UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE INGENIERÍA

PROGRAMA ACADÉMICO DE INGENIERÍA DE REDES Y COMUNICACIONES

Diseño de la capa de control de una red lan basada en sdn para las redes de campus utilizando las buenas practicas de opendaylight

TESIS

Para optar el título profesional de Ingeniero de Redes y Comunicaciones

AUTOR

Quispe Poma, Jhonatan Jose (0000-0002-5886-3832)

ASESOR:

Gonzales Figueroa, Renatto Gustavo (0000-0003-3658-3415)

Lima, 03 de Mayo de 2021

DEDICATORIA

A mis padres y a mi hermana por su apoyo incondicional en todo momento, a mi tía querida que descansa en paz en el cielo y a mi familia en general por ser mi soporte para llevar a cabo mi carrera con éxito

RESUMEN

El presente trabajo de tesis tiene como finalidad, explicar cómo las redes definidas por software se convierten en un elemento clave de una estrategia de diferenciación para las redes de campus. Mediante la priorización del consumo de tráfico de datos y la administración de la red LAN a través de un controlador SDN que permita distribuir adecuadamente el ancho de banda, reducir el tiempo de comunicación entre los dispositivos de red y gestionar la red adecuadamente en la organización.

En el primer capítulo, se presentará los aspectos introductorios del proyecto. En esta parte, se describirá la organización objetivo y su campo de acción, la problemática a la cual está expuesta la organización. Además, se planteará el objetivo general y los objetivos específicos del proyecto y también, la justificación, los indicadores de logro. así como el estado del arte que comprende la solución propuesta.

En el segundo capítulo, se detallará las tecnologías asociadas a las redes definidas por software y toda información sujeta a este tema de investigación. A partir de los cuales, se identificarán el contexto, la muestra, el diseño principal y los procedimientos a realizar. Asimismo, se analizarán normas, estándares, políticas y buenas prácticas usadas para el tema de investigación.

En el tercer capítulo, se plantea el problema identificado en la organización objetivo. Analizando su alcance, causa e impacto en la organización. De igual manera, se describirá en detalle, el entorno donde será desplegada la solución y los requerimientos necesarios para cumplir con el tema propuesto.

En el cuarto capítulo, la propuesta del diseño de red definida por software será desarrollada, en donde se elaborarán las especificaciones y seleccionarán los recursos que logren cumplir el diseño de la solución.

Finalmente, en el quinto capítulo se realizará la evaluación mediante pruebas y resultados que serán debidamente justificados para el logro del proyecto de tesis.

Palabras clave: Redes de Campus; LAN; Tráfico de Datos; Software

ABSTRACT

The purpose of this tesis is to explain how software-defined networks become a key element of a differentiation strategy for campus networks. By prioritizing the consumption of data traffic and managing the LAN network through an SDN controller that allows to properly distribute the bandwidth, reduce the communication time between network devices and manage the network properly in the organization.

In the first chapter, the introductory aspects of the project will be presented. In this part, the target organization and its field of action will be described, the problem to which the organization is exposed. In addition, the general objective and the specific objectives of the project will be raised, as well as the justification, the achievement indicators. as well as the state of the art that comprises the proposed solution.

In the second chapter, the technologies associated with software-defined networks and all information subject to this research topic will be detailed. From which, the context, the sample, the main design and the procedures to be carried out will be identified. Likewise, norms, standards, policies and good practices used for the research topic will be analyzed.

In the third chapter, the problem identified in the target organization is posed. Analyzing its scope, cause and impact on the organization. Likewise, the environment where the solution will be deployed and the necessary requirements to comply with the proposed topic will be described in detail.

In the fourth chapter, the software-defined network design proposal will be developed, where the specifications will be elaborated and the resources that manage to fulfill the solution design will be selected.

Finally, in the fifth chapter, the evaluation will be carried out through tests and results that will be duly justified for the achievement of the tesis.

Keywords: Campus Networks; LAN; Data Traffic; Software

TABLA DE CONTENIDOS

INDICE DE TABLAS

INDICE DE FIGURAS

1. CAPITULO 1

En este capítulo, se presentará los aspectos introductorios del proyecto. De igual manera, se describirá la organización objetivo y su campo de acción, la problemática a la cual está expuesta la organización. Además, se planteará el objetivo general y los objetivos específicos del proyecto y también, la justificación, los indicadores de logro. así como el estado del arte que comprende la solución propuesta.

1.1. Introducción

En la actualidad, el modelo distribuido que siguen las redes se basa en diferentes protocolos, tanto a nivel de enlace como a nivel de red, necesarios para el correcto funcionamiento de la red de una organización. Este modelo es único y aplica para todos los tipos de redes, lo que en cierta medida demuestra la escalabilidad y elasticidad dentro de su entorno. Sin embargo, la aparición de tecnologías emergentes como la virtualización, internet de las cosas, el aumento del tráfico de la red y el incremento en la densidad de los dispositivos pone en la mira la operación de las redes distribuidas y convencionales en ciertos entornos. Además, los inconvenientes de las redes actuales es que no son flexibles, tampoco pueden mantener operativa una red con tantos protocolos de control que implica un costo elevado en su funcionamiento y mucho tráfico destinado a esa tarea, ya que cada dispositivo envía a intervalos regulares mensajes de difusión por cada protocolo de control que está operando. Incluso, los fabricantes de dispositivos de comunicación emplean tecnología y características propietarias para el plano de control, el cual genera una mayor dificultad en el despliegue y operación de diferentes entornos.

Por ello, están surgiendo nuevas arquitecturas de redes con propuestas capaces de soportar servicios emergentes, siendo necesario su evaluación y validación en entornos de pruebas para su posterior implementación en una organización. Es decir, deben buscarse maneras de conseguir una red controlada y capaz de responder a los problemas propios de las redes y sin un consumo de recursos tan elevado, propio de los protocolos de control tradicionales. “La tecnología SDN ofrece una solución a este problema, en las redes SDN existe un único protocolo del plano de control llamado Openflow, quien es responsable de comunicar el controlador con los dispositivos de red y dar indicaciones sobre cómo tratar el tráfico” (ONF – Open Networking Foundation) . En otras palabras, en las redes definidas por software el controlador es el único elemento de la red que conoce la topología completa y es el encargado

de gestionarla. En caso, se produzca un cambio inesperado en la red o algún fallo de un dispositivo de red, el controlador es consciente de ese cambio y puede aprovisionar nuevos flujos en tiempo real para que los dispositivos de red encaminen el tráfico sin producir pérdidas de caída de servicio o rendimiento. El controlador también es responsable de tareas avanzadas, como las políticas de seguridad, balanceo de tráfico y la calidad de servicio. De esta forma, se elimina el exceso de carga en el plano de control, liberando el ancho de banda y reduciendo los costos asociados a estos.

"La capacidad de programar la red es la característica fundamental de las redes definidas por software, aún sabiendo los diferentes aspectos en donde las SDN resuelven problemas de redes convencionales. Es necesario indicar que las capacidades de las SDN son en materia de habilidad de ser gestionada o monitorizada por aplicaciones externas totalmente independiente del controlador. Siendo de código abierto, los controladores SDN dependen de la contribución voluntaria de los usuarios para seguir incorporando mejoras e ir solucionando errores. Reciben apoyo de grandes fundaciones como ONOS y OpenDayLight, por lo que mantienen una elevada actividad y documentación actualizada. Las organizaciones observan a las redes definidas por software como una posibilidad sobre la arquitectura que otorga en cuanto a redes ágiles escalables y capacidad para soportar la nueva demanda de los usuarios finales" (ONF – Open Networking Foundation). Entre otros factores que determinan la tendencia de las SDN en las organizaciones, se tiene el siguiente:

SDN para redes de campus: La evolución de las SDN partió en un inicio para Centros de Datos, siguiendo para los proveedores de servicio de internet (ISP). Gracias a la acogida que propone las redes definidas por software, ahora se enfocan en las redes de campus (siendo complejas, continuamente escalable, entre otros).

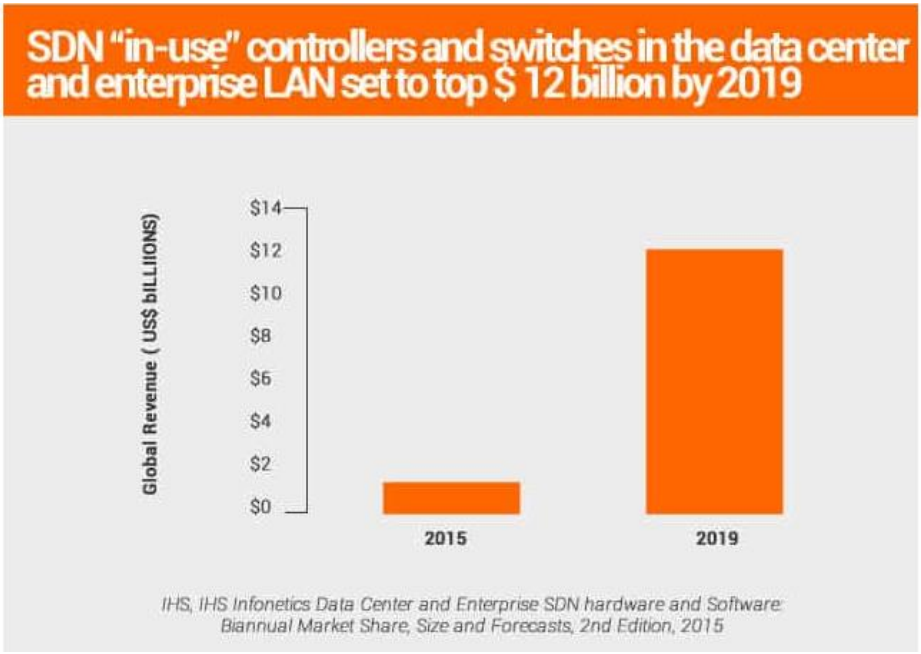


Figura 1.- Previsión para el mercado de tecnología SDN para redes de campus y centro de datos

Fuente: itsitio.com/ar/como-evoluciona-sdn-ihs

En otras palabras, "el impacto de las redes definidas por software sobre el mercado de dispositivos de red como switches Ethernet se incrementó de manera significativa en el año 2015, entonces los despliegues de SDN para empresas y centros de datos comenzaron a despegar a través del mercado de controladores y switches Ethernet SDN. Para el año 2019 ya se cuenta con una importante adquisición de esta tecnología, por lo que está claro que hacia el 2020, los campus y centros de datos lucirán significativamente diferentes en comparación de hoy" (Alan Weckel, Dell Oro Group).

1.2. Organización Objetivo

Las instituciones universitarias para este proyecto, son aquellas que tienen varias relaciones en común, es decir, son universidades en crecimiento, cuentan entre 5,000 a 10,000 estudiantes aproximadamente en todas sus modalidades de estudio (carreras universitarias, programas de postgrado, centro cultural, programas de extensión internacional, entre otros). Estas universidades tienen sus lugares en los distritos de Lima denominados campus únicos, porque toda su infraestructura es manejada dentro de ella y sin sucursales externas. Si hablamos de

infraestructura, nos referimos a que se administran y operan en base a una red jerárquica y no tienen definido una plataforma con suficiente capacidad de respuesta ante inconvenientes.

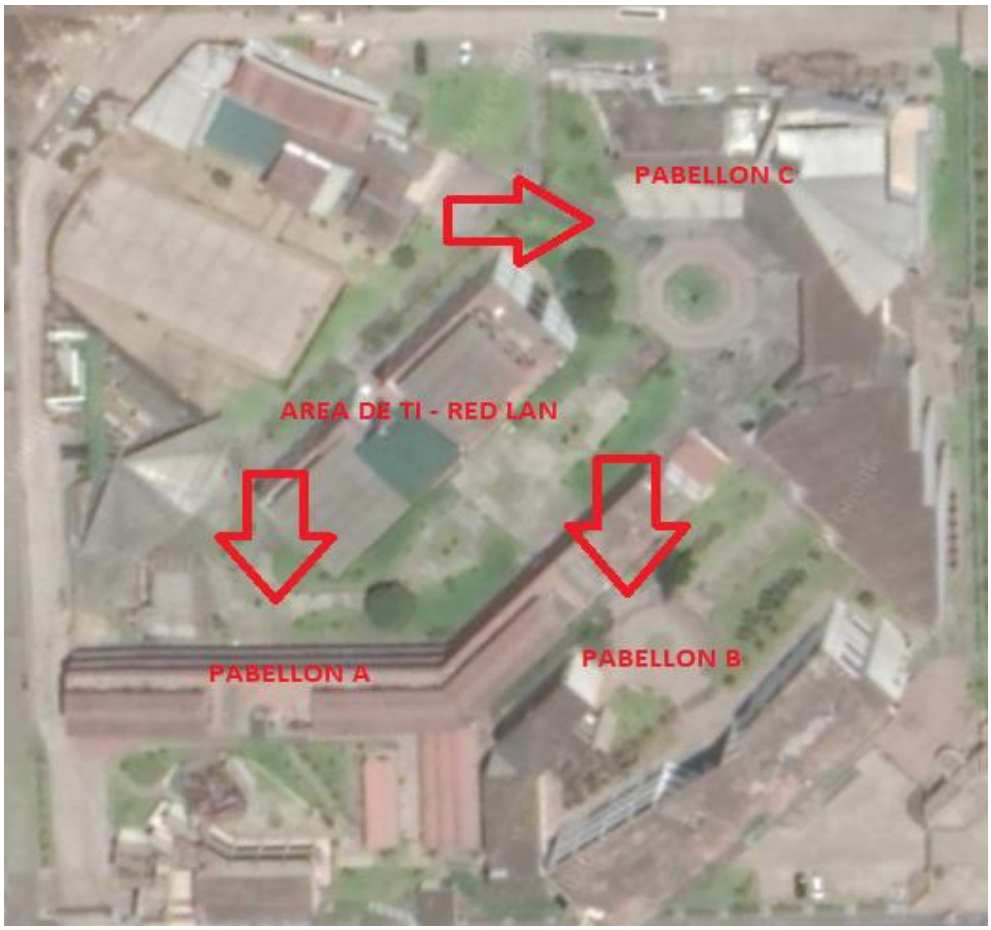


Figura 2.- Vista general de un campus universitario vía Google Earth

Fuente: Google Earth

Observando la Figura 2, tenemos el ejemplo de un campus universitario, la cual cuenta con pabellones distribuidos y enlazados al área de TI (en otras palabras, es el lugar en donde se administra la red y se alojan los servicios de video, telefonía, dispositivos de red, servidores, entre otros). En el pabellón A por ejemplo pueden encontrarse personal administrativo encargados de diversas áreas como: contabilidad, tesorería, administración y algunas autoridades del entorno universitario. En el pabellón B, se pueden distinguir las aulas de clases, laboratorios de diferentes rubros, zona deportiva y servicios generales. De igual manera, en el pabellón C, podemos encontrar algunas aulas de dictado de clase, teatro, sala de espera, entre otros. En otras palabras, todo el manejo educativo y tecnológico se brinda en un mismo lugar y con un diseño de red local.

En términos de misión y visión, estas instituciones universitarias apuestan en ser organizaciones de educación superior líderes en su rubro, formando profesionales y emprendedores para el desarrollo de la comunidad y crear un impacto positivo en el Perú. A futuro lograr ser reconocidas como universidades que participan en el derecho al acceso de educación de manera innovadora, competitiva y comprometida con el bienestar social.

Como objetivo estratégico, se considera transformar el concepto de educación basado en respeto, mejora continua, solidaridad, conocimiento, responsabilidad social asociado con las personas y la tecnología.

1.2.1. Campo de Acción

El presente proyecto tendrá como objeto de estudio la red de campus y sus servicios. Específicamente, el campo de acción es el área de TI dentro del campus universitario y en donde se encuentran alojados los dispositivos de red, equipos de telefonía, servidores, equipos terminales, entre otros.

La red de campus en mención, representan el punto central de las conexiones que se realizan desde los distintos pabellones ubicados alrededor de los campus, realizando peticiones de autenticación, intranet, acceso a laboratorios, material multimedia, servidores de archivo; es decir, prácticamente todos los servicios que ofrecen estas universidades son manejados en una infraestructura de red localizada dentro del campus.

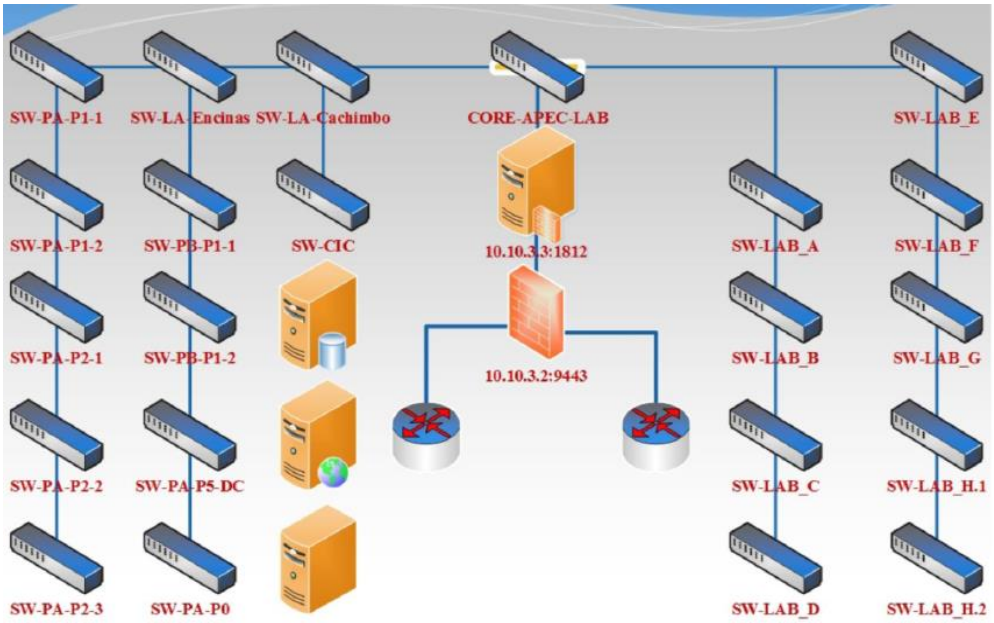


Figura 3.- Diseño de red tradicional como ejemplo de un campus universitario.
Fuente: Elaboración propia

En la Figura 3, se observan a los conmutadores Core-APEC y SW-PA/SW-LAB, que hacen referencia a la capa de núcleo y acceso en una red, respectivamente. Adicional a ello, se cuenta con servidores (web, archivos, almacenamiento) y a su vez, un firewall con dos ruteadores como salida a la WAN. Todo esto complementa la red LAN en el ejemplo del campus universitario.

1.3. Identificación del Problema

1.3.1. Situación Problemática

Las instituciones universitarias en mención, son conscientes que las redes de datos crecen y para satisfacer las necesidades de nuevos dispositivos con diferentes opciones de rendimiento y servicios, se debe escalar. Se mencionan las siguientes situaciones:

- La diversidad de los dispositivos de comunicación en la red local se debe a características adicionales que provee cada fabricante, ya que pueden ser de utilidad en diferentes circunstancias. Esto trae consigo, que todos los dispositivos de red no interactúen correctamente debido a incompatibilidad entre cada fabricante que propone su propia tecnología o trabajan con un estándar que es diferente o que es único en su uso. Por esta razón, si se presenta un fallo o bug en los dispositivos de comunicación

estos deben esperar hasta que el propio fabricante coloque a disposición un parche o reléase del sistema operativo donde está el inconveniente.

- Los dispositivos como ruteadores o conmutadores de las redes LAN al estar compuestos por hardware (puertos de red, procesadores, memoria flash) y software (sistema operativo). Cada uno con funciones como reenvío de paquetes y procesar rutas en hardware, y el sistema operativo que permite administrar la memoria del equipo en software. Hacen al momento de realizar un cambio en la configuración del equipo, se debe usar su interfaz de configuración y el inconveniente radica al existir varios enrutadores en la red porque esta tarea requiere de tiempo por el número de equipos, y una planificación adecuada para no introducir errores de configuración. Las universidades en sus redes de campus requieren asistir en la configuración de varios nodos y de manera simultánea, no logrando hacerlo posible por la problemática mencionada.
- Otra situación es el aumento del número de alumnos, esto trae consigo un elevado consumo de tráfico debido a las aplicaciones propias de las entidades universitarias como videoconferencia, clases virtuales, uso de app, entre otros. La red cada vez queda limitada porque no es capaz de soportar requerimientos de ancho de banda que utilizan las aplicaciones, es decir, no existe aprovisionamiento de la red.

Por lo mencionado, se puede determinar que estas problemáticas pueden resultar críticas si es que no se manejan adecuadamente en cada institución universitaria, con el constante aumento de estudiantes en cada una de ellas esto puede resultar en una mala imagen a nivel educativo e institucional.

1.3.2. Problema a Resolver

El problema a resolver es la dificultad en la distribución del tráfico de datos en la red de campus de una universidad

1.4 Objetivo General y Objetivos Específicos

1.4.1. Objetivo General

Diseñar la capa de control de una red LAN basada en SDN para la red de campus de una universidad que permita distribuir adecuadamente el tráfico de datos utilizando las buenas prácticas de OpenDayLight.

1.4.2. Objetivos Específicos

- Distribuir el consumo de ancho de banda por tipo de usuario en la red LAN bajo el enfoque de OpenDayLight
- Reducir el tiempo de comunicación entre los conmutadores de core/distribución para generar tablas de flujo del tráfico de la red LAN basado en el módulo L2-Switch de OpenDayLight
- Proponer una red LAN escalable en cuanto a equipamiento tecnológico y logre soportar el crecimiento de usuarios

1.4.5. Indicadores de Logro de los Objetivos

Objetivo Específico	Indicador de Logro	Métrica
OE1: Distribuir el consumo de ancho de banda por tipo de usuario en la red LAN del campus universitario	Distribución adecuada del ancho de banda sobre los tipos de usuarios de la red LAN.	Ancho de banda (Mbps) Tráfico (TCP/UDP) Milisegundos
OE2: Reducir el tiempo de comunicación entre los conmutadores de core/acceso para generar tablas de flujo del tráfico de la red LAN basado en el módulo L2-Switch de OpenDayLight	Creación de una red SDN que incluye conmutadores de core/acceso y terminales obteniendo su tiempo de ejecución. Posterior a ello, se establecen las tablas de flujo de la red LAN	Número de secuencias Duración (segundos) Cantidad de puertos Cantidad de paquetes
OE3: Proponer una red LAN escalable en cuanto a equipamiento tecnológico y pueda soportar el crecimiento de usuarios	Diseño de la topología de red Dispositivos de red y otros recursos de hardware/software que conformen la red LAN	Cantidad de dispositivos de red Esquema lógico de la red

1.5. Justificación

- El presente proyecto, busca reducir las quejas de los usuarios en el uso de los servicios como la lentitud o errores de conexión a través de videoconferencias, llamada de voz, entre otros. Ofreciendo una correcta designación de ancho de banda por el área de trabajo con mayor carga laboral.

- La propuesta busca corregir la distribución del tráfico de datos utilizando menos hardware o dispositivos de red físicos y añadiendo nuevas funcionalidades a través de software propia de la plataforma SDN. Esto permitirá un manejo eficiente en las configuraciones y un uso correcto sin interrupciones en las redes de campus.

- Al tratarse de una solución basada en software, se podrá provisionar todas las aplicaciones que se desee otorgar a los usuarios finales. Por lo tanto, al presentarse como una plataforma centralizada la red SDN tendrá la capacidad de efectuar solicitudes o cambios de manera automática sobre el tráfico de red, para evitar interrupciones en el funcionamiento de las aplicaciones.

- El presente proyecto ofrece una solución con tendencia a crecer ampliamente. La organización se beneficiará con las ventajas de esta tecnología como el ahorro de costos en la obtención de recursos de red.

- Al tratarse de un diseño SDN sobre la red LAN de la organización, esta reutilizará los dispositivos de red y solo se aplicarán algunos ajustes de actualización para su funcionamiento en la nueva red.

1.6 Estado del Arte

Las redes definidas por software (SDN), son una forma de administrar redes basadas en una arquitectura dinámica, manejable, adaptable y de costo eficiente. Siendo ideal para las altas demandas de ancho de banda y la naturaleza dinámica de las aplicaciones actuales. Esta arquitectura desacopla el control de la red y la funcionalidad de reenvío de información permitiendo que el control de la red pueda ser completamente programable

logrando que la infraestructura de red subyacente sea abstraída por las aplicaciones y servicios de red.

