de salida.
- Permite que la entrada de flujo de salida utilice la acción de salida en la lista de acciones para reflejarla.
- El encolamiento se transporta desde las tablas de ingreso a la salida.
- Las características de la tabla para establecer la primera tabla de salida.
- Las características de las tablas sirven para identificar la tabla a usar para ingresar y/o salir.
- Introduzca comandos de solicitud de características de tabla para actualizaciones de características de tabla más sencillas (FOUNDATION, 2014).

1.6.1.1 Controladores OpenFlow

Un controlador es una entidad centralizada para toda la red OpenFlow que se encarga de indicarle al conmutador OpenFlow la serie de parámetros que definirán a cada flujo y cómo los paquetes que coinciden con el flujo deben de ser procesados (Park & Baack, 2012).

El controlador centralizado es quien mantiene, en tiempo real, la información de la red para definir las rutas a seguir por los flujos a seguir en los enrutadores y conmutadores de manera individual. Con esta información, el controlador organiza el envío de datos a través de todos los dispositivos de la red. Esto permite la automatización y aprovisionamiento

dinámico, logrando la distribución necesaria en entornos virtualizados y de redes en la nube (McGillicuddy, 2011).

Un controlador SDN puede ser descrito de forma general como un sistema de software o colección de sistemas que ofrecen:

- Gestión del estado de la red, que implica una base de datos. Estas bases de datos sirven como un repositorio para la información de configuración temporal e información sobre la topología de la red.
- Un modelo de datos de alto nivel que captura las relaciones entre los recursos gestionados, las políticas y otros servicios prestados por el controlador. En muchos casos estos modelos de datos se construyen utilizando el lenguaje de modelado Yang.
- Un mecanismo de descubrimiento de dispositivos, topología y servicio; un sistema de cálculo de ruta y, potencialmente, otros servicios de información centrados en la red o en los recursos.
- Una sesión de control segura sobre TCP entre el controlador y los agentes asociados en los elementos de la red, por el ejemplo con el uso del protocolo TLS.
- Un protocolo basado en estándares (OpenFlow) para obtener el estado de la red impulsado por las aplicaciones de los elementos de red.
- Un conjunto de APIs, a menudo RESTful, que exponen los servicios del controlador a las aplicaciones de gestión. Esto facilita la mayor parte de la interacción del controlador con estas aplicaciones. Esta interfaz se representa a partir del modelo de datos que describe los servicios y funciones del controlador. En algunos casos, el controlador y su API son parte de un entorno de desarrollo que genera el código de la API a partir del modelo de datos.
- Algunos controladores ofrecen entornos de desarrollo robustos que permiten la expansión de las capacidades básicas del núcleo y la posterior publicación de las APIs para los nuevos

módulos, incluyendo los que soportan la expansión dinámica de las capacidades del controlador (Alejandro García Centeno, 2014).

En la tabla 1.1 se describen brevemente las características de los controladores actuales:

Tabla 1. 1. Características de los controladores

	Beacon	Floodlight	NOX	POX	ODL
Soporte OpenFlow	OF v1.0	OF v1.0, v1.2, v1.3 y v1.4 (beta)	OF v1.0	OF v1.0	OF v1.0, v1.3
Virtualización	Mininet y Open Vswitch	Mininet y Open Vswitch	Mininet y Open Vswitch	Mininet y Open Vswitch	Mininet y Open Vswitch
Lenguaje de desarrollo	Java	Java	C++	Python	Java
Provee REST API	No	Si	No	No	Si
Interfaz Gráfica	Web	Web	Python+,QT4	Python+, QT4, Web	Web
Soporte de plataformas	Linux, Mac OS, Windows y Android para móviles	Linux, Mac OS, Windows	Linux	Linux, Mac OS, Windows	Linux, Mac OS, Windows
Soporte de OpenStack	No	Si	No	No	Si
Multiprocesos	Si	Si	Si	No	Si
Código Abierto	Si	Si	Si	Si	Si
Tiempo en el mercado (aprox)	5 años	3 años	7 años	2 años	1 año
Documentación	Buena	Buena	Media	Pobre	Media

Fuente: (Moreno, 2015)

NOX: creado por Nicira en el 2008, y dado a los investigadores, soporta Linux, aplicaciones Python y una API C++. Fue el primer controlador de código abierto que utilizaba OpenFlow v1.0 para controlar y monitorear los conmutadores. Se basa en eventos y su función es asincrónica (Pinilla, 2015).

POX: creado a base del primer controlador abierto NOX, se implementa en Python completamente. Puede trabajarse en Windows, Mac

OS o Linux. Es de uso fácil, compuesto de varias APIs, y enfocado para investigaciones y educación (Icaza, 2016) (Pinilla, 2015).

Beacon: se basó en su totalidad en Java. Creado en el 2010 el primero con este lenguaje de funcionamiento independiente para brindar soporte multi-threading. Este controlador tiene múltiples funciones de procesos, usado para la implementación del controlador. Emplea la librería Spring, quien brinda el mejoramiento del software, como por ejemplo Web Framework (Moreno, 2015).

Beacon usa la implementación Java OpenFlowJ. Es posible diferenciar cuatro módulos principales cada uno con su API en el controlador (Moreno, 2015).

- Administrador de dispositivos: responsable de anotar tanto los conmutadores que fueron revisados como su información (direcciones Ethernet e IPs usadas, últimas conexiones, protocolos usados, etc.)
- Topología: responsable de anotar los enlaces entre los conmutadores, además de recibir los nuevos enlaces o los eliminados.
- Enrutamiento: brinda un camino mucho más rápido para realizar el direccionamiento entre los equipos de la red.
- Web: brinda la interfaz de acceso para el usuario (Moreno, 2015).

Floodlight: controlador open-source basado en Java con origen en Beacon. Soporta OpenFlow en todas sus versiones con la utilización de la librería OpenFlowJ-Loxi, también puede trabajar con OpenStack. Este controlador logra interconectar tanto con equipos de redes físicas como virtuales, obteniendo un alto rendimiento de gestión. Las aplicaciones y módulos implementados trabajan mediante API y REST (Moreno, 2015) (Icaza, 2016).

ODL (OpenDaylight): se encuentra registrado en OpenDaylight Foundation. Nace del controlador Beacon bajo lenguaje Java, dentro de Linux Fundation. Brinda soporte a OpenSatack, ayudando a la

administración de la red. Utiliza protocolos abiertos para proporcionar control centralizado y programático y monitorización de dispositivos de red (Icaza, 2016) (Moreno, 2015) (Documentation, 2017).

OpenDaylight proporciona una interfaz que le permite conectar dispositivos de red rápida e inteligentemente para un rendimiento óptimo de la red (Documentation, 2017). También tiene soporte para una gama amplia y creciente de protocolos de red más allá de OpenFlow, incluyendo SNMP, NETCONF, OVSDB, BGP, PCEP, LISP y más (Documentation, 2017).

A continuación se mencionaran las principales características que se deben tomar en cuenta al momento de valorar el controlador SDN:

1. **Soporte OpenFlow:** el administrador debe conocer cuáles son las especificaciones técnicas de las versiones que tiene OpenFlow para conocer lo que el controlador soporta, y saber las opciones que brindan los proveedores para las migraciones a las nuevas versiones. Es necesario conocer todas las características de cada una de las versiones, porque no todas tienen las mismas opciones, como el IPv6.
2. **Virtualización de la red:** esta característica permite a los administradores crear dinámicamente las redes virtuales basadas en políticas, disociadas de las redes físicas, para satisfacer una amplia gama de requisitos como la ampliación horizontal de la capacidad, sin afectar los flujos existentes. Otra de las muchas ventajas de la virtualización de red es que permite un completo aislamiento entre cada segmento de red lo que es muy útil por razones de seguridad como mantener aislados los datos generados por un grupo de usuarios de otros usuarios y permitir a los desarrolladores de aplicaciones ejecutar las mismas en un entorno de trabajo sin afectar el tráfico. Para cumplir estos requisitos de manera eficiente, en los controladores SDN se deben configurar las redes virtuales de forma centralizada, con total aislamiento unas de otras, y dichas configuraciones deben estar automatizadas.

3. **Funcionalidad de la red:** para el aumento de la flexibilidad en términos de cómo los flujos son en rutados, es necesario que el controlador SDN pueda decidir el enrutamiento basado en los múltiples campos de la cabecera de OpenFlow. Además es primordial que el controlador pueda determinar los parámetros de QoS flujo por flujo. Una distinta y significativa funcionalidad que debe tener un controlador SDN es la capacidad para encontrar varias rutas desde el origen del flujo a su destino y para dividir el tráfico de un flujo dado a través de diversos enlaces. Esto capacidad excluye la necesidad de STP y aumenta el rendimiento y la escalabilidad de la red permitiendo, también, eliminar la necesidad de añadir a la complejidad de la red nuevos protocolos como TRILL o SPB.
4. **Escalabilidad:** una consideración fundamental con respecto a la escalabilidad de una red SDN es el número de conmutadores que un controlador SDN puede soportar. En la actualidad se debe esperar que los controladores soporten un mínimo de 100 conmutadores, pero en última instancia esto depende de las aplicaciones que soportan. Otro factor que limita la escalabilidad de una red SDN es la proliferación de entradas en la tabla de flujo, ya que sin algún tipo de optimización, se requiere de una entrada salto por alto para cada flujo. Al evaluar los controladores SDN, es necesario asegurarse que el controlador puede disminuir el impacto de sobrecarga de difusión de red, la cual limita la escalabilidad de la arquitectura de red implementada y reducir al mínimo la proliferación de las entradas de la tabla de flujo. Otro aspecto de la escalabilidad es la capacidad del controlador de SDN para crear una SDN que pueda abarcar múltiples sitios. Esta capacidad permite el movimiento de máquinas virtuales y el almacenamiento virtual entre sitios. Para maximizar el beneficio de esta capacidad, el controlador SDN debe permitir que las políticas de red para el enrutamiento y reenvío se apliquen automáticamente para la migración de servidores y / o almacenamiento

5. **Rendimiento:** una de las principales funciones de un controlador SDN es establecer flujos. Por ello, dos de los indicadores claves de rendimiento asociados con un controlador SDN son el tiempo de conformación de flujo y el número de flujos por segundo que puede establecer el controlador. Estas métricas de desempeño influyen en gran medida cuando se requiere añadir controladores como, por ejemplo, cuando los conmutadores inician más flujos de los que pueden ser soportados por el controlador o los controladores SDN existentes.

6. **Programación de red:** una de las características fundamentales de las SDN es la existencia de interfaces para la programación del controlador, lo que posibilita que este ofrezca varias funcionalidades. Un controlador SDN también puede soportar la programación, proporcionando plantillas que permitan la creación de secuencias de comandos CLI con las que es posible la programación dinámica de la red.
7. **Confiabilidad:** una de las técnicas que un controlador SDN puede utilizar para aumentar la fiabilidad de la red, es la capacidad de descubrir múltiples caminos desde el origen hasta el destino lo cual puede realizar si continuamente controla la topología de la red. Si el controlador SDN establece varias rutas entre el origen y el destino, la disponibilidad de la solución no se ve afectada por la interrupción de un solo enlace. Alternativamente, si el controlador SDN sólo establece una única ruta del origen al destino, cuando ocurra un fallo en un enlace, el controlador debe ser capaz de redirigir el tráfico rápidamente a un enlace activo. Relativo a la disponibilidad de las conexiones externas, es importante que el controlador soporte tecnologías alternativas de diseño, como el VRRP y MC LAG, que tienen como objetivo aumentar la fiabilidad de la red. En cuanto a la disponibilidad del controlador en sí mismo, es fundamental que el mismo se construya utilizando

redundancia tanto para las características de hardware como para las de software. También es imprescindible que el controlador SDN permita agrupaciones (clusters).

8. **Seguridad en la red:** para brindar seguridad en la red, el controlador SDN debe poder tolerarla autenticación y autorización. Los controladores SDN son propensos a tener ataques mal intencionados, lo que hace que sus conexiones de control sean limitadas y debe ser apto para detectar posibilidades de ataques que se puedan producir.
9. **Monitorización centralizada y visualización:** el controlador debe usar los datos obtenidos mediante OpenFlow para poder reconocer en la red los problemas, y poder modificar la ruta de flujo de datos. Adicional debe identificar el tráfico que se debe controlar, se debe poder visualizar los flujos tanto de la red física como de la red virtual, mientras se obtiene información de cada uno. Así mismo, debe permitir monitorear al controlador mediante los medios habituales como lo es SNMP. Además, el controlador SDN, debe soportar los distintos MIBs tanto privados como los estándares, para la administración de la red virtual.
10. **Fabricantes de controladores SDN:** varios fabricantes al ver la progresiva tendencia hacia las SDN, han ingresado al mercado y muchos han mencionado su interés en incursionar también. Por la inestabilidad de SDN y del controlador en el mercado, las características que deben llenar las expectativas tanto a nivel técnico como la comercial de los vendedores. Existe un reto entre lo técnico y financiero para los proveedores, que no pueden permitir el ampliar la red SDN sin desfavorecer la adquisición de los controladores quienes deben permanecer actualizadas según cómo evolucione SDN.
11. **Soporte de plataformas:** los sistemas operativos que utilizan los controladores deben ser multiplataforma, para ofrecer flexibilidad e independencia cuando son instaurados. Existen

empresas que les gustaría que los controladores trabajen con softwares abiertos.

12. **Procesamiento:** cuando se valora un controlador se toma en cuenta si soporta de forma simultánea a los distintos procesos, ya que es posible que afecte a los núcleos del CPU. Los controladores si son mono procesos deben correrse en hardware de un solo CPU, estos son utilizados en pequeñas redes; al igual que los controladores que soportan múltiples procesos deben trabajar con múltiples CPUs, estos son usados en empresas. (Alejandro García Centeno, 2014).

1.6.1.2 Conmutadores OpenFlow

Tiene dos tipos de conmutadores, Conmutadores OpenFlow y Conmutadores híbridos. Los OpenFlow sólo soportan operaciones OpenFlow, mientras que los otros tienen la posibilidad de manejar una o varias VLANs, en modo OpenFlow y el resto para trabajar en modo normal (Hidalgo I. D., 2014).

Los conmutadores OpenFlow constan de uno o más tablas de flujos, quienes realizan la búsqueda de paquetes hacia un canal OpenFlow de un controlador externo. El controlador gestiona el conmutador a través del protocolo. Con el uso de este protocolo, se puede agregar, eliminar el flujo de entradas, tanto reactiva y proactivamente (Ben Pfaff, 2011).

1.6.1.3 Puertos OpenFlow

Los puertos OpenFlow son tres:

- **Puertos físicos:** corresponden a la interfaz de hardware del conmutador. En ambientes virtualizados representan los puertos creados virtualmente sobre el conmutador virtual. La asignación de una interfaz con un puerto es unívoca.
- **Puertos lógicos:** no tienen correspondencia a un puerto físico como tal y son utilizados en métodos non-OpenFlow (túneles, agregación). Un puerto lógico puede estar

relacionado a varios puertos físicos. La diferencia fundamental entre un puerto lógico y un físico, es que el primero tiene un campo de metadata extra llamado Tunnel-ID.

- **Puertos reservados:** para acciones específicas, como por ejemplo el envío de información al controlador, inundaciones, etc. Algunos de estos puertos reservados son requeridos en comunicaciones OpenFlow, entre estos el puerto all, puerto controller, puerto table, puerto in_port y el puerto an. (Barona, 2013).

1.6.1.4 Tablas OpenFlow

Cada tabla de flujo contiene un grupo de entradas; cada entrada de flujo campos coincidentes, contadores e instrucciones que son aplicables en cada campo coincidente (Ben Pfaff, 2011).

Existen tres tipos de tablas:

- **Tabla de flujo:** permite relacionar los paquetes entrantes con un flujo y el conjunto de acciones específicas que debe llevar a cabo. Puede existir una o varias tablas de flujo las cuales funcionan como Pipeline.
- **Tabla de grupo**: un grupo representa un conjunto de acciones para inundación u operaciones de reenvió más complejas. Permite el reenvío de múltiples entradas de flujos hacia un solo identificador, similar a un Gateway. Este proceso permite que acciones de salida comunes sean tratadas de forma más eficiente.
- **Tabla Meter:** puede desencadenar algunas acciones de performance de un flujo, como calidad de servicio (Barona, 2013).

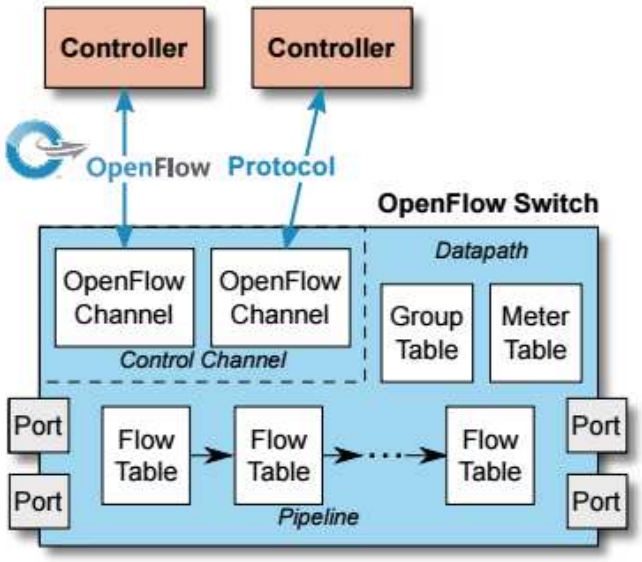


Figura 1. 4. Conmutador OpenFlow

Fuente: (Fundation, 2014)

La cola OpenFlow, de todos los conmutadores OpenFlow, consta de múltiples tablas de flujo, cada uno consta de múltiples flujos de entradas. La cola OpenFlow define el proceso en como los paquetes interactúan con las tablas de flujo. Un conmutador OpenFlow con solamente una tabla de flujo es válido, en estos casos el proceso Pipeline es simplificado (Ben Pfaff, 2011).

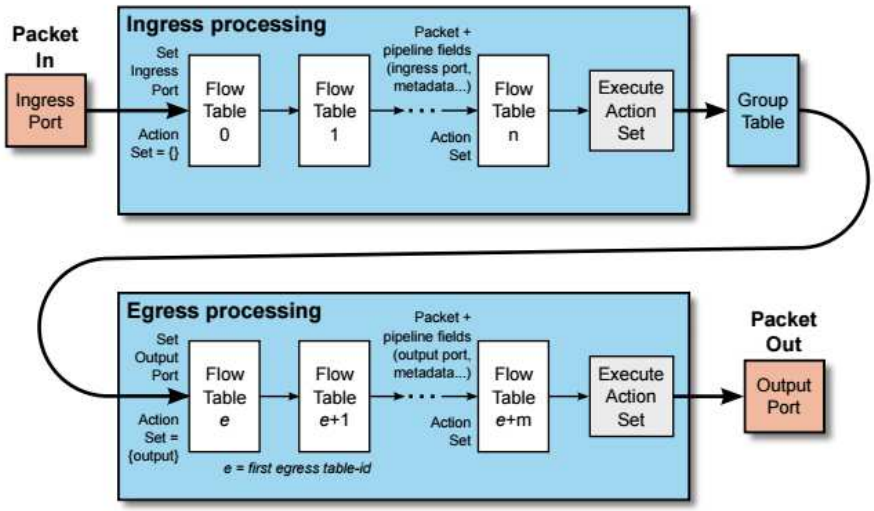


Figura 1. 5. Flujo de Paquetes a través de OpenFlow Pipeline.

Fuente: (Fundation, 2014)

Las tablas de flujo de un conmutador OpenFlow son enumeradas secuencialmente. El proceso de formación de la cola siempre empieza en el primer flujo de la tabla: el paquete se compara primero con las primeras entradas de flujo. Dependiendo del resultado de la primera tabla se pueden utilizar las otras tablas de flujo (Ben Pfaff, 2011).

Las tablas de flujos contienen múltiples entradas que están compuesta por:

- **Campo de coincidencia:** establece los prerrequisitos para que a un paquete se le aplique una serie de instrucciones, los campos que se pueden evaluar son los encabezados de paquetes, puertos lógicos y físicos y de metadatos.
- **Prioridad:** establece un valor para que sea evaluado el flujo en el proceso de formación de la cola.
- **Contadores:** se actualiza cada vez que es procesado un paquete.
- **Instrucciones:** contiene una serie de acciones, ejecutadas por el proceso de formación de la cola.
- **Tiempo de expiración:** máximo tiempo que permanece una entrada de flujo, ya sea porque no se utiliza durante un espacio de tiempo o simplemente fue creado para un tiempo determinado.
- **Cookies:** valor seleccionado por el controlador para filtrar las estadísticas o modificaciones que se le hace a un flujo.
- **Banderas:** banderas alteran la forma en que las entradas de flujo se gestionan, por ejemplo, la bandera OFPFF_SEND_FLOW_REM desencadena el flujo de mensajes eliminados para esa entrada (Hidalgo I. D., 2014).

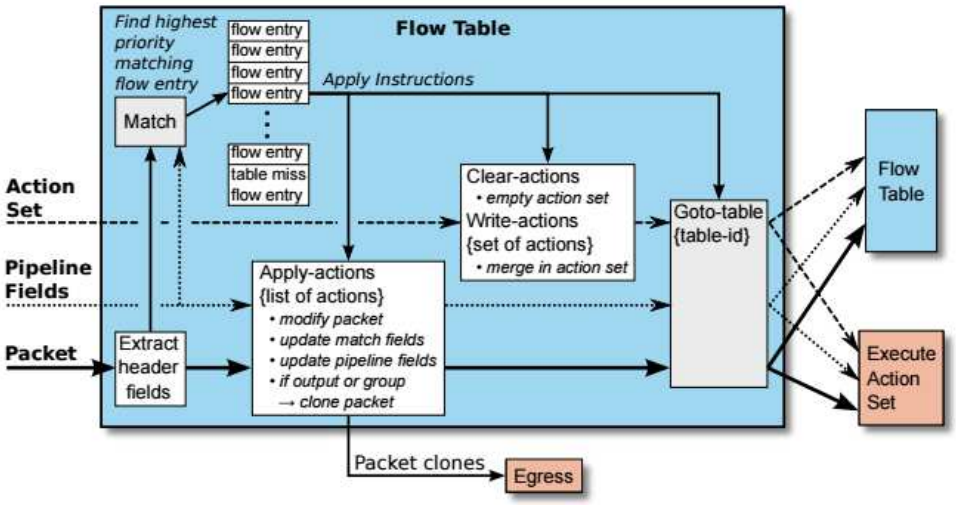


Figura 1. 6. Tabla de flujo.

Fuente: (Fundation, 2014)

1.6.1.5 Tabla de Grupo.

Una tabla de grupo consta de entradas de grupo. La posibilidad de que una entrada de flujo apunte a un grupo permite que OpenFlow represente métodos adicionales de reenvío (FOUNDATION, 2014).

Cada entrada de grupo tiene un identificador de grupo que contiene:

- **Identificador de Grupo:** 32 bits que identifica de forma exclusiva el grupo OpenFlow.
- **Tipo de Grupo:** para determinar la semántica de un grupo.
- **Contadores:** actualizado cuando los paquetes son procesados por un grupo.
- **Contenedores de acción:** una lista ordenada de contenedores de acción, donde cada contenedor contiene un conjunto de acciones que se deben ejecutar con sus parámetros asociados (FOUNDATION, 2014).

➢ **Tipo de Grupo.**

A continuación se definen los tipos de grupos:

- **Todo:** ejecutar todos los contenedores del grupo. Este grupo se utiliza para el reenvio de multidifusión (multicast) o difusión (broadcast). El paquete se clona

para cada contenedor del grupo. Si un contenedor dirige el paquete directamente a un puerto de entrada, este paquete clonado es descartado. Si el controlador quiere reenviar al puerto de entrada, el puerto debe incluir un contenedor extra que incluya una acción de salida al puerto virtual OFPP_IN_PORT.

- **Selecto:** ejecutar un contenedor en el grupo. Los paquetes se envían un único del grupo, basado en un algoritmo de selección externo a OpenFlow. Cuando cae un puerto especificado en un contenedor de un grupo seleccionado, el conmutador puede restringir la selección del contenedor para al resto (aquellos con acciones de reenvio a puertos activos) en lugar de descartar los paquetes destinados a ese puerto. Este comportamiento puede reducir la interrupción por un enlace o conmutador caído.
- **Indirecto:** ejecuta el contenedor definido en el grupo. Permite múltiples flujos o grupos apunten a un identificador de grupo común, apoyando más rápido, lo que permite una convergencia más rápida y eficiente. Este tipo de grupo es idéntico a un grupo con un solo contenedor.
- **Conmutación rápida ante errores:** ejecuta el primer contenedor activo. Cada contenedor de acción se encuentra asociado a un puerto y/o grupo específico que controla su funcionamiento. Este tipo de grupo permite que el conmutador para cambiar el reenvío sin la intervención del controlador. Si no hay contenedores activos, los paquetes se descartan. (FOUNDATION, 2014).

1.6.1.6 Campos de coincidencias.

La Tabla 1.2 muestra los campos de coincidencia con los cuales son comparados los paquetes de entrada. Si el conmutador soporta máscaras de bits arbitrarios en los campos de origen y destino Ethernet y/o los campos de origen y destino IP, estas máscaras pueden especificar con mayor precisión las coincidencias de los paquetes de entrada con los campos de la tabla. Los campos en el OpenFlow están listos en la Tabla 1.2 y los detalles de las propiedades de cada campo se describen en la Tabla A.1 (ver en anexos). Además de las cabeceras de los paquetes, las coincidencias también se pueden realizar en contra de los campos de puertos de ingreso y metadatos. El metadato puede ser usado para pasar información entre las tablas del conmutador (FOUNDATION, 2014).

Tabla 1. 2. Campos de los paquetes que utilizados para que coincida con las entradas de flujo.

Ingress Port	Metadata	Ether src	Ether dst	Ether type	VLAN id	VLAN priority	MPLS label	MPLS traffic class	IPv4 src	IPv4 dst	IPv4 proto / ARP opcode	IPv4 ToS bits	TCP / UDP / SCTP src port ICMP Type	TCP / UDP / SCTP dst port ICMP Code

Fuente: (FOUNDATION, 2014)

1.6.1.7 Contadores.

Los contadores pueden ser mantenidos por cada tabla, flujo de entrada, puerto, cola, grupo, grupo de contenedores, medidor de la tasa de paquetes y meta data. Los contadores compatibles con OpenFlow pueden ser implementados mediante software y mantenidos encuestando los

contadores de hardware con rangos más limitados. La tabla 1.3 contiene el conjunto de contadores definidos por la especificación (FOUNDATION, 2014).

Tabla 1.3 Lista de contadores.