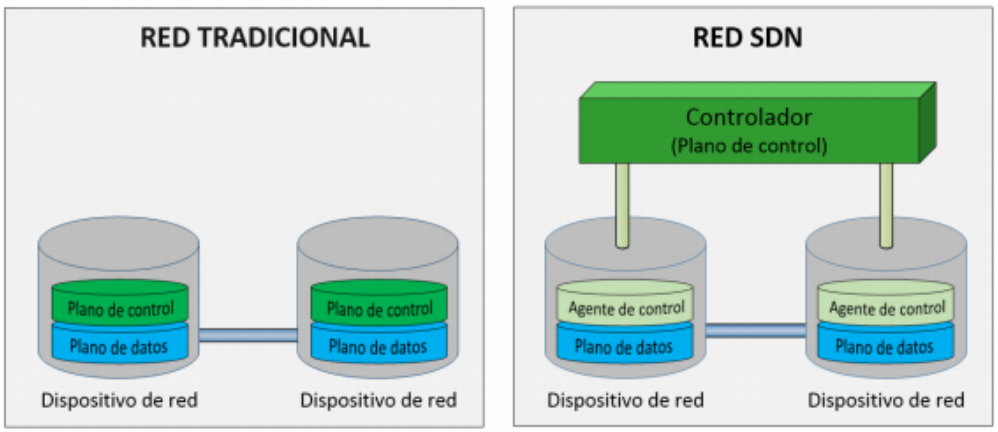


Figura 4.- Red Tradicional vs Red SDN

Fuente: Redes definidas por software, Raúl Álvarez Pinilla (Politécnica de Madrid)

Existen elementos que intervienen en las redes definidas por software, en este contexto existen muchos proveedores, en donde ofrecen sus propias arquitecturas de red. Sin embargo, todas estos proveedores o fabricantes tienen siempre alguna versión de un controlador SDN o API.

- Controlador SDN: Es el gestor de la red en donde ofrece una vista centralizada de dicha red en general y permiten a los administradores o encargados del manejo de la red, ejecutar o emitir órdenes a los conmutadores y enrutadores en el plano de reenvío.

- API hacia el sur: Esta interface se usa para transmitir información a los conmutadores y enrutadores. OpenFlow ha sido considerado el primer estándar SDN, era el API original en dirección sur y sigue siendo uno de los protocolos comunes.

- API hacia el norte: Esta interface se usa para que pueda comunicarse con las aplicaciones del negocio. Permite a los gestores de red configurar el tráfico y determinar servicios de manera programable.

1.6.1 Antecedentes

En un escenario de una red tradicional, la mayor parte de las funciones establecidas a esta red son aplicadas en un dispositivo dedicado (como router o switch), a partir de esto se puede señalar que una red tradicional de datos en gran parte se centra en hardware. Ciertas características elementales que adopta este enfoque para desarrollar equipos de red son:

- Los dispositivos de red pertenecen a un propietario (fabricante).
- La configuración de cada dispositivo que se encuentra dentro de la red es aplicada de manera individual.
- Las funciones como el aprovisionamiento, los cambios establecidos en la infraestructura de red y otros, se encuentran expuestos a errores.

Entonces, con el surgimiento de la internet por los años 90, la demanda de las redes de datos creció exponencialmente superando cualquier expectativa de desarrollo y evolución, provocando que ciertas aplicaciones que se consideraban antiguas de alguna manera fueran sustituidas por otras que se plantearon como novedosas a partir de las necesidades de los usuarios, como el correo electrónico y la transferencia de archivos. Esto obligó a investigadores de la industria a diseñar y experimentar propuestas basadas en despliegue de nuevos protocolos de red. Tomando en cuenta que las redes de aquel entonces no tenían la posibilidad de ser manejadas por medio de la programación, surgieron las redes activas permitiendo inyectar una programación en los nodos intermedios de los recursos de red disponibles. Sin embargo, esto hacia una operación de complejidad alta en la gestión de los equipos.

Para el siglo XVI, el incremento del volumen de tráfico de las redes ya era preocupante. Además, el contar con infraestructuras de redes más fiables, cada vez se reflejaban con mayor exigencia. Este hecho, hizo que los investigadores determinen enfoques más viables para la administración de las redes, con la idea de separar los planos de control y datos teniendo como resultado que los fabricantes de dispositivos de red, apliquen a sus equipos la posibilidad de aplicar la lógica de reenvío de paquetes directamente en el hardware sin contar con la ayuda del software propietario.

Para todos estos escenarios limitantes, SDN se presenta como una solución que está dispuesta a romper el modelo común que han manejado las redes desde su concepción

con la separación de los planos de control y datos de los dispositivos de red (donde no es necesario que estos se encuentren en el chasis).

El concepto de redes definidas por software surgió a través de un grupo de investigadores de la Universidad de Standford, siendo ellos los que crearon y que es hoy en la actualidad, el protocolo Openflow (establecido por la ONF). La Open Network Foundation fundada en el año 2011 por Scott Shenker y Nick McKeown, es una organización que buscaba fomentar el protocolo OpenFlow, la creación de estándares y la implantación de SDN más allá de entornos universitarios.

Algunas investigaciones que nacieron en las redes definidas por software a lo largo de los años, tenemos a las siguientes: Active Networks, Open Signaling, DCAN, Netconf, Ethane y OpenFlow.

1.6.2 Ventajas y Desventajas

Las redes definidas por software (SDN) ofrecen una red centralizada y programable que puede proporcionar de forma dinámica para abordar las necesidades cambiantes de las empresas. También ofrece las siguientes ventajas:

- **Directamente programable:** La política de SDN en la red es programable porque las funciones de control están desacopladas de las funciones de reenvío lo que permite que la red se configure mediante programación.

- **Administración centralizada:** La inteligencia de la red esta lógicamente centralizada en un controlador SDN que mantiene una vista general de la red. Aparece en las aplicaciones y en las políticas de red SDN como un único conmutador lógico.

- **Reduce Capex:** Las redes definidas por software limitan la necesidad de comprar hardware de red basado en ASIC (Circuito integrado de aplicación específica), entre otros componentes.

- **Reduce Opex:** Las SDN permiten el control algorítmico de la red de elementos o dispositivos como enrutadores o conmutadores. Al ser programable otorga la

capacidad de automatizar el aprovisionamiento de las redes y reduce significativamente el tiempo de administración y posibilidad de algún error humano.

- **Flexibilidad:** Las SDN ayudan a las organizaciones a implementar rápidamente nuevas aplicaciones, servicios e infraestructura para cumplir con sus necesidades.

- **Innovación:** De igual manera, las redes definidas por software permiten a las organizaciones crear nuevas aplicaciones, servicios, modelos que pueden ofrecer más valor a la red establecida.

Por otro lado, las SDN también ofrecen ciertas desventajas en cuanto a su desarrollo ya que está en constante evolución. Sin embargo, se mencionan algunas de consideración.

- La falta de confiabilidad y rendimiento comprobado para distintos entornos hacen a las SDN, una tecnología que no encuentra su grado de madurez pero sigue en constante crecimiento.

- Si bien en un inicio no era interoperable, hoy en día se sigue desarrollando un controlador SDN que permita una completa interoperabilidad de los elementos que conforman la red de una organización.

- Cuenta con una arquitectura específica, lenguaje de programación, proyectos de código abierto, entre otros ítems necesarios para el funcionamiento del controlador SDN. Sin embargo, aún posee ciertas deficiencias a nivel de seguridad para sus proyectos desarrollados.

Todas estas desventajas colocan a las redes definidas por software como una tecnología en constante desarrollo y que estarán reduciéndose conforme su desarrollo madure. De todas maneras, las SDN son una opción viable que resuelve las problemáticas actuales de las redes tradicionales.

1.6.3 Fabricantes, Desarrolladores y Vendedores

Las redes definidas por software han suscitado un gran interés en la industria de las redes de computadoras. Ya sea como una amenaza o como una oportunidad, prácticamente todas las empresas fabricantes de equipos, las creadoras de software, empresas de solución de virtualización, computación en la nube, entre otros. Han desarrollado sus propias soluciones basadas en SDN.

Son los fabricantes de equipos los que más han reaccionado al auge de las SDN. En principio, son empresas que tienen por perder ya que las redes podrían pasar de equipos costosos con firmware propietario a equipos genéricos, que simplemente conmutarán señales, interpretarán mensajes OpenFlow y gestionarán sus tablas de flujo. Sin embargo, la reacción de los fabricantes no es homogénea, prácticamente todas emplean el protocolo OpenFlow y algunas de ellas la sitúan como una solución propietaria.

A continuación, se analizarán las principales soluciones propuestas por diversas compañías relevantes.

- **Lumina Networks Inc.**

  El controlador SDN es una versión de calidad garantizada del controlador OpenDaylight líder en la industria con licencia para redes de producción. En combinación con Lumina NetDev Services, los proveedores pueden implementar redes definidas por software en su propia línea de tiempo utilizando enfoques de desarrollo Agile. Lumina ofrece interoperabilidad de múltiples proveedores basada en un plano de control común y contribuye a la comunidad de código abierto para garantizar una compatibilidad del 100% con la base de código de OpenDaylight.

  A continuación, se detalla la arquitectura SDN del controlador Lumina Networks en el cual adopta una serie de medidas propias del fabricante, pero conservando la arquitectura original de las redes definidas por software. (Ver Figura 5)

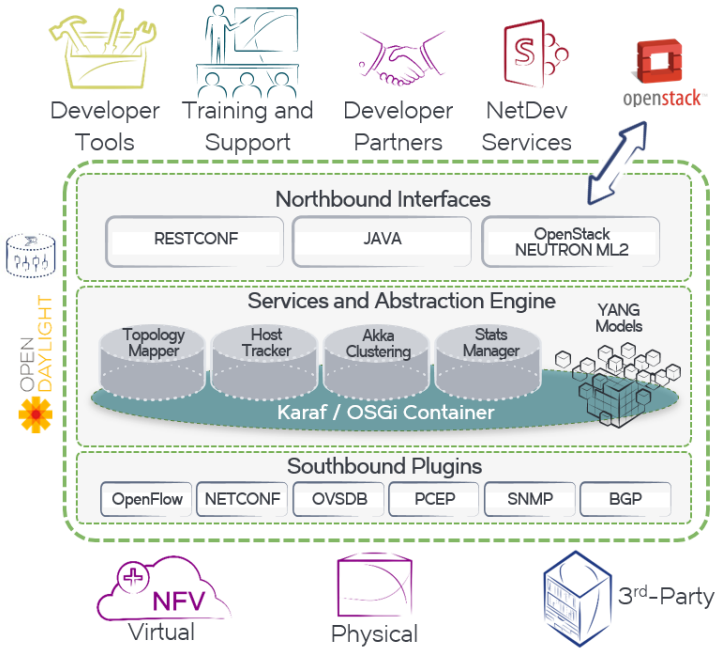


Figura 5.- Arquitectura SDN de Controlador Lumina Networks

Fuente: luminanetworks.com/products

Podemos indicar que Lumina junto con OpenDayLight propone una serie de compatibilidad con protocolos OpenFlow, NetConf, BGP y OVSDB, los cuales trabajan en función de tráfico de datos en su API hacia el sur. Esta solución esta enfocada para centro de datos, redes domésticas y otros entornos donde el objetivo sea la automatización/balanceo de carga para un mejor manejo de la red.

- **Big Switch Networks**

  A través de su controlador Big Cloud Fabric, este fabricante ofrece diseñar una arquitectura redundante de conmutadores lógicos que consta de cientos de conmutadores. Su panel único de administración de vidrio ofrece flujos de trabajo de red basados en intención para simplificar y acelerar las operaciones de TI. Brinda operaciones para la automatización de red y visibilidad global para entornos virtualizados. Big Switch está orientado para centros de datos/redes domesticas donde es importante el monitoreo de la red y su evolución.

- **B4N de Brain4Net**

  Este fabricante ofrece una plataforma de servicio completa de software para la infraestructura de red de varios proveedores. El controlador B4N es el componente principal de la plataforma de servicios B4N que proporciona un punto de control unificado de la red compatible con SDN y simplifica la administración y el aprovisionamiento de la red. Brain4Net se destaca como un proveedor genuino de software SDN/NFV con un amplio ecosistema de socios tecnológicos. Enfocado principalmente para infraestructuras de redes con virtualización y gestión del mismo.

- **CPLANE Networks**

  Este fabricante integra recursos en la nube y redes virtuales para nubes altamente distribuidas, en una única plataforma integrada. Las API abiertas hacia el norte brindan una integración de servicio en la nube consolidada para aplicaciones de SDN, NFV e IoT. A continuación, se observa la metodología propuesta de CPlane.

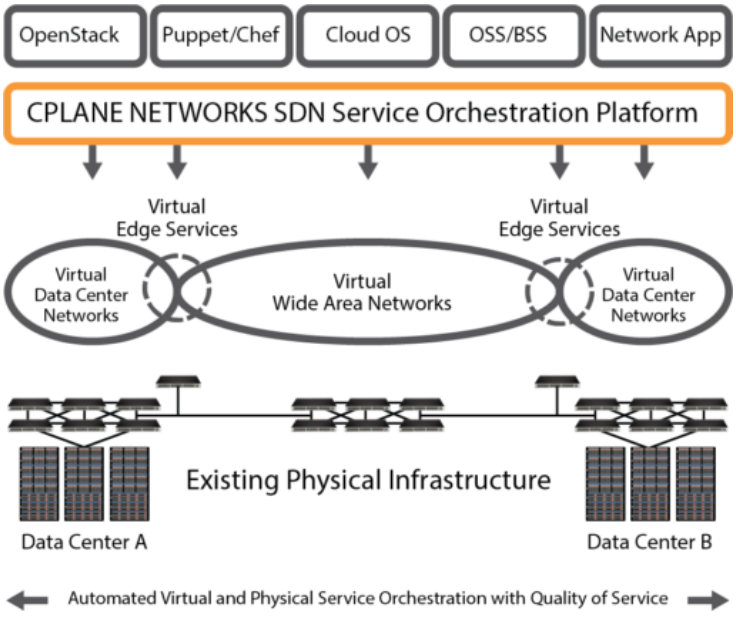


Figura 6.- Arquitectura SDN de CPLANE Networks

Fuente: www.cplanenetworks.com/resourcecenter/

CPlane como una solución de software permite automatizar y administrar la plataforma de nubes distribuidas, y con redes integradas definidas por software bajo una infraestructura de red existente, tal como se observa en la Figura 6.

- **Juniper Networks**

  Mediante su solución Juniper Networks Contrail, este fabricante ofrece una solución de software abierta y basada en estándares que ofrece virtualización de red y automatización de servicios para la nube. Esta solución también maneja su propia arquitectura basada en código abierto y APIs de alto nivel. Ofrece soluciones aparte de Contrail como: NorthStar, Estela, Insight, Junos Space. Sin embargo, la mayoría de estas soluciones son enfocadas hacia centros de datos masivos, operadores con gran carga de tráfico de datos por lo que es una solución completa a nivel WAN.

- **Cisco Open SDN Controller**

  A través de este controlador, la compañía Cisco ofrece una solución de código abierto, construido en una plataforma altamente escalable con OpenDaylight, aplicación de APIs y protocolos como BGP, Netconf, BGP-LS, PCEP y OpenFlow. Como se muestra en la siguiente imagen:

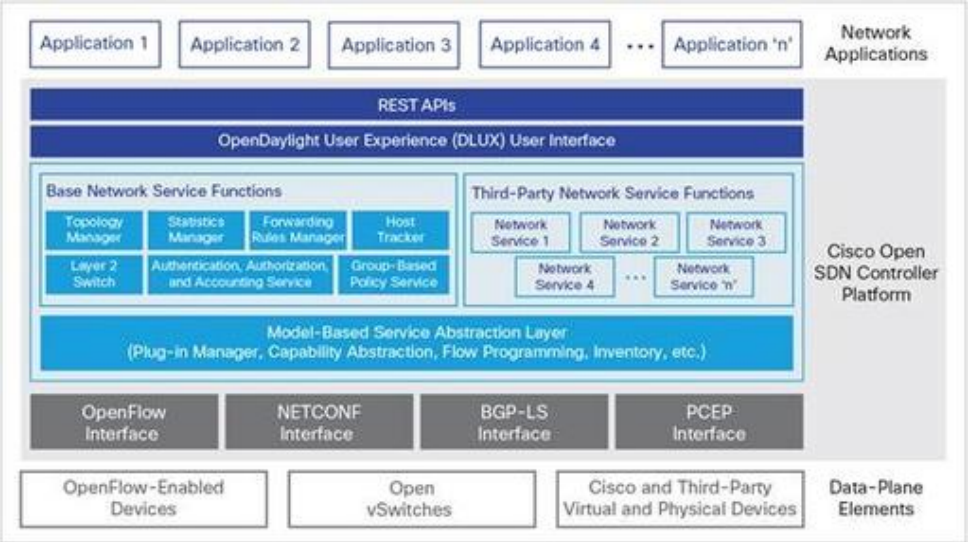


Figura 7.- Arquitectura SDN Cisco ACI

Fuente: www.cisco.com/c/en/us/products/cisco-aci/

Este fabricante también ofrece soluciones para entornos grandes como centros de datos, operadores WAN y también ofrece dispositivos de red sean enrutadores o conmutadores compatibles con protocolo SDN por lo que es útil al utilizar otro controlador de código abierto.

- **NOX/POX:** De primera generación, es un controlador hecho para OpenFlow en sus inicios. Siendo NOX de código abierto, se escribió en C++ y Python aún recibe actualizaciones y es más rápido para su función de monitoreo de eventos y programación de una serie de tareas de manera simple.

- **RYU:** Es un controlador Python basado en OpenSource, trabaja con extensiones Nicira y con OpenStack. Su principal beneficio es que se puede integrar con OpenFlow pero también ofrece un rendimiento desfavorable para entornos grandes.
- **FLOODLIGHT:** También es un controlador OpenSource basado en Java y es impulsado por una serie de fabricante siendo el más resaltante Big Switch Networks. Entre sus desventajas puede resultar complejo en su programación, más aún si tenemos entornos como centros de datos o redes de campus.
- **MININET:** Es un emulador de red que posee una colección de hosts finales, conmutadores, enlaces y controladores en un solo núcleo bajo Linux. Con el fin de simular un entorno de producción mediante SDN y OpenFlow utilizando línea de comandos (CLI) se puede interactuar y verificar la red de una organización.

- **MINIEDIT:** Como se ha podido observar, la creación de una red virtual en Mininet requiere la identificación y elección correcta de la serie de opciones en esta herramienta. Sin embargo, al ser una solución más concreta se obtiene Miniedit (el cual es una carpeta con diversos ejemplos gráficos que hace un uso potencial de Mininet).

- **OPENDAYLIGHT:** Es un proyecto de **código abierto (Open Source)** el cual tiene como objetivo acelerar e incrementar la difusión de la innovación en el diseño e implementación de un estándar abierto y transparente de redes definidas por software. Actualmente el proyecto tiene el apoyo de grandes y reconocidas compañías como: Juniper, Brocade, Cisco, Citrix, IBM, Ericsson, Microsoft, Nec, Red Hat, VMWare. Es parte de OpenFlow, como también es un protocolo propio que es compatible con distintos fabricantes.

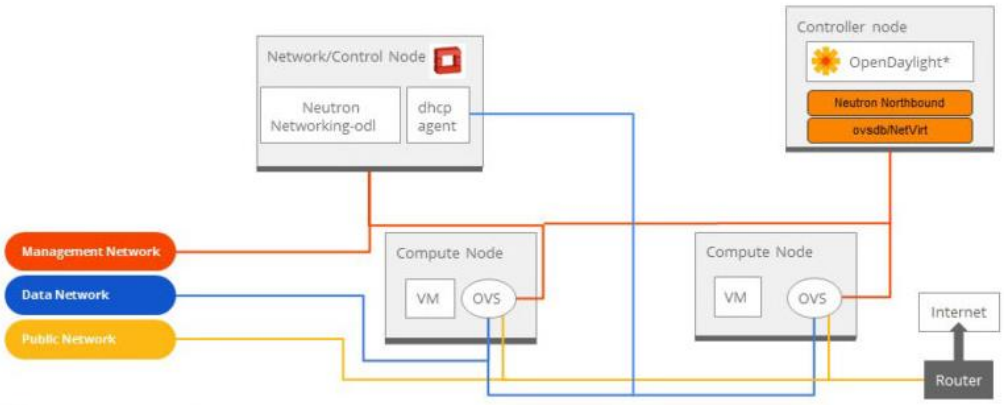


Figura 8.- Arquitectura OpenDayLight e integración OpenStack

Fuente: www.opendaylight.org/cloud-and-nfv

Sobre OpenDayLight podemos indicar que es un controlador de código abierto más estable hasta el momento, proporciona soluciones para entornos de TI como centros de datos, redes de campus y domésticas. Es más sencillo su manejo de programabilidad sobre todo para automatizar una organización con tráfico de datos, aplicaciones de red, entre otros.

1.6.4 Normativa, Legislación y Buenas Prácticas

- **ONF**: Es un consorcio, sin ánimo de lucro, dedicada a la transformación de las redes a través del desarrollo y la estandarización de una arquitectura única llamada SDN. Se lanzó por primera vez en 2011 como portador estándar de redes definidas por software y es liderada por socios operadores como AT, China Unicom, Comcast, Google. Telekom y Verizon. La ONF está estrechamente relacionada con SDN porque el primero inició el movimiento con el desarrollo de las redes por software.

- **IETF:** (Grupo de trabajo de Ingeniería de Internet) es una gran comunidad internacional abierta de diseñadores de redes, operadores, proveedores e investigadores relacionados por la evolución de la arquitectura de Internet. Relacionado a las SDN emite incluso el RFC 7426 – Arquitectura y Estructura de Capas. En este documento proporciona referencia a la comunidad de investigación basado en estándares.

- **CAB:** (Consejo asesor de Chips). Este consejo junto con la ONF se dedica al intercambio de ideas en relación de los desarrollos de las SDN, debido a que uno depende de otro en el desarrollo de los controladores para uso del tipo de entorno organizativo. La relación de CAB con las redes definidas por software están enfocadas en el desarrollo de los chips propios de Intel y Broadcom para los controladores y dispositivos alineados a SDN.

- **ETSI: (**Instituto Europeo de Normas de Telecomunicaciones). Esta organización sin fines de lucro permite adoptar las soluciones SDN sobre ciertas plataformas tecnológicas tales como NFV. Trabaja en conjunto con la ONF para proporcionar los alcances de ambas tecnologías y lograr una solución ágil.

- **ATIS:** (Alianza para las soluciones de la industria de las telecomunicaciones). Encargada de desarrollar los estándares y soluciones que se crean en la industria de las tecnologías de la información. Emite esfuerzos para beneficios de los servicios en la nube, es decir, su trabajo hace posible la innovación en el desarrollo de nuevas redes definidas por software.

- **FUNDACIÓN LINUX:** Una entidad que integra la gobernanza de los proyectos participantes para mejorar la excelencia operativa, simplificar la participación de los miembros y aumentar la colaboración entre los proyectos de redes de código abierto. En cuanto a SDN, esta organización plantea en un inicio la OPEN-O (Open Orchestration) un esfuerzo colaborativo para desarrollar el primer marco de referencia de software abierto y que permita desplegar las redes definidas por software y la virtualización de redes.

1.6.5 Buenas Prácticas

Entre las buenas prácticas de SDN, estas se aplican no por la arquitectura propuesta o la elección del controlador definido para ello. Debemos entender que cualquier configuración, puesta en producción de una solución tecnológica independientemente de lo que pueda ofrecer, muchas veces es el punto quiebre para que dicha solución pueda no presentar inconvenientes futuros.

La ONF a través de sus distintos documentos, hace énfasis en la parte de seguridad siendo uno de los pilares fundamentales al planificar una red definida por software. Por ello, se deben seguir los siguientes lineamientos al momento de optar por esta solución.

- **La selección del controlador SDN:** Se debe realizar siguiendo los criterios expuestos a lo largo de este documento, por ejemplo: soporte del protocolo OpenFlow, el controlador debe ser de código abierto, el ecosistema de las aplicaciones y las API, arquitectura, lenguaje de programación en los que fueron realizados, la compatibilidad con los equipos de red, la existencia de interfaces para la programación del controlador y capacidad de almacenamiento. También es importante el acceso a la documentación de cada fabricante de tal forma que posibilite la instalación, configuración, programación y evaluación. Finalmente, los o el controlador seleccionado deben estar basados en estándares o normativas vigentes.

- **La selección del emulador de diseño SDN:** Sea Mininet u otra herramienta de simulación para el diseño de la red, debe verificarse si es de código abierto y sea capaz de crear redes con host, conmutadores, controladores y enlaces virtuales. El emulador posee información suficiente en su documentación sobre todo de API de programación.

- **La selección de la versión del protocolo OpenFlow:** Este protocolo constituye la base de las redes definidas por software, siendo importante en el inicio del diseño de una red SDN. OpenFlow ha evolucionado durante el proceso de estandarización de la ONF, a partir de la versión 1.0 donde solo existen 12 campos coincidentes y una sola tabla de flujo a la última versión que cuenta con varias tablas de flujo, más de 41 campos, así como nuevas funciones.

- **La implementación del campo de pruebas:** Una vez se tenga los pasos anteriores listos en su diseño, se deben realizar las pruebas necesarias previo a su despliegue final en una organización. Para ello, se debe escoger un entorno programable de tipo multiplataforma que proporcione análisis del código, depuración gráfica, integración con VCS/DVCS y soporte para el desarrollo web. Adicionalmente a ello, se debe realizar lo siguiente:

  Pruebas de escalabilidad en base al desarrollo de las aplicaciones, evaluar la topología de forma virtual y el controlador SDN. La aplicación SDN que permita en tiempo real detectar intrusos en la red, así como aplicar políticas de acceso a la red en todo su conjunto. Evaluar el impacto de latencia en la red y la tasa de transferencia de datos cuando aumenta el tamaño de la red SDN.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
TRADICIONAL	0,183	0,101	0,103	0,088	0,087	0,085	0,087	0,088	0,086	0,086	0,089	0,086	0,086	0,085	0,089	0,087	0,088	0,088	0,087	0,088
SDN	22,900	0,891	0,087	0,087	0,085	0,083	0,084	0,084	0,085	0,087	0,089	0,082	0,085	0,083	0,085	0,084	0,086	0,084	0,086	0,080

Figura 9.- Ejemplo de una comparación de retardo aplicando las buenas prácticas y siguiendo lineamientos de los fabricantes (SDN vs Red Tradicional).

Fuente: www.researchgate.net/profile/Yanko_Antonio_Murio

Una buena práctica para un caso de uso específico es la medición de retardo en una red convencional, en este caso se sugiere medir el rendimiento de la tecnología o llamados pruebas de escalabilidad, en SDN denominado “benchmarking”. En donde se crean varios scripts para crear nodos y topologías de forma automática, concurrente e interactuando con el emulador de diseño seleccionado.

1.6.6 Uso y Tendencias SDN

El surgimiento de las redes definidas por software es una tendencia a la que ya está contribuyendo buena parte de los miembros de la industria, en donde quiere marcar y un después en el mercado de las comunicaciones. Cada vez se genera una mayor cantidad de datos a lo largo y ancho de la web, y dentro de los propios equipos informáticos, que vuelve casi inmanejable su control y amenaza con verdaderos cuellos de botella en el centro de datos. La suma de todos estos factores junto con otras tendencias como Big Data o Cloud Computing requiere de los proveedores de servicios una calidad de conexión sin precedentes, más flexible y sobre todo menos dependiente de una persona.
Sin embargo, el concepto de "Redes definidas por software" y según el consenso al que se llegó en los últimos años en el "Open Networking Summit", Evento el cual se celebra cada año con participación de principales fundadores y fabricantes de tecnologías, la diferenciación y las tendencias en las SDN llevaría a la gestión práctica de las redes que ya no dependería de una solución de hardware, sino de un controlador de software más inteligente y preparado para sacar su rendimiento al máximo.
A continuación, algunos factores que determinan la tendencia de las SDN en las organizaciones.

- **Virtualización creciente:** Hoy en día, se observan a los costos como principal factor influyente en la elección de una solución virtualizada para servicios de red y otros dispositivos de configuración. En esta evolución, logra aparecer el programa OpenDayLight (el cual detallaremos más adelante).

- **SDN para redes de campus:** La evolución de las SDN partió en un inicio para Centros de Datos, siguiendo para los proveedores de servicio (ISP). Gracias a la acogida que propone las redes definidas por software, ahora se enfocan en las redes de campus (siendo complejas, continuamente escalable, entre otros).

- **Innovación:** Debido a que las SDN en un principio fueron desarrollados de manera específica. Podemos decir que ya existen soluciones propias para determinado entorno de una organización, es decir, diseñadas para determinado tipo de sector.

1.6.7 Casos de Éxito/Proyectos de Investigación

Para este ítem, se realizaron búsquedas de casos de éxito a nivel de la región y otros proyectos de investigación de manera global sobre tráfico de datos con SDN. Muchos de los proyectos están en desarrollo, otros elaboraron una serie de pautas a seguir en un determinado ámbito como redes domésticas o campus. Lo más estable son las migraciones de una red tradicional a una SDN en un centro de datos como se podrá revisar en los siguientes casos.

- **Proyecto de Diseño y optimización de controladores SDN en una red WAN, Colombia (2018)**

  Este caso corresponde a un ámbito universitario como la Universidad de Santo Tomás de Bogotá, en donde se planteó una propuesta de dos controladores SDN para que lograrán administrar toda la red de la sede principal de la UTSA (Universidad Santo Tomás). El proyecto tuvo apoyo de estudiantes locales, profesores e ingenieros de telecomunicaciones de un proveedor denominado IMT Atlantique y otros colaboradores, siendo la problemática el determinar la ubicación y cantidad de controladores que deben desplegarse en la red de la UTSA, considerando un diseño de red y aspectos como balanceo de carga, latencia, jitter, calidad de servicio y escalabilidad. Cabe mencionar, que este proyecto de investigación aún no ha sido resuelto puesto que se tiene objetivo general, objetivos específicos, el cronograma de trabajo, presupuesto del proyecto dado que la UTSA cuenta con sedes externas o sucursales en las cuales es necesario investigar si es suficiente un solo controlador o dos controladores SDN, debido a que se maneja una gran carga de tráfico de datos y el cual requieren pruebas, aplicar técnicas, entre otros.

- **Proyecto de Estudio de técnicas de ingeniería de tráfico basadas en SDN, Colombia (2018)**

  El proyecto como su nombre lo indica, se trata de un proyecto de investigación de la Universidad de Cantabria en el cuál es posible determinar técnicas de ingeniería de tráfico adoptadas para diferentes entornos como un centro de datos o red de campus. Este proyecto nos hace referencia que para un mejor aprovechamiento de SDN a través de un prototipo o una red programable, pueda utilizarse el balanceo de carga o monitoreo de red basado en algoritmos y demostrar a través de una simulador o software virtual, los resultados ejecutados en un entorno de prueba o laboratorio.

Como validación de la prueba, el autor del proyecto realiza la implementación de ambos casos de uso y concluye que no necesariamente una red o entorno SDN puede solucionar los problemas de la organización de manera eventual, sino que es mucho más que eso al poder guardar configuraciones de las redes e implementarlas cuando sea necesario.

- **Proyecto de Diseño e implementación de un controlador SDN/OpenFlow para una red de campus académica, Perú (2015)**

El proyecto esta orientado a la red local de la Pontificia Universidad Católica del Perú (PUCP), en donde presenta una serie de irregularidades en la red como procesamiento de datos, el uso de varias aplicaciones, ampliación de enlaces entre los dispositivos de red, crecimiento del centro de datos dentro del campus y la virtualización. En otras palabras, este proyecto busca centralizar toda la configuración de la red PUCP en un controlador SDN y que este sea el responsable de administrar las conexiones, enlaces y la red de campus. El controlador elegido es la plataforma Floodlight y capaz de soportar toda la migración de la red PUCP a SDN y finalmente para ello, se realizó una simulación de manera virtual sobre la plataforma mencionada que determinaron la elección del proyecto.

- **Proyecto de Implementación de tecnología SDN para control de acceso y calidad de servicio en redes domésticas, ESPE (2018)**

El proyecto realizado como parte de investigación de la institución educativa ESPE de las fuerzas armadas, propone una implementación basado en SDN para redes locales y como ejemplo, utiliza un router físico y con compatibilidad para el funcionamiento del protocolo OpenFlow asociado a un controlador SDN y otros terminales. El objetivo general del proyecto es evaluar el uso de la tecnología sdn y de acuerdo a ello, diseñar una red programable que permita comparar con una red tradicional el uso de protocolos TCP, UDP, latencia y jitter, el rendimiento de los mismos en ambos escenarios.

- **Proyectos de implementación SDN a nivel mundial para entornos de nube, tráfico de datos, aplicaciones y gestión de la red**

Tenemos varias organizaciones que cuentan con SDN en sus infraestructuras de redes, mencionaremos algunas destacadas y como se indica a continuación:

Alibaba Group: Es una organización conocida por ser una cadena de comercio electrónico que vende sus productos a través de la web, al tener sus datos almacenados en la nube decidieron adoptar SDN para las aplicaciones de su red el cual soporta la creciente demanda de consumidores.

AT&T Labs: Esta organización optó por desarrollar su propio controlador utilizando OpenDayLight como marco. Esto con el fin de adoptarlo como un controlador SDN que sirva para controlar y administrar las redes de la compañía.

Century Link: Pertenece al grupo de operadores de servicio que permiten alojar centros de datos con carga masiva para sus clientes. Por ello, están en trabajo de pruebas de desarrollo con SDN de código abierto que permita crear su "Oficina central rediseñada como centro de datos" (CORD), el cual implica un nuevo comienzo como operador.

Telecom: Es un proveedor de servicios en Argentina, que eligió adoptar OpenDayLight por su flexibilidad y variedad de uso. Como primera fase implementaron la capacidad del tráfico de datos que permita mejorar la experiencia de sus clientes y reducir costos.

Telefónica: Esta organización se unió en el desarrollo y mejoras de aportes para OpenDayLight, creando un grupo de asesores específicamente para ello. La idea de Telefónica es transmitir la experiencia de implementar SDN en sus centros de datos hacia otros clientes a nivel mundial.

En conclusión, se puede observar que la mayoría de proyectos acerca de SDN en la región están aún en etapa de estudio e investigación, otros proyectos se encuentran en proceso y a la espera de obtener resultados como la ingeniería de tráfico o calidad de servicio. Por ello, es necesario mencionar que hasta el momento existen migraciones e implementaciones de una red tradicional a un entorno SDN basado en centros de datos, entornos ISP y redes domésticas como se menciona en los casos de éxito. Es importante mencionar que las redes de campus al estar constantemente expuestas a

un crecimiento constante de alumnado y otro personal, se vuelve critico para el negocio por lo que la tecnología tiene un papel fundamental en soportar sus procesos y servicios, la SDN propone una solución no solo para ingeniería de tráfico, sino a nivel de una red correctamente desplegada a través de sus diversos componentes y otras características que se presentan en el estado del arte.

En referencia al aporte académico, el uso de SDN a través de la ingeniería de tráfico para entornos de campus se está proponiendo cada vez con mayor dedicación. Se están utilizando las técnicas de tráfico como balanceo de carga o calidad de servicio (en paralelo con otras características de la tecnología SDN), para mejorar la capacidad de respuesta ante nuevas aplicaciones y casos como: clases virtuales, video conferencia, servicios propios de la organización y con más razón por la situación actual que enfrenta el mundo. Esto permite al alumnado en general, tener un mejor acceso a los servicios que ofrece su entorno universitario en cualquier momento y sin retraso o caída de servicio alguno. Si bien es cierto, no existe una mayor profundización del tema de tráfico basado en SDN, si se cuenta con gran cantidad de documentación que permitirá el desarrollo del presente proyecto y asimismo, servirá como referencia para otros trabajos relacionados al tema y que se desarrollarán en adelante.

2 CAPITULO 2: MARCO TEORICO

En este capítulo, se detallará las tecnologías asociadas a las redes definidas por software y toda información sujeta a este tema de investigación. A partir de los cuales, se identificarán el contexto, la muestra, el diseño principal y los procedimientos a realizar.

2.1 Redes de Datos

En la actualidad, se conoce a una red de datos como una vinculación de dos o más dispositivos informáticos con el propósito de compartir datos. Las redes están construidas con una mezcla de hardware y software, incluyendo el cableado necesario para conectar los equipos. Una red de datos es una red de telecomunicaciones requiere de un proceso en donde existe un emisor, un mensaje, un medio y un receptor deben comunicarse para facilitar el intercambio de datos. La finalidad de la red de datos es compartir los recursos, la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la transmisión de la velocidad de los datos y reducir el costo general de estas acciones.

La estructura y modo de funcionamiento de las redes de datos actuales están definidas en varios estándares, siendo el más importante el modelo TCP/IP basado en el modelo de referencia OSI que se detallará más adelante.

2.1.1 Topologías

La topología de red es un concepto muy importante en el diseño de una red de datos tradicional. Por esta razón, es fundamental conocer los diferentes tipos de topología de red como bus, estrella, malla, anillo y árbol, ya que estas definen la manera en que los dispositivos informáticos se encuentran conectadas entre sí.

2.1.1.1 Topología de Anillo

Es un tipo de topología de red simple, en donde las estaciones de trabajo se encuentran conectadas entre sí en forma de un anillo. La información viaja en un solo sentido, por lo tanto, si un nodo deja de funcionar se cae la red, esta deja de fluir información con los otros nodos de comunicación.

2.1.1.2 Topología de Àrbol

Es una topología sencilla en donde las conexiones entre nodos (terminales o computadoras) están dispuestas en forma de árbol. Similar a una topología estrella. Si un nodo falla, no se presenta inconveniente entre los nodos siguientes

2.1.1.3 Topología Estrella

La distribución de la información va desde un punto central hacia todos los destino o nodos de la red. En la actualidad, es muy utilizada por su eficiencia y su ventaja es si un nodo falla, la red continuará trabajando sin inconveniente.

2.1.1.4 Topología de Malla

Esta definida como una topología de trama, se trata de una interconexión de terminales entre sí, es muy utilizada en las redes WAN y su importancia es que la información viaja en diferentes caminos ante la falla de cualquier nodo.

2.1.2 Clasificación y Estándares de las Redes de Datos

Como se mencionó, las redes se configuran con el objetivo de transmitir datos de un sistema a otro o de disponer recursos en común, como servidores, base de datos o impresoras. En función del tamaño y del alcance de la red de ordenadores, se puede establecer una diferenciación entre diversas dimensiones de red. Entre los tipos de redes más importantes tenemos:

2.1.2.1 Red de Área Local (LAN)

Esta red está formada por más de un ordenador, en donde puede incluir dos ordenadores en una casa o empresa. Un estándar muy frecuente para redes de área local por cable es Ethernet. Otras opciones ya antiguas son las tecnologías de red ARCNET, FDDI y Token Ring, este tipo de red LAN fue desarrollado para posibilitar la rápida transmisión de cantidades de datos más grandes. En función de la estructura de la red y del medio de transmisión utilizado se puede hablar de un rendimiento de 10 a 1000 megabit.

2.1.2.2 Red de Área Metropolitana (MAN)

Es una red de telecomunicaciones de banda ancha que comunica varias redes LAN en una zona geográficamente cercana. En donde actúan varios routers de alto rendimiento y en

donde, supone una técnica especial de transmisión con la que se pueden construir redes de tipo CE1.0 y CE2.0. El estándar para estas redes fue desarrollado con IEEE802.16 junto con la WMAN como red inalámbrica de mayor rendimiento en entornos regionales.

2.1.2.3 Red de Área Amplia (WAN)

Estas redes se extienden por zonas geográficas como países o continentes, siendo el número de redes locales o terminales individuales que forman parte de la WAN como ilimitado. Si bien en una red local se conecta en base a Ethernet, en las redes WAN emplean técnicas como IP/MPLS, PDH, SONET, ATM. En la mayoría de casos, suele pertenecer a una organización de manera privada, incluso los proveedores de servicios hacen uso de este tipo de red para conectar redes corporativas locales y a través de Internet.

2.2 Calidad de Servicio

La calidad de servicio (QoS) por sus siglas en inglés, ha sido definida por la UIT° como: "La totalidad de las características de un servicio de telecomunicaciones que determinan su capacidad para satisfacer las necesidades explícitas e implícitas del usuario del servicio, donde las características deben ser observables y/o mesurables". Es decir, la calidad de servicio es un conjunto de estrategias que implementa el administrador o encargado de la red sobre los recursos del ambiente, para garantizar que las expectativas de los usuarios de un determinado servicio se cumplan.

Por otro lado, una clase de servicio (CoS) representa un conjunto de tráfico que requiere características específicas de retardo, pérdida de paquetes y jitter en la red. A modo de concepto, una clase de servicio se refiere a un grupo de aplicaciones con características y requisitos de rendimiento, como datos de alto rendimiento para aplicaciones en la web y el correo electrónico, o una clase de servicio de telefonía para tráfico en tiempo real, como voz y otros servicios de telefonía

---

°Unión Internacional de Comunicaciones

2.2.1 Arquitectura básica

La arquitectura básica para garantizar calidad de servicio en una red establece hasta tres elementos fundamentales: Metodología, En la cual serán tratados los paquetes dentro de los dispositivos intermedios de la red (por ejemplo: encolamiento, programación y modelado de tráfico). Otro tipo es la etiqueta de paquetes, En donde los elementos de red sean capaces de coordinar la comunicación de extremo a extremo.

2.2.2 Niveles de Servicio

Los niveles de servicio corresponden a las capacidades reales, es decir, la capacidad de la red para prestar el servicio necesario para un tráfico específico de extremo a extremo. Los servicios difieren en su nivel de "medición en QoS", que describe que tan estricta puede ser la limitación del servicio en características como: ancho de banda, retardo, jitter y pérdidas.

A continuación, se presentan tres niveles básicos de calidad de servicio extremo a extremo, que se disponen en una red de comunicación.

- Servicio de mejor esfuerzo (Best Effort), en el cual todos los paquetes son tratados de la misma forma, es decir, no hay calidad de servicio especificada.
- Servicios diferenciados (DiffServ), en el cual cierto tráfico se trata mejor al resto (a través de un manejo más rápido, más ancho de banda en promedio, menor perdida).
- Servicio garantizado, se refiere a una reserva absoluta de recursos de red para tráfico específico.

2.2.3 Aplicación de SDN en la calidad de servicio

Las redes transportan una gran cantidad de servicios como datos, voz y video. Los proveedores de servicio (ISP) y empresas con infraestructura propia, implementan mecanismos para dar un tratamiento diferenciado el tráfico según lo requerimientos de sus clientes, considerando la criticidad de los servicios y el tipo de información. Entonces, el objetivo fundamental de cualquier mecanismo de QoS es asegurar que la congestión excesiva en la red no interfiera con los paquetes asegurados con calidad de servicio, ante esto es importante definir que los mecanismos de QoS no crean una capacidad adicional en la red, sino que se prioriza el tráfico y la asignación de capacidad para los paquetes cuando la red se congestiona.

Existen varios protocolos que tienen capacidades de calidad de servicio como es el caso de OpenFlow para las redes SDN y NETCONF (Protocolo de Configuración de Red). En el caso de OpenFlow, este provee calidad de servicio a través de un mecanismo de colas. El ciclo de vida del QoS se representa con cinco operaciones principales: Creación de colas, adición del flujo de QoS, Modificación del flujo de QoS, supresión del flujo de QoS y supresión de colas.

2.3 Redes Definidas por Software

Las redes definidas por software son una arquitectura emergente que se compone de un grupo de técnicas usadas para facilitar el diseño, desarrollo y operación de servicios de red de una manera dinámica y escalable, separando el plano de control y el plano de datos. Siendo esta una definición tentativa propuesta por la IETF°, indicando que no es una descripción final para el desarrollo en que se encuentra hasta la actualidad.

2.3.1 Arquitectura de una red SDN

Algunas características de la arquitectura que propone una SDN son la adaptabilidad, la escalabilidad y el bajo costo de implementación, cualidades que la hacen ideal para las aplicaciones actuales de ancho de banda elevado. La separación del plano de control y el plano de datos, provee una arquitectura programable que permite administrar la red, ya que las funciones de envío y recepción de datos están desacopladas de los procesos de administración quedando abstraída la infraestructura subyacente para las aplicaciones y los servicios de red.

2.3.1.1 Capa de Aplicación

Las aplicaciones SDN comunican sus requisitos a la red a través de una API que conecta con la capa de control, y están diseñadas para satisfacer las necesidades de los usuarios. Entre algunos ejemplos tenemos: Enrutamiento adaptativo, itinerancia sin interrupciones, mantenimiento de la red, seguridad de la red, virtualización de la red y cloud computing

2.3.1.2 Capa de Control

De manera centralizada, el controlador es el componente más importante de la arquitectura SDN ya que gestiona la capa de aplicación e infraestructura mediante dos interfaces, una con cada plano adjunto. Además, se debe monitorizar todos los elementos para dar una visión global de la red. Mediante la comunicación con el plano de infraestructura, se recoge el estado de la red y, según las exigencias de las aplicaciones, actualiza en los dispositivos las reglas de reenvío, ya que pueden producirse cambios como recuperación tras un fallo, migración de máquinas virtuales o balance de carga. También se debe mantener una validez y consistencia a fin de evitar bucles o agujeros de seguridad.

2.3.1.3 Capa de Infraestructura

Esta capa consta de los dispositivos de hardware de conmutación que forman una red y realizan dos tareas de acuerdo a sus dos componentes lógicos: Control y Datos.

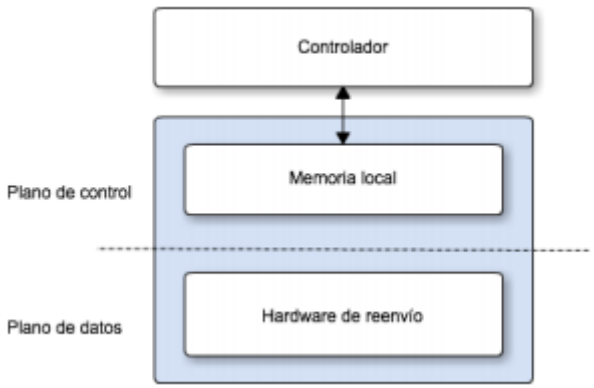


Figura 10: Dispositivo en la Capa de Infraestructura

Fuente: riunet.upv.es/bitstream/heandle/OpenFlowSequence

Es importante mencionar el comportamiento de un dispositivo SDN al recibir un paquete, el primer paquete de un flujo se envía al controlador para su procesado e inspección de la cabecera del paquete, actualizando las tablas de reenvío. Una vez llegan más paquetes de dicho flujo, estos se reenvían de acuerdo a la tabla, lo que se traduce en mayor sencillez al fabricarlos y obtener menos costo. Otro punto a tocar son los ejemplos reales en implementaciones con dispositivos SDN según su naturaleza como: Implementación en una PC, implementación en hardware de red abierta e implementación por parte de un fabricante

2.4 Protocolo de red en entornos SDN

2.4.1 OpenFlow

La relación de un software de control separado de la red es visto como una implementación real de SDN, estandarizando la forma en la que el controlador se comunica con los dispositivos, permitiendo la programación de las tablas de flujos por parte de las aplicaciones, software y especificando cómo migrar el control de la red al controlador. El protocolo OpenFlow aprovecha el hecho de que la mayoría de los conmutadores y enrutadores Ethernet actuales contienen tablas de flujo (construidas a partir de memorias TCAM y RAM que realizan la gestión interna) para funciones como cortafuegos, calidad de servicio o pruebas estadísticas. OpenFlow dispone de tres partes como mínimo.

2.5 Interfaces y Lenguajes de Programación

2.5.1 Interfaces de programación de aplicaciones (API)

Dentro de los dispositivos OpenFlow, un camino a través de una secuencia de tablas de flujo define como será manejado el tráfico. Cuando llega un nuevo paquete se inicia un proceso de búsqueda en la primera tabla de flujo y termina con una coincidencia en una de las tablas o es descartado o enviado al controlador en caso de no encontrar ninguna regla para procesar ese tipo de tráfico. Una regla de flujo puede ser definida a partir de la combinación de diferentes tipos de campos coincidentes. Usualmente se instala en estos dispositivos una regla predeterminada que envía los paquetes al controlador o procesamiento tradicional (no OpenFlow) en el conmutador cuando no se encuentra ninguna coincidencia. Todas las reglas son instaladas por una aplicación SDN a través de la API hacia el norte con el controlador que es quien finalmente le envía información (reglas y acciones) al elemento de la capa de infraestructura utilizando la interface hacia el sur.

A continuación, se detallará cada interface y sus propósitos en una arquitectura SDN.

2.5.1.1 Northbound API o Interface hacia el Norte

La interface hacia el norte desempeña un papel crucial en la adopción de SDN ya que permite a los desarrolladores la libertad de desplegar sus aplicaciones para generar ingresos sin ser afectados y limitado por la complejidad de las redes subyacentes. Para

ello, la Northbound tiene que permitir que las aplicaciones puedan expresar sus necesidades y limitaciones en el lenguaje de programación específico de la aplicación, y el controlador SDN debe traducir esos requisitos en el lenguaje empleado en la capa de infraestructura para realizar la provisión de recursos y servicios para así satisfacer los requisitos de la aplicación.