Contador	Bits	
Por Tabla de Flujo		
Referencia del Contador (entradas activas)	32	Requerido
Paquetes de Búsquedas	64	Opcional
Paquetes de Coincidencia	64	Opcional
Por Flujo de Entrada		
	64	Opcional
Paquetes Recibidos	64	Opcional
Duración (segundos)	32	Requerido
Duración (nanosegundos)	32	Opcional
Por Puerto		
Paquetes Recibidos	64	Requerido
Paquetes Transmitidos	64	Requerido
Bytes Recibidos	64	Opcional
Bytes Transmitidos	64	Opcional
Drops Recibidos	64	Opcional
Drops Transmitidos	64	Opcional
Errores Recibidos	64	Opcional
Errores Transmitidos	64	Opcional
Errores Recibidos en la Alineación de trama	64	Opcional
Errores de Saturación Recibidos	64	Opcional
Errores CRC Recibidos	64	Requerido
Colisiones	64	Opcional
Duración (segundos)	32	Requerido
Duración (nanosegundos)	32	Opcional
Por Cola		
Paquetes Transmitidos	64	Requerido
Bytes Transmitidos	64	Opcional
Errores de Saturación Transmitidos	64	Opcional
Duración (segundos)	32	Requerido
Duración (nanosegundos)	32	Opcional
Por Grupo		
Contador de Referencia (entradas de flujo)	32	Opcional
Contenedor de Paquete	64	Opcional
Byte Contenedor	64	Opcional
Duración (segundos)	32	Requerido
Duración (nanosegundos)	32	Opcional
Por Grupo de Contenedor		
Contenedor de Paquete	64	Opcional
Byte Contenedor	64	Opcional
Medidor de la Tasa de Paquetes		
Contenedor de Flujo	32	Opcional
Contenedor de Byte de entradas	64	Opcional
	64	Opcional
Duración (segundos)	32	Requerido
Duración (nanosegundos)	32	Opcional
Por Meter Band		
Contenedor de Paquete	64	Opcional
Contenedor de Byte	64	Opcional

Fuente: (FOUNDATION, 2014)

1.6.1.8 Instrucción.

Cada entrada de flujo contiene un conjunto de instrucciones que se ejecutan cuando un paquete coincide con la entrada. Estas instrucciones dan lugar a cambios en el paquete, el conjunto de acciones y/o el procesamiento del encolamiento (FOUNDATION, 2014).

No se requiere un conmutador para soportar todos los tipos de instrucciones, sólo aquellos marcados con "Instrucción Requerida" a continuación. El controlador también puede consultar al conmutador acerca de cuál de los tipos de "Instrucción Opcional" soporta:

- *Instrucción Opcional:* **Apply-Actions (Acciones Aplicadas) action (acción) *(s)*:** aplica la (s) acción (es) específica (s) inmediatamente, sin ningún cambio en el conjunto de acciones. Esta instrucción puede usarse para modificar el paquete entre dos tablas o para ejecutar múltiples acciones del mismo tipo. Las acciones se especifican como una lista de acciones
- *Instrucción Opcional:* **Clear-Actions (Acciones de Limpieza):** limpia todas las acciones en conjunto de manera inmediata.
- *Instrucción Requerida:* **Write-Actions action (Acción de escritura acción) *(s)*:** combina la acción (s) especificada en el conjunto de la acción actual. Si existe una acción del tipo dato en el conjunto actual, sobrescribir, de lo contrario añadirlo. Si una acción de campo definida con un tipo de campo dado existe en el conjunto actual, se sobrescribe, de lo contrario, se agrega.
- *Instrucción Opcional:* **Write-Metadata *metadata / mask (Escribir-Metadata metadata / mascara)*:** escribe el valor de metadatos de máscaras en el campo de metadatos. Las máscara específica las que deben ser modificados de los bits de registro de metadatos (i.e. new metadata = old metadata & ˜mask | value & mask).

- *Instrucción Opcional:* **Stat-Trigger *stat thresholds***: Genere un suceso para el controlador si algunas de las estadísticas de flujo cruzan uno de los valores de stat thersholds.
- *Instrucción Requerida:* **Goto-Table *next-table-id*:** indica la siguiente tabla del proceso de encolamiento. El identificador de la tabla debe ser mayor que el id de la tabla actual. Las entradas de flujo de la última tabla del encolamiento no pueden incluir esta instrucción. No se requieren conmutadores OpenFlow con una sola tabla de flujo para implementar esta instrucción (FOUNDATION, 2014).

El conjunto de instrucciones asociada con una entrada de flujo que contiene un máximo de instrucción de cada tipo. Las instrucciones del experimentador son identificadas por su experimentador-id y experimentador-tipo, por lo tanto, el conjunto de instrucciones puede contener un máximo de una instrucción experimentador para cada combinación de experimentador-id y experimentador de tipo. Las instrucciones del conjunto se ejecutan en el orden especificado por esta lista anterior. En la práctica, las únicas restricciones se dan cuando se ejecuta antes de la instrucción Write-Action y que Goto-Table se ejecuta en último lugar (FOUNDATION, 2014).

1.6.1.9 Action Set

Una Action Set se encuentra asociada con cada paquete. Se encuentra vacía por defecto. Una entrada de flujo puede modificar la acción que se establece mediante una instrucción Write-Accion o una instrucción Clear-Action asociada a una en particular. El conjunto de acciones se realiza entre las tablas de flujo. Cuando un conjunto de instrucciones no contiene una instrucción Goto-Table, cuando el procesamiento de encolamiento se detiene y las acciones del paquete se ejecutan (FOUNDATION, 2014).

El conjunto de acciones para el procesamiento de salida se inicializa al comienzo del procesamiento de salida con una acción de salida para el

puerto de salida actual, mientras que el conjunto de acciones para el proceso de ingreso comienza vacío (FOUNDATION, 2014).

Las acciones de un conjunto de acciones se aplican en el orden especificado a continuación, sin importar el orden en que se agregaron al conjunto. Si un conjunto de acciones contiene una acción de grupo, las acciones apropiadas del contenedor del grupo también se ven aplicadas en el siguiente orden especificado. El conmutador puede apoyar la acción arbitraria del orden de ejecuciones a través de la lista de acciones de la instrucción Apply-Actions.

1. **Copy TTL interno:** aplica copy TTL para acciones internas.
2. **Pop:** aplica todas las etiquetas pop de las acciones del paquete.
3. **Push-MPLS:** aplicar la acción de push de etiquetas MPLS al paquete.
4. **Push-PBB:** aplica la acción de push de etiqueta PBB al paquete.
5. **Push-VLAN:** aplica la acción de push de etiquetas VLAN del paquete.
6. **Copy TTL externo:** aplica la copy TTL hacia fuera de la acción al paquete.
7. **Decremento TTL:** aplica decremento de la acción TTL al paquete.
8. **Set:** aplica todas las acciones de campo establecido al paquete.
9. **QoS:** aplica todas las acciones QoS, como el contador y establecer la cola en el paquete.
10. **Grupo:** se especifica una acción de grupo, aplicada en las acciones del contenedor del grupo relevante en un orden especificado por una lista.
11. **Salida (output):** si no es especificada la acción del grupo, el paquete será enviado por un puerto específico de la lista (FOUNDATION, 2014).

1.6.1.10 Canal OpenFlow

Es la interfaz que conecta al conmutador OpenFlow con el controlador, mediante la cual puede administrar y gestionar al conmutador (Barona, 2013).

El conmutador puede tener varios canales OpenFlow cada uno con un controlador diferente. Cuando el controlador se encuentra en la misma red que administra el conmutador, el controlador estará en modo in-band, caso contrario se encontrará en modo out-band. El conmutador y el controlador usualmente se comunican a través de una conexión segura con TLS (Barona, 2013).

Por defecto el canal OpenFlow entre un conmutador y un controlador es una conexión de red única, sin embargo el canal puede estar compuesto por una conexión principal y algunas auxiliares. Cada conexión desde el conmutador al controlador se identifica mediante el *datapath ID* y de un *auxiliary ID*. Estas clases de condiciones se las conoce como auxiliares (Barona, 2013).

1.6.1.11 Mensajes OpenFlow

Se tiene tres clases de mensajes:

- **Controlador del conmutador:** los mensajes del controlador/conmutador son iniciados por el controlador y pueden o no requerir una respuesta del conmutador:
  - **Características (feautres):** el controlador puede solicitar la identidad y las capacidades básicas de un conmutador enviando una solicitud de características; El conmutador debe responder con una respuesta de características que especifica la identidad y las capacidades básicas del conmutador. Esto se realiza comúnmente al establecer el canal OpenFlow.
  - **Configuración:** el controlador es capaz de establecer y consultar parámetros de configuración en el

conmutador. El conmutador sólo responde a una consulta del controlador.

- **Modificación de estado (modify-state):** los mensajes de estado de modificación son enviados por el controlador para gestionar el estado en los conmutadores. Su propósito principal es agregar, eliminar y modificar las entradas de flujo / grupo e insertar / quitar los buckets de acción del grupo en las tablas de OpenFlow y establecer las propiedades del puerto del conmutador.
- **Estado de lectura (read-state):** los mensajes de estado de lectura son utilizados por el controlador para recopilar diversas informaciones del conmutador, como la configuración actual, estadísticas y capacidades. La mayoría de las solicitudes y respuestas de estado de lectura se implementan utilizando secuencias de mensajes de varias partes
- **Salida de paquetes (packet-out):** estos son utilizados por el controlador para enviar paquetes fuera de un puerto especificado en el conmutador y para reenviar paquetes recibidos a través de mensajes de paquetes de entrada (packet-in). Los mensajes de salida de paquetes (packet-out) deben contener un paquete completo o una ID de búfer que haga referencia a un paquete almacenado en el conmutador. El mensaje también debe contener una lista de acciones que se aplicarán en el orden en que se especifican; Una lista vacía de acciones descarta el paquete.
- **Barrier:** los mensajes de solicitud / respuesta de barrier son utilizados por el controlador para asegurar que se han cumplido las dependencias de los mensajes o para recibir notificaciones para las operaciones completadas.

- **Solicitud role (role-request):** el controlador utiliza los mensajes de solicitud de función para establecer la función de su canal OpenFlow, establecer su ID de controlador o consultarlos. Esto es útil sobre todo cuando el conmutador se conecta a varios controladores
- **Configuración asíncrona (asynchronous-configuration):** los mensajes de configuración asíncrona son utilizados por el controlador para establecer un filtro adicional en los mensajes asíncronos que desea recibir en su canal OpenFlow o para consultar ese filtro. Esto es útil sobre todo cuando el conmutador se conecta a múltiples controladores y normalmente se realiza al establecer el canal OpenFlow (Hidalgo I. D., 2014).

➢ **Asíncrono (asynchronous): l**os mensajes asíncronos se envían sin que un controlador los solicite desde un conmutador. Los conmutadores envían mensajes asincrónicos a los controladores para denotar un cambio de estado de llegada o cambio de paquete. A continuación se describen los principales tipos de mensajes asíncronos.

- **Packet-in:** transfiere el control de un paquete al controlador. Para todos los paquetes reenviados al puerto reservado de CONTROLLER utilizando una entrada de flujo o la entrada de flujo de falta de tabla, siempre se envía en un paquete a los controladores. Otro procesamiento, como la comprobación TTL, también puede generar eventos de paquete para enviar paquetes al controlador. Si un paquete está almacenado en la memoria intermedia, se puede configurar el número de bytes del paquete original a incluir en el paquete de entrada. De forma predeterminada, es 128 bytes. Para el paquete de entrada generado por una acción de salida en unas entradas de flujo o grupo de buckets, se puede

especificar de forma individual en la propia acción de salida, para otros paquetes de entrada se puede configurar dentro de la configuración del conmutador.

- **Flujo eliminado (flow-removed):** informa al controlador acerca de la eliminación de una entrada de flujo de una tabla. Los mensajes eliminados por flujo sólo se envían para las entradas de flujo con el indicador OFPFF_SEND_FLOW_REM establecido. Se generan como resultado de una solicitud de eliminación de flujo de controlador o del proceso de caducidad de flujo de conmutador cuando se sobrepasa uno de los tiempos de espera de flujo
- **Estado del puerto (port-status):** el conmutador notifica al controlador que un puerto cambio de estado. Estos eventos incluyen el cambio en los eventos de configuración del puerto, por ejemplo, si fue bajado directamente por un usuario, y los eventos de cambio de estado del puerto, por ejemplo, si el enlace se redujo.
- **Role-status:** informar al controlador de un cambio de su papel. Cuando un nuevo controlador se elige como maestro, se espera que el conmutador envíe mensajes de estado de función al controlador maestro anterior.
- **Estado del controlador (controller-status):** informa al controlador cuando cambia el estado de un canal OpenFlow. Esto puede ayudar al procesamiento de conmutación por error si los controladores pierden la capacidad de comunicarse entre sí.
- **Monitor de flujo (Flow-monitor):** Informar al controlador de un cambio en una tabla de flujo. Un controlador puede definir un conjunto de monitores para rastrear los cambios en las tablas de flujo (Hidalgo I. D., 2014).

- **Simétrico (symmetric):** los mensajes simétricos se envían sin solicitud, en cualquier dirección
    - **Hello:** los mensajes se intercambian entre el controlador y el conmutador, que se utilizan para iniciar la conexión entre los dos.
    - **Echo:** *request / reply* utilizado de forma principal para confirmar que hay conexión entre el controlador y el conmutador, y sirve para medir la latencia o el ancho de banda.
    - **Error:** los mensajes de error son utilizados por el conmutador o el controlador para notificar los problemas al otro lado de la conexión. Son utilizados principalmente por el conmutador para indicar una falla de una petición iniciada por el controlador.
    - **Experimentador (experimenter):** los mensajes del experimentador proporcionan una forma estándar para que los conmutadores de OpenFlow ofrezcan funcionalidad adicional dentro del espacio de tipo de mensaje OpenFlow. Este es un área de puesta en escena para las características de futuras revisiones de OpenFlow (Hidalgo I. D., 2014).

1.6.2 OpenStack

Este proyecto nace en octubre del 2010, por la empresa Rackspace Cloud y por la agencia espacial estadounidense NASA. Actualmente es administrada por la Fundación OpenStack con el apoyo de más de 150 empresas, entre las que se pueden mencionar son Rackspace, Oracle, AMD, Cisco, Canonical, IBM, HP, Dell Red Hat, Suse Linux, VMware, Yahoo y KIO Networks en América Latina (Nelson Rodríguez, 2014).

Es un software de código abierto que permite la implementación de una Infraestructure as a Service (Iaas) a través de múltiples servicios que,

de manera coordinada, cumplen diferentes propósitos para lograr el correcto funcionamiento de dicha infraestructura (Brian Galarza, 2015).

OpenStack cree en un open source, diseño y desarrollo abierto, todo en una comunidad abierta que fomenta la participación de cualquiera. La visión a largo plazo de OpenStack es producir una plataforma omnipresente de cloud computing de código abierto que satisfaga las necesidades de los proveedores de nube públicos y privados, independientemente del tamaño. Los servicios de OpenStack controlan grandes agrupaciones de recursos de computación, almacenamiento y redes en un centro de datos (OPENSTACK, 2017).

Esta plataforma ayuda con la creación de instancias virtuales, que contienen sistemas operativos en la que es posible instalar una gran cantidad de aplicaciones como instancias para administrador de contenedores (Docker) o instancias de bases de datos no relacionales (MongoDB), entre otros (Hernández, 2015).

OpenStack se encuentra totalmente escrito en Python y es el tercer proyecto open source en importancia a nivel mundial; y se lo describe como “un sistema operativo de cloud”, por ser el coordinador de los recursos que sustentan a los servicios (Nelson Rodríguez, 2014).

La arquitectura, como se muestra en la figura 1.7, recomendada se encuentra pensada para desplegarse en múltiples equipos debido a la complejidad de las tareas y la carga del computador, usualmente se recomienda utilizar tres servidores, uno sería utilizado como maestro (controlador), uno para la gestión de la red y otro para alojar las instancias virtuales (computadoras) (Hernández, 2015).

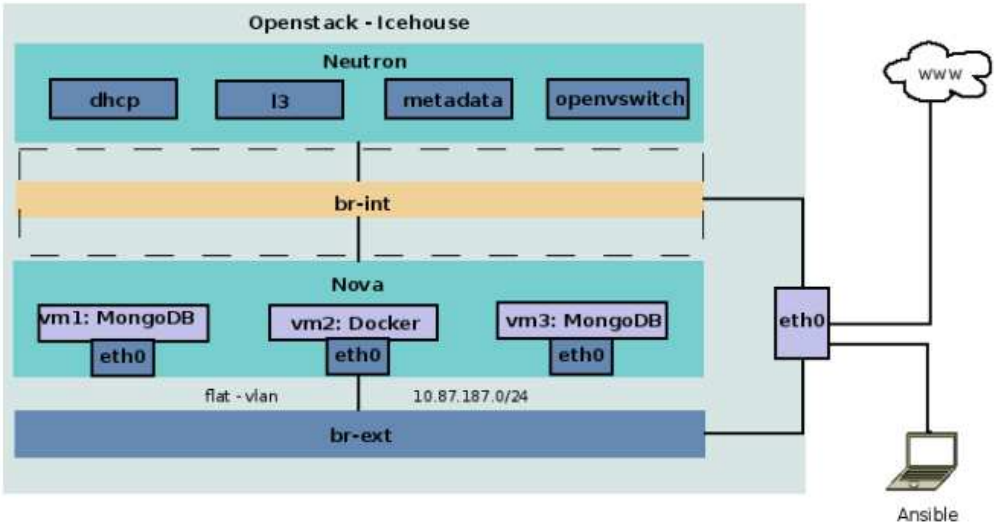


Figura 1. 7. Arquitectura OpenStack

Fuente: **(Hernández, 2015)**

La nube de OpenStack (ver figura 1.8) se encuentra compuesta de cuatro nodos con distintas funciones dependiendo de los componentes instalados, que a continuación se mencionan:

- **Nodo de control (Control node):** encargado de la gestión de las instancias con Nova y de la orquestación del resto de componentes.
- **Nodo computacional (Compute node):** encargado de la ejecución de las instancias como máquinas virtuales sobre un hipervisor. Los protocolos de red de almacenamiento y el plugin de red Swicth.
- **Nodo de red (Network node):** encargado de la comunicación de las redes internas con el exterior lo cual permite network connectivity-as-a-service, mediante Quantum que está basado en OpenFlow.
- **Nodo de almacenamiento (Storage node):** Nodo encargado de la gestión del almacenamiento. Los principales componentes son Glance, Cinder y Swift (Hernández, 2015).

Cada servicio proporciona una API abierta para que todos estos recursos puedan administrarse a través de un panel que proporcione a los

administradores de control mientras que habilita a los usuarios a proporcionar recursos a través de una interfaz web, un cliente de línea de comandos o kits de desarrollo de software que admiten la API. Muchas API de OpenStack son extensibles, lo que significa que puede mantener la compatibilidad con un conjunto básico de llamadas mientras proporciona acceso a más recursos e innova a través de extensiones de API (OPENSTACK, 2017).

El proyecto OpenStack es una colaboración global de desarrolladores y tecnólogos de computación en nube. El proyecto produce una plataforma abierta de cloud computing estándar tanto para nubes públicas como privadas. Al centrarse en la facilidad de implementación, escalabilidad masiva, una variedad de características enriquecidas y una extensibilidad enorme, el proyecto tiene como objetivo ofrecer una solución de nube práctica y confiable para todo tipo de organizaciones (OPENSTACK, 2017).

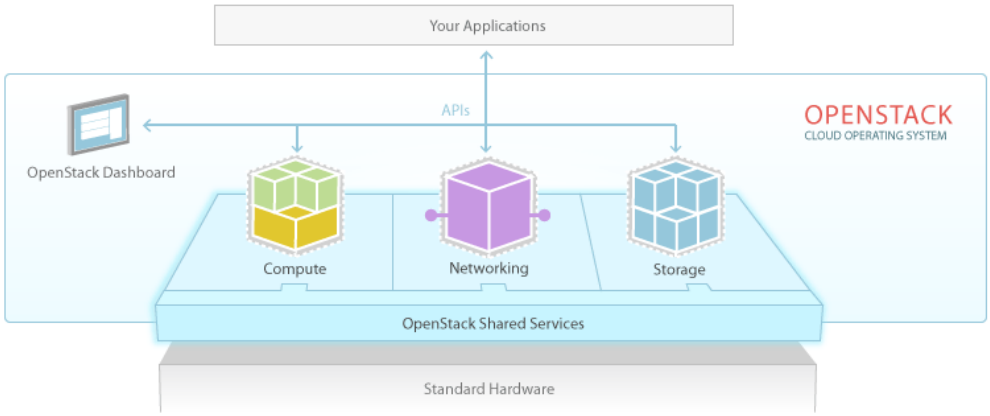


Figura 1. 8. Nube OpenStack

Fuente: (openstack.org, 2015)

La arquitectura de la red posee distintos componentes lógicos de gran importancia, al tratarse de un sistema con una sola interfaz de red se optó por un esquema de red plano, es decir, tanto las instancias como el servidor de Openstack, tienen direcciones IP de la misma sud-red, estas no cuentan con su propio direccionamiento interno o forman parte de una red

segmentada, de haber sido de este modo se requiere de un enrutador lógico gestionado por Neutron para la intercomunicación entre la red de las instancias y el exterior (Hernández, 2015).

Cada instancia tendrá una interfaz virtual de la red que se encuentra conectada a la interfaz física del equipo a través de una tercera interfaz lógica conocida como puente (bridge), esta comunicación entre interfaces es gestionada por el servicio openswitch (plugin Neutron) (Hernández, 2015).

Por otra parte la asignación de direcciones IP es gestionada por el servidor DHCP, el servidor de Metadata permite que las instancias accedan a información del servicio de computo, y el servicio de L3 provee capacidades de red como forwarding y NAT (Hernández, 2015).

La arquitectura conceptual se muestra mediante la figura 1.9:

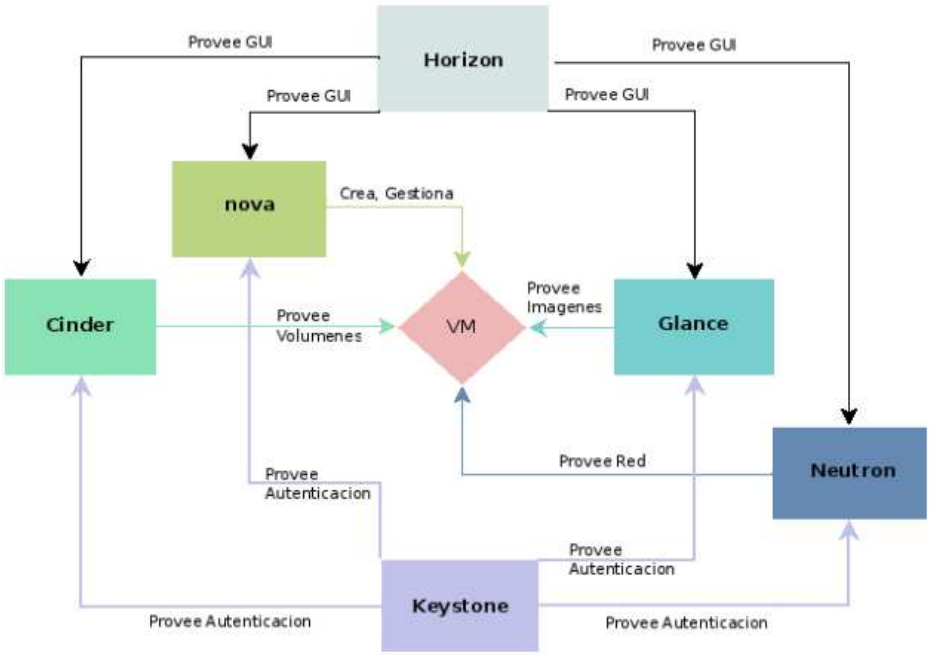


Figura 1. 9. Arquitectura conceptual OpenStack

Fuente: (Hernández, 2015)

Mediante la tabla A.2 (ver en Anexos), se mostrará los servicios que brinda OpenStack.

1.6.3 NETCONF

El protocolo NETCONF define un mecanismo simple a través del cual se puede gestionar un dispositivo de red, se puede recuperar información de datos de configuración y se pueden cargar y manipular nuevos datos de configuración. El protocolo permite al dispositivo exponer una interfaz de API. Las aplicaciones pueden utilizar esta API sencilla para enviar y recibir conjuntos de datos de configuración completos y parciales ((IETF), 2011).

Usa el método remoto RPC, y lo codifica mediante XML, luego lo envía desde un servidor con una sesión segura. El servidor brinda una respuesta codificada en XML. El contenido de la solicitud y la respuesta se describen completamente en DTD XML o esquemas XML, o ambos, permitiendo a ambas partes reconocer las restricciones de sintaxis impuestas en el intercambio ((IETF), 2011).

Un aspecto clave de NETCONF es que permite que la funcionalidad del protocolo de gestión refleje de cerca la funcionalidad nativa del dispositivo. Esto reduce los costos de implementación y permite el acceso oportuno a las nuevas características. Además, las aplicaciones pueden acceder tanto al contenido sintáctico como semántico de la interfaz de usuario nativa del dispositivo ((IETF), 2011).

Una característica particular de este protocolo en particular que lo diferencia de los otros, es que permite a los dispositivos exponer una API utilizada por las aplicaciones para enviar y recibir configuraciones completas o parciales (Rojas, 2013).

Son utilizadas sesiones para realizar el intercambio de datos de configuraciones de los dispositivos de la red. Una sesión de NETCONF, es la conexión lógica entre un administrador de red o una aplicación de configuración de red y un dispositivo de red, el cual debe soportar al menos una sesión NETCONF (Rojas, 2013).

Una sesión NETCONF es la conexión lógica entre un administrador de red o una aplicación de configuración de red y un dispositivo de red. Un dispositivo debe soportar por lo menos una sesión NETCONF y puede

soportar múltiples sesiones. Los atributos globales de configuración pueden ser cambiados durante alguna sesión autorizada, y los efectos son visibles en todas las sesiones. Los atributos específicos de una sesión afecta solo a la sesión en la cual fueron cambiados (Rojas, 2013).

NETCONF utiliza un simple mecanismo basado en RPC para facilitar la comunicación entre un cliente y un servidor. El cliente puede ser un script o una aplicación que normalmente se ejecuta como parte de un administrador de red. El servidor normalmente es un dispositivo de red. Los términos "dispositivo" y "servidor" se utilizan indistintamente en este documento, así como "cliente" y "aplicación" ((IETF), 2011).

La entrega de los datos durante la conexión debe ser confiable y secuencial. Adicionalmente, los recursos solicitados por un servidor para una conexión particular, deben ser automáticamente liberados cuando se cierra la conexión, haciendo la recuperación de fallos sea simple y robusta (Rojas, 2013).

1.6.3.1 Arquitectura NETCONF

La arquitectura se puede dividir en cuatro capas:

1. Capa de transporte seguro provee un camino de comunicación entre el cliente y el servidor. NETCONF se puede superponer sobre cualquier protocolo de transporte que tenga un conjunto básico de requerimientos.
2. Capa de mensajes que proporcionan un mecanismo simple de estructuración de mensajes de transporte, para la codificación de RPCs y notificaciones.
3. Capa de operaciones que define el conjunto de operaciones base del protocolo, llamados como métodos RPC con parámetros codificados en XML.
4. Capa de contenido que se encuentra fuera del alcance de RFC6241 (Rojas, 2013).