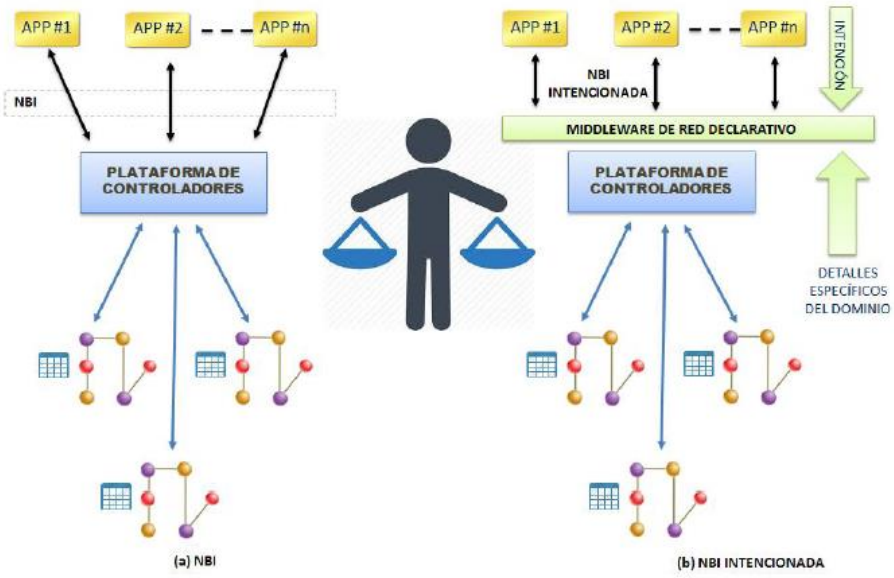


Figura 11: API en dirección hacia el norte

Fuente: PlataformadepruebasparaevaluardesempeñoSDN_AntonioMarin

2.5.1.2 Southbound API o Interface hacia el Sur

Las interfaces hacia el sur (API hacia el sur) son los puentes de conexión entre los elementos de control los elementos de reenvío, y el instrumento fundamental para separar las funciones de control de las del plano de datos. Sin embargo, esta API están todavía fuertemente ligadas a los elementos de reenvío de la infraestructura física o virtual subyacente.

El protocolo OpenFlow ha sido el estándar abierto hacia el sur más aceptado e implementado para las SDN. El protocolo proporciona una especificación para implementar los dispositivos de reenvío, así como el canal de comunicación entre los dispositivos de los planos de datos y control (por ejemplo: entre conmutadores y controladores). OpenFlow ofrece tres fuentes de información para los sistemas operativos de red. En primer lugar, el envío por parte de los dispositivos de reenvío de mensajes de eventos cuando cambia el estado de un enlace o puerto. En segundo lugar, el envío de

estadísticas de flujo al controlador. El tercero y más importante, son los mensajes "PACKET_IN" enviados por los dispositivos de la capa de infraestructura hacia el controlador cuando estos elementos no saben qué hacer con los paquetes entrantes. Estos canales de información son la vía principal mediante la cual el NOS recibe información de la red.

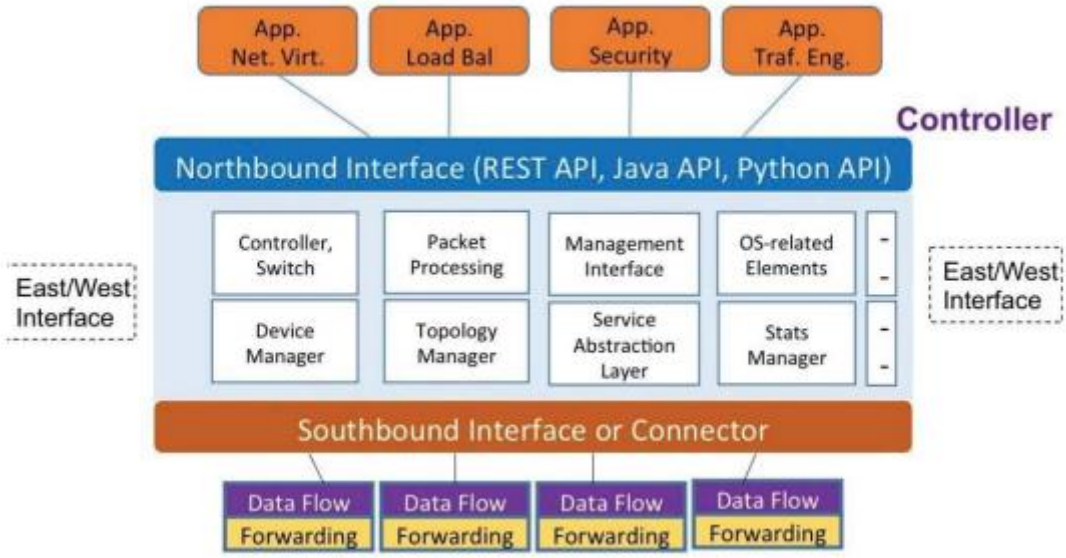


Figura 12: API en dirección hacia el sur y hacia el norte

Fuente: oa.upm.es/51526/1/TFG_PABLO_SAYAUS_COBOS

2.5.2 Lenguaje de Programación Python

2.5.2.1 Pox

El controlador Pox es la evolución por asi decirlo del controlador NOX clásico, este controlador permite un rápido desarrollo y creación de prototipos de software de control de red usando el lenguaje de programación Python. Es un controlador de varios existentes como Floodlight, Reflector, Trema, entre otros. En donde nos permiten crear aplicaciones para gestionar una red e interactuar con switches OpenFlow. Pox es también un controlador base para algunos experimentos en SDN, básicamente a este controlador se lo ha usado para implementar varios prototipos de SDN.

2.5.2.2 Pyretic

Es un lenguaje de programación Python para SDN que junto con el controlador Pox, permiten a los administradores de red realizar aplicaciones modulares y robustas,

reutilizando módulos y código fuente o partiendo de un punto determinado. Pyretic es un lenguaje asociado a Python, ya que todos los módulos se los escribe en dicho lenguaje, y todas las aplicaciones realizadas en Pyretic pueden ser perfectamente ejecutadas en un servidor controlador que trabaje a la par con conmutadores de red y el protocolo OpenFlow. (GitHub, 2014)

2.5.3 Lenguaje de Programación Java

Este lenguaje de programación orientado a objetos fue diseñado específicamente para tener pocas dependencias en su implementación como fuera posible. Su intención es permitir que los desarrolladores de aplicaciones escriban el programa una vez y lo ejecuten en cualquier dispositivo, lo que quiere decir que el código es ejecutado en una plataforma no tiene que ser necesariamente recopilado para correr en otra. Una característica importante es la independencia de la plataforma, el cual significa que programas escritos en el lenguaje java puede ejecutarse en cualquier tipo de hardware.
Esto nos indica, porque muchos fabricantes adoptan java en sus controladores SDN ya que depende del entorno a desplegar la solución y el fabricante ofrece con determinados lenguajes de programación, simplificando la operación en el hardware.

2.5.4 Lenguaje de Programación C++

Es un lenguaje que puede ser utilizado para controlar el comportamiento de un dispositivo. Consiste en un conjunto de reglas semánticas que definen su estructura y el significado de sus elementos. Es muy potente en lo que se refiere a creación de sistemas complejos y puede compilar y ejecutar código de C, ya viene con librerías para realizar esta labor.
En referencia a las SDN, al igual que Java y otros lenguajes de programación se complementan con los fabricantes en controladores de tipo SDN. Cada uno varía en relación al uso y el tipo de compatibilidad que la organización busque para cubrir sus necesidades.

2.6 Herramientas de diseño SDN

2.6.1 Mininet

Es un emulador que permite crear redes de máquinas virtuales, switches, controladores y enlaces, implementados en un dispositivo físico que ejecuta el kernel estándar de Linux.

Tiene como cualidad adicional que sus switches soportan OpenFlow, característica útil para simular enrutamiento personalizado altamente flexible y otras características de las redes definidas por software (SDN).
Mininet apoya la investigación, el desarrollo, el aprendizaje, la creación de prototipos, pruebas, depuración, y cualquier otra tarea que podrían beneficiar de tener una red experimental completa en un ordenador portátil u otro PC, esta y otras características como las mencionadas a continuación describen lo que es Mininet.

- Proporciona un entorno de pruebas simple y económico para el desarrollo de aplicaciones OpenFlow.
- Permite a múltiples desarrolladores trabajar de forma concurrente e independiente sobre la misma topología.
- Permite realizar pruebas en topologías complejas, sin la necesidad de cablear una red física.
- Incluye una interfaz de línea de comandos (CLI) que reconoce la topología y al protocolo OpenFlow, para la realización de pruebas y depuración del funcionamiento de toda red.
- Soporta topologías personalizadas, e incluye un conjunto básico de topologías listas para usar sin necesidad de programación.
- También proporciona una API de Python sencilla y extensible para la creación de redes personalizadas y posible experimentación con estas (MiniEdit).

Mininet proporciona un método sencillo para determinar el comportamiento correcto del sistema y, en cierta medida compatible con el rendimiento en la implementación con hardware real, del mismo modo para experimentar con topologías personalizadas.

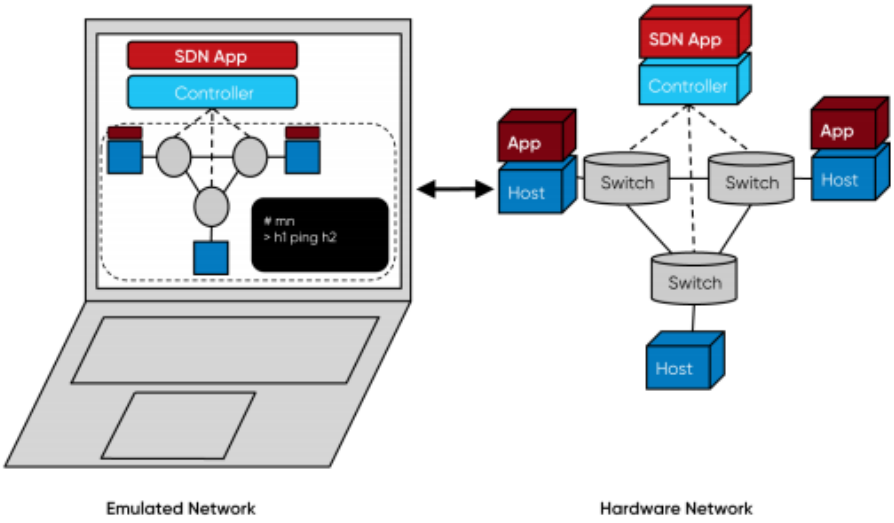


Figura 13: Emulación de redes en Mininet

Fuente: www.udistrital.edu.co/bitstream/IbarraLancherosSneider

Las redes en Mininet ejecutan un código real, incluyendo aplicaciones estándar de red Unix/Linux, así como el kernel real de Linux y la pila de red (cualquier extensión de kernel que tenga disponible, siempre y cuando sean compatibles con el sistema, como el Wireshark). Debido a esto, el código desarrollado y probado en Mininet, para un controlador OpenFlow, switch modificado, o dispositivo final, se puede trasladar a un sistema real con cambios mínimos para las pruebas, la evaluación de rendimiento y posterior implementación. Es importante destacar que esto significa que un diseño que funciona en Mininet por lo general puede pasar directamente a los switches reales.

2.6.2 Actualización de Mininet

Dentro de Mininet existen actualizaciones que permiten utilizar fácilmente la creación y ejecución de experimentos tanto simples como complejos en Mininet, utilizando scripts de Python y como Mininet es un proyecto de código abierto, se puede examinar su código fuente, corregir los errores, problemas de archivos, peticiones de características, y enviar solicitudes de parches. Si bien los desarrolladores de este simulador están en constante investigación para solucionar algún inconveniente que pueda presentarse y dentro de las limitaciones que encontramos, tenemos que es conveniente ejecutarlo en un solo sistema por lo que impone límites de recursos. Por ejemplo: si un servidor tiene 4 Ghz de velocidad en su CPU y puede cambiar alrededor de 4 Gbps de tráfico simulado, se tendrán

que equilibrar y compartir esos recursos entre los hosts virtuales y switches. (Doxygen, 2015).

2.6.3 Topologías en Mininet

Para la creación de topologías por defecto en Mininet, se debe tener en claro la simbología y esta se realiza de la siguiente manera:

Hx > Host

Sx > Switch

Cx > Controller

$ > Comando en Shell

 # > Comando como root

Mininet > Comando dentro de Mininet

$Sudo mn

Inicia Mininet con una topología por default con 1 switch, 1 controlador y 2 hosts.

Syntaxis:

Mininet> nodo comando

Colocando el nodo frente a un comando, se indica que el comando está siendo ejecutado en aquel nodo.

Es posible utilizar el nombre del nodo para sustituir la dirección IP.

Mininet>h2 ping -c4 h3

Comandos:

Para salir de Mininet: *mininet>exit*

En caso se requiera abrir un terminal para el nodo*: mininet>xterm nodo*

Para crear o eliminar un link entre dos nodos: *mininet>link node1 node2 up or down*

Prueba de conectividad entre dos nodos: *mininet>pingall*

Muestra de lista de comando en Mininet: *mininet>help*

Para limpiar la topología: *#mn -c*

La creación de topologías es sencilla y rápida, salvo se restringe al momento de pretender hacer una topología personalizada. A continuación, se explicarán los tipos de topología que pueden ser utilizadas en Mininet.

2.6.3.1 Topología Única

Consiste de un único conmutador conectado a un número determinado de hosts. Un switch conectado a N hosts, se crea con el siguiente comando:

$sudo mn—topo single, N

N es el número de hosts deseados

La desventaja de esta topología es que el usuario se encuentra amarrado a usar un solo conmutador. La creación de una topología de 3 hosts (H1, H2, H3) conectados a un switch (S1) en el siguiente ejemplo:

mininet@mininet-vm: $sudo mn –topo single, 3
****Creating network*
****Adding controller*
****Adding hosts:*
H1 H2 H3
****Adding switches:*
S1
****Adding links:*
(H1, S1) (H2, S1) (H3, S1)
****Configuring hosts*
H1 H2 H3
****Starting controller*
****Starting 1 switches*
S1

2.6.3.2 Topología Lineal

Esta topología consta de un determinado número de conmutadores interconectados de forma lineal. Cada conmutador tiene un host conectado a él, para crear esta topología se usa el siguiente comando:

$sudo mn –topo linear, N

En donde N es el número de conmutadores y hosts que se desean añadir a la topología. Además, se permite un manejo más flexible en cuanto a la agregación de conmutadores, la limitante es que el número de conmutadores debe ser igual al número de hosts, ya que

necesariamente cada host se conecta a un conmutador. De esa manera, limita el uso de esta topología en las topologías personalizadas.

$sudo mn –topo linear, N

N será el número de switches y hosts. Ahora, la creación de una topología lineal de 4 host y 4 switches.

mininet@mininet-vm: $sudo mn –topo linear, 4
****Creating network*
****Adding controller*
****Adding hosts:*
H1 H2 H3 H4
****Adding switches:*
S1 S2 S3 S4
****Adding links:*
(H1, S1) (H2, S2) (H3, S3) (H4, S4) (S1, S2) (S2, S3) (S3, S4)
****Starting controller*
****Starting 4 switches*
S1 S2 S3 S4
****Starting CLI:*
Mininet>

2.6.3.3 Topología de Árbol

En este caso es posible crear una topología en forma de árbol, el comando para la creación de esta topología es:

$sudo mn –topo tree, Depth=N, fanout=M

N es el nivel de profundidad del árbol que se desea tener.
M es un parámetro denominado esparcimiento. Si los parámetros M y N son iguales a dos, se tendrán dos niveles, el primero con un conmutador y el segundo con dos, conectados a cada conmutador del nivel dos, se tendrá dos hosts.

$sudo mn –topo tree, Depth=n, fanout=m

Crear una topología de árbol con profundidad N y anchura M. Ejemplo de creación de una topología en forma de árbol de 2 como profundidad y 2 de ancho:

mininet@mininet-vm: $sudo mn –topo tree, Depth=2, fanout=2

****Creating network*

****Adding controller*

****Adding hosts:*

H1 H2 H3 H4

****Adding switches:*

S1 S2 S3

****Adding links:*

(H1, S2) (H2, S2) (H3, S3) (H4, S3) (S1, S2) (S1, S3)

****Configuring hosts*

H1 H2 H3 H4

****Starting controller*

****Starting 2 switches*

S1 S2 S3

****Starting CLI:*

Mininet>

2.6.3.4 Topología personalizada

Para topologías personalizadas, es necesario crear un archivo en Python con su topología (Doxygen, 2015).

$sudo mn –custom mytopologia.py –topo mytopologia

Las topologías customizadas se quedan en la ruta ./mininet/custom. Para la creación de topologías personalizadas en mininet, observamos la siguiente imagen.

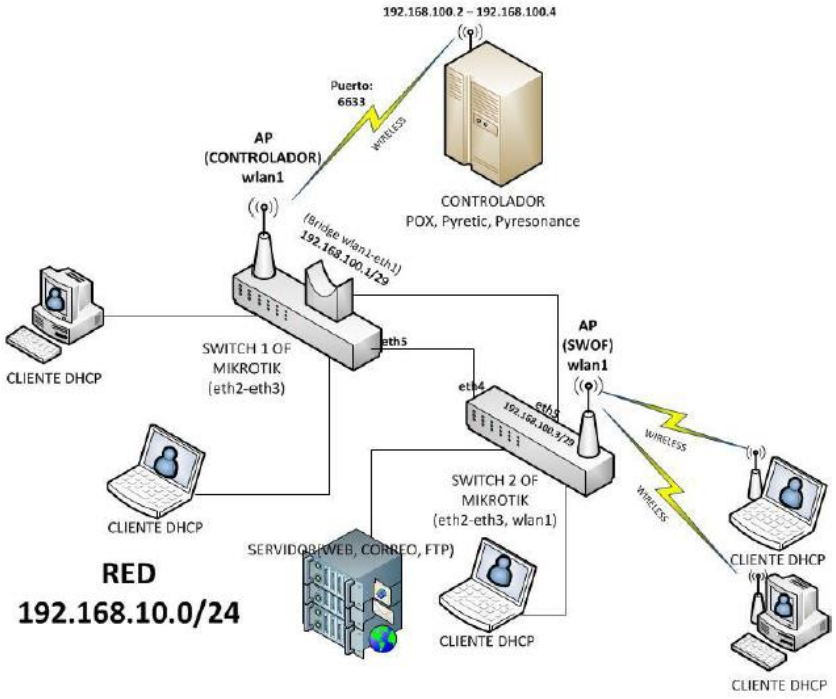


Figura 14: Simulación en Mininet usando la topología personalizada.
Fuente: www.udistrital.edu.co/bitstream/IbarraLancherosSneider

Para ejecutar un archivo con una topología personalizada, se debe dirigir a la ubicación del mismo y ejecutamos el siguiente comando:

Sudo Python nombre_archivo.py

En este caso, se utilizó el archivo topologíaSDN.py ubicada en "/mininet" de la máquina virtual utilizada y en el código, se activa un controlador remoto que se debe inicializar. Entonces, la ejecución del archivo que contiene la topología de la imagen mostrada es la siguiente:

mininet@mininet-vm: $ cd mininet

mininet@mininet-vm: /mininet$ sudo python topologíaSDN.py

Registro de las conexiones de los hosts:

H1 H1 -eth0: S1 -eth1

H2 H2 -eth0: S1 -eth2

H3 H3 -eth0: S2 -eth1

H4 H4 -eth0: S2 -eth2

Mininet>

2.6.4 Miniedit

Otra forma de crear topologías es mediante la utilidad MiniEdit descrita en Python, que se encuentra en el directorio "/miniedit/examples". Esta es una interfaz gráfica simple, como se muestra en la siguiente figura.

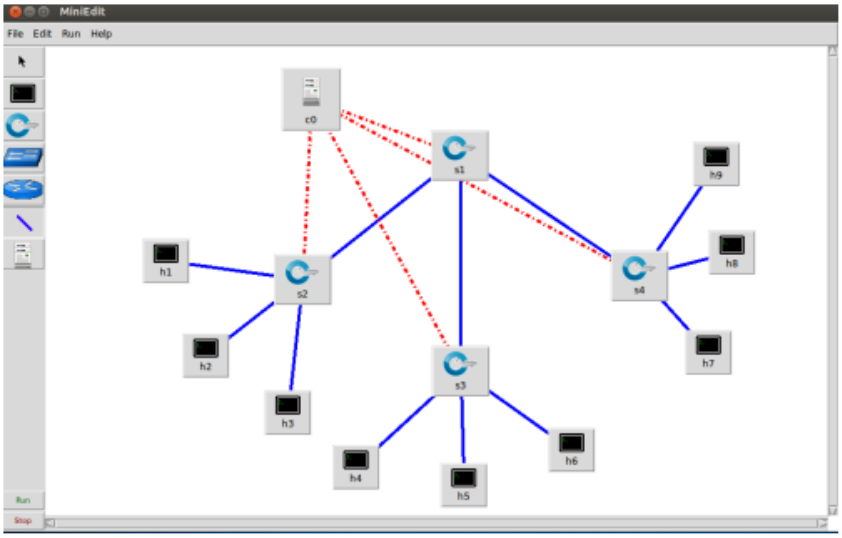


Figura 15: Interfaz gráfica para crear topologías en MiniEdit

Fuente: www.udistrital.edu.co/bitstream/IbarraLancherosSneider

En la figura 15, se muestra una topología que se compone de 4 switches conectados mediante enlaces representados con líneas continuas, y 9 hosts conectados a los vSwitches. Adicionalmente, los switches se comunican con el controlador central, a través de enlaces representados por medio de líneas punteadas. La topología creada con los dos métodos descritos es la misma, pero es evidente que es mucho más intuitivo el proceso gráfico. Esta interfaz permite contar con una barra de herramientas realmente sencilla se puede crear múltiples topologías y configurar características en los hosts.

2.6.5 Open vSwitch

Es una plataforma Open Source para sistemas basados en Linux que permite la virtualización de switches multicapa con calidad de producción. Está diseñado para facilitar la automatización de la red a través de extensiones programables y el soporte a interfaces y protocolos de administración estándar como NetFlow, sFlow, LAC, entre otros. La estructura de OVS es modular y consta de cuatro de ellos, cada uno incluye servicios enfocados a facilitar la administración: seguridad, monitoreo, QoS y controla automatizado.

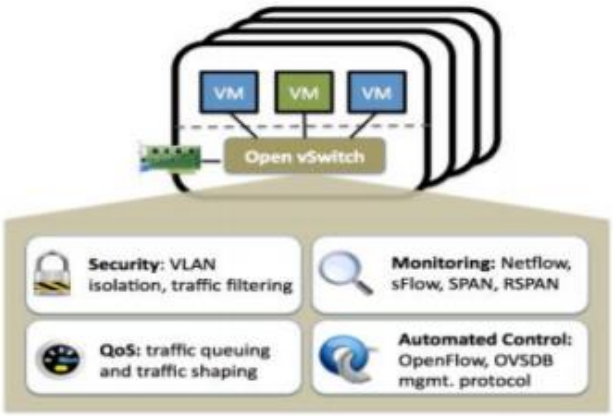


Figura 16: Módulos de Open vSwitch

Fuente: dit.upm.es/postgrado/TFM_Salinas_Jardon

Entre las características principales de OVS están:

- **Redes dinámicas**

  Incluye una serie de características que le permiten responder y adaptarse a cambios en la red, basándose en la información de la topología con la que cuenta y que almacena en la base de datos OVSDB.

- **Etiquetas lógicas**

  Las etiquetas lógicas identifican de manera única a cada elemento de la red a través del etiquetado de éstas e incluye varios métodos para especificar y mantener las reglas de etiquetado.

- **Integración de hardware**

  Permite la integración de elementos de red físicos, encargándose del reenvío del tráfico entre estos y las máquinas virtuales.

- **Movilidad**

  Cada entidad de la red (sea máquina virtual o infraestructura física) debe ser fácilmente identificable y capaz de ser migrado sin representar mayores dificultades.

2.6.6 Controlador SDN

El plano de control es una parte esencial de la arquitectura SDN. Como se ha mencionado en el estado del arte, un controlador básicamente añade y elimina entradas en la tabla de flujos en los dispositivos de la capa de infraestructura. Aunque existen numerosos controladores disponibles y que soportan diferentes protocolos hacia el sur, en este trabajo serán estudiados los que soportan el protocolo OpenFlow.

Existen diversos controladores y plataformas de control con arquitecturas y diseños variados. El primer controlador SDN con soporte para el protocolo OpenFlow, fue el NOX y fue escrito en el lenguaje de programación C++ y estaba destinado a ser ejecutado en distribuciones de Linux.

2.6.6.1 Especificaciones

Existe gran variedad de opciones entre las que se puede elegir, por lo que se deberá tomar en cuenta algunos aspectos fundamentales para decantarse por uno o por otro:

- Entorno: Se refiere al tipo de red donde se introducirá el controlador (física o virtual), la demanda de recursos informáticos que deberá soportar, el número de clientes que podrá atender, la topología y tamaño de la red, etc.
- Características propias de la plataforma: Lenguaje en el que está desarrollado, plataformas soportadas, módulos externos instalables, versiones de OpenFlow que soporta, tipo de interfaz (GUI/CLI), compatibilidad con servicios virtualizados o hardware físico, etc.
- Documentación: Por último y no menos importante, se encuentra el soporte que hay detrás de la plataforma: manuales de uso, tutoriales, foros, datasheets, comunidades de usuarios, casos de uso, etc.