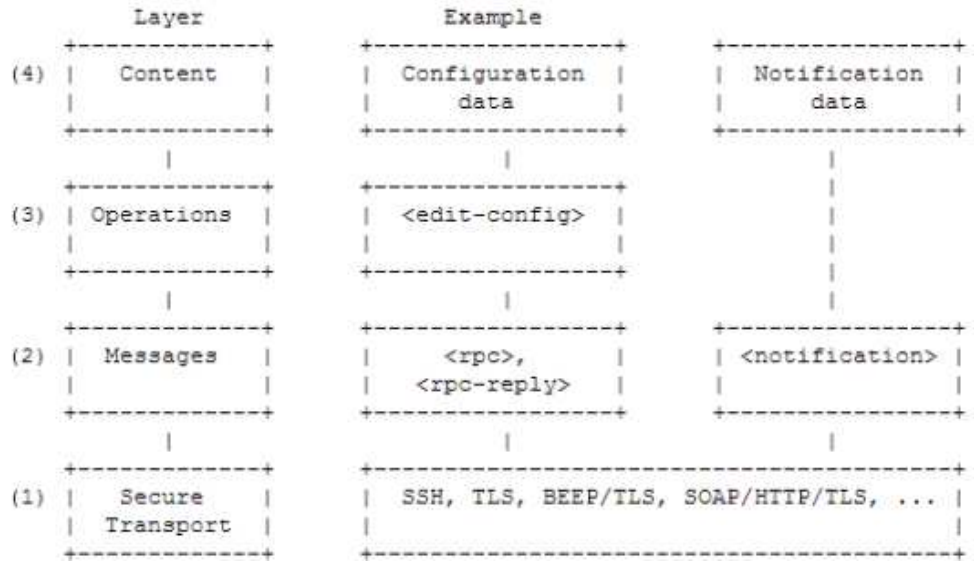


Figura 1. 10. Arquitectura NETCONF

Fuente: ((IETF), 2011)

1.6.3.2 Protocolo de transporte NETCONF

El protocolo de transporte obligatorio es SSH, para permitir la interoperabilidad de gestión y es el encargado de la autenticación del servidor en el servidor y viceversa. Cada una de los pares asume que la información de la autenticación de la conexión ha sido validada por el protocolo de transporte, usando mecanismos lo suficientemente confiables, y que la entidad de los pares ha sido lo suficiente probada (Rojas, 2013).

Siempre debe contar con la configuración de control de acceso SSH (o de otros protocolos que sean soportables en los equipos), para que un cliente pueda autenticarse utilizando los parámetros requeridos. Los permisos de acceso otorgados deben ser cumplidos durante toda la sesión (Rojas, 2013).

1.6.3.3 Formato de codificación XML.

Permite una jerarquización compleja de los datos, los cuales se expresan en formato texto que pueden ser leídos, guardados y manipulados, tanto con herramientas tradicionales de texto, como con herramientas específicas de XML (Rojas, 2013).

Todos los mensajes NETCONF deben estar bien formados en XML y codificados en UTF-8 la cual se encuentra especificado en la RFC368. Si un par recibe un mensaje <rpc> que no está bien formado en XML o no está codificado en UTF-8, deberá responder con un mensaje de error de “mensaje mal formado”. Si la respuesta no es enviada por alguna razón, el servidor debe terminar la sesión (Rojas, 2013).

1.6.3.4 Elementos RCP y RCP-REPLAY.

RCP es usado para encerrar las solicitudes NETCONF enviadas de un cliente a un servidor. Este elemento tiene un atributo obligatorio: “message-id”, el cual es un string escogido por quien envía el RPC y el cual comúnmente se va incrementando en una unidad. Quien recibe el RPC no debe codificar o interpretar este srting, sino que simplemente debe guardarlo y usarlo como atributo de “mensaje-id” en el mensaje <rcp-repley>. Quien envía el RCP debe asegurarse que el valor del “message-id” esta normalizado de acuerdo a las reglas de normalización de los valores de los atributos de XML, definidas en si es que desea que se devuelva sin ser codificado (Rojas, 2013).

Si atributos adicionales están presenten en el elemento <rpc>, el par NETCONF debe retomarlos sin realizarles modificaciones en el elemento <rcp-replay>. Esto incluye cualquier atributo “xmlns” (Rojas, 2013).

RCP-REPLAY es un mensaje enviado en respuesta a un mensaje rcp. El elemento <rcp-replay> tiene un atributo obligatorio: “message-id”, el cual es igual al atributo “message-id” del <rcp> al cual está respondiendo. El servidor NETCONF debe también retomar en el elemento <rcp-replay>, atributos adicionales incluidos en el elemento <rcp> sin ningún tipo de cambio. Los datos de respuesta son codificados como uno o más elementos hijos del elemento <rcp-replay> (Rojas, 2013).

1.6.3.5 Operaciones básicas del protocolo NETCONF

Este protocolo provee un pequeño conjunto de operaciones de bajo nivel para gestionar la configuración de dispositivos y recuperar información de estado de los dispositivos. La base del protocolo provee operaciones para recuperar, configurar, copiar y borrar configuraciones del almacenamiento de datos. La base del protocolo incluye las siguientes operaciones (Rojas, 2013):

- Get
- Get-config
- Edit-config
- Copy-config
- Delete-config
- Lock
- Unlock
- Close-session
- Kill-session (Rojas, 2013).

Una operación de protocolo puede fallar por varias razones, entre las que se pueden encontrar que la operación no es soportada. El dispositivo que inicia una solicitud, no debe asumir que toda operación será exitosa. Los valores retomados en cualquier <rpc-replay>, deben ser revisados para verificar si corresponden a errores (Rojas, 2013).

1.6.3.6 Lenguaje YANG para el protocolo de configuración NETCONF

Es un lenguaje de modelado de datos utilizado para moldear los datos de configuración y los datos de estado manipulados por el protocolo de configuración de red NETCONF, por las RPCs y por las notificaciones de NETCONF. También es usado para moldear las capas de operación y contenido del protocolo de gestión (Rojas, 2013).

Este lenguaje se encuentra definido en el RFC 6020, como el modelo de datos definido en un módulo YANG es representado por XML y como las operaciones NETCONF son usadas para manipular los datos (Rojas, 2013).

Proporciona una descripción clara y concisa de los nodos, así como la interacción entre estos nodos. Los módulos y submódulos son utilizados por YANG, para contener la estructura de los modelos de datos. Un módulo puede importar datos provenientes de otros módulos externos, e incluir, e incluir datos provenientes de submódulos. También, el contenido de la jerarquía de un módulo puede ser aumentado, adicionándole otros nodos de datos definidos en otro módulo (Rojas, 2013).

También establece un balance entre el modelado de datos de alto nivel y el de bajo nivel. El lector del módulo YANG mantiene la vista de alto nivel del modelo de datos, mientras comprende cómo los datos serán codificados en las operaciones NETCONF (Rojas, 2013).

Es un lenguaje extensible, permitiendo que declaraciones de extensión puedan ser definidas por organismos de normalización, proveedores e individuales. La sintaxis de la declaración les permite a estas extensiones coexistir de forma natural con declaraciones YANG normalizadas (Rojas, 2013).

Mantiene compatibilidad con SNMP’s, SMIv2. Los modulos MIB de SIMv2-based pueden ser automáticamente trasladados en módulos YANG para acceso de solo lectura. Sin embargo, YANG no se ocupa de la reversión de YANG a SMIv2 (Rojas, 2013).

CAPÍTULO 2: MIGRACIÓN DE UN CENTRO DE DATOS A SDN

2.1 Migración de un Centro de Datos a Redes Definidas por Software (SDN)

El despliegue de SDN en un centro de datos nuevo es relativamente sencillo, sólo tendría que tomarse en cuenta que el equipamiento tenga soporte para esta nueva tecnología. En cambio, la mayoría de los operadores no se pueden dar el lujo de hacer una migración dura hacia SDN de un centro de datos en producción. La planificación es esencial para allanar el camino hacia una migración gradual y definitiva a esta nueva tecnología (FOUNDATION, 2014).

Para llegar al destino, se deben afrontar una serie de problemas que pasan por el costo, el rendimiento, la disponibilidad del servicio que se presta, la administración y la seguridad. Consiente de esta problemática, la ONF estableció un grupo de trabajo, para discutir temas de seguridad en SDN, que aborda en un resumen las implicaciones en cuanto a seguridad y las consideraciones de implementar SDN en un centro de datos (FOUNDATION, 2014).

Para llevar a cabo la migración se plantean 4 consideraciones o preguntas iniciales (FOUNDATION, 2014):

- ¿Cuáles son las metas de la migración a SDN?
- ¿Cuáles son los primeros pasos para lograr esas metas?
- ¿Cuáles son las opciones o posibles estrategias de migración?
- ¿Si se conocen experiencias previas de migración, cómo podrían contribuir a la estrategia actual? (FOUNDATION, 2014)

La migración a SDN puede suponer un reto desalentador y desafiante, es una tecnología nueva que muchos consideran aún inmadura. Sin embargo, mientras más tiempo se dedique a responder las preguntas anteriores, mejores resultados se conseguirán durante la migración. Los pasos claves para una migración de un centro de datos a SDN son (FOUNDATION, 2014):

- Identificar y priorizar los requisitos básicos que debe cumplir la red SDN. Se debe tener bien claro que la red definida por software no pueden cumplir todos los requisitos iniciales de una red tradicional.
- Preparar la red para la migración. Como se muestra en la figura 2.1, probablemente sea mejor un estado intermedio en que convivan la tecnología tradicional de redes con SDN o un estado intermedio en que sea estándar antes de la migración definitiva.
- Implementar la migración en fases. La migración de los dispositivos requerirá drivers y métodos específicos para cada tipo.
- Validar los resultados. Una vez que se complete la migración, la red final debe ser validada teniendo en cuenta los requisitos y expectativas que se espera de ella (FOUNDATION, 2014).

Figura 2. 1. Etapas de Migración

Fuente: (FOUNDATION, 2014)

2.2 Escenarios de migración para SDN

Los escenarios de migración se dividen en tres categorías principales: de una red tradicional (*legacy*) a una SDN pura (ver figura 2.2), a una red mixta y a una red híbrida. A diferencia de los últimos dos escenarios, la migración de una red tradicional a una SDN pura es el menos complejo porque no se necesita soporte para la integración e interoperabilidad con equipamiento no OpenFlow (FOUNDATION, 2014).

El escenario que comprende la migración hacia una red mixta supone la coexistencia de los nuevos dispositivos OpenFlow con los tradicionales, como conmutadores y enrutadores, e interfaces al plano de control de la red tradicional. Los dispositivos OpenFlow y los tradicionales deben intercambiar información de enrutamiento a través del plano de control de la red antigua. El despliegue de una red híbrida supone el uso de dispositivos OpenFlow, tradicionales e híbridos OpenFlow/tradicionales con interfaces al controlador SDN y hacia el plano de control de la red antigua. Los tres escenarios de migración a SDN son relevantes y aplicables a múltiples segmentos y niveles de la red (FOUNDATION, 2014).

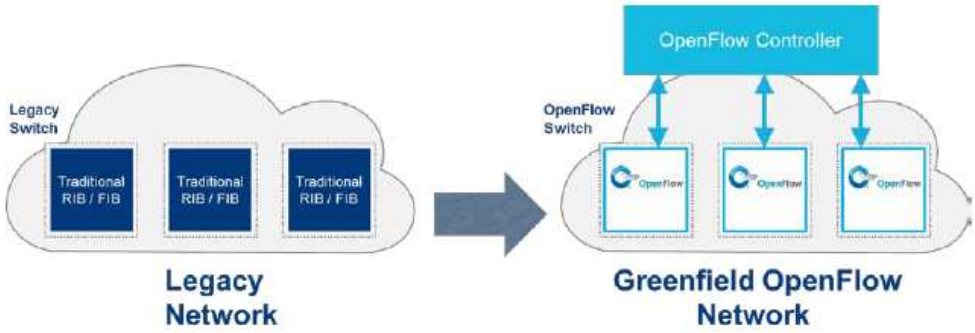


Figura 2. 2. Migración de una red tradicional (*legacy*) a una SDN pura.

Fuente: (FOUNDATION, 2014)

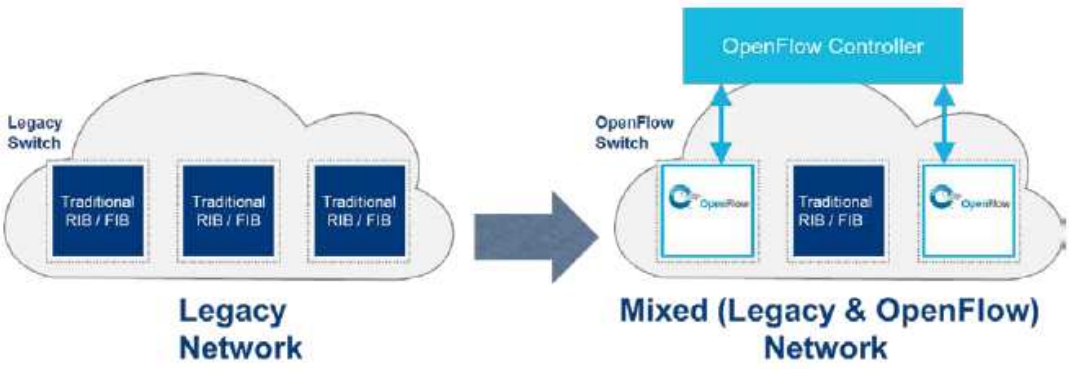


Figura 2. 3. Migración a una red mixta.

Fuente: (FOUNDATION, 2014)

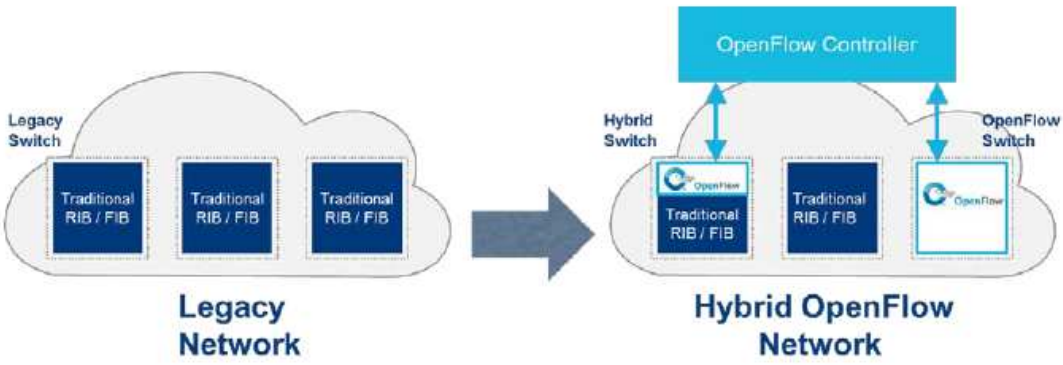


Figura 2. 4. Red Híbrida SDN

Fuente: (FOUNDATION, 2014)

Dos de los ejemplos más publicitados de migración hacia SDN son los de la Universidad de Stanford y Google. En ambos casos la migración fue hacia una red híbrida. Una SDN híbrida permite a los ingenieros de red introducir nuevas tecnologías SDN, como OpenFlow, en entornos tradicionales, sin una revisión completa de la arquitectura de red. En una SDN híbrida, los ingenieros pueden ejecutar tecnologías SDN y protocolos de conmutación estándar de forma simultánea sobre el hardware físico. Un administrador de red puede configurar el plano de control de SDN para descubrir y controlar ciertos flujos de tráfico, mientras que los protocolos de red distribuida tradicionales continúan dirigiendo el resto del tráfico en la red (FOUNDATION, 2014).

El estándar OpenFlow v1.3 incluye especificaciones para las interacciones híbridas entre OpenFlow y el tráfico que no es OpenFlow para permitir la migración temprana a SDN. Éste estándar especifica dos tipos de conmutadores compatibles con OpenFlow: OpenFlow puros e híbridos. Los conmutadores OpenFlow híbridos soportan OpenFlow y la tecnología de conmutación tradicional Ethernet. Muchos fabricantes de hardware de red que han añadido el soporte de hardware a sus conmutadores y enrutadores ofrecen la habilidad de hacerlos funcionar en modo híbrido (FOUNDATION, 2014).

En una migración se deben tener en cuenta los siguientes aspectos:

- Se deben identificar los escenarios de red junto con las directrices y recomendaciones de despliegue.
- La red objetio y sus requisitos esenciales debes estar plenamente identificados. No todos los requisitos de la red de inicio tradicional pueden ser satisfechos, al menos incialmente, por la red SDN de destino.
- El objetivo que persigue la implementación de la tecnología es simplificar la red y disminuir el costo de operación. Unobjetivo secundario es mejorar la utilización.
- La migración misma a la red de destino puede ser una fuente de riesgos. Las interrupciones durante la migración, el deterioro de las herramientas de diagnóstico y supervisión, o simplemente la extensión y el rendimient de la nueva tecnología, son condiciones que se pueden encontrar durante las etapas intermedias.

Basado en el estándar OpenFlow, se deben cumplir los siguientes objetivos y requisitos de alto nivel:

- El software de red de destino debe ser compatible con la capacidad de programación, a través de las API, capaces de extender y combinación la funcionalidad a través de la exposición de las características de los dispositivos subyacentes.
- La red de destino debe ser reparable, soportando acutalizaciones de software dinámicas, con interrupciones del servicio de forma mínima y con actualizaciones automatizadas y reversión.
- La red de destino soporta la heterogeneidad, con múltiples dispositivos de diferentes proveedores. La migración de servicios debe considerarse a través de esta infraestructua y herramientas de organización del flujo de trabajo son opcionales.

- La red destino debe ser fácil de mantener dentro del conjunto necesario de software, herramientas y simuladores. Cualquiera de las herramientas existentes deben ser comprobadas para trabajar con la red, se deben definir o desarrollar herramientas alternativas para garantizar el funcionamiento y trasnparencia.
- La red de partida puede requerir preparación y necesidad de transformarse en un estado intermedio limpio del cual el resto de la migración puede prodeder de forma segura es necesario especificar recomendaciones, directrices y herramientas para esta fase de preparación.
- Una vez que se complete la migración, la red de destino debe ser validada contra una serie de documentos de requisitos o expectativas. Se deben identificar directrices, sistemas y herramientas para validar la migración completa.

2.4 Casos de migraciones exitosas

2.4.1 Migración de Google.

La migración de la WAN de Google se llevó a cabo para aumentar la escalabilidad, flexibilidad y agilidad en la gestión de la red que brinda a través de Internet los servicios de Google, incluyendo Google+, Gmail, YouTube, Google Maps, y otros (Foundation, 2014) (Sushant Jain, 2013).

Google posee dos redes separadas y con requerimientos diferentes. Una red WAN que une múltiples centros de datos (B4) y una red que intercambia tráfico con otros dominios de Internet y que brinda los servicios más populares de la compañía. Ambas redes soportan miles de aplicaciones que mueven grandes volúmenes de tráfico y son sensibles a la latencia, todas administradas con diferentes niveles de prioridad (Foundation, 2014) (Sushant Jain, 2013).

La red interna de Google es en la actualidad una red basada en OpenFlow y un conocido caso de uso de SDN. Esta red fue construida con una arquitectura de tres capas: infraestructura, de controladores y de

servicios globales. La capa de infraestructura no realiza funciones complejas, sólo envía tráfico. La capa de controladores está compuesta por servidores controladores de red (NCS) que alojan a los controladores OpenFlow y a las aplicaciones de control de la red (NCA). La capa de servicios globales está compuesta por aplicaciones que permiten el control centralizado de toda la red (Foundation, 2014) (Sushant Jain, 2013).

La migración híbrida para Google B4 se desarrolló en tres fases:

1. La red inicial como se muestra en la figura 2.5. En la fase inicial la red interconecta los centros de datos a través de nodos tradicionales que utilizan E/IBGP y enrutamiento ISIS. Los nodos de borde interconectan los centros de datos de la red (Foundation, 2014).

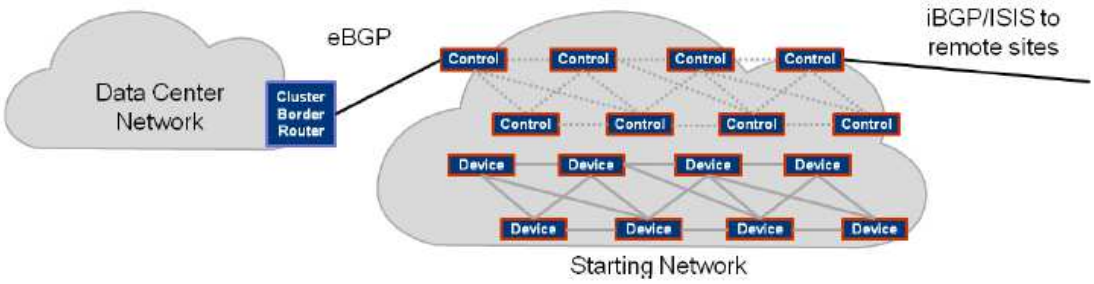


Figura 2. 5. Inicio de red B4

Fuente: (Foundation, 2014)

2. En la figura 2.6 se presenta la fase de implementación. En esta fase la red es mixta, un subconjunto de los nodos de la red son híbridos OpenFlow/tradicionales y son controlados de forma centralizada con Paxos, un controlador de OpenFlow, y para el enrutamiento se utiliza Quagga adaptado a los requerimientos de Google (Foundation, 2014).

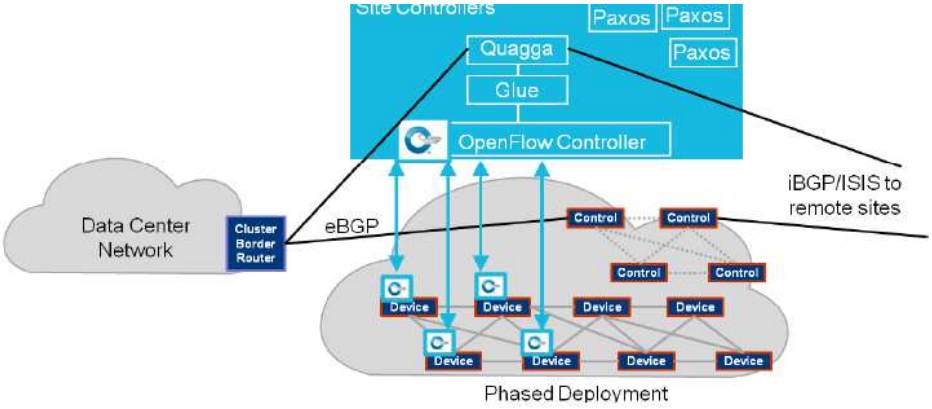


Figura 2. 6. Implementación de una red mixta en B4

Fuente: (Foundation, 2014)

3. De acuerdo a la figura 2.7 la red de destino. En esta fase final, todos los nodos son híbridos. El controlador maneja toda la red. No hay una correspondencia directa entre el centro de datos y la red. El controlador asimismo tiene un servidor de TE que dirige la ingeniería de tráfico en la red (Foundation, 2014).

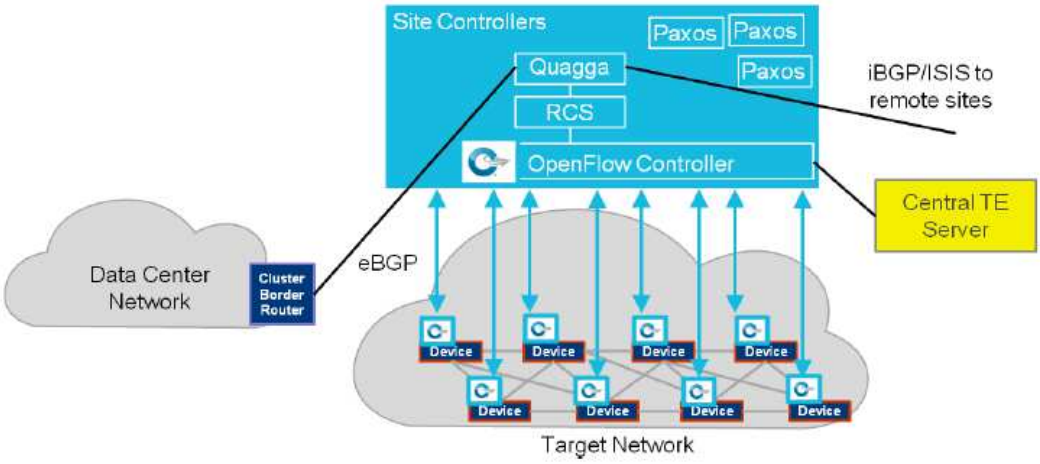


Figura 2. 7. Red de Destino B4.

Fuente: **(Foundation, 2014)**

2.4.1.1 Objetivos

Los objetivos de la migración van a la par con los objetivos de la red Goolge:

- Implementar el enrutamiento tradicional para crear rutas graduales que permitan habilitar OpenFlow en las dos redes de Google.
- Utilizar BGP como paso previo al uso de protocolos propietarios.
- Realizada una migración en tres etapas desde una arquitectura donde los planos de control y datos están distribuidos hacia una arquitectura con el plano de control descentralizado físicamente (Foundation, 2014)

En el caso de Google, la red interna no sólo lleva más tráfico que la red de cara a Internet, sino que la tasa del aumento de tráfico es aún mayor. Esto a que la red interna soporta la copia de datos, de respaldo o de las aplicaciones de usuario para que estén altamente disponible, a gran escala de un centro de datos a otros. La red interna basada en OpenFlow permite el uso de aplicaciones como la ingeniería de tráfico. Además, se adapta fácilmente a los fallos y cambios en los patrones de comunicación (Foundation, 2014).

Google adopta una arquitectura SDN, para la WAN que interconecta sus centros de datos, para implementar protocolos de enrutamiento e ingeniería de tráfico adaptados a sus requerimientos. El diseño de esta red SDN se enfoca en:

1. Reconocer los errores y fallas de la red, los que deben ser notificados para el mejoramiento y de ser factible el cambio o eliminación de las mismas;
2. Centralizar el control de la red. Los protocolos de red pueden correr en servicios que ejecutan protocolos estándares y propietarios (Foundation, 2014).

SDN simplifica la gestión de la red aumentando su eficiencia. Soporta, además, el uso de protocolos estándares e ingeniería de tráfico, primera aplicación SDN utilizada para:

1. Forzar el control en el borde de la red para tomar decisiones al adjudicar recursos entre demandas competidoras durante periodos de restricciones.

2. Utilizar múltiples caminos de reenvio y túneles para aprovechar la capacidad de red disponible de acuerdo con la prioridad de la aplicación.

3. Reasignar dinámicamente el ancho de banda ante fallas de enlace, o en los conmutadores, o ante cambios en la demanda de las aplicaciones (Foundation, 2014).

2.4.1.2 Enfoque de la migración

El método de migración comprende la unión de la red destino con el enrutamiento dado, lo que brinda una ruta paulatina para que OpenFlow acceda a la red de producción (Foundation, 2014).

Para que el despliegue de la tecnología SDN sea gradual, y asegurar así la interoperabilidad, se deben soportar los protocolos de enrutamiento distribuidos que utiliza la red inicial (Foundation, 2014).