Dada que la lista de opciones open source es extensa, en los siguientes párrafos nos concentraremos en tres de ellos: POX/NOX por ser el primero de los controladores SDN en ser desarrollado y OpenDaylight (ODL) y Floodlight por ser dos de los controladores más usados actualmente, al contar con el respaldo de grandes empresas y organizaciones líderes en la rama de las telecomunicaciones.

En la siguiente tabla, se muestra una comparativa entre los principales atributos de los tres controladores mencionados sobre estas líneas y a continuación una breve reseña de

cada uno de ellos, que permitirá tener mayores elementos que influyan en el proceso de toma de decisiones durante el diseño de las redes que los contendrán.

	NOX/ POX	OpenDaylight	Floodlight
Año de lanzamiento	2008	2013	2014
Lenguaje de desarrollo	C++/Python	Java	Java
Plataformas	Linux/Windows/MacOs		
Versiones de OpenFlow soportadas	1.0	1.0 - 1.3	1.0 - 1.5
Compatibilidad con Mininet	Si	Si	Si
Integración recursos virtualizados y reales	Si	Si	Si
Interfaz gráfica	No/Web	Web	Web
API REST	No	Si	Si
Documentación	Baja	Media	Buena
Última versión	0.2.3	5 (Boron)	1.2

Tabla 1: Comparación de controladores SDN

Fuente: dit.upm.es/postgrado/TFM_Salinas_Jardon

2.6.6.2 Controlador OpenDayLight

La versióna utilizar es “Lithium”, que surge como una colaboración entre usuarios, proveedores y desarrolladores con base en sus experiencias y experimentación con las versiones anteriores. Con respecto a otros modelos, Lithium ofrece mejoras para la integración con cloud, NFV e ingeniería de tráfico a gran escala, así como frameworks para la convivencia con Openstack y OPNFV. Además, se incluye mejoras considerables en cuanto a rendimiento y productividad. se muestra el esquema de operación del controlador, donde se distinguen tres capas:

Controlador (Servicios y aplicaciones): Compuesto por las aplicaciones de alto nivel que permiten monitorear y gestionar la red a través de:

- Funciones del plano de control: AAA49, switch de capa 2, servicios LISP50, LAC51, administrador de switches OpenFlow, procesadores de topología, etc. Cuya función es la gestión del tráfico en la red.
- Aplicaciones embebidas: Routers Atrium, Genius, aplicaciones NAT52, Eman, Cardinal, entre otros. Las cuales son aplicaciones desarrolladas por terceros y que son soportadas por el controlador.

- Políticas de red: Son abstracciones de la red y permiten una gestión de alto nivel del sistema, como ejemplo están: Protocolo ALTO53, FaaS54, NEMO55, servicio de políticas basadas en grupo, entre otros.
- Aplicaciones independientes: Son aplicaciones desarrolladas por terceros que pueden ser integradas al controlador a través de APIs REST o NETCONF56. Por mencionar algunas están Openstack, Chef, Puppet.

Southbound APIs y plugins de protocolos: Conformado por los módulos que permitirán la comunicación entre el controlador y los elementos del plano de datos. Como se puede observar, ofrece soporte a diversos protocolos y servicios como: OpenFlow, BGP, IoT57, LISP, NETCONF, SXP58, entre otros.

Elementos del plano de datos: Son los elementos genéricos que soportarán el plano de datos de la red y que serán programados y gestionados por el controlador: switches virtuales (Open vSwitch) e infraestructura física, tanto SDN, convencionales e híbridos.

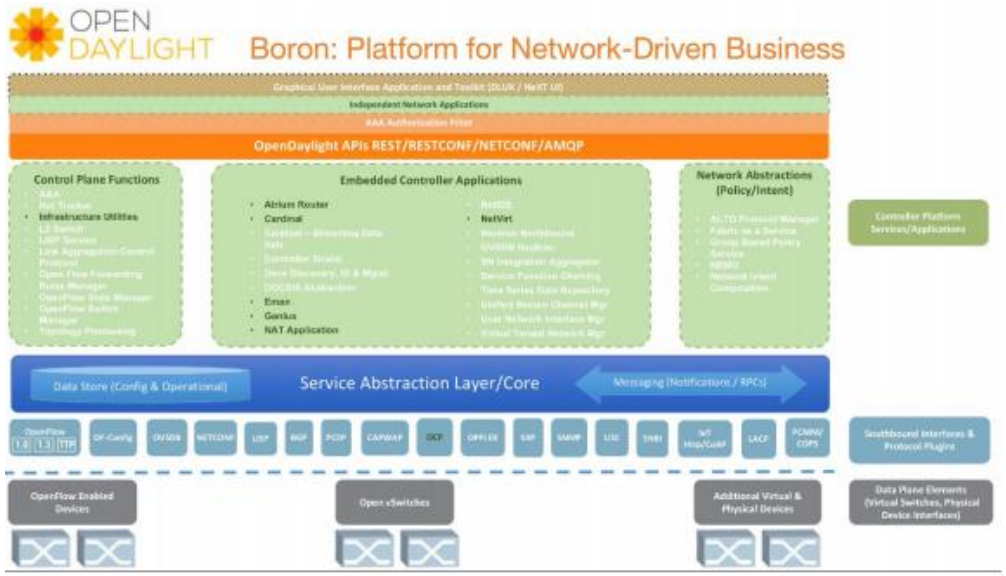


Figura 17: Estructura y operación del controlador OpenDayLight

Fuente: dit.upm.es/postgrado/TFM_Salinas_Jardon

Sobre estas capas se encuentra la API REST y la interfaz gráfica de OpenDayLight, a través de las cuales el usuario podrá gestionar la plataforma como una única entidad, facilitando dicha tarea y permitiendo que gracias a su estructura modular, se desarrollen soluciones a la medida de las necesidades del usuario.

2.7 Normativa de las Redes definidas por Software

2.7.1 UIT-T77

Esta resolución con nombre de “Fortalecimiento de la normalización de las redes definidas por software en el Sector de Normalización de las Telecomunicaciones”, indica un listado del apoyo que se brinda a los diferentes entornos como:

- A medida que se desarrolla y consolida la tecnología de redes definidas por software (SDN), muchas organizaciones están participando en la normalización de la SDN,
- Las SDN cambiarán profundamente el panorama de la industria de las telecomunicaciones y las tecnologías de la información y la comunicación en las próximas décadas, y pueden aportar múltiples beneficios al sector de las telecomunicaciones.
- Nuevas tecnologías incipientes, como la virtualización de las funciones de red (NFV), pueden dar soporte a las SDN, ya que proporcionan infraestructura virtualizada sobre la cual puede funcionar el software de las SDN.
- Las SDN permitirá integrar una amplia gama de tecnologías que permiten servicios de red basada en la nube y de telecomunicaciones, al tiempo que se reconoce la labor que se realiza en otras organizaciones como en el Grupo de Especificación de la Industria (ISG), sobre el Instituto Europeo de Normas de Telecomunicaciones (ETSI), Proyecto Orquestador Abierto (OPEN-O).

°International Telecommunications Union (ITU)

2.7.2 RFC-7426

Tratado por el Grupo de Trabajo de Investigación en Internet (IRTF)°, con título “Redes definidas por software (SDN): Capas y Terminología de Arquitectura”, se refieren a un nuevo enfoque para programabilidad de la red, es decir, la capacidad de inicializar, controlar, cambiar y gestionar el comportamiento de la red de forma dinámica a través de interfaces SDN enfatiza el rol del software en redes corrientes. A través de la introducción de una abstracción para el reenvío de datos, plano y al hacerlo, lo separa del plano de control. Esta separación permite ciclos de innovación más rápidos en ambos planos como la experiencia ya ha demostrado. Sin embargo, hay una creciente confusión en cuanto a qué es exactamente la SDN, cuál es la estructura de capa en una SDN su arquitectura, y

cómo las capas interactúan entre sí. Este documento, un producto de la investigación de redes definidas por software de IRTF, responde a estas preguntas y proporciona un resumen de referencia para la comunidad de investigación SDN basada en pares relevantes, literatura revisada, la serie RFC y documentos relevantes de otras organizaciones de normalización.

°Grupo de Trabajo de Investigación en Internet (IRTF)

2.7.3 Open Networking Foundation (ONF)

Es un consorcio dirigido por un operador sin fines de lucro que impulsa la transformación de la infraestructura de red y los modelos de negocios de operadores. Asimismo, es una comunidad de comunidades abierta colaborativa. Sirve como un soporte para una serie de proyectos que desarrollan soluciones al aprovechar la desagregación de la red, la economía, el software de código abierto y los estándares definidos por el software para apoyar a los operadores. ONF mantiene varios grupos de trabajo que actualmente analizan la evolución del estándar OpenFlow para atender las necesidades de los nuevos casos de uso y las implementaciones de producción. Open Networking Foundation también recibe orientación de alto nivel de parte de su Grupo de Asesoramiento Técnico (TAG) y la Junta Asesora de Chipmakers (CAB) . TAG proporciona perspectivas de múltiples proveedores y conocimiento específico de la industria con respecto a problemas técnicos relacionados con las redes definidas por software de la próxima generación. CAB sirve como un foro para que los fabricantes de chips asesoren a ONF sobre las mejores maneras de promover el ecosistema de hardware y la cadena de suministro.

Actualmente, hay más de 125 empresas que son miembros de Open Networking Foundation, que representan a TI, la nube , los proveedores de servicios de telecomunicaciones, los proveedores de equipos de red y los proveedores de servicios de silicio. Continúa ofreciendo soluciones interoperables principalmente impulsadas por OpenFlow y el Estándar de Protocolo de Administración y Configuración de OpenFlow. El grupo de trabajo de Pruebas e Interoperabilidad de ONF busca acelerar el desarrollo y la adopción de OpenFlow. Está creando activamente pruebas de conformidad, pero los detalles aún no se han entregado al público en general.

°Open Networking Foundation

3 CAPITULO 3: ANÀLISIS DEL PROBLEMA

En este capítulo, se plantea el problema identificado en la organización objetivo, analizando su alcance, causa e impacto en la organización. De igual manera, se describirá en detalle, el entorno donde será desplegada la solución y los requerimientos necesarios para cumplir con el tema propuesto.

3.1 Problema Identificado

La red de campus universitario presenta dificultad en la distribución del tráfico de datos (donde no existe un control unificado del consumo de ancho de banda) y una administración de red deficiente con muchos dispositivos de comunicación con características independientes por fabricante que dificultan su gestión y obtienen un rendimiento poco eficaz.

3.2 Análisis del Problema

La problemática identificada en el punto anterior se encuentra en un contexto en donde el ancho de banda posee deficiencias en su distribución para las áreas de trabajo que se transmite, a través de múltiples dispositivos de comunicación y que forman parte de la red LAN del campus universitario. Asimismo, existen problemas en la gestión de dicha red que son causados por factores internos y externos. Es decir, amenazas internas y externas que podrían comprometer los servicios utilizados por los usuarios como videoconferencia, acceso a navegación web, plataforma virtual de la organización, entre otros.

Para realizar el análisis de la problemática, se presentan varios puntos en la cual se realiza un diagnóstico de las posibles causas del problema identificado con anterioridad. Luego, se propone una matriz en donde se realiza una comparativa del problema, impacto y valoración que se podrían dar si no son tomadas las medidas necesarias para la solución del problema.

3.3 Campo de Estudio

El campo de estudio, se desarrolla en la red de un campus universitario en donde existe un centro de datos local ubicado dentro del mismo campus en el Área de TI. Este centro de datos contiene servidores que alojan servicios web, correo electrónico, archivos, telefonía IP, base de datos, entre otros. Además, se cuenta un router administrado por el

operador ISP de la organización, 1 firewall perimetral, conmutadores (switch core) en Virtual Chassis en alta disponibilidad y se maneja la configuración como un único switch. Lo mencionado, se complementa con conmutadores que tienen la función de switch de acceso a lo largo del campus universitario (ubicados en los diferentes pabellones y lugares en donde sea necesario su instalación). La red LAN se conecta mediante cableado de fibra óptica (desde el operador ISP hasta los conmutadores de Core y Acceso) y cableado de cobre de 1 Gbps (entre los conmutadores de acceso y los dispositivos de red/terminales). Esta velocidad en ciertas ocasiones puede saturarse debido a la cantidad de sesiones realizadas en el momento por usuarios, docentes y alumnos y como consecuencia, puede traer algún retardo o interrupción del servicio que brinda el campus universitario.

A nivel lógico, la red LAN esta segmentada por vlans basadas en nombres de los pabellones y laboratorios. Siendo el switch core quien administra todas las vlans y lo asocia con los switch de acceso para su correcta designación. No existen switches NO administrables en la red local, todos los equipos están configurados de manera que pueda evitar bucles, retardo y similares. Sin embargo, los conmutadores se encuentran fuera de garantía y desactualizados por lo que representa una vulnerabilidad que puede comprometer a la organización.

En referencia al personal, están distribuidos por perfiles como docentes, administrativos y estudiantes/alumnos asociados a servicios que brinda la universidad como Cibercampus, Intranet y plataformas que permitan interactuar entre ellos. Las reglas o políticas de seguridad son realizadas en los dispositivos perimetrales en base al perfil de cada uno de ellos (dentro del perfil docente existen tal cantidad de personas, lo mismo ocurre con administrativos y estudiantes), de tal manera que al configurar o agregar algo nuevo, no se vean afectados el resto de perfiles.

3.3.1 Deficiencias en la topología actual de la red LAN y dispositivos de comunicación con fallas y obsoletos

Actualmente, la red LAN del campus universitario está formada por un router (salida hacia internet), un firewall perimetral, switch core y switch de acceso. Esto nos indica, que no existe una jerarquía correcta en el diseño de la red y que sea capaz de administrar eficazmente la red de la organización. Se cuenta con un firewall totalmente desactualizado (sin poder agregar funcionalidades para una nueva configuración), un switch interno que solo interconecta los equipos entre aulas, pabellones y otras áreas.

Para el análisis de este problema, se muestra la topología de red actual del campus universitario.

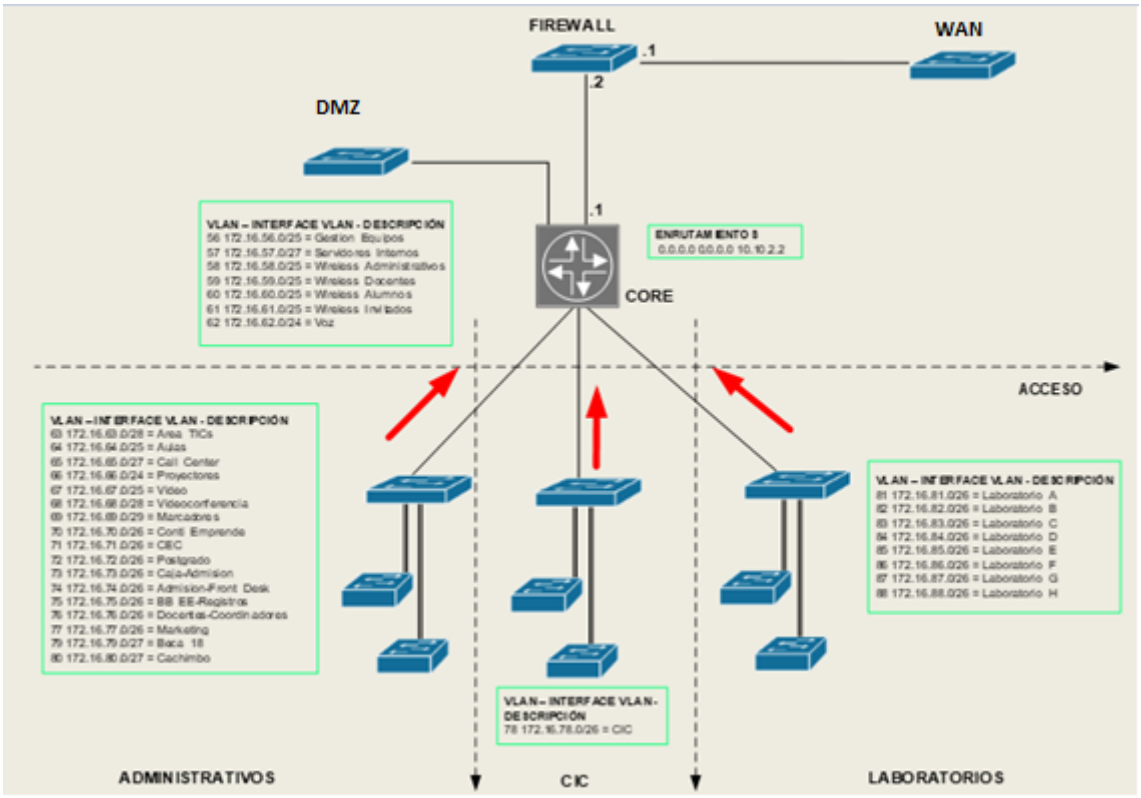


Figura 18: Topología de red actual del campus universitario

Fuente: Elaboración Propia

De la Figura 18, se puede destacar el enlace WAN que sostiene los 3 enlaces de internet hasta los switch de acceso explicados, una topología de red sencilla que no concuerda con las necesidades de la organización. Por ejemplo: se presenta una topología de red con niveles de core y acceso omitiendo el nivel de distribución que es su límite entre ambas. Entonces, la capa de núcleo y su conectividad se basa en políticas y entre ellas tenemos la conexión de redes locales independientes y controlar el tráfico que circula entre ellas.

La capa o nivel de distribución ausente en una topología de red llega a ser preocupante porque no hay un filtro del tráfico entrante y saliente para administrar la seguridad y el tráfico en mención. Asimismo, los segmentos de red están asociados a un único switch core y tampoco posee una red estable Por ello, ante una nueva estructura de red con tecnología sofisticada; la topología de red actual tendría que sufrir modificaciones para

poder mejorar por completo (empezando por el estado de los elementos de red que lo conforman hasta los requerimientos necesarios para su puesta en producción).

Por otro lado, los dispositivos de comunicación adquiridos por la organización son colocados sin una evaluación adecuada omitiendo las necesidades que requiere la red. La organización no cuenta con un estándar para la adquisición de los dispositivos de comunicación, por lo que la red local trabaja con equipos de diferentes marcas. Entre estos podemos nombrar a los conmutadores, los cuales tienen la tarea de interconectar los distintos equipos de red.

Entre los conmutadores desactualizados en cada área de trabajo y de diferentes características, se presentan los siguientes:

Figura 19: Actualmente Switch 3COM Baseline Plus 2952 descontinuado y sin actualización alguna

Figura 20: Juniper EX2200 24 T se encuentra descontinuado y sin actualización

Figura 21: 3COM Baseline totalmente descontinuado y sin actualización.

En las figuras 19, 20 y 21, se puede observar que los conmutadores están totalmente obsoletos y sin ningún respaldo del fabricante. Estos equipos, se encuentran ubicados en cada área de la organización de forma “standalone” (es decir, instalado únicamente sin otro equipo del mismo fabricante como respaldo). Lo mencionado genera una posible interrupción total de comunicación en una determinada área de trabajo de la red LAN, debido a que no existe un stack o tecnología de chassis que pueda soportar la interrupción de la red e inmediatamente después de forma automática, no paralice la comunicación sino siga funcionando sin alteraciones. Otra forma, es reemplazando el conmutador con falla por otro dispositivo de otra marca.

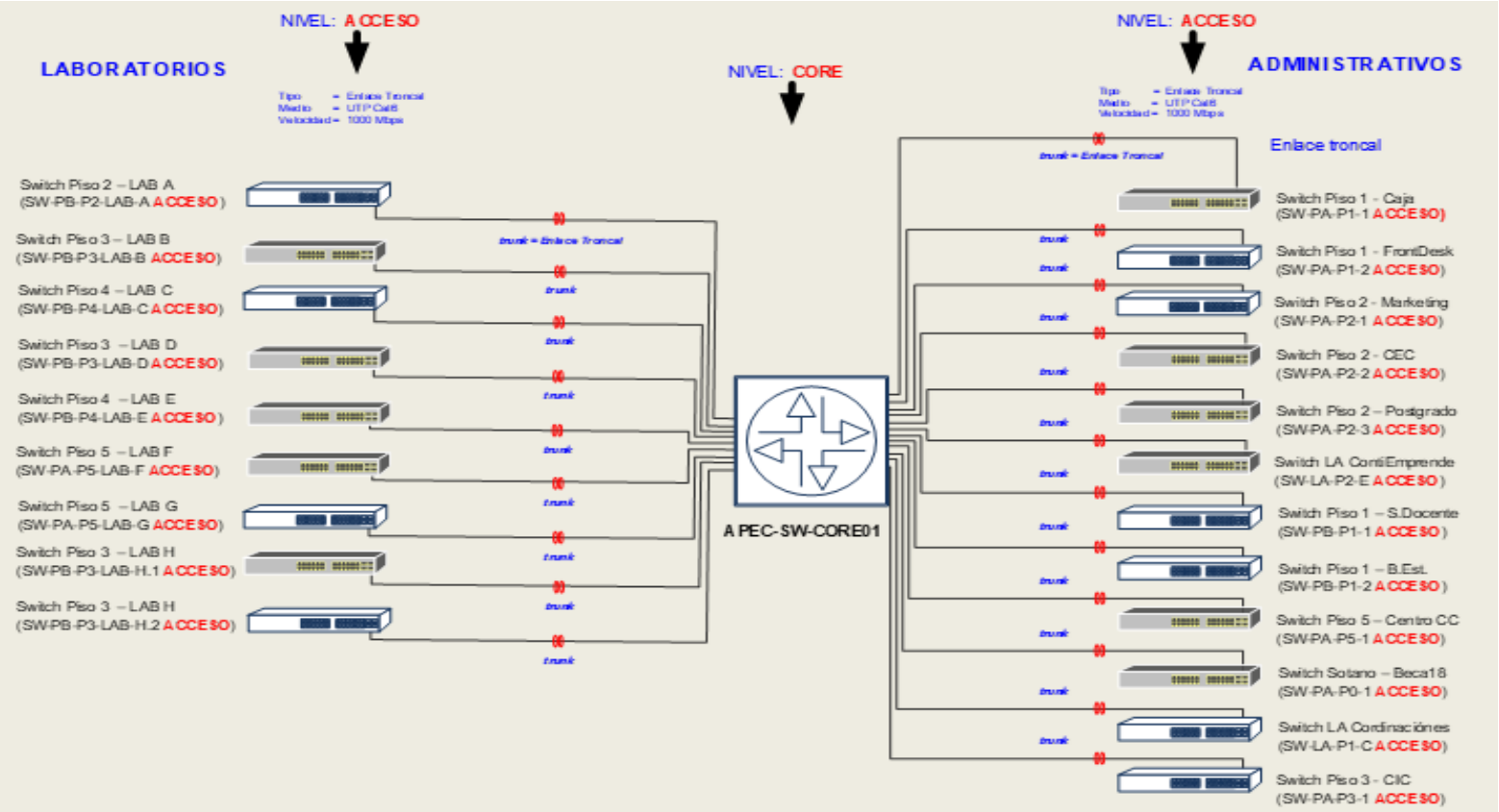


Figura 22: Topologia de Red en relación a la diversidad de conmutadores en la red del campus universitario

Fuente: Elaboración propia

En la Figura 22, se observan los dispositivos de red de las áreas de laboratorios y administrativos conectados directamente a un switch central, lo que refleja una topología de red con switches de acceso y core con diversas marcas. Por ejemplo: Los switch de color rojo representan a la marca 3COM Baseline y los switch de color azul son HP V1910. A continuación, se propone una tabla con los dispositivos de red desactualizados y otras características, basado en la topología de red actual.