Análisis de deficiencias:

- **Protocolo OpenFlow:** se encuentra en sus inicios y es muy básico, sin embargo, como muestra el desarrollo, es lo suficientemente bueno para muchas aplicaciones de la red.
- **Tolerancia a fallos en varios controladores OpenFlow:** se debe proveer múltiples controladores OpenFlow, esto supone un reto para la administración pues debe dividir las funcionalidades entre controladores.
- **División de las funciones:** aún no queda claro cuales funciones radican en los dispositivos de redes en cuales de los

controladores. La configuración de los dispositivos de red sigue siendo una asignatura pendiente.

- **Flujo de programación:** en redes grandes, la programación de flujos individuales puede tomarse su tiempo (Foundation, 2014).

2.4.2 Migración de Universidad de Stanford.

La motivación principal de la Universidad de Stanford para la migración SDN fue para obtener un mayor dominio del tráfico de la red y para experimentar con esta nueva tecnología. La meta fue migrar algunas VLAN y usuarios, principalmente los conectados de forma inalámbrica, hacia un control OpenFlow. La migración se llevó a cabo en dos edificios (Foundation, 2014).

Se migró una VLAN, se desplegaron seis conmutadores habilitados para OpenFlow y 14 puntos de acceso a WiFi. Esta VLAN conecta a Internet a los servidores en las aulas y a los usuarios inalámbricos. Los puntos de acceso inalámbricos están basados en las placas PC Engines ALIX y corren un SO Linux descargado del sitio de OpenFlow (Foundation, 2014).

2.4.2.1 Descripción general

- **Edificio de William Gates CS:** en principio la red se encontraba basada en el legado de los conmutadores HP ProCurve habilitada en 2 armarios en el sector 3A de la edificación y 6 armarios de formación CIS/CIX. En la edificación de William Gates existían VLAN y con una subred de prefijo 24 con una designación de IP a la sección de investigación. Inicialmente no contaba con OpenFlow en el hardware. El área puntual que se cambió a OpenFlow fue la VLAN 74 con 25 usuarios conectados a la red cableada con ancho de banda ascendente de 2 Gbps.

- **Edificio Paul Allen CIS:** asimismo cuenta con conmutadores HP ProCurve habilitada en 6 armarios

ubicados en cada piso incluido el sótano, 4 en total. Inicialmente no existía soporte para OpenFlow en los conmutadores. Se migró la VLAN 98 que contaba con más de 50 puntos de trabajo (Foundation, 2014).

En los armarios no existe redundancia pero los conmutadores de acceso, se encuentran se conectan a conmutadores de distribución, localizados en el sótano. Estos a su vez se interconectan a enrutadores redundantes de Cisco que forman el núcleo del campus. Los conmutadores ejecutan STP para evitar bucles. La red de la Universidad de Stanford era administrada por el software Zenoss de código abierto en conjunto con configuraciones basadas en CLI. (Foundation, 2014).

A continuación se detallan los principales requisitos para garantizar la migración a la red de destino:

a) La red con una disponibilidad mayor al 99.9%;

b) Se debe tener un esquema a prueba de fallos para devolver la red su estado anterior;

c) El desempeño de la red debe ser semejante al de las redes tradicionales;

d) La experiencia del usuario no debe verse afectada de ninguna manera (Foundation, 2014).

2.4.2.2 Monitoreo de Infraestructura

Es esencial para el despliegue un esquema robusto de monitoreo de la red y del tráfico. La infraestructura de monitoreo recopila información en dos planos:

1. **Plano de control:** la mayoría de los controladores archivan la información de nivel de flujo basado en los mensajes entrantes packet_in y flow_exp mensajes. Esa información se puede consultar utilizando REST u otra API. Las

estadísticas principales que se recopilan son para flow_arrival_rate y active_flows.

2. **Plano de datos:** en la Universidad de Stanford el monitoreo se basa en algunos nodos de monitores dedicados ejecutando ping y wget entre sí para recopilar información sobre el switch_cpu_utilization, flow_setup_time, RTT, wget_delay, y loss_rate. Estos se recogen antes y después de la migración de OpenFlow (Foundation, 2014).

La mayoría de las herramientas utilizadas por Stanford son estándar, como ping, tcpdump, y wget. En casos seleccionados, se implementaron herramientas especiales para realizar el monitoreo basado en la disponibilidad de sondas y de API. Por ejemplo, el controlador NOX no expone una API para consultar las estadísticas del plano de control. En ese caso, se realizó un tcpdump para archivar la comunicación del controlador, después se analizó la captura de paquetes utilizando oftrace para revelar las estadísticas necesarias. En un segundo lugar, en caso de que no hubiera sondas de repuesto disponibles, las máquinas de usuario se utilizaron como sondas ejecutando ofpeck en ellas y haciéndolas reportar las estadísticas de los planos de datos directamente a la base de datos MySQL (Foundation, 2014).

2.4.2.3 Objetivos

Los objetivos principales para el uso de OpenFlow fueron:

- Impulsar la investigación y experimentos a través de SDN;
- Revisar y comprender la nueva tecnología SDN;
- Realizar aportes a la comunidad y a las definiciones de OpenFlow (Foundation, 2014).

Para las siguientes 3 capas fue necesario investigación y entendimiento:

1. **Capa de plano de datos:** varios proveedores estaban construyendo nuevos conmutadores habilitados para OpenFlow o añadiendo soporte OpenFlow a los existentes. Era necesaria una plataforma para experimentar con estos conmutadores. El despliegue de OpenFlow cumple este objetivo, algunos del os resultados del despliegue incluyen la certificación de la estabilidad de cada dispositivo de hardware de conmutación y el análisis de sus límites de rendimiento.

2. **Plataforma de controladores:** de la misma forma que en el punto 1, se deseaba comprender las capacidades, límites de rendimiento y la estabilidad de las plataformas de controladores de código abierto y comercial. La implementación fue usada para este fin (Foundation, 2014).

Las aplicaciones o innovación: la motivación para la implementación de SDN fue la necesidad de innovar en la red y liberarse de su osificación. Con esta finalidad se crearon distintas aplicaciones para demostrar la capacidad de esta nueva arquitectura. Se consiguió con el aplicativo FlowVisor, establecer una porción de la red para ser usado como segmento de pruebas (Foundation, 2014).

2.4.2.4 Arquitectura SDN de la Universidad de Stanford

La red final abarcó los edificios William Gates CS y Paul Allen CIS con cobertura variable y cada uno funcionando como una isla separada (Foundation, 2014).

Como se muestra en la figura 2.8, en el edificio William Gates CS se habilitó para OpenFlow la red usada en el ala 3A. Se desplegaron seis conmutadores de 48 puertos 1GE, 30 puntos de acceso (AP) WiFi y una estación base WiMAX. Las pruebas incluyeron los siguientes dispositivos:

- Conmutadores habilitados para OpenFlow de HP (ProCurve 5406ZL), NEC (IP8800), Toroki (LS4810) y Pronto (3240 y

3290). Las configuraciones de VLAN en cada conmutador eran usados para aislar la red no OpenFlow.

- AP Wi-Fi basados en las cajas ALIX PCEngine con interfaces duales 802.11g. Los AP corren un SO Linux descargado del sitio de OpenFlow y fueron activados para ser alimentados por Ethernet (PoE).

- Estación base WiMAX de NEC (Foundation, 2014).

En el caso del edificio Paul Allen CIS, se habilitó para OpenFlow la VLAN 98 que abarca todo el edificio. Se desplegaron seis conmutadores Ethernet OpenFlow de 48 puertos 1GE, 14 AP Wifi. Conectaba los servidores en las salas de clase y los usuarios inalámbricos a Internet. Para el banco de pruebas se desplegaron los mismos conmutadores HP y AP utilizados en el edificio William Gates CS (Foundation, 2014).

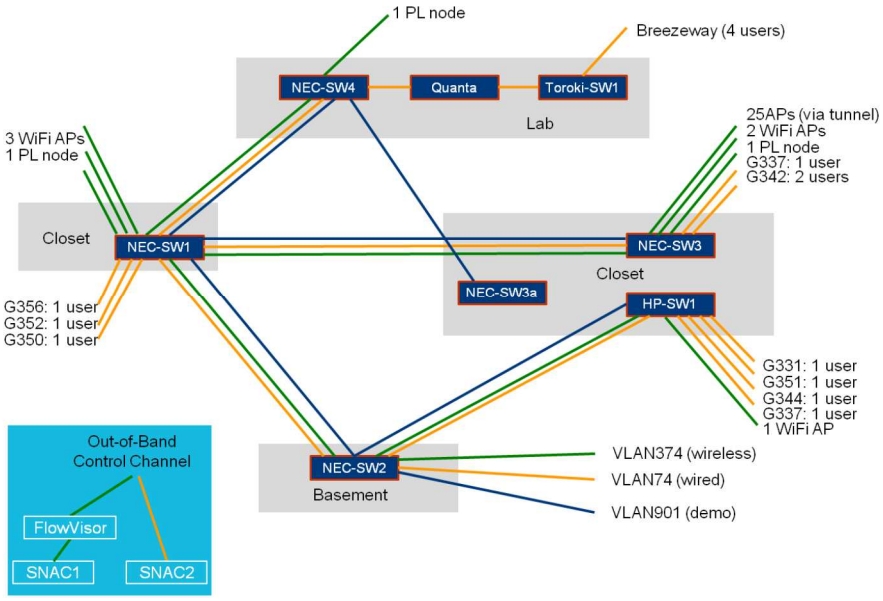


Figura 2. 8. Ala habilitada para OpenFlow del edificio William Gates de Stanford.

Fuente: (Foundation, 2014)

2.4.2.5 Enfoque de la migración

El enfoque adoptado fue mover gradualmente a los usuarios y luego las VLAN al control basado en OpenFlow. Para la administración del riesgo involucrado en el despliegue de la nueva tecnología, se llevaron a cabo las siguientes 4 fases:

1. Añadir soporte OpenFlow en el hardware: en la mayor parte del hardware se requiere actualización del firmware para soporte de OpenFlow. Se realizó de manera paulatina.

2. Comprobar el soporte OpenFlow conmutador: se comprobó la compatibilidad con OpenFlow añadiendo una VLAN experimental adoro hosts de prueba al conmutador, y permitiendo que estos sean administrados por el controlador externo. Cuando se tuvo la comprobación de la estabilidad del funcionamiento, se pasó a la siguiente etapa.

3. Migrar usuarios a la nueva red: para disminuir las caídas, se creó una red no OpenFlow y los usuarios fueron migrados de forma segura a esa red antes de poner en producción el tráfico OpenFlow. Para realizarlo se ejecutaron los siguientes pasos:

    A. Agregar una nueva subred de producción;

    B. Migrar a los usuarios de forma paulatina a la nueva subred;

    C. Probar conectividad de la subred.

4. Habilitar OpenFlow para la nueva subred: cuando ya se comprobó que la subred se encuentra operativa, el control OpenFlow fue habilitado configurando el controlador. Nuevamente, la veracidad y la accesibilidad, el rendimiento y la estabilidad se verificaron utilizando las herramientas de monitoreo descritas con anterioridad y la información de la experiencia del usuario recopilada mediante encuestas (Foundation, 2014).

Tomar en consideración que la VLAN de producción cableada abarcaba tanto redes OpenFlow como no OpenFlow, mientras que la VLAN de producción inalámbrica era gestionada exclusivamente por OpenFlow (Foundation, 2014).

El propósito final de la implementación de Stanford fue expandir el soporte de OpenFlow a otras VLAN para luego comunicarlas con un enrutador L3 (Foundation, 2014).

2.4.2.6 Dependencias de destino

La implementación de la red de destino incorpora diferentes controladores, adjuntando los siguientes:

- NOX;
- SNAC;
- NEC Trema;
- BigSwitch Controller (Foundation, 2014).

Adjunto al controlador, Stanford además investigó diferentes versiones del firmware del conmutador, la FlowVisor, herramientas de organización GENI y distintas aplicaciones de prueba (Foundation, 2014).

En Stanford se desarrollaron varias herramientas de depuración, con soporte OpenFlow, para la solución de los problemas que surgieron en la red.

La mayoría de estas herramientas son:

- Oftrace: es un analizador OpenFlow de volcado de tráfico de control / biblioteca de rastreo.
- Disector de Wireshark para OpenFlow
- MiniNet: paquete de emulación de red que utiliza espacios de nombres de red.
- Ofrewind: Reproducción de eventos de la red mediante la reproducción de tráfico de control y del plano de datos.

- Hassel y NetPlumber: verificación de la política de red en tiempo real y depuración.
- ATPG: generación automática de paquetes de prueba para depuración en red (Foundation, 2014).

2.4.2.7 Análisis de las deficiencias

Durante la actualización, se siguieron procedimientos estrictos para asegurar un solo cambio en cualquier momento y también para revertir los cambios realizados en caso de deterioro del estado de la red. No se contó con la posibilidad de realizar salvas de la configuración de los equipos OpenFlow en el interior del firmware para revertir automáticamente las configuraciones; en Stanford se trabajó sobre todo para contribuir al desarrollo de esta nueva tecnología (Foundation, 2014).

Entre las deficiencias detectadas la principal es la necesidad de una mayor interoperabilidad entre la parte OpenFlow y la parte no OpenFlow, incluidos los controladores y conmutadores OpenFlow. Algunas de las características que faltaban en el despliegue de la red fueron:

- Los controladores utilizados no admitían el protocolo STP;
- El sistema SDN no pudo descubrir los conmutadores no OpenFlow en la topología;
- Los conmutadores utilizados no funcionaron bien con la agregación de enlaces LACP;
- El sistema SDN no tiene una visibilidad completa sobre los flujos y los usuarios que abarcan tanto los segmentos OpenFlow y segmentos no OpenFlow de la red (Foundation, 2014).

La aceptación posterior a la migración:

Utilizando la infraestructura de monitoreo se recopiló información, como se muestra en la figura 2.9 y 2.10. Esta información se usó para determinar si el comportamiento de la red era aceptable.

- **Corrección y accesibilidad:** la finalización de las solicitudes de hecho fue el principal factor que confirmó la corrección y la accesibilidad.

- **Rendimiento:** las estadísticas se monitorean tanto en el plano de control como en el plano de datos. Estas estadísticas fueron correlacionadas para identificar anomalías y comportamientos incorrectos.

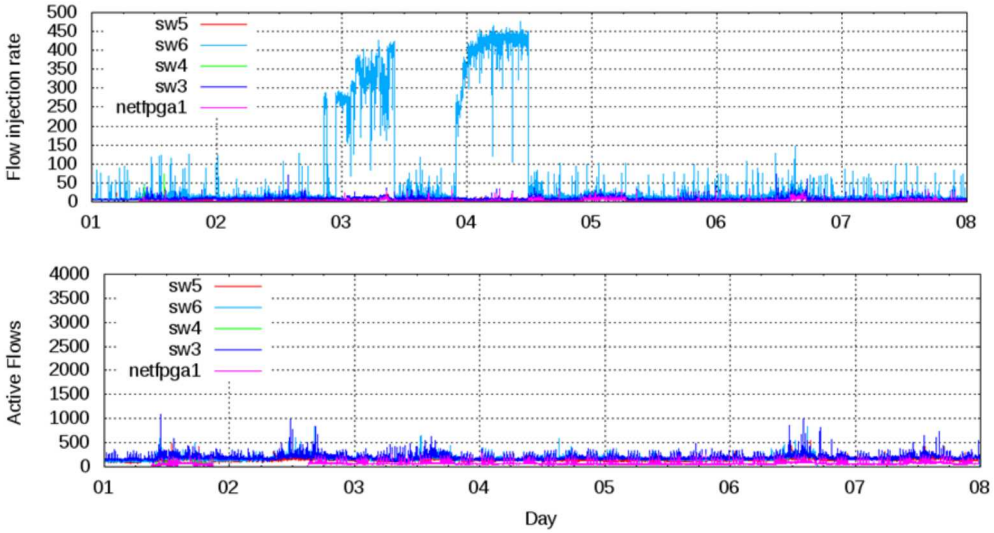


Figura 2. 9. Ilustración de las estadísticas del plano de control, cuando se utilizó el controlador SNAC

Fuente: (Foundation, 2014)

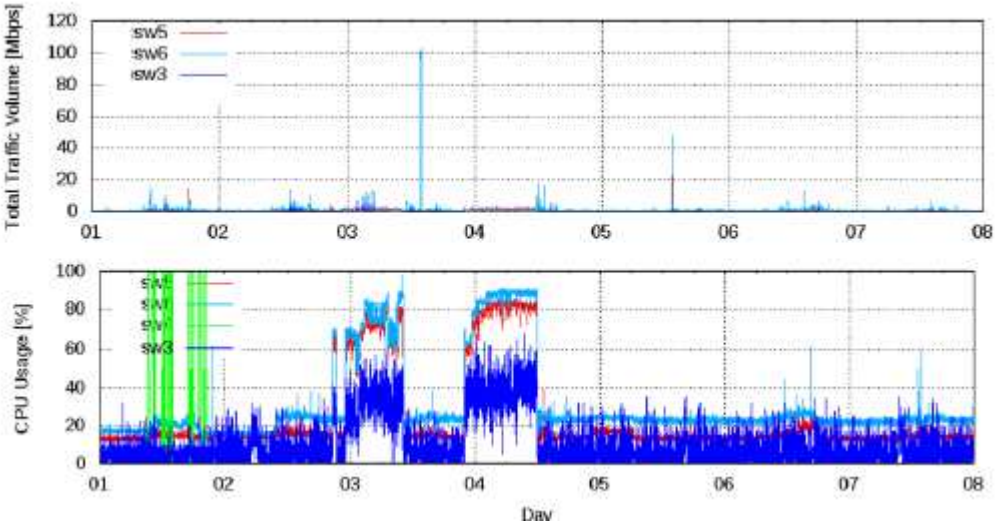


Figura 2. 10. Volumen de tráfico y uso de la unidad de procesamiento central (CPU)

Fuente: (Foundation, 2014)

- **Estabilidad:** para la estabilidad, las estadísticas se controlaron durante un largo período de tiempo. Las estadísticas se representaron con frecuencia en un gráfico, como se muestra en la Figura 2.11, para verificar la estabilidad y el estado de la red.

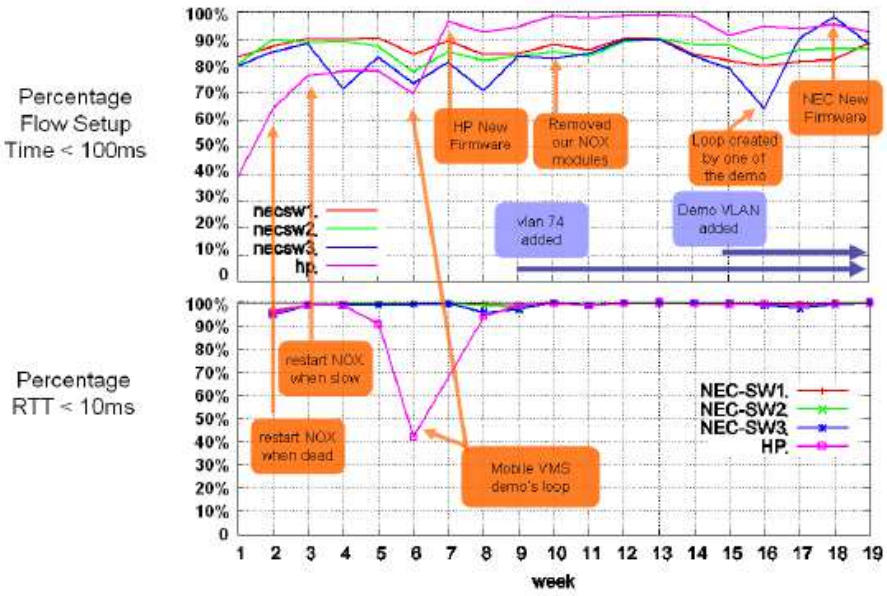


Figura 2. 11. Gráfico de progresión de las estadísticas del plano de datos para verificar la estabilidad.

Fuente: (Foundation, 2014)

La estabilidad de la red mejoró gradualmente a medida que fue madurando la comprensión de la tecnología, de los conmutadores y de la red. Una vez que se estabilizó la red con la nueva tecnología, los usuarios comenzaron a ver un servicio consistentemente aceptable (Foundation, 2014)

La migración a OpenFlow de la red de campus de Stanford se produjo en 3 fases:

1. Prueba de concepto con despliegue WiFi y una pequeña red de producción.

2. Se dividió la red en una parte para investigación y otra en producción, esta última mucho más grande. Uno de los

objetivos de la migración fue comprender la tecnología y realizar aportes a la misma.

3. Despliegue de la tecnología en 3 edificios (Foundation, 2014).

Durante cada fase, hubo una semana de planificación, una semana de cambio seguido de 6 meses de uso (Foundation, 2014).

2.4.2.8 Consideraciones de seguridad en la Red.

Las redes seguras son fundamentales para todas las empresas, especialme

nte con su mayor migración a la nube y la ola de innovación que se desencadena por SDN. Junto con muchos beneficios, SDN plantea nuevas amenazas, particularmente con la aparición de la nube, BYOD y entornos virtualizados. Es fundamental considerar las amenazas, la exposición al riesgo, el impacto operacional, el rendimiento, la escala y el cumplimiento en el centro de datos del futuro basado en SDN ((ONF), 2013).

La tabla A.3 (ver en anexos) muestra un resumen de las consideraciones de seguridad a tomar.

2.5 Migración a SDN.

2.5.1 Enfoques de migración

En principio se pueden definir dos enfoques generales para llevar a cabo la migración a SDN: migración directa o en fases, no obstante podrían seguirse otros enfoques en dependencia del tipo de red.

En el primer enfoque, ilustrado en la Figura 2.12, se actualizan directamente los equipos de la red existentes con agentes OpenFlow, se deshabilita de esta forma la máquina de control en el dispositivo pasando esta función al controlador OpenFlow (Foundation, 2014).

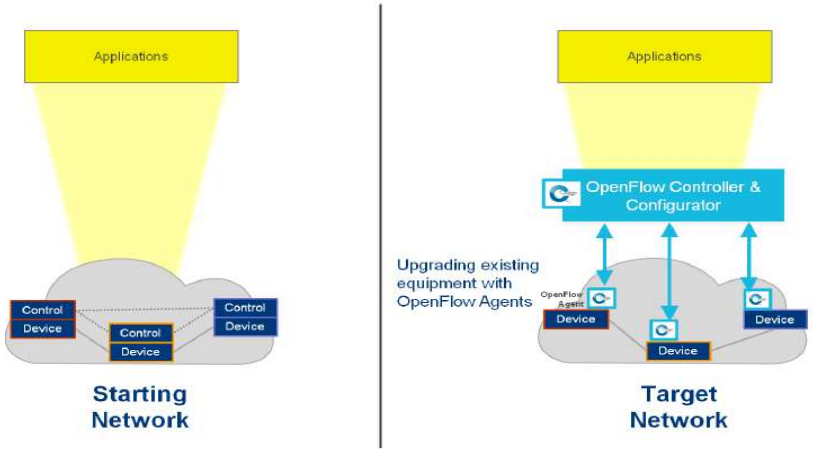


Figura 2. 12. Actualización directa

Fuente: (Foundation, 2014)

El segundo, que supone una migración gradual, incluye un enfoque por fases, que se ilustra en la figura 2.13, en el que los dispositivos OpenFlow se despliegan conjuntamente con los dispositivos existentes. Las operaciones de red se mantienen tanto por la máquina de control en los dispositivos tradicionales como por el controlador OpenFlow. Una vez que los servicios se han migrado a la red de destino SDN, y se comprueba su correcto funcionamiento, se desactivan los dispositivos tradicionales (Foundation, 2014).

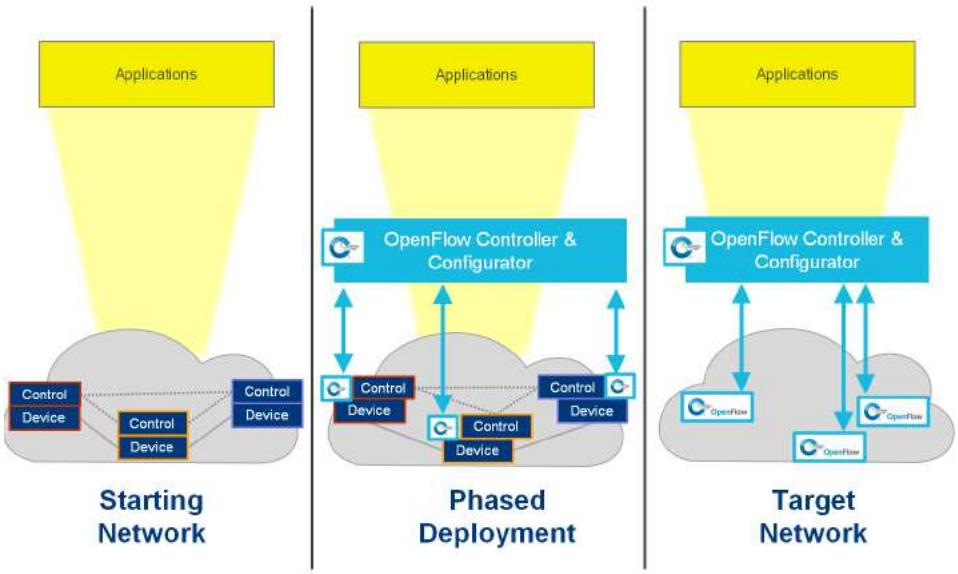


Figura 2. 13. Migración gradual

Fuente: (Foundation, 2014)

Las migraciones de red varían tanto como las redes. Pueden incluir las dos variantes antes mencionadas: actualizaciones directas de los dispositivos con agentes OpenFlow o en paralelo la introducción de dispositivos OpenFlow con el equipamiento existente que luego de la migración es removido a la red. Además de esto, se pueden realizar despliegues Greenfield o migraciones parciales donde se utilizan varias variantes de SDN OpenFlow o no OpenFlow en una parte de la red (Foundation, 2014).

La migración también puede incluir migraciones parciales, donde los límites de dominio estén habilitados para OpenFlow (como entre la red de acceso y la red metro en la figura 2.14) mientras que los dominios no lo son. También puede incluir el caso en el que algunos dominios estén habilitados para OpenFlow pero los dominios adyacentes no (Foundation, 2014).

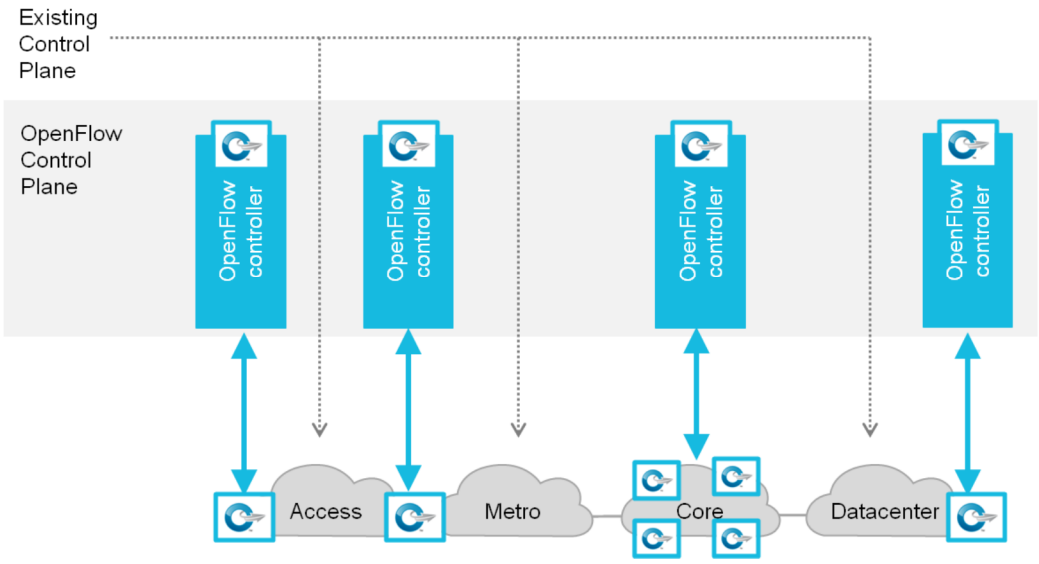


Figura 2. 14. Diversidad en las implementaciones de red

Fuente: (Foundation, 2014)

Como ya se comentó y puede verse en la figura 2.15, los dispositivos pueden clasificarse como tradicionales *(legacy*), OpenFlow o híbridos (OpenFlow/tradicionales). Los tradicionales son conmutador/enrutador que tienen integrado tanto el plano de control como el de reenvio. En los dispositivos OpenFlow sólo se implementa el plano de reenvió porque el plano de control reside en un dispositivo externo, el controlador OpenFlow.

El término híbrido se refiere a dispositivos con control tradicional y plano de datos y además con capacidades OpenFlow (Foundation, 2014).

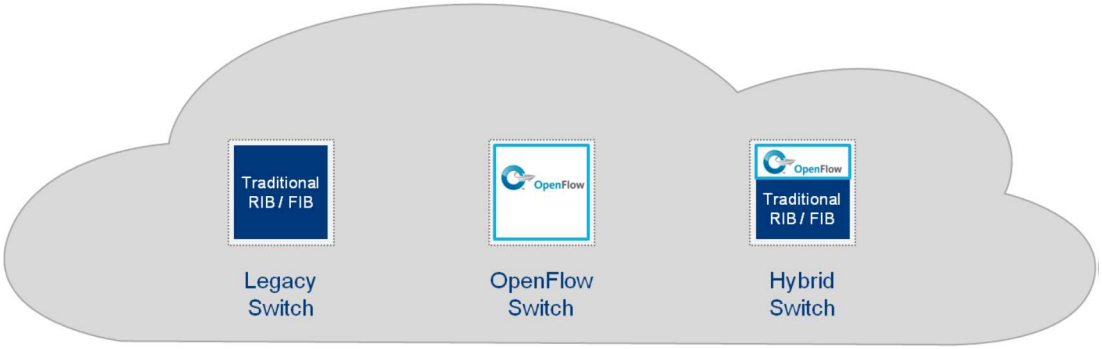


Figura 2. 15. Tipos de dispositivos

Fuente: (Foundation, 2014)

De los dos enfoques de migración definidas por el Estatuto del Grupo de Migración, se pueden reafirmar los enfoques de migración usando la terminología anterior como sigue:

- **Greenfield (red SDN completamente nueva).** En este enfoque se pueden dar dos casos: una red nueva que se implementaba basada en SDN o una red en producción que se actualiza a SDN reemplazando la máquina de control de los dispositivos por el agente OpenFlow y se cede el control a un dispositivo externo llamado controlador de OpenFlow (Foundation, 2014).

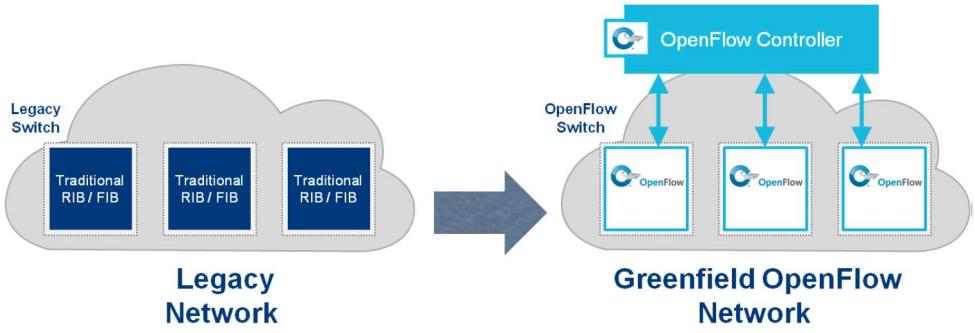


Figura 2. 16. Enfoque Greenfield o red SDN completamente nueva

Fuente: (Foundation, 2014)

- **Mixto.** En este enfoque de migración se asume que la red final estará compuesta por dispositivos tradicionales y OpenFlow. Los nuevos dispositivos OpenFlow deberán comunicarse con las máquinas de control en los dispositivos tradicionales con los que coexisten. También el nuevo controlador OpenFlow y los dispositivos tradicionales tendrán que intercambiar información, de L2 o L3, a través de la máquina de control (Foundation, 2014)

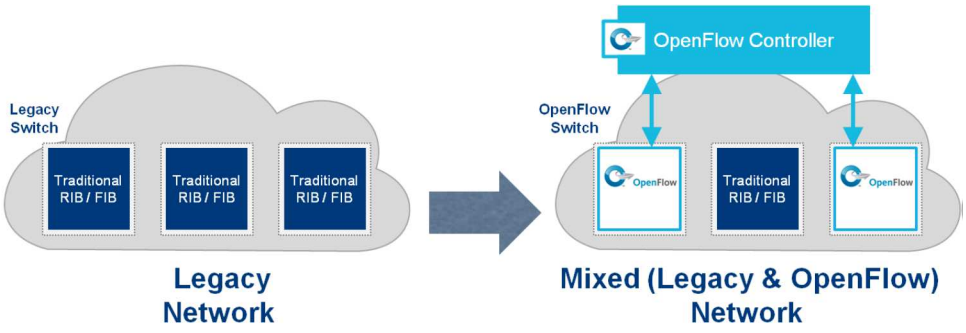


Figura 2. 17. Enfoque mixto

Fuente: **(Foundation, 2014)**

- **Híbrido.** Este enfoque va más allá del mixto pues plantea la coexistencia entre los dispositivos tradicionales, los OpenFlow nativos y los dispositivos híbridos OpenFlow/tradicionales. En este escenario, los dispositivos híbridos se comunican con el controlador OpenFlow y con la máquina de control en los dispositivos tradicionales (Foundation, 2014)

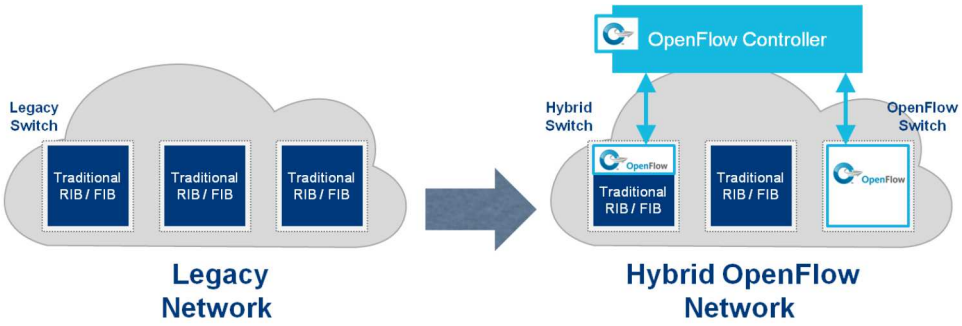


Figura 2.18. Enfoque híbrido.

Fuente: (Foundation, 2014)

Los enfoques mixto e híbrido son ejemplos de la migración por fases que contempla el grupo de migración de la ONF. En todos los casos, estas migraciones contemplan la migración de un solo dominio de red. En muchos casos, la motivación para migrar hacia OpenFlow es permitir seleccionar distintos servicios. En otras palabras, se desea OpenFlow para habilitar un servicio de extremo a extremo. El soporte de dicho servicio con OpenFlow requerirá la introducción de un controlador OpenFlow junto con los dispositivos OpenFlow subyacentes, ya sea en una configuración totalmente nueva, mixta o híbrida (Foundation, 2014).

2.5.2 Tipos de redes

Según el grupo de trabajo de migración de la ONF se podría presentar la migración en cuatro categorías principales: un campus, el centro de datos de una empresa, un centro de datos que dé servicio a múltiples inquilinos y en un proveedor de Servicio / WAN. Cada una de estas categorías tiene varias subcategorías a considerar, aunque no es una lista exhaustiva, a continuación se esbozan algunas de las características de cada una de ellas (Foundation, 2014).

- Las redes de campus normalmente se componen de varios edificios, cada uno de ellos con su armario de telecomunicaciones, generalmente cada edificos se conecta a un nodo central o centro de operaciones de la red. Los componentes de la red del campus incluyen backbone o dorsal del campus con un punto de la salida a la red WAN que se asocia típicamente a un centro de datos. En muchos casos, la red y el centro de datos están divididos lógicamente ya sea para dar servicios a diferentes departamentos, instalaciones de administración o a los recursos de TI de tofo el campus (Foundation, 2014).

- Los centros de datos empresariales pueden variar en tamaño, pero por lo general se componen de recursos de red utilizados

para interconectar diferentes subredes de servidores (ya sea físicas o virtuales) junto con el almacenamiento asociado (NAS o SAN) y la seguridad y funciones de red (por ejemplo, balanceo de carga). Los requisitos para la creación de SDN pueden variar, pero los servicios orientados a las aplicaciones ocupan un lugar destacado en la lista (Foundation, 2014).

- Los centros de datos con múltiples clientes se han beneficiado enormemente de las SDN. Estos centros de datos comparten muchos aspectos del típico centro de datos de una empresa, sin embargo, estos múltiples inquilinos deben compartir por lo general los mismos recursos físicos. La virtualización de los recursos informáticos es casi una necesidad, con características robustas como la migración de máquinas virtuales que facilita una variedad de capacidades, incluyendo de equilibrio de recursos, el mantenimiento, y recuperación de desastres. Los conmutadores por software dentro de los propios recursos informáticos son un componente dominante de la arquitectura. El efecto neto es que partes del centro de datos se mueven y cambian, exigiendo que la red de superposición se mueva y cambie para hacerse eco de esos cambios. Cada vez más, sin embargo, los dispositivos de SDN ayudan frente a estos requisitos (Foundation, 2014).

- Los proveedores de servicios o de infraestructura WAN introduce una diversidad significativa. Las arquitecturas de red y los requisitos de los proveedores de servicios varían, por ejemplo, un Proveedor de Servicio Móvil Celular tendrá una red de radio; junto con una red backhaul móvil conectada a una red de acceso y, por último, una red de núcleo. Actualmente se están desarrollando y desplegando diferentes aplicaciones de OpenFlow y SDN que son usadas por los proveedores para administrar sus recursos, el ejemplo de Google que fue detallado en epígrafes anteriores (Foundation, 2014).

2.6 Estrategia de Migración.

La estrategia de migración a SDN persigue unir toda o casi toda la red en una infraestructura centralizada que permita la adaptación dinámica de la red a las condiciones cambiantes de su funcionamiento facilitando así la gestión de los dispositivos y servicios de la red.

En este trabajo se propone una migración en tres fases.

- Preparación: donde se definen las metas y límites de la migración. La idea principal de esta fase es identificar y priorizar los requisitos básicos que debe cumplir la red SDN.
- Planeación: en esta fase se define la especificación funcional y el plan del proyecto de migración.
- Migración: es en esta última etapa donde se desarrolla la migración, para esto se deben realizar todas las pruebas necesarias hasta darle solución a los problemas que se presenten durante el proceso de conformación de la red SDN final o red objetivo.

A continuación se describen las tareas a realizar en cada una de las fases:

Preparación de la migración

1. Defina un proyecto de migración donde se establezcan las metas, alcance, restricciones y suposiciones. Tenga en cuenta que la SDN no pueden cumplir todos los requisitos iniciales de una red tradicional. Es importante que se tenga una visión clara sobre cómo la tecnología SDN beneficiará al centro de datos, incluyendo su impacto en la infraestructura de red que ya está en uso. Planee cómo la SDN impactará en su arquitectura general de red a largo plazo.
2. Analice los retos de implementación de la SDN. Muchas ofertas de esta tecnología hoy son incompletas o requieren una amplia personalización. Se debe tener claridad sobre si el personal de IT tiene la capacidad para la instalación de la SDN o si es

necesaria una formación adicional. Mientras no se cumpla esta tarea no debe continuar el proceso de migración.

3. Defina el enfoque de la migración: método directo o un enfoque por fases. En el método directo se actualizarán los equipos de red existentes con los agentes OpenFlow. En el enfoque por fases, los dispositivos OpenFlow se despliegan conjuntamente con los dispositivos existentes. A menos que el centro de datos sea nuevo probablemente sea mejor un estado intermedio en que convivan la tecnología tradicional de redes con SDN.
4. Identifique un caso específico del uso inicial para SDN. Por ejemplo, reducir el tiempo necesario para la seguridad de nuevas (o migrantes) máquinas virtuales o para facilitar las garantías de calidad de servicio en toda la red WAN privada.
5. Defina la red inicio, que puede ser la totalidad de la red o sólo una parte si se considerara conveniente, y la red objetivo en la que finalmente todos los nodos permiten OpenFlow.
6. Defina la estructura del equipo que llevará a cabo el proyecto.

Planeación de la migración

1. Realice un análisis detallado del impacto de la migración en los servicios existentes. Defina opciones alternativas para mitigar los posibles desafíos que se pueden encontrar durante la migración.
2. Cree listas de verificación previa y posterior a la migración con muestras específicas de aplicaciones y/o prefijos de destino de origen que se utilizarán para verificaciones de conectividad y continuidad del servicio. La realización de evaluaciones previas y posteriores a la migración a su debido tiempo ayuda a garantizar que se puedan excluir los problemas y fracasos relacionados con la no migración.
3. Debe crearse un procedimiento para seguir el proceso de migración paso a paso con procedimientos de respaldo claramente documentados en caso de resultados inesperados.

Vale la pena investigar si los procedimientos que revierten la configuración a la red inicial pueden ser automatizados para minimizar la interrupción en caso de deterioro del rendimiento.

4. Se deben analizar detalladamente las características de OpenFlow y las capacidades deseadas en el controlador y en el conmutador OpenFlow para garantizar que el conjunto de características sea coherente con los requisitos.

Migración

1. Todas las herramientas de administración de red necesarias deben estar provisionadas para que la red migrada funcione correctamente y supervise el tráfico y los dispositivos durante y después de la migración.
2. Como hay varias versiones de OpenFlow, es importante verificar la compatibilidad entre las versiones del protocolo OpenFlow implementadas en el controlador y el conmutador.
3. Los dispositivos OpenFlow deben actualizarse para ejecutar el firmware de hardware y código adecuado antes de que se pueda iniciar la migración.
4. Se debe confirmar la conectividad entre el controlador y los dispositivos OpenFlow de la red.
5. En un entorno mixto, se puede crear un servicio ficticio como VPN del cliente para verificar la disponibilidad del servicio.
6. Se debe estar atento a la solución de problemas que se presenten en la migración. Pueden emplearse pasos de solución de problemas apropiados tales como ping, seguimiento o acceso a una aplicación para comprobar la conectividad.

2.6.1 Consideraciones de Seguridad

SDN proporciona un modelo centralizado de inteligencia y control, que brinda la flexibilidad necesaria para combatir las amenazas contra las redes. Esta nueva arquitectura tiene el potencial de ser aún más seguro que los métodos tradicionales mediante una detección más rápida de amenazas y mecanismos de respuesta más granulares. No obstante, durante el proceso de migración, incluso cuando las redes tradicionales y SDN coexisten, es necesario mantener redes seguras y aisladas. Los servicios de seguridad existentes deberán migrarse a una red SDN habilitada para OpenFlow manteniendo, de forma clara y precisa, las políticas y los recursos de seguridad entre las redes de partida y de destino (Foundation, 2014).

Una forma de migrar los mecanismos de seguridad a una red SDN son:

1. Comenzar con una parte de red experimental (por ejemplo una VLAN)
2. Probar esa porción experimental con soluciones de seguridad SDN abierta (por ejemplo, Security Enhanced Floodlight).
3. Habilitar para OpenFlow y probar las soluciones de seguridad en una nueva parte de la red (por ejemplo, otra VLAN)
4. Poco a poco mover a los usuarios a esta nueva red segura (Foundation, 2014).

En una red SDN se le debe prestar especial atención al controlador ya que se convierte en un punto único de fallo del entorno. Si una persona no autorizada consigue acceso al controlador, la red en su totalidad queda expuesta porque la separación del plano de control y el plano de datos convierte a los enrutadores y conmutadores de la red en dispositivos “tontos”, cuya gestión queda en manos de ese controlador. También los errores humanos dentro de la configuración del controlador pueden tener un efecto dominó en toda la red ((ONF), 2013).

Además de las réplicas y copias de seguridad que se deben implementar, para garantizar la seguridad del controlador SDN, se le debe aprovisionar de seguridad tanto a nivel de SO, a nivel de aplicación y a nivel de API ((ONF), 2013).

- Seguridad en el nivel de SO: a nivel de SO hay dos puertas principales de ataque: acceso por consola a la VM donde está el controlador, si es abierto, o el equipo de propósito específico de un vendedor y el acceso por SSH. El acceso a la consola está sujeto a las medidas de seguridad de la plataforma donde se implemente, el equipo encargado de su configuración debe tener bien en cuenta estas medidas. El acceso por SSH se debe prohibir a usuarios con privilegios de administración (root), sólo a los usuarios que administran el equipo (con menos privilegios) que una vez dentro podrán ganar en privilegios. Se debe estar atentos a las políticas de cambio de contraseña. En este nivel se debe mantener también un registro de los niveles de consumo de todos los componentes (CPU, memoria, interfaces de red, etc.) para fijar unos umbrales que permitan detectar cambios en el comportamiento establecido como normal.
- Seguridad a nivel de aplicación: utilizar conexiones por SSH para cifrar todas las contraseñas y todo el tráfico con el controlador. En este nivel puede ser perjudicial que las contraseñas de usuarios y administración residan en el mismo fichero.
- Nivel de API: para minimizar la exposición de contraseñas en las llamadas de la API se deben establecer mecanismos como la generación de un token hash de la contraseña para cada llamada que se realiza ((ONF), 2013).

La comunicación entre el controlador y los dispositivos de la red debe ir cifrada para garantizar su seguridad. Deben implementarse versiones de OpenFlow sobre TLS para asegurar que ningún intruso puede descifrar, alterar o suplantar la comunicación entre el controlador SDN y los agentes. Se deben implementar además mecanismos de autenticación avanzados, ejemplo mediante un sistema multifactor que vaya más allá del típico desafío usuario y contraseña, de modo que los atacantes deban pasar varias barreras para llegar al controlador. Otras barreras que se pueden implementaron son las poderosas herramientas ya conocidas en las redes tradicionales como firewalls de última generación, IPS, entre otras ((ONF), 2013).

2.6.2 Solución SDN para CISCO.

Teniendo en cuenta que la mayoría de los centros de datos del país utilizan equipamiento CISCO, a continuación se describe la solución SDN que brinda en el mercado esta compañía.

La solución SDN de Cisco utiliza ACI para la presentación de algunas de las tendencias informáticas que configuran la necesidad de una nueva arquitectura de red, que incluye:

- Cambiar la dirección de tráfico: el centro de datos está cambiando de arquitecturas de aplicaciones cliente-servidor tradicional a modelos en los que se están transfiriendo significativamente una alta cantidad de datos de una máquina a otra. El resultado es un cambio de las direcciones de tráfico norte-sur a más tráfico este-oeste en el centro de datos.
- La movilidad de TI: los usuarios exigen más flexibilidad de llevar su propio dispositivo (BYOD), para que los portátiles personales, tabletas y teléfonos inteligentes se puedan utilizar para acceder a información corporativa.
- El aumento de los servicios en la nube: los servicios de nube pública disponibles, de compañías multinacionales de acceso libre por los usuarios, han dado a los departamentos de TI corporativos un vistazo de autoservicio y demuestran lo ágiles

que pueden ser las aplicaciones y los servicios. Sin embargo, a diferencia de los entornos de nube pública, los entornos de nube privada deben cumplir con estrictos requisitos de seguridad, que no pueden ser sacrificados por una mayor agilidad.

- Los datos grandes necesitan un mayor ancho de banda: las empresas están invirtiendo en grandes aplicaciones para facilitar la mejor forma de tomar decisiones empresariales. Sin embargo, estas aplicaciones requieren un procesamiento paralelo masivo a través de cientos o miles de servidores. La demanda para manejar enormes grupos de datos, está colocando mayor estrés y carga en la red y conduciendo la necesidad de una mayor capacidad (CISCO, 2014).

Para brindar agilidad y simplicidad en la infraestructura del centro de datos, se requiere un nuevo lenguaje que describa la intención de la conectividad para que el usuario final no necesite conocimientos de redes para describir los requisitos de conectividad (CISCO, 2014).

Debido a que este modelo de política, disociada no existía antes, se crea un modelo de este tipo. Es llamada política basada en grupos (GBP) y es un proyecto de trabajo en OpenStack y OpenDaylight (CISCO, 2014).

ACI realiza un amplio uso de la política basada en grupos en su modelo de políticas centrado en aplicaciones, en el que la conectividad se define mediante la consolidación de los puntos finales (físicos o virtuales) en grupos de puntos finales (EPG). La figura 2.19 proporciona una visión general de este modelo. (CISCO, 2014)

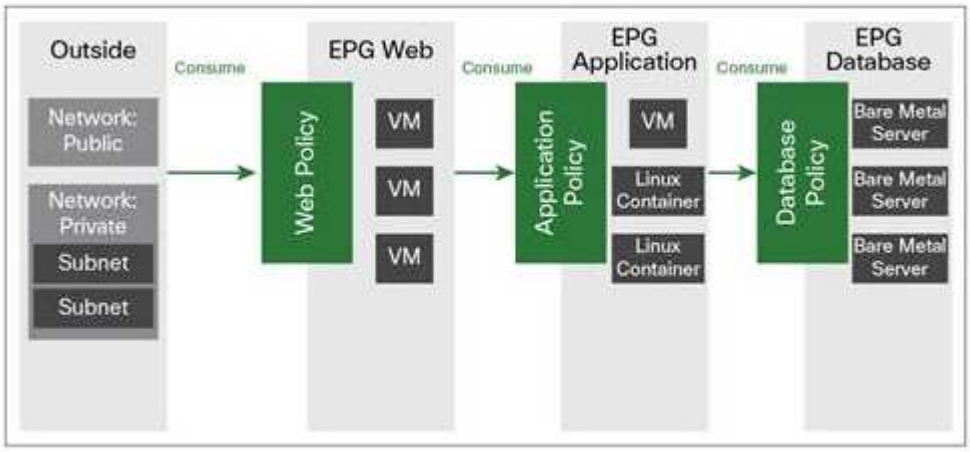


Figura 2. 19. Modelo de política centrada en la aplicación

Fuente: (CISCO, 2014)

El controlador de infraestructura de directivas de aplicaciones de Cisco (APIC), tiene como función principal la de proporcionar mecanismos de resolución de políticas para la red ACI y los dispositivos conectados a la red (ver figura 2.20). La automatización se proporciona como resultado directo de la resolución de la política y genera sus efectos en la red ACI, de modo que los usuarios finales ya no tienen que trabajar con cada elemento de la red y asegurarse manualmente de que todas las políticas están configuradas adecuadamente. (CISCO, 2014)

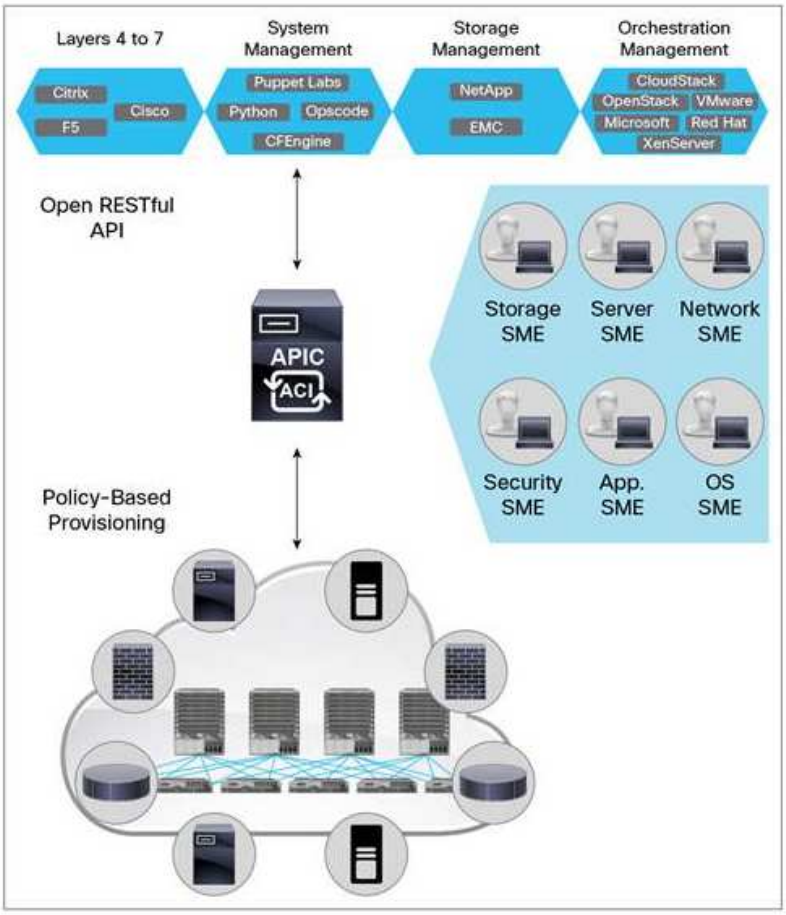


Figura 2.20 El papel de APIC en la red ACI

Fuente: (CISCO, 2014)

APIC tiene unas APIs completamente abiertas para que los usuarios puedan usar las llamadas basadas en REST (Representational State Transfer) (a través de XML o JavaScript Object Notation [JSON]) para proporcionar, administrar, supervisar o solucionar problemas del sistema. Además, APIC incluye una CLI y una GUI como puntos centrales de administración para toda la red ACI. (CISCO, 2014)

Al diseñar la red ACI, Cisco necesita considerar todos los nuevos retos que enfrenta el centro de datos, pero también necesitaba entender y atender los desafíos existentes. La red ACI (figura 2.21) está diseñada para satisfacer las necesidades de hoy y las necesidades de mañana, con los siguientes objetivos principales:

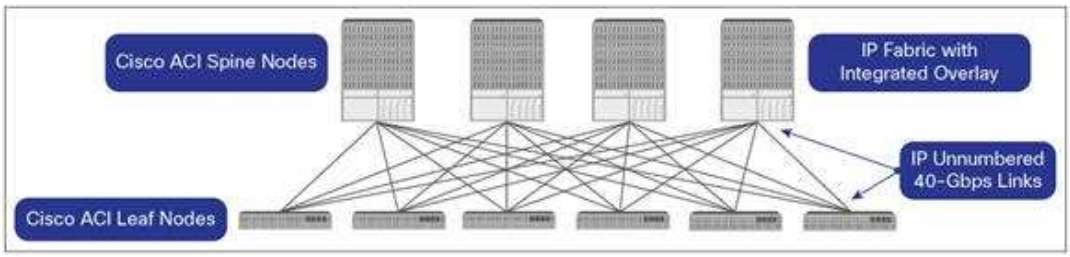


Figura 2. 21. Red de ACI

Fuente: (CISCO, 2014)

- Red escalable: la red ACI está diseñada con base en uno de los modelos de diseño de red más eficientes y escalables: un gráfico bipartito está conectada a cada columna vertebral y a la inversa. Para reducir la probabilidad de hotspots de actividad que se forman en la red, todos los dispositivos se conectan a los nodos de la red. Este enfoque permite que la red proporcione una forma sencilla de escalar el número de dispositivos conectados, añadiendo más nodos. Si la cantidad de ancho de banda transversal que está dando servicio a la red necesita ser aumentada, el administrador simplemente tiene que agregar nodos. Esta flexibilidad permite que la red empiece en un ambiente pequeño, pero gradualmente crezca hasta un ambiente mucho más grande si surge la necesidad. La red también se construye utilizando interfaces IP enrutadas basadas en estándares, ofreciendo mayor estabilidad en implementaciones de mayor escala.
- Extensibilidad: la red ACI es altamente extensible. El administrador de la estructura puede integrar redes virtuales, así como servicios de capa 4 a 7 (firewalls, equilibradores de carga, etc.). Esta integración permite al usuario final especificar los requisitos de conectividad mediante la política basada en grupos en APIC y la configuración para redes virtuales y para los servicios de la Capa 4 a 7 se reproduce automáticamente en los sistemas finales respectivos, eliminando la necesidad de que el usuario final coordine la conectividad y las políticas a

través de esos dispositivos. Futuras versiones de software también incluirán la integración del enroutador WAN.