DISPOSITIVO (SWITCH)	USO O ÁREA DE APLICACIÓN	CANTIDAD	ANTIGÜEDAD	FUNCION	ESTADO
3COM Baseline Switch 2952-SFP	CAJA (PISO 1)	1	7 años	SW-ACCESO	SIN SOPORTE
3COM Baseline Switch 2952-SFP	SERVICE DESK	1	7 años	SW-ACCESO	SIN SOPORTE
HP V1910-48G Switch JE009A	PLATAFORMA	2	6 años	SW-ACCESO	SIN SOPORTE
Baseline Switch 2924-SFP Plus	POSTGRADO (PISO 1)	2	6 años	SW-ACCESO	SIN SOPORTE
HP V1910-48G Switch JE009A	PABELLON F_ADM	2	6 años	SW-ACCESO	SIN SOPORTE
Juniper EX2200-24T Series	PABELLON F_AULAS	2	7 años	SW-ACCESO	SIN SOPORTE
HP V1910-48G Switch JE009A	LABORATORIO A (PISO 2)	1	6 años	SW-ACCESO	SIN SOPORTE
3COM Baseline Switch 2952-SFP	LABORATORIO B (PISO 3)	1	7 años	SW-ACCESO	SIN SOPORTE
HP V1910-48G Switch JE009A	LABORATORIO C (PISO 4)	1	6 años	SW-ACCESO	SIN SOPORTE
3COM Baseline Switch 2952-SFP	LABORATORIO D (PISO 3)	1	7 años	SW-ACCESO	SIN SOPORTE
3COM Baseline Switch 2952-SFP	LABORATORIO E (PISO 4)	1	7 años	SW-ACCESO	SIN SOPORTE
3COM Baseline Switch 2952-SFP	LABORATORIO F (PISO 5)	1	7 años	SW-ACCESO	SIN SOPORTE
HP V1910-48G Switch JE009A	LABORATORIO G (PISO 3)	1	6 años	SW-ACCESO	SIN SOPORTE
Baseline Switch 2924-SFP Plus	LABORATORIO H (PISO 3)	2	6 años	SW-ACCESO	SIN SOPORTE
Baseline Switch 2924-SFP Plus	PABELLON F_401_SC	1	6 años	SW-ACCESO	SIN SOPORTE
Juniper EX2200-24T Series	PABELLON F_302_SC	1	7 años	SW-ACCESO	SIN SOPORTE
Juniper EX2200-24T Series	PABELLON F_301_SC	1	7 años	SW-ACCESO	SIN SOPORTE
3COM Baseline Switch 2952-SFP	PABELLON F_202_SC	1	7 años	SW-ACCESO	SIN SOPORTE
Juniper EX2200-24T Series	PABELLON F_201_SC	1	7 años	SW-ACCESO	SIN SOPORTE
3COM Baseline Switch 2952-SFP	INFRAESTRUCTURA	1	7 años	SW-ACCESO	SIN SOPORTE
Juniper EX2200-24T Series	DIRECCIÓN TI	1	7 años	SW-ACCESO	SIN SOPORTE
HP V1910-48G Switch JE009A	CIC (PISO 1)	2	6 años	SW-ACCESO	SIN SOPORTE

Tabla 2: Lista de los dispositivos de red de la topología actual del campus universitario
Fuente: Elaboración propia

En la Tabla 2, se muestra la lista de los equipos desactualizados donde se indica el área de aplicación, la antigüedad, función y el estado actual. Esta lista, se debe considerar en caso se realice un cambio o se elimine un equipo en la topología de red.

3.3.2 Inadecuada distribución de ancho de banda en las áreas de trabajo

En cuanto a la distribución del ancho de banda. El campus universitario cuenta hasta con 3 proveedores de servicio de internet (ISP), con el fin de distribuir eficazmente el ancho

de banda para las áreas o servicios que lo requieran. Sin embargo, esto no se ha podido ver reflejado sobre los usuarios finales, ya que persisten inconvenientes que impiden desarrollar sus actividades con normalidad.

Para ello, se realizará un análisis desde los enlaces hasta la categoría y usuarios que utilizan con mayor frecuencia el ancho de banda sin restricción alguna.

Name	Location	Members Count	Addresses
Grupo_Movistar		38	red_172.16.10.0 red_172.16.11.0 red_172.16.12.0 red_172.16.13.0 red_172.16.14.0 red_172.16.15.0 red_172.16.16.0 more...
Grupo_Fiberlux		22	red_172.16.121.0 red_172.16.122.0 red_172.16.123.0 red_172.16.22.0 red_172.16.23.0 red_172.16.24.0 red_172.16.27.0 more...
MPLS_LIMA		8	10.10.5.0 172.16.101.0 172.16.102.0 172.16.103.0 172.16.104.0

Figura 23: Enlaces Movistar, Fiberlux, MPLS del operador ISP (Campus universitario)

Fuente: Reporte de equipo perimetral PA

En la Figura 23, podemos observar que existen grupos por cada enlace mencionado. Por ejemplo: el Grupo Movistar contiene hasta 38 segmentos de red que trabajan, lo mismo sucede con el Grupo Fiberlux que contiene hasta 22 segmentos de red y el Grupo MPLS con 8 segmentos. Todo ellos están declarados en el equipo perimetral.

Ahora veremos la regla aplicada para estos grupos, tomando como ejemplo el Grupo Fiberlux y como está declarado en el dispositivo.

		Source			Destination			
Name	Tag	Zone/Interface	Address	User	Address	Application	Service	Action
Lan_to_Enlace_Fiberl...	none	LAN	Grupo_Fiberlux	any	~~Grupo_Fiberlux~~ ~~Grupo_Movistar~~ ~~MPLS_AREQUIPA~~ ~~MPLS_LIMA~~ ~~Red-DMZ~~	any	any	forward

Figura 24: Regla LAN-to-Enlace Fiberlux

Fuente: Reporte de equipo perimetral PA

En la Figura 24, podemos verificar que la regla LAN-to-Enlace-Fiberlux aplica la salida de las redes internas declaradas hacia el enlace Fiberlux. Si bien esta regla ayuda en la distribución de los segmentos de red y el ancho de banda, ello no implica que no se presente alguna saturación o lentitud en la red LAN. Debido a la parte de "application", este se encuentra en "any" por lo que sin importar que tipo de servicio o acceso se use, el tráfico seguirá incrementándose.

Mencionaremos la cantidad de Megabytes contratado por la organización términos de ancho de banda.

SEDE	OPERADOR DE INTERNET	CANTIDAD DE MB	REDES INTERNAS
RED LAN DEL CAMPUS UNIVERSITARIO	MOVISTAR	150 MB	Todas las redes con excepción de Aulas y Labs
	FIBERLUX	100 MB	Redes de Aulas y Laboratorios
	MPLS-LIMA	80 MB	Redes de Servidores, Desarrollo e Infraestruc.
	ENLACE-BCKP	50 MB	Sin uso

Tabla 3: Cantidad de MB contratados por el campus universitario

Fuente: Elaboración propia

En la Tabla 3, se puede revisar la cantidad de ancho de banda asociado a cada operador de internet. El enlace-bckp es un enlace que ha sido dado de baja, pero para un historial se refleja en la tabla mencionada. Estos enlaces son gestionados por el equipo perimetral quien se encarga de dirigir la salida a la WAN de los segmentos de red internos.

Continuando con el análisis, pasaremos a observar el consumo que genera actualmente la red LAN.

Figura 25: Resumen total del consumo de ancho de banda en el campus universitario
Fuente: Report_EX_APEC

En la Figura 25, se puede observar el consumo masivo del ancho de banda generado por diferentes categorías. Por ejemplo, en el Top 8 de Aplicaciones Internas más utilizadas tenemos 39 Gb como indicador Inbound de uso por los usuarios. A diferencia de los 13 Gb utilizados por el tipo Outbound, esto representa un consumo excesivo si lo vemos por aplicación o categoría.

En la pestaña “Recreational” se menciona una lista con las categorías más utilizadas, lo cual desglosaremos en la siguiente Tabla 8, el cual nos indicará las aplicaciones/servicios utilizados por los laboratorios y cuales no deberían ser usadas.

LABORATORIOS	APLICACIONES/SERVICIOS PERMITIDOS	APLICACIONES/SERVICIOS USADOS	TOTAL DE SERVICIOS (SIN PERMISO)
LABORATORIO A	Descargas, Cibercampus, Navegación Web y herramientas de cursos	Streaming, Messenger, Descargas, Juegos, Redes Sociales	4 servicios que no deberian ser usados
LABORATORIO B	Descargas, Cibercampus, Navegación Web y herramientas de cursos	Streaming, Messenger, Descargas, Juegos, Redes Sociales	4 servicios que no deberian ser usados
LABORATORIO C	Descargas, Cibercampus, Navegación Web y herramientas de cursos	Streaming, Messenger, Descargas, Juegos, Redes Sociales	4 servicios que no deberian ser usados
LABORATORIO D	Descargas, Cibercampus, Navegación Web y herramientas de cursos	Streaming, Messenger, Descargas, Juegos, Redes Sociales	4 servicios que no deberian ser usados
LABORATORIO E	Descargas, Cibercampus, Navegación Web y herramientas de cursos	Streaming, Messenger, Descargas, Juegos, Redes Sociales	4 servicios que no deberian ser usados
LABORATORIO F	Descargas, Cibercampus, Navegación Web y herramientas de cursos	Streaming, Messenger, Descargas, Juegos, Redes Sociales	4 servicios que no deberian ser usados
LABORATORIO G	Descargas, Cibercampus, Navegación Web y herramientas de cursos	Streaming, Messenger, Descargas, Juegos, Redes Sociales	4 servicios que no deberian ser usados
LABORATORIO H	Descargas, Cibercampus, Navegación Web y herramientas de cursos	Streaming, Messenger, Descargas, Juegos, Redes Sociales	4 servicios que no deberian ser usados

Tabla 4: Aplicaciones/servicios de los laboratorios del campus universitario

Fuente: Elaboración propia

En la Tabla 4, se observa las aplicaciones o servicios que utiliza cada laboratorio dentro del campus (asociado al resumen de la Figura 38 y la estadística de la Figura 39), se puede determinar que hay 4 servicios que son usados de manera libre y sin filtros. Esto lleva a un consumo mayor de ancho de banda que no se tiene previsto en la universidad y por ello, se presentan inconvenientes en otras áreas de trabajo. Por ejemplo, las aplicaciones o servicios permitidos en los laboratorios son descargas de archivos, páginas web de la universidad, navegación web en general y herramientas del curso que se requiera en el momento.

Por otro lado, las aplicaciones o servicios no permitidas son Streaming, Messenger, descargas peer-to-peer, juegos y redes sociales que no tienen un filtro adecuado y puede conectarse cualquier usuario que ingrese al laboratorio respectivo, generando un consumo mayor de ancho de banda en la red.

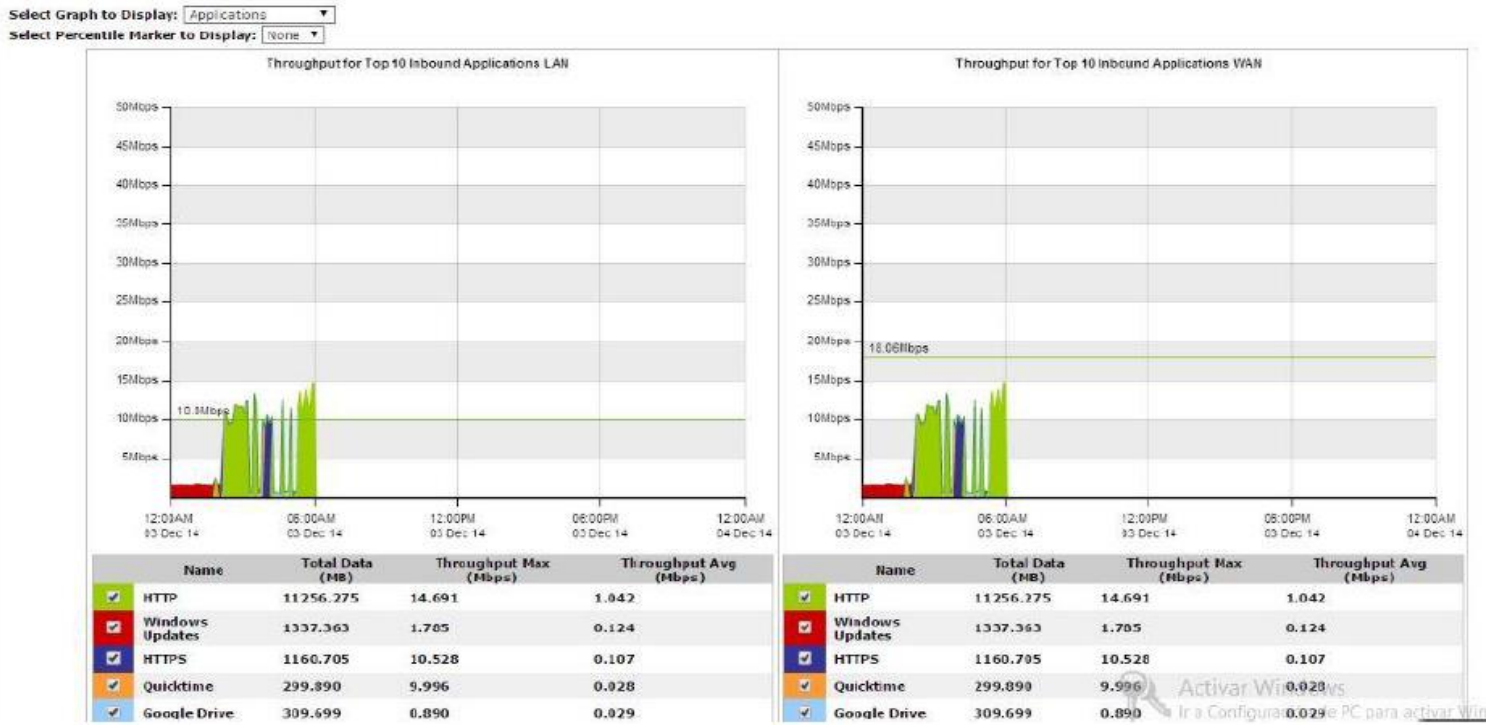
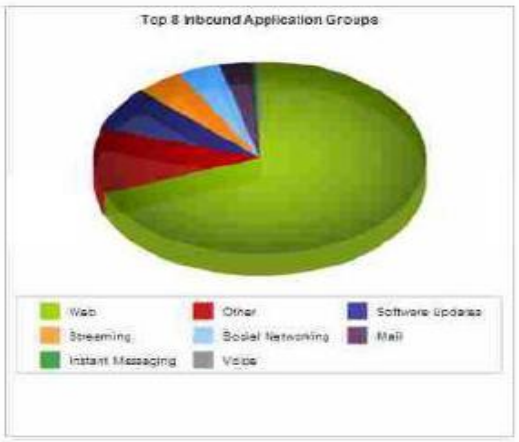
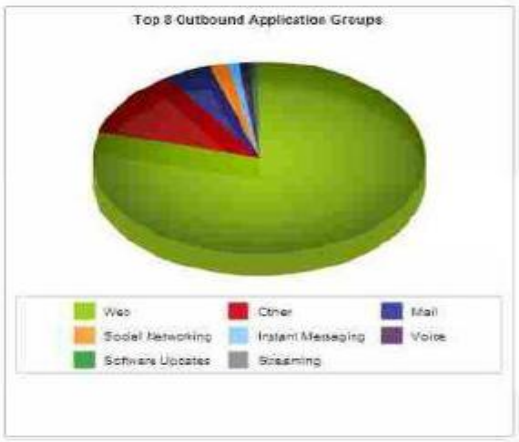


Figura 26: Estadística del consumo de las categorías/aplicaciones en tiempo real del campus universitario

Fuente: Report_EX_APEC

En la Figura 26, se muestra categorías de mayor consumo. Por ejemplo, el tráfico HTTP por el color representado indica que tiene un uso excesivo entre las horas promedio, al igual que HTTPS contienen un consumo elevado sea por navegación web, visibilidad de videos, streaming o incluso por descargas de todo tipo.





Top 30 Inbound Application Groups

Name [+] Show Details	Packets	Data (MB)	Throughput (kbps) Average	Max	Flows
Web	37111058	41489.812	125.77	10345.52	16790
Other	5930775	6657.614	94.82	9616.54	1738
Software Updates	3078964	4378.286	503.32	11510.63	394
Streaming	2037813	2812.427	288.35	8932.62	352
Social Networking	2552712	2484.914	35.81	1474.34	2848
Mail	2528149	1912.144	17.49	3770.98	1897
Instant Messaging	573452	247.675	5.69	1108.54	1738
Voice	515152	188.658	51.12	2584.63	394
Thin Client	164633	85.679	50.73	159.8	

Figura 27: Top de las aplicaciones/categorías con mayor uso a nivel throughput

Fuente: Report_EX_APEC

La Figura 27, nos muestra una lista de las aplicaciones más utilizadas. En este caso, el tráfico web es lo que representa el mayor consumo tanto de entrada como de salida, generando posible saturación o lentitud en las horas de trabajo y como lo indicamos anteriormente, no hay un control unificado o distribución correcta del ancho de banda por más que estén bloqueadas algunas aplicaciones.

En referencia a la Figura 40, el reporte indica específicamente el top de aplicaciones/categorías con mayor uso. Sin embargo, para entenderlo en detalle se propone las políticas de la organización y como está distribuido por el tipo de perfil de usuario (docente, administrativos y alumnos), En donde se establecen 11 categorías de acceso, esto con la finalidad de agrupar usuarios y delimitar los accesos según sus necesidades.

CATEGORIA 1 C1	CATEGORIA 2 C2	CATEGORIA 3 C3	CATEGORIA 4 C4	CATEGORIA 5 C5	CATEGORIA 6 C6	CATEGORIA 7 C7	CATEGORIA 8 C8	CATEGORIA 9 C9	CATEGORIA 10 C10	CATEGORIA 11 C11
Servicio de la CEC	C1	C2	C3	C4	C4	C6	C6	C6	C9	Internet Privilegiado
	Internet									
		Gubernamentales								
			Bancos							
				FTP	Prensa Escrita					
						Redes Sociales	Media - Audio/Video	Redes Sociales		
								Media - Audio/Video		
									Aplicaciones	
CUSTOM C 1	CUSTOM C 2	CUSTOM C 3	CUSTOM C 4	CUSTOM C 5	CUSTOM C 6	CUSTOM C 7	CUSTOM C 8	CUSTOM C 9	CUSTOM C 10	CUSTOM C 11

Tabla 5: Clasificación de categorías para el perfil de usuario administrativo

Fuente: Elaboración propia

Como indica la Tabla 5, el perfil de usuario administrativo debe trabajar entre la categoría 1 al 11, esto basado en el tipo de persona administrativa. En donde algunos como el área de caja que ingresa a bancos y web similares, entonces trabajará con el perfil de categoría C4 y asi sucesivamente con otros usuarios que se encuentran dentro del perfil

administrativos. Por otro lado, los usuarios docentes y estudiantes se establecen en 10 categorías de acceso con la finalidad de agrupar laboratorios y delimitar acceso según las necesidades de los cursos que lo requieran como se muestra en la siguiente tabla:

CATEGORIA 0 C0	CATEGORIA 1 C1	CATEGORIA 2 C2	CATEGORIA 3 C3	CATEGORIA 4 C4	CATEGORIA 5 C5	CATEGORIA 6 C6	CATEGORIA 7 C7	CATEGORIA 8 C8	CATEGORIA 9 C9	CATEGORIA 10 C10
RESTRINGUIDOS	Servicio de la CEC	C1	NO DEFINIDO	NO DEFINIDO	NO DEFINIDO	C2	NO DEFINIDO	C6	NO DEFINIDO	NO DEFINIDO
		Internet				Comercio				
		Guberbamentales				Negocios		Media - Audio/Video		
CUSTOM C 0	CUSTOM C 1	CUSTOM C 2	CUSTOM C 3	CUSTOM C 4	CUSTOM C 5	CUSTOM C 6	CUSTOM C 7	CUSTOM C 8	CUSTOM C 9	CUSTOM C 10

Tabla 6: Clasificación de categorías por perfil de usuario (docente y alumnos)
Fuente: Elaboración propia

Las categorías de la Tabla 6, hacen referencia a los docentes y alumnos, la cual ha sido diseñada por la organización en donde se distinguen dos tipos de políticas.

- Políticas de restricción en los segmentos de red de aulas y laboratorios que permita garantizar el rendimiento del servicio de internet.
- Políticas basadas en un ancho de banda determinado para los segmentos de red.

Entonces, se trabaja de igual manera que el perfil de tipo administrativo en donde en tal horario, el laboratorio A puede hacer uso de Audio/Streaming y esto corresponde a la categoría 8.

Lo mencionado entre los dispositivos desactualizados y el consumo de ancho de banda, es reflejado en algunos equipos de red en donde se hicieron mediciones en las áreas de trabajo (los números mostrados en rojo son producto de errores y otros problemas asociados a estos dispositivos), su porcentaje de disponibilidad y tráfico de datos.

DISPOSITIVOS DE RED	INTERFACE	PACKETS SENT	PACKETS LOST	TIME UNAVAILABLE (Minutes)	PERCENT AVAILABLE
SW_PABELLON_F_ADM	LOCAL	894	9	1	99,96
SW_PABELLON_F_AULAS	LOCAL	603	156	491,9	73,11
SW_PABELLON_PLATAFORMA	LOCAL	837	321	1041,42	60,5
SW_PABELLON_F_60X	LOCAL	837	17	20,99	99,2
SW_PABELLON_F_50X	LOCAL	600	135	521,22	71,22
SW_PABELLON_F_40X	LOCAL	606	165	511,2	72,32
SW_PABELLON_F_30X	LOCAL	735	240	625,3	77,11
SW_PABELLON_F_20X	LOCAL	680	185	675,4	69,8

DESEMPEÑO	%
ÓPTIMO	90-100
REGULAR	70-80
DEFICIENTE	50-60

Tabla 7: Medición de desempeño de los dispositivos de red en la red de campus universitario

Fuente: Elaboración propia en base a Ping Availability

En la Tabla 7, se puede verificar algunos conmutadores asociados a las áreas de trabajo con su respectivo reporte de tráfico como paquetes enviados, pérdidos e interrupción en minutos. Cabe mencionar, que estos resultados son tomados de manera anual por lo que estas medidas son del año pasado (2019). El segmento SW_PABELLON_F_PLATAFORMA, se refiere a que presenta una tasa de disponibilidad muy baja (marcado de color rojo en la tabla); por lo que necesita una atención inmediata y en la parte inferior, se observa el criterio de desempeño aprobado por la organización como parámetros de medición.

3.4 Causas del Problema

En esta parte, se relacionarán los problemas identificados con las causas que lo originan, si bien se mencionaron los problemas, estos serán colocados en una matriz seguido de las causas para un mejor entendimiento.

PROBLEMAS IDENTIFICADOS	CAUSAS
Dispositivos de comunicación con fallas y obsoletos	1- Falta de mantenimiento y actualización en los dispositivos. 2- Dispositivos adquiridos sin estudio previo al crecimiento de los usuarios 3- Mal diseño inicial de los dispositivos de comunicación sobre la red LAN
	4- Al manejar múltiples dispositivos de comunicación, ocasionan diversas tareas de gestión de acceso 5- Las tareas de soporte TI se realizan en los equipos de los usuarios y algunas veces sobre los dispositivos de comunicación y las tareas de mantenimiento de la infraestructura local son extensas al manejar una diversidad de equipos con problemas
Inadecuada distribución de ancho de banda en las áreas de trabajo	1- En el campus universitario, existe saturación de la red por el uso de aplicaciones/categorias sin medición de ancho de banda 2- No existe control del tráfico o reglas sobre las áreas de trabajo para medir su uso excesivo.
Deficiencia en la topología actual de la red LAN	1- Dispositivos de comunicación como switches cumpliendo el rol de distribución y acceso; y también el switch core como único elemento importante se encuentra sin respaldo actual 2- Equipo perimetral encargado de administrar 3 enlaces sin la capacidad suficiente para cumplir el rol y no controlar el tráfico

Tabla 8: Matriz del problema y las causas que lo generaron

Fuente: Elaboración propia

3.5 Impacto del Problema

Para una mejor evaluación del impacto, se propone una tabla a fin de establecer un valor a cada problema identificado.

IMPACTO	DESCRIPCIÓN	VALOR
GRAVE	De presentarse el problema, este tendría un alto impacto en la Universidad Continental	ALTO
MODERADO	De presentarse el problema, este tendría un impacto medio en la Universidad Continental	MEDIO
LEVE	De presentarse el problema, este tendría un bajo impacto en la Universidad Continental	BAJO

Tabla 9: Valoración de Impacto

Fuente: Elaboración Propia

A continuación, se mencionarán los problemas identificados con el impacto que ocasionaría la aplicación de cada uno. Además, se colocará una valorización al impacto de acuerdo a la percepción de la organización (Impacto grave, moderado y leve).