- Simplicidad: aunque existen numerosos protocolos y características en el dominio de redes, el papel de la red es muy simple: proporcionar cualquier conectividad en cualquier lugar. En lugar de soportar numerosos protocolos y características diferentes, la red ACI está diseñado teniendo en cuenta los casos de uso del centro de datos. Se ha elegido un único protocolo de puerta de enlace interior (IGP) como protocolo de descubrimiento de nodo de la red subyacente: sistema intermedio a sistema intermedio (IS-IS). IS-IS es un protocolo de estado de enlace que detecta de manera muy eficiente fallos de enlaces y se recupera de tales fallos. La LAN virtual extensible basada en estándares (VXLAN) proporciona una superposición simple para el tráfico orientado a los inquilinos, soportando el puente completo de capa 2 y el enrutamiento de capa 3 en toda la red.
- Flexibilidad: la red ACI admite la capacidad nativa para permitir a los usuarios conectar cualquier host en cualquier parte de toda la estructura. Mediante el uso de la superposición de VXLAN sin penalización integrada, el tráfico puede ser flexiblemente puenteado y enrutado a través del tejido entero. Además, la red ACI puede proporcionar normalización para múltiples tipos de encapsulación diferentes que llegan de los hosts o sus respectivos hipervisores, incluyendo VLAN, VXLAN y Virtualización de red utilizando NVGRE (Generic Routing Encapsulation). Esta característica permite que los hosts físicos, virtuales y basados en contenedores coexistan en la misma infraestructura compartida. La red ACI puede soportar los requisitos modernos de los centros de datos y los requisitos de las aplicaciones basadas en los ordenadores convencionales.
- Eficiencia: un beneficio inherente a la arquitectura gráfica bipartita la red ACI es que cada anfitrión esta exactamente dos

saltos físicos lejos de cada otro anfitrión en la red. Por lo tanto, para grandes cargas de trabajo de datos que requieren una cantidad significativa de tráfico este-oeste entre máquinas, la red ACI se proporciona predecible de baja latencia a escala. Este enfoque ofrece un soporte eficiente para las aplicaciones tradicionales del centro de datos. La red ACI puede superar otras redes tradicionales con eficiencia de ancho de banda de red, ya que puede tener en cuenta el tiempo de llegada de paquetes, la congestión de la red de extremo a extremo y el cambio de flujo para tomar decisiones de equilibrio de carga más inteligentes (CISCO, 2014).

2.6.3 Solución SDN para Huawei.

La solución de interconexión escalable en nube de Huawei está diseñada para construir redes de centros de datos en la nube que proporcionan acceso de alta densidad, capacidad de búfer grande y ancho de banda alto sin sobreescritura (ver figura 2.22). La solución proporciona interconexiones de alta velocidad dentro y entre centros de datos, creando las redes de datos más grandes de la industria. Cada centro admite numeración de servidores de alta velocidad en decenas de miles, y los transceptores ópticos de multiplexación por división de longitud de onda (WDM) proporcionan hasta 80 * 100G de interconexión de larga distancia entre centros de datos. Múltiples centros pueden ser gestionados por una federación de controladores (TECHNOLOGIES, 2017).

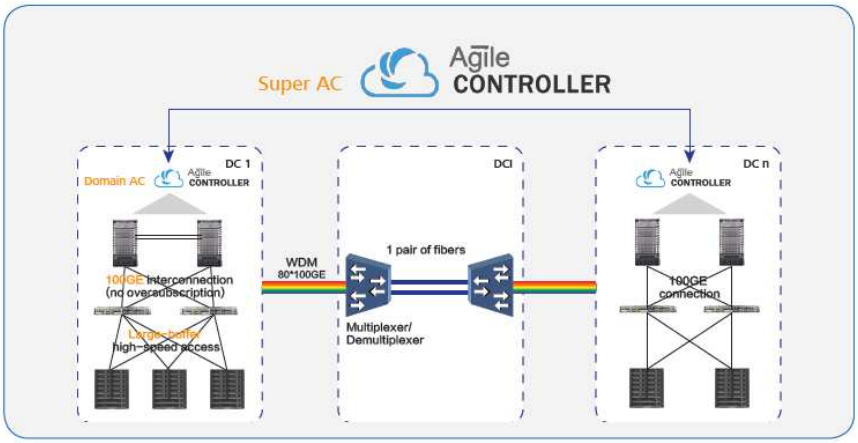


Figura 2. 222. Arquitectura SDN Huawei

Fuente: **(TECHNOLOGIES, 2017)**

Las tecnologías de big data y de minería de datos se encuentran evolucionando, las aplicaciones centralizadas están en crecimiento y el tiempo de vida de los equipos en decrecimiento. En ocasiones, las arquitecturas se encuentran desactualizadas, lo que limita la modernización de servicios y afecta el desarrollo de los consumidores (HUAWEI, 2017).

En la figura 2.23, se muestra el funcionamiento en tiempo real junto con la virtualización, trabajando en conjunto y con los cambios que implica.

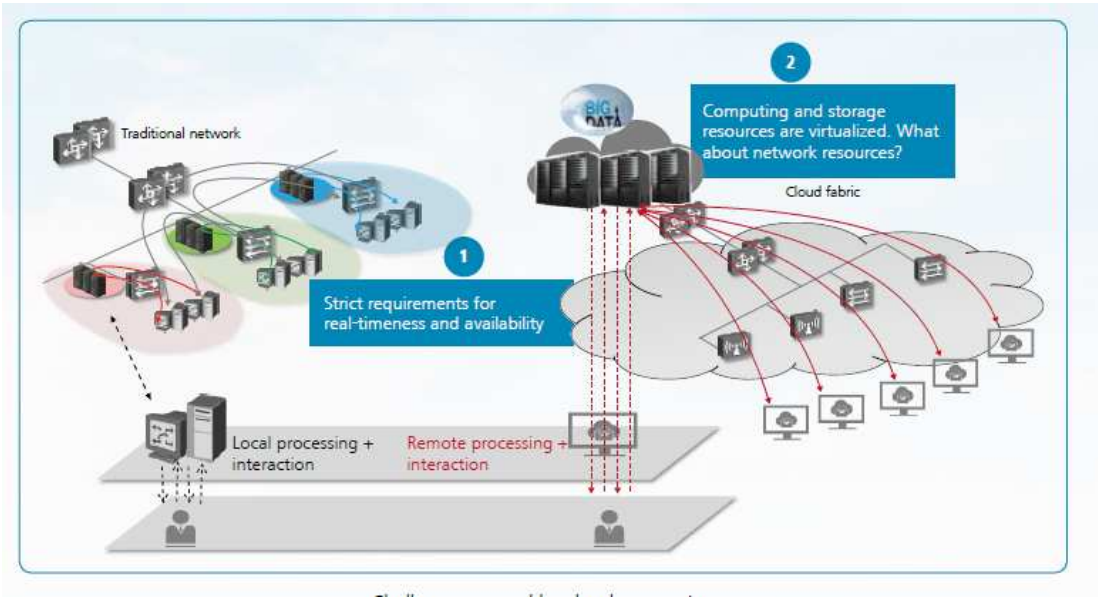


Figura 2. 233. Cambios causados por trabajo en la nube.

Fuente: (Huawei Technologies Co., 2014)

La solución Cloud Fabric en SDN de Huawei es para la configuración de redes, el desarrollo de servicios como el acceso a entornos tanto como físicos y cloud y de VM/contenedor. "Las capacidades de automatización reducen el tiempo de aprovisionamiento de los servicios de semanas a minutos, en línea con las tendencias evolutivas de los Data Center actuales y las demandas de los clientes" (HUAWEI, 2017).

En la figura 2.24, se pude observar como desde un dispositivo móvil, es posible el acceso a múltiples aplicaciones, tanto para trabajo como para entretenimiento.

Figura 2. 244. Beneficios de usar SDN.

Fuente: (Huawei Technologies Co., 2014)

Esta solución se ha creado para permitir que los usuarios puedan acostumbrarse a los rápidos cambios de los servicios que brinda la nube. Esta faculta la elaboración de una red fácil, adaptable y libre de un centro de datos en la nube, para apresurar la migración digital de las compañías. "Es una suite que incluye una solución de despliegue automatizado, la solución Fabric Insight para tareas detalladas de O&M, una solución de interconexión escalable y un ecosistema abierto" (Huawei, 2017).

Está tecnología ayuda a la elaboración de redes de última generación para un centro de datos de nube. Los principales equipos utilizados son base a la serie CloudEngine y el Agile Controller. El CloudEngine tienen la capacidad más grande en los cuales forman partes conmutadores físicos y virtuales. Esta solución une varios equipos para transmisión, enrutamiento, seguridad y gestión de red. Esto ayuda a tener una solución confiable para un centro de datos (Huawei, 2017).

Las características que brinda un centro de datos Cloud Fabric 5.0, son las siguientes:

- Búsqueda de servicios de forma automático en minutos.
- Detallar y ubicar de forma inteligente las fallas en minutos.
- Alta capacidad, escalabilidad y flexibilidad en la red.
- Se basa en arquitectura SD de campus.
- Accesos sin importar hora o lugar a las aplicaciones.
- Usa un cálculo de borde y procesamiento en tiempo real.
- Seguridad en 4 partes (chip/SO/canales/plataformas)
- Una VPN en la nube que permite múltiples conexiones a la vez.
- Control de varias redes completas, con "despliegue de políticas de red y asignación de recursos integrados de extremo a extremo (E2E)"
- Alto nivel de seguridad en la red mediante Agile Controller, a nivel de cloud/canal/dispositivo en ambientes como centro de datos, campus y BYOD.
- Puede detectar 12 clases de amenazas en big data, con un 99% o tal vez más de efectividad.
- Se puede tener un soporte para 12 modelos de servicios de valor añadido (VAS) en cloud (Technologies, 2017).

La solución admite 100G de larga distancia DCI, como se muestra en la figura 2.25. Los conmutadores de la serie CE12800 proporcionan grandes tablas de enrutamiento y amplias funciones de WAN incluyendo MPLS VPN. Integran funciones de conmutador y enrutador, reduciendo los costos de equipos en los centros de datos. Los transceptores ópticos WDM

de larga duración de Huawei simplifican en gran medida los enlaces DCI (TECHNOLOGIES, 2017).

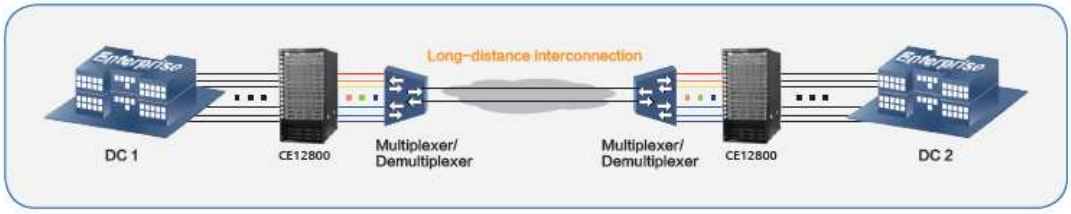


Figura 2. 255. Larga distancia de interconexión.

Fuente: (TECHNOLOGIES, 2017)

Huawei se dedica a maximizar los beneficios para los clientes por medio de soluciones de compensación que desacoplan el software del hardware y proporcionan una alta orquestación de servicios y capacidades de automatización. Estas soluciones crean redes ágiles para mejorar la agilidad de los servicios (TECHNOLOGIES, 2017).

CONCLUSIONES

Al realizar la migración hacia SDN, se tiene una mayor efectividad en la administración, ampliación de la red y sobre todo para realizar mantenimientos y dar una solución a los inconvenientes que se presenten en el tráfico de la red, durante horas de trabajo y sobre todo en momentos en los cuales no son horarios de trabajos de oficina, para tener acceso de forma remota desde cualquier punto. Esto ayuda a contar con una mayor agilidad al momento de dar solución a inconvenientes y para que pueda crecer de forma rápida y oportuna.

Por ser SDN una tecnología nueva es posible para un centro de datos, poder contar con un amplio abanico de posibilidades para mejoras y crecimientos dentro de la red de gestión como en la de implementación. Es de gran ayuda para dar mantenimiento y solución a la red, todo lo contrario con lo que sucede con una red tradicional, en la cual es necesario estar de forma presencial para lograr realizar cualquier actividad requerida, en su lugar SDN brinda al administrador la facilidad de hacerlo de forma remota sin tener que afectar el tráfico de datos.

Sin bien es cierto que en una red tradicional se puede usar una VPN para administración o mantenimientos, más si no existiese internet en el centro de datos, no será posible el acceso, con SDN se puede acceder a los servidores que se encuentran en la nube mediante las aplicaciones que se hayan creado para este tipo de afectaciones, como forma de contingencia para dar soluciones inmediatas.

Con lo antes mencionado se tiene ahorro de recursos y de tiempos, que podrán ser dedicados a otros trabajos de mejoras para la red, e incluso poder brindar atención a usuarios finales con otros tipos de requerimientos sin afectaciones de ningún tipo.

La SDN no solo ayuda para realizar un rápido mantenimiento sino ayuda a tener una escalabilidad mucho más ágil y en un menor tiempo, es posible crear aplicaciones dependiendo de las necesidades que se

presenten para su administración en el tráfico de la red sea este alto o bajo. Se obtiene una gran ventaja en lo referente a la seguridad, porque es posible un monitoreo más eficaz y el detectar más ataques a la red se vuelve más sencillo al tener configuradas las políticas de seguridad con sus distintos tipos de alarmas que son posibles configurar con las aplicaciones antes creadas para cada segmento de la red.

La estrategia planteada brinda distintas opciones que pueden tomarse en cuenta al momento de mejorar o ampliar la red, de acuerdo a las necesidades y los avances tecnológicos que se presentan, que hace que se fuerce el cambio de acuerdo a las necesidades que surjan, por poder aplicarse en cualquier empresa que posea un pequeño, mediano o grande centro de datos.

El análisis previo que se realiza en el centro de datos de la infraestructura y de su tráfico es lo que va a determinar la estrategia más apropiada para realizar la migración hacia SDN. La decisión de los protocolos, herramientas de gestión y su combinación de todo, va de la mano de forma congruente para su funcionamiento y desarrollo. Las decisiones de la estrategia que se tome para realizar la migración, será lo que determine el éxito al pasar del tiempo, de los distintos cambios que se desprendan de allí, es decir, al realizar ampliaciones y actualizaciones en la red, todo tendrá como origen la estrategia que se utilizó en primera instancia para su migración.

RECOMENDACIONES

Al terminar la tesis, luego de la información que se recolecto, se recomienda:

- ✓ Para mejoras en el futuro, es recomendable que tanto profesionales como estudiantes y docentes, desarrollen aplicaciones, para optimizar y mejorar las migraciones en los centros de datos, con el fin de lograr implementaciones rápidas y eficaces.
- ✓ También se recomienda revisar las alternativas que brindan los distintos fabricantes para valorar las posibles potencialidades que pueden ofrecer otros protocolos o tecnologías.
- ✓ Se recomienda, antes de la migración, revisar los costos de equipamiento, para el uso de equipos netamente indispensables, pensando que en un futuro puedan ser usados al crecer el centro de datos estos mismos equipos o reemplazo de tarjetas de aumento de capacidad.
- ✓ Es recomendable una investigación, para comprobar en qué otras áreas de las telecomunicaciones pueden ser utilizadas las SDN principalmente en la 5G.

BIBLIOGRAFÍA

(IETF), I. E. (2011). *Network Configuration Protocol (NETCONF).* Obtenido de RFC-6241: https://tools.ietf.org/html/rfc6241

(ONF), O. N. (8 de Octubre de 2013). *SDN Security Considerations in the Data Center.* Obtenido de ONF Solution Brief: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjTubbVysPUAhUC5iYKHW10C0wQFghGMAA&url=https%3A%2F%2Fwww.opennetworking.org%2Fimages%2Fstories%2Fdownloads%2Fsdn-resources%2Fsolution-briefs%2Fsb-security-data-center

CISCO. (2014). *Is Cisco Application Centric Infrastructure an SDN Technology?* Obtenido de Document ID:1458600776404817: http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-733456.html

Documentation, O. (2017). *OpenDaylight Project.* Obtenido de Release Beryllium: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&cad=rja&uact=8&ved=0ahUKEwiT_PjksLfUAhXF7CYKHaNwAUMQFghKMAc&url=https%3A%2F%2Freadthedocs.org%2Fprojects%2Fopendaylight%2Fdownloads%2Fpdf%2Fstable-beryllium%2F&usg=AFQjCNG2kI575lPTsbmo6bEmAI1

Foundation, O. N. (2014). *Migration Use Cases and Methods.* Obtenido de Migration Working Group: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiZ69TYu8PUAhXF5iYKHQ5uAUYQFggrMAA&url=https%3A%2F%2Fwww.opennetworking.org%2Fimages%2Fstories%2Fdownloads%2Fsdn-resources%2Fuse-cases%2FMigration-WG-Use-Cases.pdf&us

FOUNDATION, O. N. (2014). *opennetworking.org.* Recuperado el 23 de JULIO de 2016, de opennetworking.org: www.opennetworking.org

HUAWEI. (2017). *Solución Cloud Fabric de despliegue automatizado basado en SDN* . Obtenido de http://e.huawei.com/es/solutions/technical/sdn/software-defined-data-center-network/network_automation

Huawei. (2017). *Soluciones de red de Data Center definida por software* . Obtenido de http://e.huawei.com/es/solutions/technical/sdn/software-defined-data-center-network

Huawei Technologies Co., L. (2014). *Huawei Agile Network Solution Brochure (Detailed Version)*. Obtenido de http://e.huawei.com/es/marketing-material/onLineView?MaterialID={DC4E7894-D6AC-46D2-B579-7E7EB6D6F1EA}

Icaza, J. A. (2016). *Universidad Politécnica de Madrid.* Obtenido de DISEÑO DE ESCENARIOS VIRTUALES DE DISTRIBUCIÓN DE CONTENIDO MULTIMEDIA CON SOPORTE DE REDES DEFINIDAS POR SOFTWARE: www.dit.upm.es/posgrado/doc/TFM/.../TFM_Jose_Andres_Marzo_Icaza_2016.pdf

Moreno, I. J. (2015). *Estudio de las redes definidas por software y escenarios virtuales de red orientados al aprendizaje.* Madrid: Universidad Politécnica de Madrid. Obtenido de https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiRwuDEk6DUAhWIVyYKHf3vCjIQFgglMAA&url=http%3A%2F%2Fwww.dit.upm.es%2Fposgrado%2Fdoc%2FTFM%2FTFMs2014-2015%2FTFM_Javier_Cano_Moreno_2015.pdf&usg=AFQjCNGyD6CEWkjDPhdLbu2xv2aGTiJYCw&ca

OPENSTACK. (FEBRERO de 2017). *OPENSTACK.ORG.* Obtenido de https://www.openstack.org

Pinilla, R. A. (2015). *Universida Politécnica de Madrid.* Obtenido de Estudio de las Redes Definidas por Software mediante el Desarrollo de Escenarios Virtuales Basados en el controlador OpenDaylight.: http://oa.upm.es/42968/

Sushant Jain, A. K. (2013). *SIGCOMM'13.* Obtenido de B4: Experience with a Globally-Deployed Software Defined WAN.: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwifu-SipdfUAhVLOiYKHQz8Ah0QFggpMAA&url=https%3A%2F%2Fpeople.eecs.berkeley.edu%2F~sylvia%2Fcs268-2014%2Fpapers%2Fb4-sigcomm13.pdf&usg=AFQjCNF3zV8mPiD2LpVvDNKPGbwXDdsy6

TECHNOLOGIES, H. (2017). *HUAWEI CloudFabric 5.0 Data Center Network Solution*. Obtenido de http://e.huawei.com/es/marketing-material/onLineView?MaterialID={B8A79E47-0251-4689-84ED-12E447EFD482}

Technologies, H. (2017). *Soluciones flexibles de SDN*. Obtenido de http://e.huawei.com/es/solutions/technical/sdn

GLOSARIO

ACI: Infraestructura Centrada de Aplicaciones. **(**Application Centric Infrastructure)

ACTION BUCKET: un conjunto de acciones en un grupo. El grupo seleccionará uno o más paquetes.

ACTION SET: un conjunto de acciones asociadas con el paquete que se acumulan mientras el paquete es procesado por cada tabla las que se ejecutan en un orden especificado cuando el conjunto de instrucciones finaliza el procesamiento de la canalización.

AMD: Micro Dispositivos Avanzado (Advanced Micro Devices)

API: Interfaces de Programación de Aplicaciones (Application Programming Information)

ATS: Interruptor de Transferencia Automática (Automatic Transfer Switch)

AWS: Servicos Web de Amazón (Amazon Web Services)

BYOD: Traiga su Propio Dispositivo (Bring Your Own Device)

CCTV: Circuito Cerrado de Televisión (Closed Circuit Television)

CERT: Equipo de Respuesta ante Emergencias Informáticas

CLI: Interfaz de Línea de Comando (Command Line Interface)

CPU: Unidad de Procesamiento Central (Central Processing Unit)

DCI: Centro de datos de Interconexión. (Data center interconnection)

DHCP: Protocolo de configuración Dinámica de Host (Dynamic Host Configuration Protocol)

ElasticTree: Ahorro de energía en redes de centros de datos.

FlowVisor: es un controlador OpenFlow de propósito especial que actúa como un proxy transparente entre los conmutadores OpenFlow y varios controladores OpenFlow.

HPE: Hewlett Packard Enterprise

IBM: International Business Machines

IP: Protocolo de Internet (Internet Ptotocol)

LC: Conector Lucent (Lucent Connector)

MC LAG: Multi-Chassis Link Aggregation Group

MIBs: Bases de Información de Gestión (Management Information Bases)

MPLS: MultiProtocol Label Switching

NASA: Administración Nacional de la Aeronáutica y del Espacio (National Aeronautics and Space Administration)

NAT: Traducción de Direcciones de Red (Network Address Translation)

NEC: Nippon Electric Company

NETCONF: Network Configuration Protocol

NoSQL: no sólo SQL

ODF: Organizadores de Fibra Óptica

OM: Optical Monomodo

ONF: Fundación de Red Abierta (Open Networking Fundation)
PCI DSS: Estándar de seguridad de datos de la industria de tarjetas de pago (Payment Card Industry Data Security Standard)

PE: Proveedor Edge (Provider Edge)

PLC: Controlador Lógico Programable (Programmable Logic Controller)

PUE: Efectividad de uso de Energía (Power USage Effectiveness)

QoS: Calidad de Servicio (Quality of Service)

REST: Transferencia de estado representacional (Representational State Transfer)

RPC: Remote Producere Call

SDN: Redes Definidas por Software (Software Defined Networking)

SMI: Structure of Management Information

SNMP: Protocolo Simple de Gestión de Redes (Simple Network Management)

SPB: Shortest Path Bridging

SQL: Lenguaje de Consulta Estructurada (Structured Query Language)

SSH: Secure Shell

STP: Protocolo de Árbol Extendido (Spanning Tree Protocol)

TCP: Protocolo de Control de Transmisión (Transmission Control Protocol)

TLS: Seguridad de la Capa de Transporte (Transport Layer Security)

TLV: Tipo, Longitud, Valor (Type, Length, Value)

TRILL: Transparent Interconnection of Lots of Links

TTL: Tiempo de vida (Time to Live)

UMA: Unidad Mejorada de Aire

Using all Wireless Network Around Me: Uso de toda la red inalámbrica de alrededor.

VLAN: Red de Área Local Virtual (Virtual Local Area Network)

VPN: Red Privada Virtual (Virtual Private Network)

VRRP: Protocolo Virtual de Redundancia (Virtual Redundancy Protocol)

WAN: Red de Área Amplia (Wide Area Network)

WiFi: Wireless Fidelity

WiMAX: Worldwide Interoperability for Microwave Access

XML: Extensible Markup Language

YANG: Lenguaje de modelado usado por el modelo de configuración y datos del NETCONF

ANEXOS

Tabla A. 4. El campo longitud y la forma en que se debe aplicar a fluir entradas.