PROBLEMAS IDENTIFICADOS	IMPACTO	VALOR
Dispositivos de comunicación con fallas y obsoletos	1- Paralización de las actividades de trabajo de los usuarios	ALTO
	2- Demora para los usuarios en encontrar una solución de respaldo ante el problema ocurrido	MEDIO
	3- Mala imagen institucional en temas de infraestructura tecnológica	ALTO
	4- Posible rotación de personal del área de Soporte TI por el exceso de horas que necesitan para atender el inconveniente reportado	MEDIO
	5- Posibilidad de pago de horas extra para las áreas de TI sobre cumplir todas las funciones del área y los problemas reportados	BAJO
	6- Gastos extra en recursos de la red LAN para mantener operativo los servicios en general	MEDIO
Inadecuada distribución de ancho de banda en las áreas de trabajo	1- Saturación total en la red LAN por el consumo excesivo de ancho de banda	ALTO
	2- Horas extra en los usuarios de las áreas de trabajo para terminar sus actividades por la paralización de un determinado servicio	MEDIO
	3- Peligro de amenaza al no tener control sobre el uso del ancho de banda y ante ello, los usuarios pueden estar expuestos externamente	MEDIO
Deficiencia en la topología actual de la red LAN	1- Equipos de comunicación que pueden dejar de funcionar por los distintos roles que cumplen hasta la fecha	ALTO
	2- Capacidad insuficiente de la red ante nuevos requerimientos que puedan surgir en la organización	MEDIO

Tabla 10: Matriz de Impacto de los problemas identificados

Fuente: Elaboración propia

3.6 Lista de Interesados

Para realizar el análisis y definición de los requerimientos del proyecto, se deben identificar los interesados del proyecto y luego se definirán los requerimientos que serán propuestos para la solución final.

Interesados	Cargo	Organización a que pertenece	Categoría de interesado	Nivel interés (Bajo, Medio, Alto)	Nivel influencia (Bajo, Medio, Alto)
Luis Contreras	Gerente de TI	Campus Universitario	Patrocinador	Alto	Alto
Usuarios administrativos y estudiantes	Terceros	Campus Universitario	Cliente	Medio	Medio
Jefes de Áreas de Trabajo	Jefes de Áreas	Campus Universitario	Usuario	Alto	Medio
José Barrios	Gerente Ejecutivo	Campus Universitario	Alta Dirección	Medio	Alto
Sunedu	Organismo Público	Sunedu	Entidad reguladora	Bajo	Medio
José Guardia	Sub-Gerente Comercial	Proveedores de Campus Universitario	Proveedor	Medio	Alto
Angel Dávila	Administrador de TI	Campus Universitario	Director Proyecto	Alto	Alto
Carlos Carrascal	Analista de TI	Campus Universitario	Miembro proyecto	Alto	Medio

Tabla 11: Lista de Interesados del proyecto

Fuente: Elaboración propia

3.7 Toma de Requerimientos

A continuación, se observará en detalle los requerimientos planteados en base al análisis desarrollado a través de la siguiente tabla:

OBJ. ESPECIFICO	NRO REQUERIMIENTO	REQUERIMIENTO	INTERESADO
OE1	1	En base a las politicias o categorias de acceso por tipo de usuarios, se debe determinar la cantidad de tráfico adecuada para cada uno de ellos	Administrador de TI, Analista de TI y Proveedor de UC
	2	Determinar si el uso de los 3 enlaces de internet (ancho de banda) son suficientes. En todo caso, la solución debe ser capaz de distribuir correctamente el consumo realizado por los usuarios	Administrador de TI y Analista de TI
OE2	3	El requerimiento es poder reducir los tiempos de acceso a un recurso de TI o dispositivo de red	Administrador de TI, Jefes de Área, Usuarios Adm. Y Estudiantes
	4	Lograr mantener la visibilidad y comunicación de todos los dispositivos de red sin interrupción alguna a través de la solución	Administrador de TI, Jefes de Áreas
OE3	5	La necesidad de contar con una solución basada en un ambiente virtual que permita flexibilidad, sin depender únicamente de hardware y poder gestionar de manera unificada	Administrador de TI, Jefes de Área, Usuarios Adm. Y Estudiantes
	6	La organización busca tener una red capáz de soportar un crecimiento constante de usuarios y para ello, requiere una infraestructura de red adecuada y escalable	Administrador de TI, Jefes de Áreas

Tabla 12: Lista de requerimientos del proyecto

Fuente: Elaboración propia

4 CAPITULO 4: DISEÑO DE LA SOLUCIÓN

En este capítulo, la propuesta del diseño de red definida por software será desarrollada, en donde se elaborarán las especificaciones y seleccionarán los recursos que logren cumplir el diseño de la solución.

4.1 Descripción

Teniendo en cuenta los requerimientos del capítulo anterior, se definen las especificaciones de una red definida por software sobre la red LAN del campus universitario. Estas especificaciones deben cumplir con los requerimientos previamente establecidos, los cuales buscan solucionar los problemas identificados en el proyecto.

El método para realizar el desarrollo de las especificaciones, serán obtenidos partiendo de los requerimientos y resultados definidos anteriormente en el capítulo 3, como determinar el consumo del ancho de banda, el monitoreó de los equipos de red y características de cada uno de ellos y adicional a lo mencionado, se logró verificar las políticas en base a categorías de uso para determinar el tráfico de los servicios actuales que generan consumo de red en la organización.

Previo al desarrollo de los requerimientos, se procede a observar la topología de red actual del campus universitario, el cual será nuestro punto de partida. (Ver Figura 45).
Asimismo, se podrá determinar el cálculo de ancho de banda para cada servicio de red que utilizan los usuarios finales en la organización. Viendo en detalle las fórmulas aplicadas bajo el enfoque de calidad propuesto en este proyecto (evaluando los enlaces de internet actuales y si son suficientes para soportar la demanda actual). Por otro lado, se establecerán perfiles a los usuarios distinguidos por área de trabajo o carrera y también, se diseñará nuevos dispositivos de red en donde se necesite para que pueda complementar la solución propuesta a este proyecto.

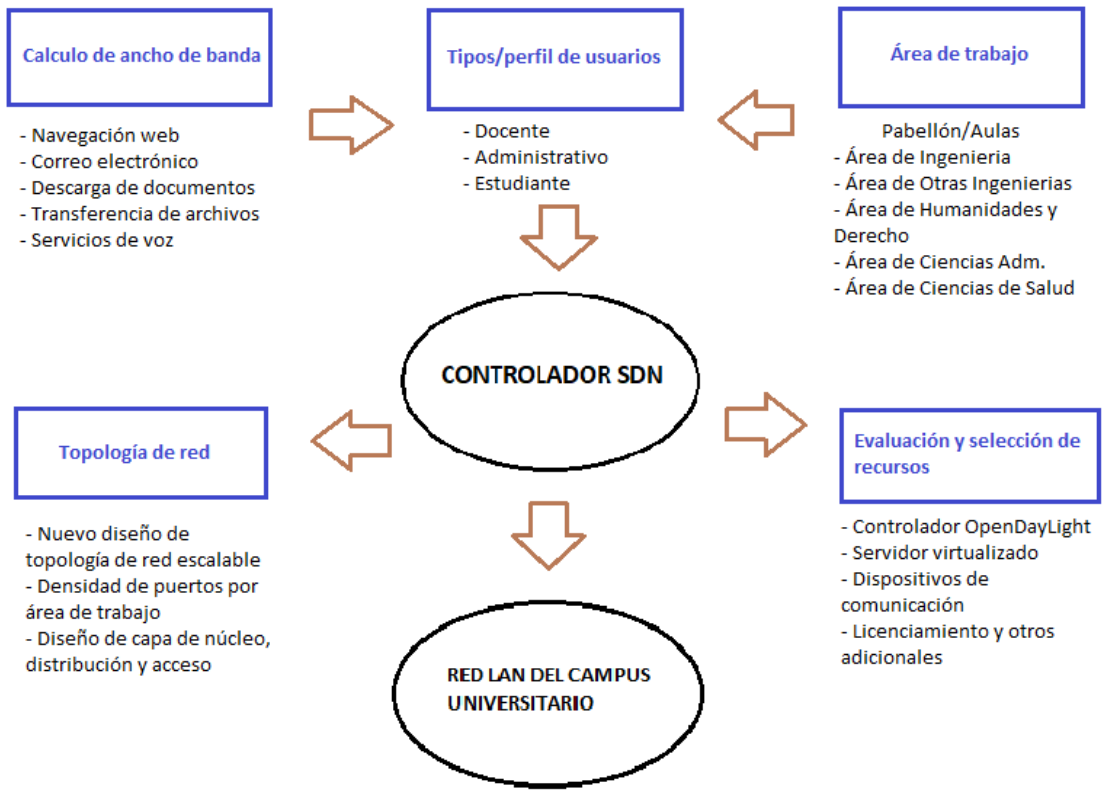


DIAGRAMA DE LA ESTRUCTURA DEL DISEÑO DE PROYECTO

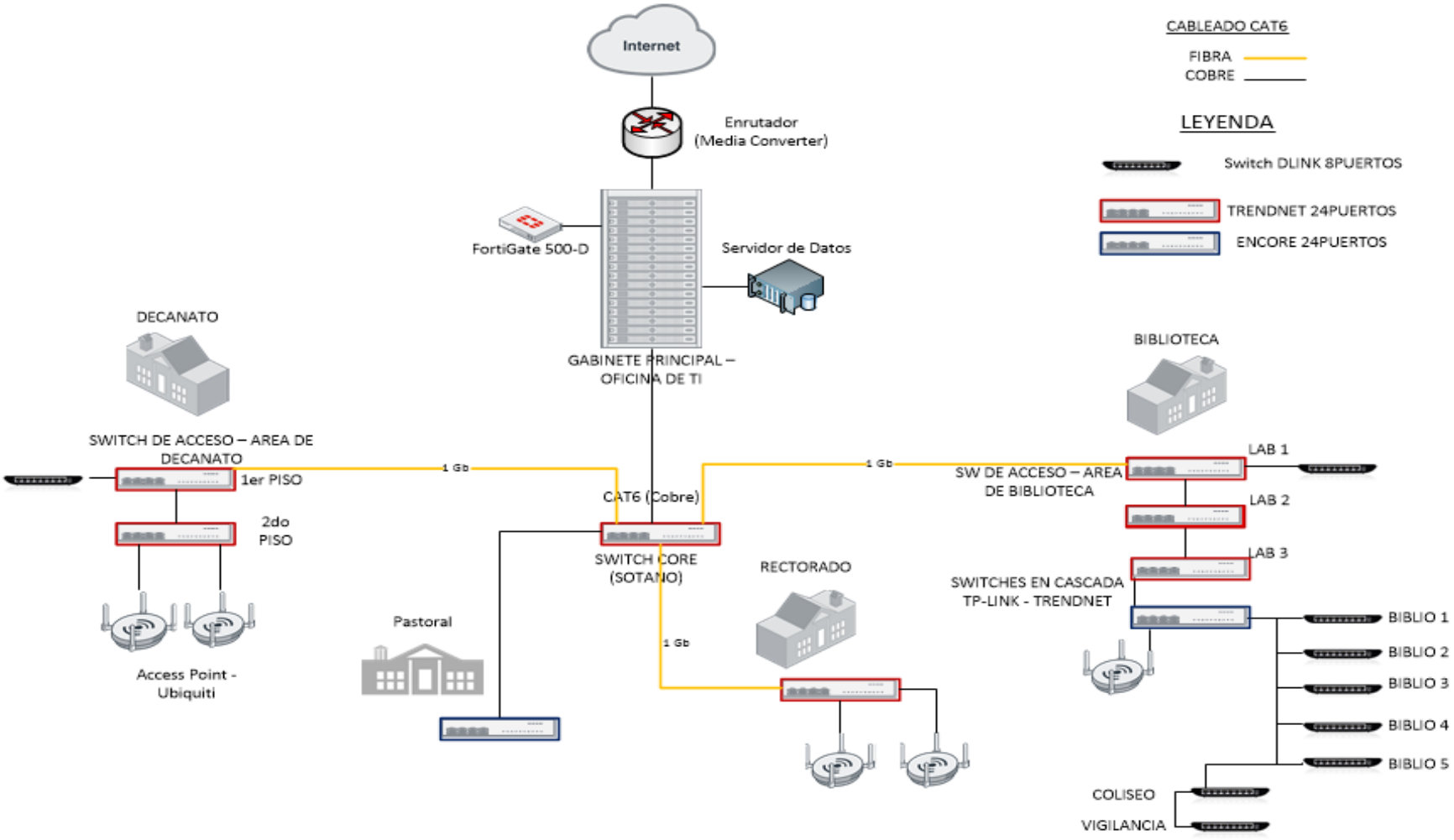


Figura 28: Topología de red del campus universitario

En la Figura 28, se puede observar la topología de red actual donde se utiliza fibra óptica de manera externa e internamente se maneja por cobre. Las áreas de trabajo están diseñadas bajo una topología estrella distribuida y de tal manera, se puede agregar tráfico a mayor velocidad hacia el nodo central.

Empezando por el controlador SDN, se propone sus cálculos en función de la cantidad de switches que posee la organización y también tendrá el control del ancho de banda. Mientras el router, se encargará de sus funciones de enrutamiento.

Como indica OpenDayLight en su documentación oficial es necesario aplicar cálculos sobre el ancho de banda en las áreas de trabajo del entorno universitario. Con los datos obtenidos en este proyecto y con los resultados se aplicarán en el API correspondiente del prototipo SDN propuesto.

Para hallar el cálculo de la velocidad de transmisión por carrera o área de trabajo. Será aplicada mediante la siguiente fórmula:

$$AB_{promedio} = \frac{AB}{\#\ estaciones}$$

ÁREA DE TRABAJO	DISTRIBUCION DE ANCHO DE BANDA	Nro. DE CONEXIONES	VELOCIDAD DE TRANS. POR CONEXIÓN
Pab_F_Ingeniería	17 MB	60	1,33 MB
Pab_Otras_Ingenierías	20 MB	95	0,94 MB
Pab_ Humanidades y Derecho	10 MB	50	1,60 MB
Pab_ Ciencias de Administración y Emp.	20 MB	78	1,23 MB
Pab_ Ciencias de la Salud	20 MB	56	1,43 MB
TOTAL	87 MB	339	6,53 MB

Tabla 13: Áreas de trabajo para el cálculo de ancho de banda

Fuente: Elaboración propia

En la Tabla 13, se observa las áreas de trabajo involucradas en el cálculo del ancho de banda a través del controlador SDN. Incluye el número de conexiones y velocidad de

transmisión actuales. Desde este punto partiremos e iremos desglosando los cálculos respectivos.

4.2 Cálculo de ancho de banda requeridos en la red LAN

En esta sección, se describen los servicios más importantes que consumen el ancho de banda del Internet en el campus universitario. La siguiente Figura 47, nos muestra en porcentaje la concurrencia en el uso de los diferentes tráficos que utilizan el internet. La navegación web es el tipo de tráfico con más frecuencia ya que este es utilizado por todos los usuarios de la red, su porcentaje de uso con referencia a los demás tráficos es de 28%. Le revisión de correo electrónico implica un porcentaje de uso del 26%, este servicio es utilizado por la mayoría de usuarios. La descarga de documentos también genera un consumo considerable del uso del internet ya que su porcentaje de uso del 20%. Transferencia de archivos también tiene un porcentaje de uso del 20%. Por último, el tráfico de Sistema de Consulta es el más bajo ya que solo lo utilizan los estudiantes, las coordinaciones con otras sedes y los jefes de áreas.

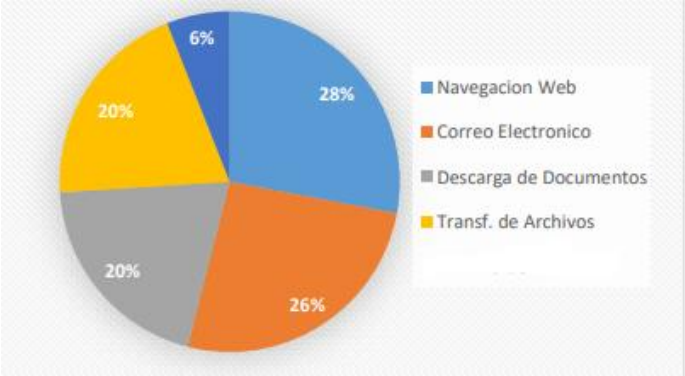


Figura 29: Servicios de red utilizados en el campus universitario
Fuente: SoporteTI_Universidad_CU

La Figura 29, refleja los datos obtenidos del área de Soporte TI de la universidad. Esta área posee una bitácora de todos los servicios de red y su relación en porcentaje de uso. De aquí se parte el análisis para los cálculos de ancho de banda como sigue a lo largo de esta sección.

Desde el punto de vista del usuario, el factor más importante es la rapidez en la que se muestra una página web después de haberla solicitado. Los retardos de varios segundos son aceptables, pero no más de 10 segundos (Instituto Europeo de Normas de Telecomunicaciones, 2005, p. 29). Para realizar el cálculo del tráfico de navegación web, se aplicará el código fuente de OpenDayLight (se puede extraer de la plataforma GitHub

con una plantilla definida, pero nosotros necesitamos hallar de forma manual para poder transformarlo a dicha plantilla) donde se establecen parámetros preferenciales y aceptables para la calidad de tráfico.

La fórmula establecida para calcular el tráfico preferencial y aceptable de la navegación web es la siguiente:

$$\boldsymbol{Navegación\ Web + B.Data = Navegación\ estable}$$

En donde la navegación web es la información y aplicaciones disponibles en los servidores de internet que tendría un tamaño aproximado de 10 KB, y el B. Data es la información en porcentaje (en otras palabras, es la compresión de datos voluminosos basado en FTP que maneja el área de redes). En cuanto a servicios de red navegación web, correo electrónico, descarga de documentos, transferencia de archivos sistema de consulta y adicional que tiene una página web. Por ejemplo: imágenes, audio, entre otros. Para el B. Data se ha especificado un valor de 200 Kb (este valor puede ser entre 200Kb a 500 Kb sugerido por OpenDayLight para su API, se sugiere un valor de 200 Kb inicial porque la cantidad de datos masivos no es muy grande y también, se puede establecer un valor de 10 Kb hasta 10 Mb.

Cálculo de velocidad estable para la navegación web

$$\boldsymbol{Navegación\ Web + B.Data = Navegación\ estable}$$

$$\frac{10\ Kbps}{2\ seg.} + \frac{200\ Kbps}{15\ seg.} = Navegación\ estable$$

$$5\ Kbps + 13.33\ Kbps = Navegación\ estable$$

$$18{,}33\ Kbps * \frac{8\ bits}{1\ byte} = Navegación\ estable$$

$$146{,}64\ Kbps = Navegación\ estable$$

En el cálculo de velocidad anterior, se observan otros datos como 2 y 15 segundos esto se relaciona con el tiempo aproximado en que se puede abrir algunas páginas web o solicitar una respuesta del sitio accedido. Lo mismo sucede para el siguiente cálculo de velocidad, en donde se establecen valores de 4 y 60 segundos, pero en referencia a un tiempo aceptable.

Cálculo de velocidad aceptable para la navegación web

$$\boldsymbol{Navegación\ Web + B.Data = Navegación\ aceptable}$$
$$\frac{10\ Kbps}{4\ seg.} + \frac{200\ Kbps}{60\ seg.} = Navegación\ aceptable$$
$$2{,}5\ Kbps + 3.33\ Kbps = Navegación\ aceptable$$
$$5,83\ Kbps * \frac{8\ bits}{1\ byte} = Navegación\ aceptable$$
$$46,66\ Kbps = Navegación\ aceptable$$

4.3 Cálculo de ancho de banda requeridos para el correo electrónico

Generalmente, el correo electrónico es un servicio de almacenamiento, este puede tolerar retrasos de varios minutos o incluso horas. Cuando el usuario se comunica con el servidor de correo local, hay una expectativa de que el correo se transfiere dentro de unos pocos segundos. Para realizar el cálculo de la velocidad requerida para el servicio de correo electrónico se emplea la misma forma con la cual se hizo el cálculo de la navegación web. En esta parte se hacen ciertas variaciones, se suman los parámetros de Navegación Web + B. Data + Correo, en donde Navegación Web utiliza un tamaño de 10 Kbps, para el B. Data se empleará 10 Kbps y para Correo se utilizarán 10 Kbps.

Cálculo de velocidad estable para el servicio de Correo Electrónico.

$$\boldsymbol{Navegación\ Web + B.Data + Correo = Correo\ Electrónico\ estable}$$
$$\frac{10\ Kbps}{2\ seg.} + \frac{10\ Kbps}{15\ seg.} + \frac{10\ Kbps}{2\ seg.} = Correo\ Electrónico\ estable$$
$$5\ Kbps + 0,66\ Kbps + 5\ Kbps = Correo\ Electrónico\ estable$$
$$10,66\ Kbps * \frac{8\ bits}{1\ byte} = Correo\ Electrónico\ estable$$
$$85,33\ Kbps = Correo\ Electrónico\ estable$$

Cálculo de velocidad aceptable para el servicio de Correo Electrónico

$$\boldsymbol{Navegación\ Web + B.Data + Correo = Correo\ Electrónico\ aceptable}$$
$$\frac{10\ Kbps}{4\ seg.} + \frac{10\ Kbps}{60\ seg.} + \frac{10\ Kbps}{4\ seg.} = Correo\ Electrónico\ aceptable$$
$$2,5\ Kbps + 0,16\ Kbps + 2,5\ Kbps = Correo\ Electrónico\ aceptable$$
$$5,16\ Kbps * \frac{8\ bits}{1\ byte} = Correo\ Electrónico\ aceptable$$
$$41,33\ Kbps = Correo\ Electrónico\ aceptable$$

4.4 Cálculo de ancho de banda para descarga de documentos

En cuanto a la velocidad de transmisión que se necesita para realizar descargas de documentos de internet, se emplea el mismo método de la navegación web con algunas modificaciones. Por ejemplo: la fórmula será igual a utilizar Navegación + B. Data donde

el primero tendrá un tamaño de 10 Kbps y el segundo será el 50% del valor máximo (5Mb) definido por la organización.

Cálculo de velocidad estable para la descarga de documentos

$$\boldsymbol{Navegación\ Web + B.Data = Descarga\ estable}$$
$$\frac{10\ Kbps}{2\ seg.} + \frac{5000\ Kbps}{15\ seg.} = Descarga\ estable$$
$$5\ Kbps + 333,33\ Kbps = Descarga\ estable$$
$$338,33\ Kbps * \frac{8\ bits}{1\ byte} = Descarga\ estable$$
$$2706,66\ Kbps = Descarga\ estable$$

Cálculo de velocidad aceptable para la descarga de documentos

$$\boldsymbol{Navegación\ Web + B.Data = Descarga\ estable}$$
$$\frac{10\ Kbps}{4\ seg.} + \frac{5000\ Kbps}{60\ seg.} = Descarga\ aceptable$$
$$2,5\ Kbps + 83,33\ Kbps = Descarga\ aceptable$$
$$85,83\ Kbps * \frac{8\ bits}{1\ byte} = Descarga\ aceptable$$
$$686,66\ Kbps = Descarga\ aceptable$$

4.5 Cálculo de la velocidad de transmisión para transferencia de archivos

Para este tipo de cálculo al igual que los demás, se emplea el mismo método (salvo por la única variación que se utilizará el B. Data y en donde Navegación Web tendrá un tamaño de 10 Kbps, para B. Data será de 5000 Kbps y para Correo se utilizará 10 Kbps. Recordar que OpenDayLight propone cálculos de ancho de banda en base a cuotas y luego, sean recopilados en el script de configuración.

Cálculo de velocidad estable para transferencia de archivos

$$\boldsymbol{Navegación\ Web + B.Data + Correo = Transfer.archivos\ estable}$$
$$\frac{10\ Kbps}{2\ seg.} + \frac{5000\ Kbps}{15\ seg.} + \frac{10\ Kbps}{2\ seg.} = Transfer.archivos\ estable$$
$$5\ Kbps + 333,33\ Kbps + 5\ Kbps = Transfer.archivos\ estable$$
$$343,33\ Kbps * \frac{8\ bits}{1\ byte} = Transfer.archivos\ estable$$
$$2746,66\ Kbps = Transfer.archivos\ estable$$

Cálculo de velocidad aceptable para transferencia de archivos

$$\boldsymbol{Navegación\ Web + B.Data + Correo = Transfer.archivos\ aceptable}$$
$$\frac{10\ Kbps}{4\ seg.} + \frac{5000\ Kbps}{60\ seg.} + \frac{10\ Kbps}{4\ seg.} = Transfer.archivos\ aceptable$$
$$2,5\ Kbps + 83,33\ Kbps + 2,5\ Kbps = Transfer.archivos\ aceptable$$

$$93,33\ Kbps * \frac{8\ bits}{1\ byte} = Transfer.archivos\ aceptable$$
$$746,64\ Kbps = Transfer.archivos\ aceptable$$

En cuanto a los diferentes tipos de tráfico, se puede tomar las velocidades de transmisión calculadas previamente y con ello distinguir una velocidad de transmisión estable y aceptable. En la siguiente Tabla 14, se ha calculado un promedio ponderado referente a las velocidades de transmisión por el índice del servicio utilizado, esto ayudará a definir un ancho de banda más preciso en cada área de trabajo del campus universitario.