Archivo	Bits	Cuándo Aplicar	Notas
Ingress Port (Puerto de Ingreso)	32	Todos los paquetes	Representación numérica del puerto de entrada, comenzando en 1. Esto puede ser un puerto virtual físico o definido por el conmutador
Metadata	64	Tabla 1 y anteriores	
Ether src (Dirección inicio de Ethernet)	48	Todos los paquetes de los puertos habilitados	Puede utilizar máscaras de bits arbitrarias
Ether dst (Dirección de destino Ethernet)	48	Todos los paquetes de los puertos habilitados	Puede utilizar máscaras de bits arbitrarias
Ether type (Tipo de Ethernet)	16	Todos los paquetes de los puertos habilitados	Tipo de protocolo que encapsula la información útil del protocolo OpenFlow, después de las etiquetas VLAN. Las tramas 802.3 tienen un tratamiento especial.
VLAN id (Id VLAN)	12	Todos los paquetes con etiquetas VLANs	Identificador VLAN de la etiqueta VLAN más externa.
VLAN priority (Prioridad VLAN)	3	Todos los paquetes con etiquetas VLANs	VLAN Campo PCP de la etiqueta VLAN más externa.
MPLS label (Etiqueta MPLS)	20	Todos los paquetes con etiquetas MPLS.	Coincide con la etiqueta más externa de MPLS
MPLS traffic class (Clase de tráfico MPLS)	3	Todos los paquetes con etiquetas MPLS.	Coincide con la etiqueta más externa de MPLS
IPv4 src (Dirección de Origen de IPv4)	32	Todos los paquetes ARP e IPv4	Puede usar mascara de subred o máscara de bits arbitraria.
IPv4 dst (Dirección de Destino de IPv4)	32	Todos los paquetes ARP e IPv4	Puede usar mascara de subred o máscara de bits arbitraria
IPv4 proto / ARP opcode (Protocolo Ipv4 / Acódigo de Operación ARP)	8	Todos los paquetes IPv4 e IPv4 over Ethernet, ARP	Sólo los 8 bits inferiores del código de operación ARP se utilizan.
IPv4 ToS bits (IPv4 ToS bits)	6	Todos los paquetes IPv4	Especifica como valor de 8 bits y situa ToS en los 6 bits superiores.
TCP / UDP / SCTP src port ICMP Type (Puerto de Origen de transporte / Tipo de ICMP)	16	Todos los paquetes TCP, UDP, SCTP e ICMP	Sólo 8 bits más bajos utilizados para el tipo protocolo ICMP
TCP / UDP / SCTP dst port ICMP Code (Puerto de Destino de Transporte / Código ICMP)	16	Todos los paquetes TCP, UDP, SCTP e ICMP	Sólo 8 bits más bajos utilizados para el código del puerto ICMP

Fuente: **(FOUNDATION, 2014)**

Tabla A.5 Servicios OpenStack

Servicio	Nombre del proyecto	Descripción
Tablero (Dashboard)	Horizonte (Horizon)	Proporciona una interfaz gráfica web basada en los servicios subyacentes de OpenStack permitiendo el lanzamiento de una instancia la asignación de direcciones IP y la configuración de los controles de acceso, etc.
Calcular (Compute)	Nova	Gestiona el ciclo de vida de las instancias de proceso en un ambiente de OpenStack. Las responsabilidades influyen la descomposición, programación y el cierre definitivo de las máquinas en la demanda.
Redes (Networking)	Neutron	Permite la conectividad de la red para uno o varios servicios de OpenStack, como OpenStack Compute. Proporciona una API para que los usuarios definan las redes y los archivos adjuntos en ellos. Tiene una arquitectura conectable que soporta varios proveedores y tecnologías de redes populares.
Almacenamiento		
Alamcenamiento de Objetos (Object Storage)	Rápido (Swift)	Almacena y recupera los objetos de datos no estructurados de su elección mediante una REST, en una API basada en HTTP. Es muy tolerante a fallos con su réplica de datos y su posible escalabilidad. Su puesta en práctica es como un servidor de archivos con los directorios montables.
Almacenamiento de Bloques (Block Storage)	Cinder	Proporciona almacenamiento persistente en bloqueo para las instancias en ejecución. Soporta dispositivos plug and play y permite gestionar, por lo tanto, todos aquellos dispositivos de almacenamiento en bloques.
Servicios Compartidos		
Servicio de Identidad (Identity Service)	Keystone	Proporciona un servicio de autenticación y autorización para otros servicios de OpenStack. Proporciona también un catálogo de endpoints para todos los servicios OpenStack
Servicio de Imagen (Image Service)	Glance	Permite almacenar y recuperar imágenes de disco de máquinas virtuales. OpenStack Compute hace uso de esta instancia durante la instancia de provisión
Telemetría (Telemetry)	Cellometer	Monitorea la nube OpenStack para la evaluación comparativa, la escalabilidad y con fines estadísticas
Servicios Alto Nivel		
Orchestration	Heat	Organiza múltiples aplicaciones en la nube de material compuesto utilizando ya sea el formato de la plantilla HOT nativo o el formato de la plantilla AWS, tanto a través de una API REST nativa de OpenStack nativo y una forma de nube compatible con la API de querys

Fuente: (Brian Galarza, 2015)

Tabla A.6 Resumen de consideraciones de Seguridad.

Desafíos de seguridad	Enfoque Autónomo (Hoy)	Enfoque basado en SDN	Beneficios de SDN
Nuevas amenazas de seguridad	Se identifica la firma de seguridad. El usuario se encuentra con las herramientas disponibles dentro del sistema. Se le niega al usuario acceso a la red. AMQ no entiende la negación. El usuario malintencionado se desplaza a otro puerto y continúa propagando el virus.	La visibilidad de la red de extremo a extremo se deriva de la configuración centralizada y del estado de la red. Los controles de grano grueso o fino implementan contramedidas en tiempo real.	El personal de operaciones puede experimentar continuamente (fuera de banda) para refinar constantemente el comportamiento de AMQ (gestión de rutas, firmas, gestión del tráfico, etc.). Reducir significativamente los recursos de la plataforma requeridos para el procesamiento de seguridad, reduciendo así CapEx, especialmente para interfaces de alta velocidad.
Perímetro de seguridad	Perímetro se define a través de objetos físicos (puertos, subredes, etc.). Cada dispositivo debe configurarse de forma estática individualmente, normalmente a través de CLI. Todo el tráfico de cada objeto físico debe ser monitoreado, normalmente usando una sola política.	El perímetro se define a través de los conceptos de capa de aplicación (grupos, tipo de dispositivo, etc.) El tráfico proveniente de dispositivos más vulnerables (es decir, fuentes externas a la empresa) puede ser examinado más intensamente que el tráfico de los dispositivos más seguros internos a la empresa.	La política se desacopla del perímetro físico para alinear mejor el procesamiento de seguridad con las amenazas. Las políticas pueden aplicarse de forma granular en función de los atributos de la capa de aplicación, no sólo de los atributos físicos, como los puertos. La complejidad de seguridad no aumenta en proporción a los

		El tráfico puede ser monitoreado independientemente de la ubicación física de la fuente. La configuración de bajo tacto es posible para todos los dispositivos de seguridad de cada dominio.	cambios en el perímetro físico y lógico, mejorando la protección para el creciente número de usuarios móviles. La supervisión coordinada y multi-capa consigue una cobertura de seguridad más completa en la pila de 7 capas.
Nueva velocidad característica. Gestión proactiva de parches.	Difícil de lograr de una manera consistente debido a la disponibilidad de recursos finitos en el dispositivo integrado.	La gestión centralizada de los parches y el despliegue de nuevas funciones son posibles mediante el control centralizado para responder rápidamente a las nuevas amenazas.	Más simple para introducir funciones mejoradas; Las operaciones simplificadas alivian la necesidad de configurar dispositivos individuales. Permite a un entorno de ejecución virtual (VEE) analizar y responder rápidamente a amenazas que cambian constantemente sin la necesidad de parchear cada dispositivo de red individual. VEE permite la creación de prototipos, pruebas y despliegues en tiempo real para responder rápidamente a las nuevas amenazas. Una operación significativamente

			más simple reduce el coste.
Alta escalabilidad	Requiere un aumento proporcional en el hardware para asegurar la cobertura en el perímetro físico.	El procesamiento de seguridad virtualizada crea las demandas de hardware (y la complejidad de la administración).	Aumenta la capacidad de procesamiento de seguridad junto con el alcance de la red y el procesamiento de seguridad adicional. Mejora la utilización porque los aumentos de capacidad pueden proporcionarse de forma temporal.

Fuente: ((ONF), 2013)

- **Visita a un Datacenter. Entrevista.**

Entrevista realizada a el Ing. Carlos Marín, Coordinador del Business Operation Center, de una empresa de tecnología con un centro de datos a nivel nacional.

El centro de datos cuenta con varias certificaciones una de ellas la "certificación Tier IV en la ciudad de Guayaquil (esto equivale a contar con una redundancia en todos los aspectos), tener una disponibilidad del 99.995%, les permite tener una caída de 18 minutos al año. La Certificación PCI DSS para tarjetas de crédito. Como un ente externo llega a los servidores con la información solo en la parte física y no lógica. CERT continuidad de negocios ISO 22301, utilizada para respaldar información crítica, mediante un análisis realizado bajo un FODA de Ishikawa se toma la decisión. El respaldo se encuentra en el centro de datos de la ciudad de Quito. Además posee las certificaciones ISO 9001 2008 en calidad y la ISO 27001 en seguridad.

En los exteriores el nivel de redundancia se encuentra del lado b que siendo el backup del lado a. Las dos salas de IT se distinguen como etapa 1 y etapa 2. En los que se trabaja con conceptos de pasillos fríos y

calientes. El enfriamiento se realiza mediante dos chillers (cada etapa en total 8 sumando los backups); enfría el agua (dejándola helada) y esta es pasada por tuberías y va hacia las UMAS, dentro de los cuarto de ITs, que quitan el frio y lo pasan por el piso falso al área de TI. El respaldo que tienen los dos chillers, en caso de daño, es un tanque de agua y en cada uno de los lados de respaldo (también utiliza agua del reservorio) con el mismo proceso.

UMA (unidad Mejorada de Agua)

En la ciudad de Quito el centro de datos tiene una certificación Tier III, esto es por no tener un tanque de agua como en Guayaquil motivo porque no es un Tier IV, por estar las instalaciones de un edificio, los chillers se encuentran en la azotea con sus respectivas redundancias.

La fuente de energización del centro de datos en ambas etapas son, la primera fuente es la energía eléctrica en los Tier IV. Para esto se decidió que la principal sea la energía de la calle, cuando se va la luz cambia a trabajar con ATS para la conmutación automática para encender el generador (por costo medio ambiente). La redundancia es n+1 funcionan dos y queda de backup uno. Con una potencia de 800kva cada generador (con dos generadores se puede permanecer).

La celda de media tensión, solo con 2 puede soportar la carga (es donde llega la energía eléctrica) que alimenta es de un máximo de 1500KHw. Es posible estar hasta 4 días con el generador que trabaja con diésel (tiempo que dura el tanque de diésel) se puede llenarlo sin necesidad

de ser apagados para dar continuidad al negocio. Todo se encuentra controlado por CCTV.

El servicio de internet en el sector que no llega por radio enlace o fibra por ubicación geográfica llega por satélite con un cuarto de enlace satelitales (cuarto satelital) tecnología banda C (más cara con antenas de gran tamaño y solo vulnerable a las manchas solares) y KU.

Se pide a clientes y proveedores de llegar con fibra óptica hasta el centro de datos, cuando no se tiene los recursos económicos o físicos se lo hace vía radio enlace con línea de vista a cerro azul y otro a mapasingue, esto llega al cuarto satelital y de ahí pasa al área de TI que ya está sectorizado con fibra.

Por tener la certificación ISO 22301, cada dos meses realizan simulacros de todas las áreas para revisar si todo funciona de manera correcta. Incluso de incendios verificar puertas de escape.

Se tiene un cuarto de Cintoteca. En un cuarto se guarda en cintas magnéticas o cartuchos con data backup de sus equipos, se encuentra ambientado de acuerdo a la cinta con una UMA pequeña, cuarto considerado crítico con vigilancia CCTV y con un agente de marca Ecaro para apagado del fuego. Una parte se encuentra comprada y separada por una jaula en la cual no se tiene ningún tipo de administración por parte de la empresa solo alquilan el área.

En el interior se encuentra el BOC (Centro de Operaciones de Negocios); el sistema CCTV para monitorear el centro de datos de forma interna y externa. El monitor 1 con certificación PCI uno de los requisitos es que se deben almacenar 90 días de video de todas las cámaras de seguridad. En el monitor 2 se encuentra el monitoreo eléctrico con software Scada, utiliza 400Kw. Al irse la luz los rangos bajan a cero. Funciona un minuto el UPS hasta cargar los generadores y que se sincronizan, si no arrancan los UPS puede esperar 10 minutos. La energía se encuentra entre los 6 generadores pertenecientes a la etapa 1. La etapa 2 se encuentra vendida y funciona de la misma forma. Con solo un generador es suficiente

por ser de 800 Kw cada uno, mas es distribuida la capacidad eléctrica entre los 6 para que todos puedan funcionar.

El monitoreo de servicio de clientes es de tres formas. Zabick es un software free con plataforma Linux, el monitoreo de SNMP y todo lo que tenga. Cuenta con un agente para verificación capacidades de servidores. Se puede configurar umbrales para enviar alarmas de seguridad, también en los CPU, etc. El monitoreo de las UMAs es mediante SNMP, temperatura y humedad. Las cámaras también, pero solo para monitoreo no para grabar.

Se pueden realizar diagramas de las redes. Alarmas para tomar acciones a seguir con sus tiempos de alarmas y se envía mediante e-mail hacia el BOC para notificación. Los colores para sus respectivas clasificaciones e identificaciones de grado del problema son: rojo warning, azul informativo, naranja no clasificado.

Utilizan cisco Nexus en toda la red metro, se maneja con topología cisco. Capa de acceso Nexus 2000; capa de distribución Nexus 5000; capa de Core Nexus 7000 actualmente se está migrando a equipos ASR 9000 para hacer netamente conmutación en datas centers (aún no migrado) en pruebas en el área de networking de evaluación.

En la capa de Core utiliza Nexus 7K, el equipo de Core conocido como PE en el mundo MPLS, conecta a los PE de Guayaquil y se une a la red Metro Ethernet a nivel nacional, de la misma forma funciona en la ciudad de Quito.

El servicio de virtualización. Se transforma máquinas físicas a virtuales a través de un clouster, con un almacenamiento mediante storas. El Winvwer fue la pionera, además usa Zitrix (servidores DNS). Se tienen aproximadamente 800 máquinas. Envía alarmas de disco duro lleno, CPU alto y RAM alta. Es configurable, ejemplo 80% para envió. Se utiliza el programa Viewer Convert para virtualización por encontrarse todo embebido.

El área de TI. En los pasillos de TI, por ser un Tier IV, todo tiene redundancia. Entra la fibra por lado a y b (backup). El cuarto de Crooss conexiones se encuentran tanto en lado a y b. Las fibras llegan de la calle al cuarto de croosing, donde convergen todos los nodos de la ciudad. Los equipos pasivos únicamente ningún equipo electrónico, únicamente ODFs. Llega la fibra de la calle. Todos los enlaces llegan allí. Todos los ODF ya están conectorizados. Entre proveedores dar servicio a un cliente externo, se utiliza una cruzada por cable UTP, por medio de los puertos asignados. Si es interno, se debe revisar de que ruta (nodo) sale hasta el cliente se realiza la cruzada.

Los tipos de fibra que utilizan son, monomodo se trabaja con OM3, conectores de fibra LC y multimodo. El centro de datos trabaja parte física y networking trabaja la parte lógica. En la parte de comunicaciones depende del cliente si desea backup o no, esto depende de su capacidad económica. Cada rack mide 2.54 cm, pueden ir hasta 45 unidades ODFs abiertos y 42 unidades ODFs cerrados. Cuarto considerado crítico, cámara CCTV y Ecaro. Pasillo caliente por no tener equipos eléctricos.

Las canaletas existen 4, una para cables UTP, una para fibra y dos para cables eléctricos.

Las UMAs, dentro de él cuarto de IT estan las UMAs que quitan el frio al agua lo ingresan por el piso falso. El tanque de Ecaro 25 da servicio al cuarto de IT. Hay un total 24 UMAs entre las etapas 1 y 2 (todo el centro de datos), cada lado 12 UMAs cada etapa 6 UMAs.

Los cuartos de servicios. Cuarto de tableros eléctricos con ATS gigantes, los que conmutan al irse la energía de la calle a los UPC y luego a los generadores eléctricos. Los tableros de distribución con ATS, el departamento eléctrico mantenimiento a los equipos. Cuarto considerado crítico con cámara CCTV y el agente Ecaro 25.

ECARO 25

El cuarto de UPS. Se tiene 7 UPS, los que entran a trabajar al irse la luz apoyadas con las baterías de 200 Kva cada una total 1400 Kva. Las celdas deben dar 1500 Kva. Se tienen baldosas perforadas (piso falso, por donde ingresa el aire frio) una parte tiene el 50% del aire para que ingrese y en otra parte el 25% del aire. Se tiene varillas estándar de 90 cm, sobre eso se construye el piso falso.

El cuarto de baterías dentro de los armarios se cambian cada año y medio, sin estar dañadas por precaución. Conectada de manera serial. Se usa la batería de camiones.

Cuarto de rectificadores eléctricos. La electrónica del centro de datos es con los PLC envían datos de monitoreo a los sistemas. Tableros que controlan las bombas. PLC, utiliza una estructura de programación en forma de escalera, para traducir a un lenguaje entendible la información para las distintas funciones configuradas. Se encuentran convertidores dentro del tablero. Cuarto considerado crítico, cámara CCTV y el agente Ecaro 25.

El cuarto de IT, con UMAs. Se trabajó con pasillo frio y pasillo caliente. El pasillo donde están los equipos está el aire frio y vota el aire caliente hacia fuera para el pasillo, para la optimización de recursos. El pasillo frio, en el cuarto de comunicaciones del centro de datos. Cada rack cerrado de

42 unidades sobre cada rack se tiene 2 ODF, cada uno tiene un ODF que se ve con el lado a y otro con el lado b.

Un servidor Nexus 2K con conexiones cobre, usa cable utp. El ODF para conexiones de fibra. Chasis Fortine por seguridad. Fortimail, Fortianalay. Todo manejado por el área de CERT.

La tecnología de almacenamiento (no se trabaja con ninguna marca específica), Cisco, 3Par y Hp.

ACR9000 para el Core del centro de datos (en prueba para reemplazar a los Nexus 7K de la capa de Core). De manera física en la ciudad de Guayaquil se tiene uno en el centro de datos, uno en Telepuerto. En la ciudad de Quito se tiene uno en el centro de datos, y otro ubicado en la calle Gosseal.

La tecnología de almacenamiento. El protocolo standar con los enclouser. Mejor topología, se direcciona a un equipo storage para que la data quede intacta. Tecnología Tripa, HP, PE, Nexus 7K y VTL para sacar backup.

El servico de housing (coloción), desde una unidad de rack a toda una etapa. Las métricas con que se mide un dato.

- ✓ PUE: eficiencia energética. Se mide por medio de una fórmula. Toda la energía del data (100%) dividir para el consumo de IT, igual a 1 o menos 1 es lo óptimo. Más de 1 se debe bajar la eficiencia energética. Utilizando pasillos inteligentes (luces led, se apagan cuando pasan)

Sala de TI

- ✓ DCI: eficiencia de infraestructura. Energía eléctrica de consumo dividido para TI. La métrica de espacios ambientales (dpto energía industrial)

Como contingencia en el caso que dejase de funcionar en la ciudad de Guayaquil, todo va hacia el centro de datos de Quito, o viceversa de ser el caso.

El costo de implementación para un centro de datos con certificación Tier IV fue de $2'000.0000. El mantenimiento mensual es de $30.000. Con un mantenimiento físico que se realiza cada 2 meses.

Las estadísticas de tráfico son de 10 Gigas. La saturación de los enlaces tiene varias opciones de redundancias y backups en el área de networking.

Los equipos que se utilizan son Cisco Nnexus (al momento se están migrando a equipos Nexus de nuevas versiones). La actualización de software luego del análisis es de 2 meses cumpliendo las pruebas más o menos 15 días con un tiempo total. La métrica de solución de backbone es de máximo 4 horas y de circuito 2 horas máximo.”

Principales marcas de equipos y sus respectivas descripciones utilizados en Ecuador para centros de datos.

- **CISCO**

Los enrutadores de servicios de agregación de la serie ASR 9000 representan un nuevo paradigma en el enrutamiento de borde y núcleo, con escalabilidad excepcional, confiabilidad de clase operadora, diseño ambientalmente consciente, increíble flexibilidad y un precio de referencia atractivo. La ASR 9000 Series tiene un amplio portafolio de productos, que van desde Cisco ASR 9001 (2 unidades de rack [2RU]) hasta el ASR 9922 (44RU), cada sistema diseñado para proporcionar verdadera fiabilidad de clase portadora El sistema operativo Cisco IOS® XR, redundancia completa del sistema y un completo complemento de esquemas de resiliencia de red. La serie ASR 9000 también ofrece inteligencia de servicios y aplicaciones centrada en la entrega de video optimizada y la agregación móvil. Por último, la serie ASR 9000 de Cisco está diseñada para simplificar y mejorar los aspectos operativos y de implementación de las redes de prestación de servicios.

Permite que cada proceso se ejecute en una memoria protegida separada, incluyendo cada protocolo de enrutamiento, junto con múltiples instancias de control, datos y planos de administración soportados. El software también soporta el procesamiento de rutas distribuidas.

Estas características proporcionan una escala excepcional, flexibilidad de servicio y alta disponibilidad:

- Arquitectura integrada de conmutador:
  - Arquitectura distribuida del conmutador.
  - Arquitectura no bloqueante de baja latencia de varios niveles
  - Inteligencia de servicio y prioridades de tráfico
- Capacidades superiores de sincronización de red con soporte para:

- Suministro Integrado de Tiempo para la Construcción Centralizada (BITS)
- Precision Time Protocol (PTP) o IEEE 1588-2008, a través de un puerto Ethernet dedicado de 10 Mbps o 100 Mbps
- Tiempo bidireccional del día (A DO) con interfaces de 10 MHz y 1 pps

Hardware

Los enrutadores de servicios de agregación de la serie ASR 9000 ofrecen una escala y densidad de 10 Gigabit Ethernet y 100 Gigabit Ethernet sin igual. Los enrutadores de la serie ASR 9000 y ASR 9900 proporcionan un plan de actualización in situ a una mayor densidad de puertos Ethernet de 10 Gigabit Ethernet y 100 Gigabit sin la necesidad de un reemplazo completo del chasis. Estas tarjetas de línea, ofrecidas en configuraciones de base ya escala extendida, se complementan con el tejido no bloqueante (en el RSP para los enrutadores ASR 9006, ASR 9010, ASR 9910 y ASR 9904 y en tarjetas de tejido separadas para el Cisco ASR 9910, ASR 9912 y ASR 9922), y por la innovadora infraestructura backplane, térmica y de energía en el chasis.

Los proveedores de servicios pueden agregar más potencia a medida que aumenta el ancho de banda y los requisitos de las funciones, agregando más tarjetas de línea al chasis. Esta capacidad se traduce en un CapEx inicialmente menor y un OpEx óptimo durante la vida del producto.

Cuenta con una infraestructura de sincronización totalmente integrada, que permite a los enrutadores tomar entradas de sincronización (por ejemplo, SynchE, Building Integrated Timing Supply [BITS] y DOCSIS® Timing Interface [DTI]) y distribuirlos sobre el backplane a cada ranura.

La infraestructura térmica optimizada de la serie ASR 9000 está diseñada para ser escalable para soportar los requisitos de capacidad

futuros. Los ventiladores de alta velocidad y eficiencia proporcionan requisitos de energía reducidos en entornos operativos normales, al tiempo que conservan la capacidad de enfriar tarjetas de líneas actuales y futuras en condiciones extremas.

Software

Los enrutadores de la serie ASR 9000 ofrecen una escala excepcional, flexibilidad de servicio y alta disponibilidad para las redes de transporte Carrier Ethernet. Los enrutadores son alimentados por el software Cisco IOS XR, un innovador sistema operativo distribuido de autocuración diseñado para funcionar siempre mientras se escala la capacidad del sistema hasta 160 Tbps. Cisco IOS XR Software también permite una solución IP / MPLS de extremo a extremo a los requisitos de los proveedores de servicios basados en el mismo software, lo que reduce la complejidad operativa de la gestión de múltiples sistemas operativos. Cisco IOS XR Software versión 3.7.2 introdujo el soporte para los enrutadores de la serie ASR 9000, diseñados para abordar la base Carrier Ethernet para la creación de redes visuales. La serie ASR 9000 mejora aún más el diseño de Ethernet Carrier Ethernet de red de próxima generación (IP NGN) para un transporte convergente, resistente, inteligente y escalable de servicios de consumo, comerciales, al por mayor y móviles.

Las aplicaciones Cisco Carrier Ethernet de la serie ASR 9000 incluyen servicios empresariales tales como VPN de capa 2 (L2VPN) y L3VPN, Televisión de Protocolo de Internet (IPTV), redes de distribución de contenido (CDN) y redes de transporte móviles de backhaul. Las características soportadas incluyen servicios de Ethernet; L2VPN; IPv4, IPv6 y L3VPN; Capa 2 y Capa 3 Multicast; IP sobre el multiplexado por división de longitud de onda denso (IPoDWDM); SyncE; EOAM y MPLS OAM; Listas de control de acceso de capa 2 y capa 3 (ACL); H - QoS; MPLS Ingeniería de Tráfico Rápida Reorientación (MPLS TE-FRR); Agregación de enlaces multi-chasis (MC-LAG); Integrated Routing y Bridging (IRB); Y Cisco Nonstop Forwarding (NSF) y Nonstop Routing (NSR).

El equipo de Cisco Services responde a sus requisitos específicos, mitiga el riesgo de los servicios generadores de ingresos existentes y ayuda a acelerar el tiempo de comercialización de los nuevos servicios de red.

- **HUAWEI**

Conmutador para Centro de Datos de la serie CloudEngine 12800 (CE12800)

La serie brinda fiabilidad carrier grade, compatibilidad con la virtualización, organización en clúster iStack y funciones de redes definidas por software para la construcción y la expansión de Centros de Datos y redes de campus. Estos modelos de conmutadores ofrecen versatilidad y un sólido rendimiento para aplicaciones multimedia basadas en un servidor, analítica de Big Data y Cloud Computing.

La conmutación elástica satisface los requisitos especializados de los usuarios, 576 puertos 100 GE, 576 puertos 40 GE, 2304 puertos 25 GE o 2304 puertos 10 GE con una capacidad de conmutación total de 178 Tbit/s por conmutador, ampliable a 356 Tbit/s.

Las tecnologías de ahorro de energía y el enfriamiento patentado y bajo demanda de la parte frontal hacia la parte posterior mantienen el rendimiento en condiciones óptimas y evitan el calentamiento de las redes.

Estos conmutadores de core de centro de datos son de fácil uso y de alto rendimiento. Tienen las siguientes características:

- Contiene funciones de virtualización que trabaja en sincronización con los entornos cloud actuales: permiten virtualizar hasta 16 conmutadores CE12800 con un solo conmutador lógico para lograr resistencia y gestión simplificada.
- Tolera TRILL (Transparent Interconnection of Lots of Links) para redes con hasta 512 nodos; con funcionalidad de red

virtual Ethernet (EVN) para que los centros de datos puedan compartir los recursos.

- Las API del sistema abierto de programabilidad (OPS) y el software de Huawei ofrecen opciones de redes flexibles y la posibilidad de suministrar servicios nuevos bajo demanda sin necesidad de reemplazar el hardware ni interrumpir el acceso a las aplicaciones.
- Trabaja en un alto nivel de eficiencia en las copias de seguridad y la duplicación de datos: diseño de matriz horizontal “ortogonal“, ancho de banda de enlace descendente de baja latencia y enormes memorias intermedias dinámicas de 18 GB para tarjetas de línea.

Conmutador para Centro de Datos de la serie CloudEngine 8800 (CE8800)

El CE8800 brinda 32 puertos 100 GE, 64 puertos 40 GE o 128 puertos 25 GE/10 GE en un solo dispositivo de 2 U que brinda throughput excepcional y baja latencia como conmutador core o de agregación para centro de datos y redes de campus de alta gama.

Se pueden unir los conmutadores de la serie CE8800 con los conmutadores CE5800, CE6800, CE7800 y CE12800 de Huawei en un ambiente virtualizado fácil de administrar y optimizado para las aplicaciones multimedia, el procesamiento de datos basado en servidores y un gran ancho de banda.

Mejore el rendimiento, la versatilidad y la fiabilidad con los conmutadores CE8800 listos para SDN.

Algunas de sus características son:

- La arquitectura avanzada permite la virtualización y la TRILL de capa 2 (Transparent Interconnection of Lots of Links) para el aprovisionamiento, la migración y la administración de políticas de seguridad en redes con hasta 512 nodos.

- Brinda una capacidad de conmutación de 6,4 Tbit/s en TOR de 2 U, rendimiento de transmisión de 2976 Mpps.
- La tecnología de clúster iStack inteligente de Huawei aumenta la fiabilidad y simplifica la gestión de la red a través de la combinación de varios conmutadores en un único conmutador lógico. De la misma forma, admite el diseño acumulado en distancias largas.
- El OPS (Open Programmability System) brinda API abiertas e integrales para ejectuar el networking flexible, la monitorización del rendimiento, la configuración dinámica y la administración de los servicios (es decir, VPN) y las políticas de seguridad.
- Con ZTP (Zero-Touch Provisioning) que facilita el despliegue rápido y sencillo, y permite la personalización de la red y la automatización de las actividades de operación y mantenimiento bajo demanda.

Conmutador para Centro de Datos de la serie CloudEngine 7800 (CE7800)

Estos conmutadores ofrecen 32 puertos de 40 GE en un solo dispositivo de 1 U que brinda throughput excepcional y baja latencia como conmutador core o de agregación para los centros de datos y redes de área de campus de alta gama. Un sistema de agrupamiento compuesto por hasta 16 conmutadores cuenta con hasta 512 puertos de acceso de 40 GE.

Es posible agregar los conmutadores de la serie CE7800 con los conmutadores CE5800, CE6800, CE8800 y CE12800 de Huawei en un entorno virtualizado fácil de administrar y optimizado para las aplicaciones multimedia, el procesamiento de datos basado en servidores y un gran ancho de banda.

Acrecienta el rendimiento, la versatilidad y la fiabilidad con una red de conmutación CE7800. Utiliza puertos de 40 Gbit/s para centro de datos, redes empresariales y cloud computing.

Estos conmutadores tienen las siguientes características:

- Admiten Border Gateway Protocol - Ethernet VPN (BGP-EVPN), que puede ejecutarse como plano de control VXLAN para simplificar la configuración VXLAN en y entre centro de datos.
- Acepta la sensibilidad a la virtualización y las redes de Transparent Interconnection of Lots of Links (TRILL) de capa 2 con hasta 512 nodos, lo que permite lograr una migración de VM en línea a gran escala, así como la migración dinámica de políticas.
- Cada uno de los puertos de 40 GE se puede usar como múltiples puertos 10 GE, lo que permite lograr un networking flexible.
- El sistema de agrupamiento más grande de la industria (iStack) incrementa la fiabilidad y admite el almacenamiento de larga distancia, lo que simplifica la administración de redes.
- El sistema abierto de programabilidad (OPS) admite numerosas interfaces de programación de aplicaciones (API) abiertas para lograr facilidad de expansión, mientras que el aprovisionamiento sin intervención (ZTP) permite lograr el despliegue sin configuración, la personalización de redes bajo demanda y tareas automatizadas de operación y mantenimiento (O&M).

Conmutador para Centro de Datos de la serie CloudEngine 6800 (CE6800)

La densidad de puertos 10 GE más alta de la industria en un conmutador TOR de 1 U (hasta 80 puertos).

Los conmutadores de la serie CE6800 de Huawei ofrecen un rendimiento de alto throughput y baja latencia para centro de datos y redes de área de campus de alta gama. Ocho puertos de vínculo superior de 40 GE/100 GE permiten un rendimiento excepcional cuando se establece un

puente con los conmutadores core que utilizan una red de Transparent Interconnection of Lots of Links (TRILL).

Es posible juntar los conmutadores CE6800 y CE12800 para implementar una plataforma de red no bloqueante.

Optimiza la densidad alta, la conmutación de baja latencia y simplifica el abastecimiento y la gestión de servicios de TI:

- La compatibilidad con el canal de fibra sobre Ethernet (FCoE) permite que una sola red transporte servicios de almacenamiento, datos y cómputo, lo que reduce los costes de construcción y mantenimiento de la red.
- El primer sistema de agrupamiento de 16 miembros de la industria y la funcionalidad SVF (matriz supervirtual) de Huawei logran la escalabilidad vertical, lo que simplifica la administración de la red y mejora la fiabilidad.
- La compatibilidad con una gran red TRILL de capa 2 (hasta 512 nodos) y la sensibilidad a la virtualización permiten lograr movilidad de políticas y migración de VM (máquinas virtuales) en línea a gran escala.
- El sistema de programabilidad abierto (OPS) admite numerosas interfaces de programación de aplicaciones (API) abiertas para lograr facilidad de expansión, mientras que el aprovisionamiento sin intervención (ZTP) permite lograr el despliegue sin configuración, la personalización de red bajo demanda y tareas automatizadas de operación y mantenimiento (O&M).

Conmutador para Centro de Datos de la serie CloudEngine 6800 (CE6800)

Cuenta con 48 puertos GE de velocidad de línea más puertos de enlace ascendente 10 GE o 40 GE para apilar hasta 16 conmutadores. Los puertos 40 GE permiten crear un grupo no bloqueante que se extiende a lo largo de las distancias geográficas existentes entre los centros de datos.

Los conmutadores CE5800 admiten redes estándares de interconexión transparente de muchos enlaces (TRILL) para el aprovisionamiento flexible de servicios y para migraciones de máquinas virtuales (VM) a gran escala. El software y las funciones de seguridad integrales del sistema VRP de Huawei garantizan un rendimiento seguro y de alta disponibilidad con bajos costos de operación y mantenimiento.

Como características se mencionan:

- La tecnología de matriz virtual superior (SVF) de Huawei permite la virtualización de múltiples conmutadores físicos para crear un conmutador lógico que simplifica la administración de la red y mejora la fiabilidad.
- Se combinan con los conmutadores CE12800 para crear un entorno de conmutación Ethernet virtualizado, convergente y fácilmente escalable.
- La flexibilidad del sistema abierto de programabilidad (OPS) permite que se admitan diversas capacidades para la personalización flexible de servicios en todas las capas de la red.
- Los módulos de ventilación configurables incluyen opciones de adelante hacia atrás y de atrás hacia adelante para optimizar el enfriamiento a medida que aumenta la capacidad.
- El aprovisionamiento sin intervención (ZTP) simplifica la configuración y el despliegue, lo que permite la personalización bajo demanda de los servicios y la automatización de las tareas de operación y mantenimiento.

- **HP**

HP MSR2000

Es un componente de la solución HPE FlexBranch, que forma parte de la completa arquitectura HPE FlexNetwork. Estos enrutadores cuentan con un diseño modular que ofrece servicios de aplicación sin igual para sucursales de tamaño pequeño a tamaño medio. Esto ofrece al departamento de TI el beneficio de reducir la complejidad y simplificar la configuración, implementación y administración.

La serie MSR2000 proporciona una infraestructura de red ágil y flexible que le permite adaptarse rápidamente a los requisitos cambiantes de la red, al mismo tiempo que ofrece servicios simultáneos integrados en una plataforma única y fácil de administrar.

Características:

- Hasta 1 reenvío Mpps; Enrutamiento, conmutación, seguridad, voz y movilidad convergentes de alto rendimiento
- Funciones de seguridad incorporadas con cifrado basado en hardware, firewall, conversión de direcciones de red (NAT) y redes privadas virtuales (VPN)
- Amplitud de conectividad LAN y WAN líder en la industria, hasta 24/48 puertos de conmutación GE integrados
- No hay complejidad adicional de licencias; Sin costo para funciones avanzadas
- Solución Zero-touch, con gestión de un solo panel de vidrio

Funcionamiento:

- Excelente rendimiento de reenvío. Proporciona un rendimiento de reenvío de hasta 1 Mpps (672 Mb / s); Cumple con las demandas de aplicación de ancho de banda de las empresas
- Potente capacidad de seguridad. La serie MSR2000 está disponible con cifrado estándar o alto, un acelerador de cifrado de hardware incorporado para mejorar el rendimiento del

cifrado; El rendimiento de encriptación IPSec puede ser de hasta 400 Mb / s con un máximo de 1.000 túneles VPN IPSec.

Arquitectura:

- Soporte de MSR OpenFlow 1.3.1.
- Plataforma multiservicio ideal. Proporciona un enrutador WAN, conmutador Ethernet, WAN 3G y 4G, firewall con estado, VPN y SIP o puerta de enlace de voz en MSR.
- Arquitectura avanzada de hardware. Soporta procesadores multinúcleo, conmutación Gigabit y bus PCIe. Dos fuentes de alimentación interna (AC o DC) compatibles con MSR2004-48 para mayor confiabilidad y flexibilidad.
- Nueva versión del sistema operativo. Se entrega con el nuevo sistema operativo Comware v7 que ofrece lo último en virtualización y enrutamiento

Conectividad:

- Virtual eXtensible LAN (VXLAN). Es una red basada en IP, utilizando el paquete "MAC in UDP" de la tecnología Layer VPN. VXLAN se puede basar en un ISP existente o las redes IP de la empresa para el sitio físico descentralizado proporciona la comunicación de capa 2 y puede proporcionar el aislamiento del servicio para los diferentes inquilinos
- Servicio Virtual de LAN Privada (VPLS). VPLS ofrece un servicio L2VPN de punto a multipunto a través de un backbone MPLS o IP. La columna vertebral es transparente a los sitios de los clientes, que pueden comunicarse entre sí como si estuvieran en la misma LAN. Los siguientes protocolos son compatibles con MSRs, RFC4447, RFC4761 y RFC4762, detección BFD en VPLS, Soporte HOPE (H-VPLS) jerárquico, recuperación de direcciones MAC en H-VPLS para acelerar la convergencia

- Conectividad de puerto de alta densidad. Proporciona puertos de conmutación LAN de 24 ó 48 Giga a bordo (todos los puertos de conmutación se pueden configurar como puertos enrutados), hasta cuatro ranuras de módulo de interfaz y hasta 30 opciones de módulo
- Varias interfaces WAN. Proporciona un enlace tradicional con E1, T1, Serial, ADSL sobre POTs, ADSL sobre ISDN, G.SHDSL, Asynchronous Transfer Mode (ATM), y enlaces ISDN; Módulos de acceso de alta densidad Fast o Giga Ethernet; Acceso a la movilidad con módulo 3G (WCDMA / HSPA) / 4G LTE SIC y módems USB 3G / 4G.
- Protección de tormenta de paquetes. Protege contra tormentas de broadcast, multicast o unicast con umbrales definidos por el usuario.
- Loopback. Soporta pruebas de loopback interno para propósitos de mantenimiento y un aumento en disponibilidad; La detección de bucle invertido protege contra el cableado incorrecto o configuraciones de red y puede habilitarse en una base por puerto o VLAN para mayor flexibilidad.
- Selección flexible del puerto. Proporciona una combinación de módulos de interfaz de fibra y cobre, soporte 100 / 1000BASE-X y detección automática de velocidad 10/100 / 1000BASE-T, más dúplex automático y MDI / MDI-X.

HP MSR3000

Los enrutadores MSR3000 utilizan las últimas CPUs multicore, ofrecen conmutación Gigabit, proporcionan un bus PCI mejorado y se suministran con la última versión del software HPE Comware para permitir un alto rendimiento con servicios concurrentes. La serie MSR3000 ofrece una plataforma de enrutamiento flexible y completa, incluyendo IPv6 y Multi-Protocols Label Switching (MPLS), con hasta 5 Mpps de capacidad de reenvío y 3.3 Gb / s de PSec VPN encriptada. Estos enrutadores también soportan módulos de HPE Open Application Platform (OAP) para ofrecer

aplicaciones HPE AllianceOne avanzadas, líderes en la industria, tales como virtualización, comunicaciones unificadas y colaboración (UC & C) y capacidades de optimización de aplicaciones.

La serie MSR3000 proporciona una infraestructura de red ágil y flexible que le permite adaptarse rápidamente a las necesidades cambiantes del negocio, al mismo tiempo que ofrece servicios simultáneos integrados en una plataforma única y fácil de gestionar.

Características:

- Hasta 5 Mpps que envían rendimiento; Soporte para múltiples servicios simultáneos
- HPE Open Application Platform (OAP) para aplicaciones HPE AllianceOne
- Funciones de seguridad incorporadas con encriptación basada en hardware, firewall con estado, traducción de direcciones de red (NAT) y redes privadas virtuales (VPN)
- No hay complejidad adicional de licencias; Sin costo para funciones avanzadas
- Solución Zero-touch, con gestión de un solo panel de vidrio

Funcionamiento:

- Excelente rendimiento de reenvio. Proporciona un rendimiento de desvío de hasta 5 Mpps (3.3 Gb / s); Cumple con las demandas de aplicación de ancho de banda de las empresas
- Potente capacidad de seguridad. La serie MSR3000 está disponible con cifrado estándar o alto, un acelerador de cifrado de hardware incorporado para mejorar el rendimiento del cifrado; El rendimiento del cifrado IPSec puede ser de hasta 3.3 Gb / s con un máximo de 4.000 túneles IPSec VPN

Arquitectura:

- Soporte de MSR OpenFlow 1.3.1

- Plataforma multiservicios ideal. Proporciona enrutador WAN, conmutador Ethernet, WAN 3G / 4G, firewall con estado, VPN y protocolo de inicio de sesión (SIP) o puerta de enlace de voz en MSR
- Arquitectura avanzada de hardware. Proporciona procesadores multinúcleo, Gigabit witching y bus PCIe; Se suministran fuentes RPS externas o fuentes de alimentación internas, y se ofrecen tarjetas CF internas y externas; Nuevos módulos MIM de alto rendimiento (HMIM) soportados.
- Nuevo sistema operativo. Se entrega con el nuevo sistema operativo Comware v7 que ofrece lo último en virtualización y enrutamiento.
- La arquitectura de la plataforma de aplicaciones. Proporciona una flexibilidad de aplicaciones y servicios sin igual, con el potencial de ofrecer la funcionalidad de múltiples dispositivos, creando ahorros de capital y de gastos operativos y una protección duradera de la inversión
- Mejora el ancho de banda de las ranuras de módulos de E / S de 100 Mb / s a 1000 Mb / sy mejora el rendimiento del enlace ascendente de 1 Gb / s a 10 Gb / s
- Multi Gigabit (MGF). Facilita la utilización del procesador principal mediante la transmisión de paquetes de capa 2 directamente a través del MGF.

Conectividad:

- Interconexión Virtual de Ethernet (EVI). EVI es una tecnología MAC-in-IP que proporciona conectividad de capa 2 entre sitios de red de capa 2 distantes a través de una red enrutada IP. Se utiliza para conectar sitios geográficamente dispersos de un centro de datos virtualizado a gran escala que requiere la adyacencia de la capa 2.

- VXLAN (Virtual eXtensible LAN). VXLAN (Virtual eXtensible LAN, red de área local virtual escalable) es una red basada en IP, utilizando el paquete "MAC in UDP" de la tecnología Layer VPN. VXLAN se puede basar en un ISP existente o las redes IP de la empresa para el sitio físico descentralizado proporciona la comunicación de capa 2, y puede proporcionar el aislamiento del servicio para los diferentes inquilinos.
- Servicio Virtual de LAN Privada (VPLS). Virtual Private LAN Service (VPLS) ofrece un servicio punto a multipunto L2VPN sobre un MPLS. O la espina dorsal de la IP. La columna vertebral es transparente para los sitios de los clientes, que pueden comunicarse entre sí como si estuvieran en la misma LAN. Los protocolos siguientes apoyan en MSRs, RFC 4447, RFC 4761, y RFC 4762, BFD detección en VPLS, Apoyo jerárquico HOPE (H-VPLS), dirección MAC recuperación en H-VPLS para acelerar la convergencia.
- Red de Movilidad (NEMO). La movilidad de red (NEMO) permite a un nodo conservar la misma dirección IP y mantener la aplicación. Conectividad cuando el nodo viaja a través de las redes. Permite el enrutamiento independiente de la ubicación de los datagramas IP en Internet
- Conectividad de puerto de alta densidad. Proporciona hasta 10 ranuras de módulo de interfaz y hasta tres puertos Gigabit Ethernet integrados, 8 ó 24 puertos GE soportados en un módulo HMIM
- Varias interfaces WAN. Proporciona enlaces tradicionales con E1, T1, Serial, ADSL sobre POTs, ADSL sobre ISDN, G.SHDSL, Asynchronous Transfer Mode (ATM).
- es ISDN; Acceso Ethernet de alta densidad con WAN Gigabit Ethernet y LAN de 4 y 9 puertos Fast / Giga Ethernet, PoE / PoE +; Acceso a la movilidad con módulos SIC 3G (WCDMA o HSPA) / 4G LTE, módems USB 3G / 4G y opciones de acceso OC3 de alta velocidad E3 / T3 y 155 Mb / s

- Protección de tormenta de paquetes. Protege contra tormentas de broadcast, multicast o unicast con umbrales definidos por el usuario
- Loopback. Soporta pruebas de loopback interno para propósitos de mantenimiento y un aumento en disponibilidad; La detección de bucle invertido protege contra el cableado incorrecto o las configuraciones de red y se puede habilitar en una base por puerto o por VLAN para una mayor flexibilidad
- Selección flexible del puerto. Proporciona una combinación de módulos de interfaz de fibra y cobre, soporte 100 / 1000BASE-X y detección automática de velocidad 10/100 / 1000BASE-T, además de dúplex automático y MDI / MDI-X

HP MSR4000

Los enrutadores MSR4000 ofrecen una plataforma de enrutamiento flexible con las últimas CPUs multinúcleo, ofrecen 10 Gigabits SFP + integrados, proporcionan un bus PCI mejorado y se suministran con la última versión del software HP Comware para permitir un alto rendimiento con servicios concurrentes. La serie MSR4000 ofrece una plataforma de enrutamiento flexible y completa, incluyendo IPv6 y conmutación de etiquetas multiprotocolo (MPLS), con una capacidad de reenvío de hasta 36 Mpps y un rendimiento encriptado de VPN de 28 Gb / s. Estos enrutadores también admiten módulos HP Open Application Platform (OAP) para ofrecer aplicaciones de socios HP AllianceOne líderes en la industria, como virtualización, comunicaciones unificadas y colaboración (UC & C), y capacidades de optimización de aplicaciones.

La serie MSR4000 ofrece una infraestructura de red ágil y flexible que le permite adaptarse rápidamente a sus necesidades empresariales cambiantes, al tiempo que ofrece servicios simultáneos integrados en una plataforma única y fácil de administrar.

Características:

- Hasta 36 Mpps que envían rendimiento; Soporte para múltiples servicios simultáneos
- Hasta 36 Mpps que envían rendimiento; Soporte para múltiples servicios simultáneos
- HP Open Application Platform (OAP) para aplicaciones HP AllianceOne
- Potente capacidad de agregación; 10GbE integrado; Soporte para hasta 64 E1 u ocho puertos E3 / T3
- Solución cero-táctil con gestión de un solo panel de vidrio:

Funcionamiento:

- Excelente rendimiento de reenvío. Proporciona un rendimiento de reenvío de hasta 36 Mpps (24,2 Gb / s); Cumple con las demandas de aplicación de ancho de banda de las empresas
- Potente capacidad de seguridad. La serie MSR4000 está disponible con cifrado estándar o alto, un acelerador de cifrado de hardware incorporado para mejorar el rendimiento del cifrado; El rendimiento del cifrado IPSec puede ser de hasta 28 Gb / s con un máximo de 10.000 túneles VPN IPSec

Arquitectura:

- Soporte de MSR OpenFlow 1.3.1
- Plataforma multiservicio ideal. Proporciona un enrutador WAN, conmutador Ethernet, firewall con estado, VPN y Protocolo de inicio de sesión (SIP) o gateway de voz todo en un dispositivo
- Arquitectura avanzada de hardware. Proporciona procesadores multinúcleo, conmutación Gigabit y bus PCIe; Dos unidades principales de procesamiento, cuatro fuentes de alimentación interna (configuración N + 1) y tarjetas CF internas

y externas; Nuevos módulos MIM de alto rendimiento (HMIM) soportados

- Nueva versión del sistema operativo. Se entrega con el nuevo sistema operativo Comware v7 que ofrece lo último en virtualización y enrutamiento
- Arquitectura distribuida con separación de datos y planos de control. Proporciona una tolerancia a fallos reducida y facilita el funcionamiento casi continuo y la interrupción del servicio sin necesidad de planear eventos planeados o no planificados; Las unidades de procesamiento de servicios (SPU) realizan el reenvío de datos, cifrado o descifrado y analizan o filtran los cajones de datos; Las unidades principales de procesamiento realizan el cálculo de rutas, avanzan el mantenimiento de las tablas y configuran y monitorean el SPU
- Conjunto de puertas programables en campo (FPGA). Mejora el ancho de banda de las ranuras de módulos de E / S de 100 Mb / s a 1000 Mb / sy mejora el rendimiento del enlace ascendente de 1 Gb / s a 10 Gb / s
- Unidad de procesamiento principal (MPU). Proporciona puerto de gestión 1GbE; Tiene por defecto 512 MB de flash interno y 2 GB de memoria DDR3
- Unidades de procesamiento de servicios (SPU). Incluye cuatro ranuras de 1000BASE-T y cuatro SFP (combinadas), dos ranuras de módulo de procesamiento de voz y memoria de 2 GB DDR3; SPU 200/300 también tiene una ranura SFP + de 10GbE; Rendimiento de retransmisión: 10 Mpps (SPU-100), 20 Mpps (SPU-200), 36 Mpps (SPU-300)

Conectividad:

- Potente capacidad de agregación. Soporta LAN 10GbE integrada y hasta 64 puertos E1 u ocho E3 / T3 y puertos de hasta 148 Giga en un chasis
- Conectividad de puerto de alta densidad. Proporciona hasta ocho ranuras para módulos de interfaz y hasta cuatro puertos Gigabit Ethernet a bordo y uno de 10 GbE
- Varias interfaces WAN. Proporciona enlaces tradicionales con E1, T1, Serial, Asynchronous Transfer Mode (ATM) e ISDN; Acceso Ethernet de alta densidad con WAN Fast Ethernet y Gigabit Ethernet con POE / POE +; Y E3 / T3 de alta velocidad, 155 Mb / s opciones de acceso OC3
- Protección contra tormentas de paquetes. Protege contra tormentas de broadcast, multicast o unicast con umbrales definidos por el usuario
- Interconexión Virtual de Ethernet (EVI). EVI es una tecnología MAC-in-IP que proporciona conectividad de capa 2 entre sitios de red de capa 2 distantes a través de una red enrutada IP. Se utiliza para conectar sitios geográficamente dispersos de un centro de datos virtualizado a gran escala que requiere una adyacencia de capa 2
- VXLAN (Virtual eXtensible LAN). VXLAN (Virtual eXtensible LAN, red de área local virtual escalable) es una red basada en IP, utilizando el paquete "MAC in UDP" de la tecnología Layer VPN. VXLAN se puede basar en un ISP existente o las redes IP de la empresa para el sitio físico descentralizado proporciona la comunicación de capa 2, y puede proporcionar el aislamiento del servicio para los diferentes inquilinos.
- Servicio Virtual Privado de Red (VPLS). El Servicio Virtual Privado de Red (VPLS) ofrece un servicio L2VPN de punto a multipunto a través de un backbone MPLS o IP. La columna vertebral es transparente para los sitios de los clientes, que pueden comunicarse entre sí como si estuvieran en la misma

LAN. Los siguientes protocolos son compatibles con MSRs, RFC4447, RFC4761 y RFC4762, detección BFD en VPLS, soporte HOPE H-VPLS), recuperación de direcciones MAC en H-VPLS para acelerar la convergencia

- Loopback. Soporta pruebas de loopback interno para propósitos de mantenimiento y un aumento en disponibilidad; La detección de bucle invertido protege contra el cableado incorrecto o las configuraciones de red y se puede habilitar en una base por puerto o por VLAN para una mayor flexibilidad
- Selección flexible del puerto. Proporciona una combinación de módulos de interfaz de fibra y cobre, soporte 100 / 1000BASE-X y detección automática de velocidad 10/100 / 1000BASE-T, además de dúplex automático y MDI / MDI-X

DECLARACIÓN Y AUTORIZACIÓN

Yo, Ochoa Brito María Jesús, con C.C: # 092160904-6 autora del trabajo de titulación: Característica de las Redes Definidas por Software (SDN) para implementación en el Ecuador previo a la obtención del título de Magíster en Telecomunicaciones en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 22 de enero de 2018

f. _____

Nombre: Ochoa Brito María Jesús

C.C: 092160904-6

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Característica de las Redes Definidas por Software (SDN) para implementación en el Ecuador		
AUTOR(ES)	María Jesús Ochoa Brito		
REVISOR(ES)/TUTOR(ES)	MSc. Orlando Philco Asqui, MSc. CelsoBohorquez Escobar / Msc. Lidice Romero Amundaray		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Sistema dePosgrado		
CARRERA:	Maestría en Telecomunicaciones		
TITULO OBTENIDO:	Magíster en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	22 de enero de 2018	**No. DE PÁGINAS:**	143
ÁREAS TEMÁTICAS:	OpenFlow, OpenStack, NETCOF, Migración, Centro de datos		
PALABRAS CLAVES/ KEYWORDS:	SDN, OpenFlow, OpenStack, NETCOF, Migración, Centro de datos.		

RESUMEN/ABSTRACT (150-250 palabras): Las redes definidas por software (SDN, por sus siglas en inglés), nacen por la necesidad de contar con una mejor administración, distribución, flexibilidad y sobre todo para tener una mejor administración del ancho de banda. La estrategia de migración para un centro de datos hacia SDN, ayuda a crear una nueva arquitectura que aumentara las posibilidades de crecimiento de la red, sin verse afectados los servicios durante el proceso. En este trabajo se presentan varias estrategias tomando en cuenta el punto de partida de la red, se describen dos ejemplos de migraciones exitosas. Para tomar la decisión de migrar un centro de datos, se deben analizar lo más conveniente, dependiendo del tráfico que maneje este, y así realizarlo ya sea de forma directa o en fases. Esta nueva tecnología, ayuda con la simplificación de los procesos y rapidez al brindar una respuesta de solicitudes, que antes podían demorar más de lo debido. La tesis tiene enfoque cuantitativo, cuyo alcance de la investigación es descriptivo y explicativo. Es descriptivo, porque se revisará información de relevancia de las redes definidas por software (SDN) y es explicativo, porque se pretende caracterizar las SDNs para futuras implementaciones en el Ecuador. Se espera despertar un gran interés en su funcionamiento al igual que en las aplicaciones que se utilizan, lo que conlleve a su implementación en los diferentes centros de datos del país.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono**: +593-4-2898576	E-mail: maryochoa@outlook.com
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	Nombre: Manuel Romero Paz, MSc.	
	Teléfono: +593-994606932	
	E-mail: manuel.romero@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	

Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	