TIPO DE TRAFICO	INDICE DE SERVICIO	VELOCIDAD DE TRANS. (Estab)	VELOCIDAD DE TRANS. (Acep)	INDICE*VELOC. TRANS. P.	INDICE*VELOC. TRANS. P.
Navegación Web	28%	146,64 Kbps	46,66 Kbps	41,06 Kbps	13,06 Kbps
Correo Electrónico	26%	85,35 Kbps	41,33 Kbps	22,18 Kbps	10,75 Kbps
Descarga de Documentos	20%	2705,66 Kbps	686,66 Kbps	541,33 Kbps	137,33 Kbps
Trans. De Archivos	20%	2746,66 Kbps	746,69 Kbps	549,33 Kbps	149,33 Kbps
Servicios de Voz	6%	146,93 Kbps	46,66 Kbps	8,81 Kbps	2,80 Kbps
TOTAL	100%	5831,93 Kbps	1567,96 Kbps	1162,20 Kbps	313,27 Kbps

Tabla 14: Velocidad de transmisión estimada por servicio (tipo de tráfico)

Fuente: Elaboración propia

Por otro lado, el algoritmo DFS es el utilizado en el diseño propuesto, mediante una serie de fórmulas, permite obtener resultados para el tráfico de red. Para esto es necesario poseer algunos datos de la organización, empezando de la siguiente manera:

TIPO DE USUARIO	INDICE DE USO
Docentes	70%
Administrativos	100%
Estudiante	50%

Tabla 15: Tipo de usuario e índice de uso

Fuente: Elaboración propia

Sobre la Tabla 15, esta hace referencia al porcentaje de uso de los usuarios mencionados (porcentajes obtenidos por registro del Área de Redes y TI) y que permitirá mediante cálculos establecidos por el algoritmo DFS, saber los resultados de lo propuesto. Tomando en cuenta los enlaces y la cantidad de ancho de banda (Ver Tabla 22).

USUARIOS DEL PABELLON F_AULAS_INGENIERIA			
TIPO DE USUARIO	CANTIDAD	INDICE DE USO	USUARIOS APROX.
Docentes	24	70 %	18
Administrativos	4	100%	4
Estudiante	178	50%	89

Tabla 16: Usuarios de la facultad o área de trabajo de Ingeniería

Fuente: Elaboración propia

En la Tabla 16, se detallan los usuarios del área de trabajo de Ingeniería, los usuarios aproximados en la red son obtenidos multiplicando la cantidad promedio por el índice de uso.

USUARIOS DEL PABELLON F_AULAS_OTRAS_INGENIERIA				
TIPO DE USUARIO	CANTIDAD	CANTIDAD PROMEDIO	INDICE DE USO	USUARIOS APROX.
Docentes	42	21	75%	16
Administrativos	5	3	100%	3
Estudiantes	675	337,5	50%	169
			TOTAL	188

Tabla 17: Usuarios de la facultad o área de trabajo de Otras Ingenierías

Fuente: Elaboración propia

En la Tabla 17, observamos el detalle de los usuarios del área de trabajo mencionada y al igual que el caso anterior, el método de cálculo es multiplicando la cantidad por el índice de uso.

USUARIOS DEL PABELLON F_AULAS_HUMANIDADES Y DERECHO			
TIPO DE USUARIO	CANTIDAD	INDICE DE USO	USUARIOS APROX.
Docentes	21	75%	16
Administrativos	2	100%	2
Estudiantes	280	50%	140
		TOTAL	158

Tabla 18: Usuarios de la facultad o área de trabajo de Humanidades y Derecho

Fuente: Elaboración propia

Acerca de la Tabla 18, se detallan los usuarios del área de trabajo mencionada, los usuarios aproximados en la red, se obtienen multiplicando la cantidad promedio por el índice de uso (al igual que los demás casos).

USUARIOS DEL PABELLON F_AULAS_CIENCIAS DE ADMINISTRACION Y EMP.				
TIPO DE USUARIO	CANTIDAD	CANTIDAD PROMEDIO	INDICE DE USO	USUARIOS APROX.
Docentes	40	20	75%	15
Administrativos	27	13	100%	13
Estudiantes	522	261	50%	130
			TOTAL	158

Tabla 19: Usuarios de la facultad o área de trabajo de Ciencias de Administración

Fuente: Elaboración propia

En la Tabla 19, observamos el detalle de los usuarios del área de trabajo mencionada y al igual que el caso anterior, el método de cálculo es multiplicando la cantidad por el índice de uso.

USUARIOS DEL PABELLON F_AULAS_CIENCIAS DE LA SALUD				
TIPO DE USUARIO	CANTIDAD	CANTIDAD PROMEDIO	INDICE DE USO	USUARIOS APROX.
Docentes	38	19	75%	14
Administrativos	19	10	100%	10
Estudiantes	521	260,5	50%	130
			TOTAL	154

Tabla 20: Usuarios de la facultad o área de trabajo de Ciencias de la Salud

Fuente: Elaboración propia

En la Tabla 20, se detallan los usuarios del área de trabajo de Ingeniería, los usuarios aproximados en la red son obtenidos multiplicando la cantidad promedio por el índice de uso.

Entonces, para realizar la medición según lo propuesto por el algoritmo DFS existen varios métodos, dependiendo de los requisitos de la red se puede optar por un costo alto si una ruta tiene menor ancho de banda o pasa por más elementos de red. En nuestro caso, se determinará por el método de “velocidad de transmisión x conexiones usadas”.

4.6 Cálculo de ancho de banda por tipo de usuario específico

Como se mencionó líneas arriba, se necesita el número de usuarios simultáneos de cada área de trabajo en donde establecemos: a los docentes y administrativos de cada área deben tener una velocidad preferencial para realizar sus labores en campus universitario y a los estudiantes, se les otorgará una velocidad aceptable.

4.6.1 Cálculo de ancho de banda para el área de trabajo de Ingeniería

(Tráfico preferencial para el Docente)

$$Velocidad\ de\ transmisión * Conexiones\ usadas = Ancho\ de\ banda\ preferencial$$

$$1162,20\ Kbps * 18 = 20919,6\ Kbps$$

$$20919,6\ Kbps * \frac{1\ Byte}{8\ bits} * \frac{1\ Mbps}{1000\ Kbps}$$

$$2,61\ Mbps = Ancho\ de\ banda\ preferencial$$

(Tráfico preferencial para Administrativos)

$$Velocidad\ de\ transmisión * Conexiones\ usadas = Ancho\ de\ banda\ preferencial$$

$$1162,20\ Kbps * 4 = 4648,8\ Kbps$$

$$4648,8\ Kbps * \frac{1\ Byte}{8\ bits} * \frac{1\ Mbps}{1000\ Kbps}$$

$$0,58\ Mbps = Ancho\ de\ banda\ preferencial$$

(Tráfico aceptable para Estudiantes)

$$Velocidad\ de\ transmisión * Conexiones\ usadas = Ancho\ de\ banda\ aceptable$$

$$313,27\ Kbps * 89 = 27881,03\ Kbps$$

$$27881,03\ Kbps * \frac{1\ Byte}{8\ bits} * \frac{1\ Mbps}{1000\ Kbps}$$

$$3,48\ Mbps = Ancho\ de\ banda\ aceptable$$

TOTAL DE ANCHO DE BANDA REQUERIDO PARA EL ÁREA DE INGENIERIA (DFS)

$$Ancho\ de\ banda\ Preferencial\ Docente + Ancho\ de\ banda\ Preferencial\ Administrativo + Ancho\ de\ banda\ Aceptable\ Estudiantes = Ancho\ de\ banda\ Total$$

$$2,61\ Mbps + 0,58\ Mbps + 3,48\ Mbps = Ancho\ de\ banda\ Total$$

$$6,67\ Mbps = Ancho\ de\ banda\ Total$$

4.6.2 Cálculo de ancho de banda para el área de trabajo de Otras Ingenierías

(Tráfico preferencial para el Docente)

$$Velocidad\ de\ transmisión * Conexiones\ usadas = Ancho\ de\ banda\ preferencial$$

$$1162,20\ Kbps * 16 = 18595,2\ Kbps$$

$$18595,2\ Kbps * \frac{1\ Byte}{8\ bits} * \frac{1\ Mbps}{1000\ Kbps}$$

$$2,32\ Mbps = Ancho\ de\ banda\ preferencial$$

(Tráfico preferencial para Administrativos)

$$Velocidad\ de\ transmisión * Conexiones\ usadas = Ancho\ de\ banda\ preferencial$$

$$1162,20\ Kbps * 3 = 3486,6\ Kbps$$

$$3486,6\ Kbps * \frac{1\ Byte}{8\ bits} * \frac{1\ Mbps}{1000\ Kbps}$$

$$0,44\ Mbps = Ancho\ de\ banda\ preferencial$$

(Tráfico aceptable para Estudiantes)

$$Velocidad\ de\ transmisión * Conexiones\ usadas = Ancho\ de\ banda\ aceptable$$

$$313,27\ Kbps * 169 = 52942,63\ Kbps$$

$$52942,63\ Kbps * \frac{1\ Byte}{8\ bits} * \frac{1\ Mbps}{1000\ Kbps}$$

$$6,62\ Mbps = Ancho\ de\ banda\ aceptable$$

TOTAL DE ANCHO DE BANDA REQUERIDO PARA OTRAS INGENIERIAS (DFS)

$$Ancho\ de\ banda\ Preferencial\ Docente + Ancho\ de\ banda\ Preferencial\ Administrativo + Ancho\ de\ banda\ Aceptable\ Estudiantes = Ancho\ de\ banda\ Total$$

$$2,32\ Mbps + 0,44\ Mbps + 6,62\ Mbps = Ancho\ de\ banda\ Total$$

$$9,38\ Mbps = Ancho\ de\ banda\ Total$$

4.6.3 Cálculo de ancho de banda para el área de trabajo de Humanidades y Derecho

(Tráfico preferencial para el Docente)

$$Velocidad\ de\ transmisión * Conexiones\ usadas = Ancho\ de\ banda\ preferencial$$

$$1162,20\ Kbps * 16 = 18595,2\ Kbps$$

$$18595,2\ Kbps * \frac{1\ Byte}{8\ bits} * \frac{1\ Mbps}{1000\ Kbps}$$

$$2,32\ Mbps = Ancho\ de\ banda\ preferencial$$

(Tráfico preferencial para Administrativos)

$$Velocidad\ de\ transmisión * Conexiones\ usadas = Ancho\ de\ banda\ preferencial$$

$$1162,20\ Kbps * 2 = 2324,4\ Kbps$$

$$2324,4\ Kbps * \frac{1\ Byte}{8\ bits} * \frac{1\ Mbps}{1000\ Kbps}$$

$$0,29\ Mbps = Ancho\ de\ banda\ preferencial$$

(Tráfico aceptable para Estudiantes)

$$Velocidad\ de\ transmisión * Conexiones\ usadas = Ancho\ de\ banda\ aceptable$$

$$313,27\ Kbps * 140 = 43857,8\ Kbps$$

$$43857,8\ Kbps * \frac{1\ Byte}{8\ bits} * \frac{1\ Mbps}{1000\ Kbps}$$

$$5,48\ Mbps = Ancho\ de\ banda\ aceptable$$

TOTAL DE ANCHO DE BANDA REQUERIDO PARA HUMANIDADES Y DERECHO (DFS)

$$Ancho\ de\ banda\ Preferencial\ Docente + Ancho\ de\ banda\ Preferencial\ Administrativo + Ancho\ de\ banda\ Aceptable\ Estudiantes = Ancho\ de\ banda\ Total$$

$$2,32\ Mbps + 0,29\ Mbps + 5,48\ Mbps = Ancho\ de\ banda\ Total$$

$$8,09\ Mbps = Ancho\ de\ banda\ Total$$

4.6.4 Cálculo de ancho de banda para el área de trabajo de Ciencias de Administración y Empresas

(Tráfico preferencial para el Docente)

$$Velocidad\ de\ transmisión * Conexiones\ usadas = Ancho\ de\ banda\ preferencial$$

$$1162,20\ Kbps * 15 = 17433\ Kbps$$

$$17433\ Kbps * \frac{1\ Byte}{8\ bits} * \frac{1\ Mbps}{1000\ Kbps}$$

$$2,18\ Mbps = Ancho\ de\ banda\ preferencial$$

(Tráfico preferencial para Administrativos)

$$Velocidad\ de\ transmisión * Conexiones\ usadas = Ancho\ de\ banda\ preferencial$$

$$1162,20\ Kbps * 12 = 13946,4\ Kbps$$

$$13946,4\ Kbps * \frac{1\ Byte}{8\ bits} * \frac{1\ Mbps}{1000\ Kbps}$$

$$1,74\ Mbps = Ancho\ de\ banda\ preferencial$$

(Tráfico aceptable para Estudiantes)

$$Velocidad\ de\ transmisión * Conexiones\ usadas = Ancho\ de\ banda\ aceptable$$

$$313,27\ Kbps * 130 = 40725,1\ Kbps$$

$$40725,1\ Kbps * \frac{1\ Byte}{8\ bits} * \frac{1\ Mbps}{1000\ Kbps}$$

$$5,01\ Mbps = Ancho\ de\ banda\ aceptable$$

TOTAL DE ANCHO DE BANDA REQUERIDO PARA CIENCIAS DE LA ADMINISTRACIÓN Y EMPRESAS (DFS)

$$Ancho\ de\ banda\ Preferencial\ Docente + Ancho\ de\ banda\ Preferencial\ Administrativo + Ancho\ de\ banda\ Aceptable\ Estudiantes = Ancho\ de\ banda\ Total$$

$$2,18\ Mbps + 1,74\ Mbps + 5,01\ Mbps = Ancho\ de\ banda\ Total$$

$$8,93\ Mbps = Ancho\ de\ banda\ Total$$

4.6.5 Cálculo de ancho de banda para el área de trabajo de Ciencias de la Salud

(Tráfico preferencial para el Docente)

$$Velocidad\ de\ transmisión * Conexiones\ usadas = Ancho\ de\ banda\ preferencial$$

$$1162,20\ Kbps * 14 = 16270,8\ Kbps$$

$$16270\ Kbps * \frac{1\ Byte}{8\ bits} * \frac{1\ Mbps}{1000\ Kbps}$$

$$2,03\ Mbps = Ancho\ de\ banda\ preferencial$$

(Tráfico preferencial para Administrativos)

$$Velocidad\ de\ transmisión * Conexiones\ usadas = Ancho\ de\ banda\ preferencial$$

$$1162,20\ Kbps * 10 = 11622\ Kbps$$

$$11622\ Kbps * \frac{1\ Byte}{8\ bits} * \frac{1\ Mbps}{1000\ Kbps}$$

$$1,45\ Mbps = Ancho\ de\ banda\ preferencial$$

(Tráfico aceptable para Estudiantes)

$$Velocidad\ de\ transmisión * Conexiones\ usadas = Ancho\ de\ banda\ aceptable$$

$$313,27\ Kbps * 130 = \ 40725,1\ Kbps$$

$$40725,1\ Kbps * \frac{1\ Byte}{8\ bits} * \frac{1\ Mbps}{1000\ Kbps}$$

$$5,01\ Mbps = Ancho\ de\ banda\ aceptable$$

TOTAL DE ANCHO DE BANDA REQUERIDO PARA CIENCIAS DE LA SALUD (DFS)

$$Ancho\ de\ banda\ Preferencial\ Docente + Ancho\ de\ banda\ Preferencial\ Administrativo + Ancho\ de\ banda\ Aceptable\ Estudiantes = Ancho\ de\ banda\ Total$$

$$2,03\ Mbps + 1,45\ Mbps + 5,01\ Mbps = Ancho\ de\ banda\ Total$$

$$8,49\ Mbps = Ancho\ de\ banda\ Total$$

Para los cálculos mostrados en especial el cálculo preferencial, se debe multiplicar el número aproximado de usuarios docentes y administrativos por la velocidad de transmisión preferencial, sería un total de 1162,20 Kbps. En cuanto al cálculo aceptable destinado al tipo de usuario estudiante, se debe multiplicar el número de estudiantes aproximado por la velocidad aceptable que sería 313,27 Kbps.

De igual manera, se observará una tabla resumen del ancho de banda en la hora pico o más alta, con un modelo de usuario aproximado. Cabe señalar que se especificó para los docentes y administrativos una velocidad de transmisión para todos los servicios y para los estudiantes una velocidad aceptable, ya que ellos son la mayoría de consumidores del ancho de banda en la hora pico. (Ver Tabla 27)

ÁREA DE TRABAJO	TIPO DE USUARIO	VELOCIDAD DE TRANS.	BW REQUERIDO	BW TOTAL
Pab_F_Ingeniería	Docente, Adm y Estudiante	1162,2 Kbps 1162,2 Kbps 313,27 Kbps	2,32 MB 0,29 MB 5,48 MB	8,09 MB
Pab_Otras_Ingenierías	Docente, Adm y Estudiante	1162,2 Kbps 1162,2 Kbps 313,27 Kbps	2,61 MB 0,58 MB 3,48 MB	6,67 MB
Pab_ Humanidades y Derecho	Docente, Adm y Estudiante	1162,2 Kbps 1162,2 Kbps 313,27 Kbps	2,18 MB 1,74 MB 5,01 MB	8,93 MB
Pab_ Ciencias de Administración y Emp.	Docente, Adm y Estudiante	1162,2 Kbps 1162,2 Kbps 313,27 Kbps	2,32 MB 0,44 MB 6,62 MB	8,93 MB
Pab_ Ciencias de la Salud	Docente, Adm y Estudiante	1162,2 Kbps 1162,2 Kbps 313,27 Kbps	2,03 MB 1,45 MB 5,01 MB	8,93 MB

Tabla 21: Cálculo de ancho de banda basado en algoritmo DFS

Fuente: Elaboración propia

En la Tabla 21, podemos observar una matriz resumen con todos los datos y los cálculos respectivos para obtener el ancho de banda o camino más eficiente. Para finalizar esta parte, se debe considerar el costo del enlace para obtener el ancho de banda recomendado.

ÁREA DE TRABAJO	BW DISPONIBLE	BW REQUERIDO	BW RECOMENDADO
Pab_F_Ingeniería	17 MB	8,09 MB	13 MB
Pab_Otras_Ingenierías	20 MB	6,67 MB	11,05 MB
Pab_ Humanidades y Derecho	10 MB	8,93 MB	12,5 MB
Pab_ Ciencias de Administración y Emp.	20 MB	9,38 MB	13 MB
Pab_ Ciencias de la Salud	20 MB	8,49 MB	12 MB
TOTAL	87 MB	41,56 MB	62 MB

Tabla 22: Ancho de banda usado y disponible

Fuente: Elaboración propia

Como se observa en la Tabla 22, podemos obtener el ancho de banda disponible y recomendado, principalmente. Con los resultados obtenidos podemos determinar que no es necesario aumentar o modificar la cantidad de ancho de banda que indica el R2 (Requerimiento 2 del proyecto), Según el cálculo, nos arroja 87 MB y 62 MB, ancho de banda disponible y recomendado, respectivamente. Si nosotros volvemos a la Tabla 12, se podrá observar que tenemos 3 enlaces con un mínimo de 100 MB por cada uno de ellos. Por lo tanto, no se sugiere la agregación de algún enlace o su modificación.

Por otro lado, se propone una nueva topología de red para la LAN del campus universitario. En la siguiente Figura 30, se podrá observar un bosquejo de lo que será la nueva topología de red y los componentes/requerimientos técnicos que son necesarios para su elaboración.

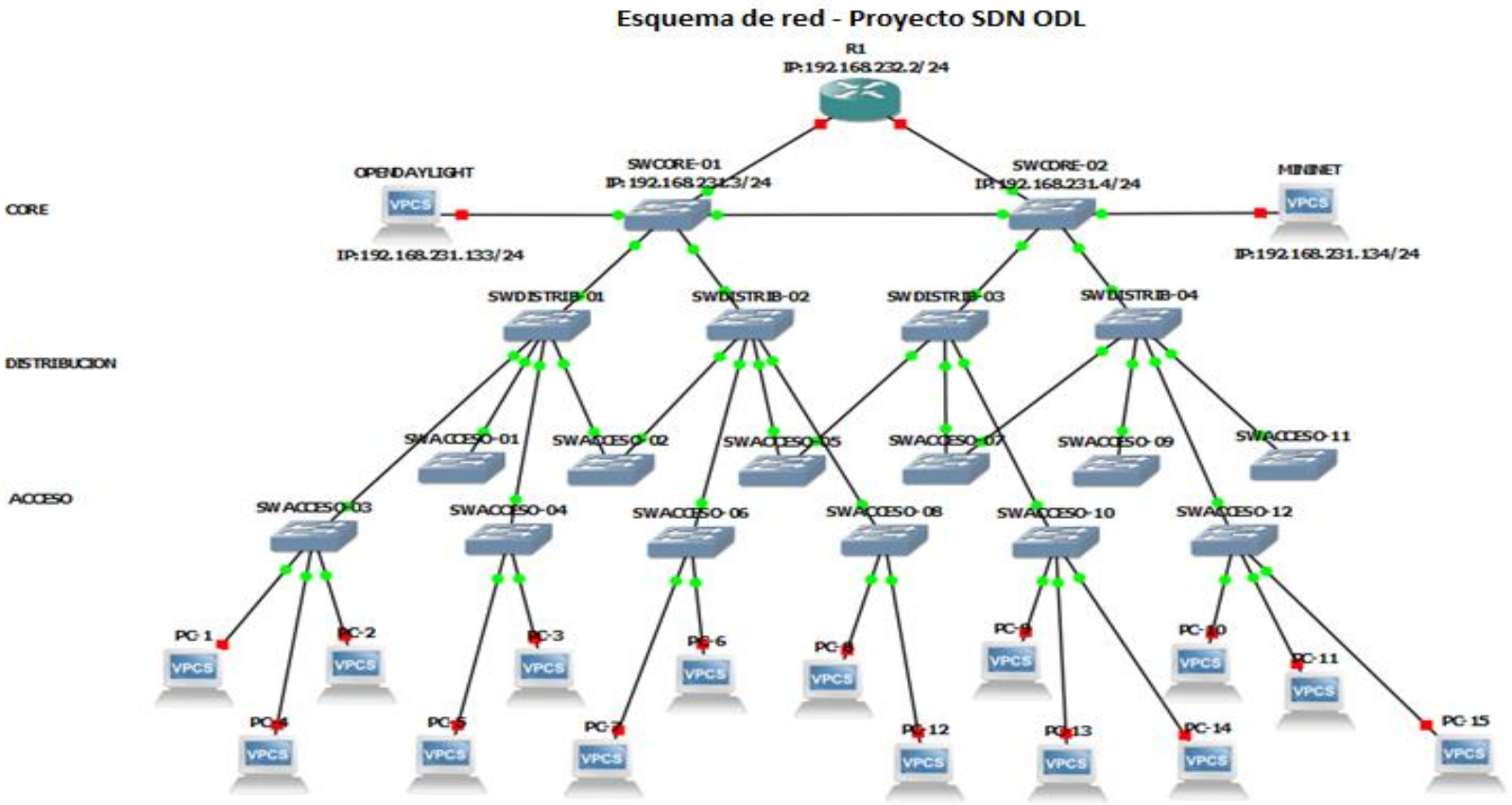


Figura 30: Esquema general de la red LAN

Fuente: Elaboración propia

4.7 Densidad de Puertos (Conmutadores de Red)

La densidad de puertos se refiere al número de puertos disponibles en un solo switch. De acuerdo a la situación actual de la red, se propone la densidad de puerto de cada switch. (Ver Tabla 23)

ÁREA DE TRABAJO	CARACTERÍSTICAS	TOTAL DE PUERTOS	DENSIDAD
SOPORTE TI	Catalyst 3850 48T	48-port 10/100/1000BASE-T	32 puertos
SERVICE DESK	Catalyst 3850 24T	24-port 10/100/1000BASE-T	15 puertos
PLATAFORMA	Catalyst 3850 12T	12-port 10/100/1000BASE-T	10 puertos
PROCESOS	Catalyst 3850 12T	12-port 10/100/1000BASE-T	10 puertos
PAB_F_ADM	Catalyst 3850 48T	48-port 10/100/1000BASE-T	42 puertos
PAB_F_SC	Catalyst 3850 48T	48-port 10/100/1000BASE-T	40 puertos
PAB_F_LABS	Catalyst 3850 24T	24-port 10/100/1000BASE-T	15 puertos
INFRAESTRUCTURA	Catalyst 3850 24T	24-port 10/100/1000BASE-T	13 puertos
DIRECCION TI	Catalyst 3850 48T	12-port 10/100/1000BASE-T	10 puertos
DESARROLLO	Catalyst 3850 24T	24-port 10/100/1000BASE-T	16 puertos
PAB_INGENIERIA	Catalyst 3850 48T	48-port 10/100/1000BASE-T	48 puertos
PAB_OTRAS_ING	Catalyst 3850 48T	48-port 10/100/1000BASE-T	48 puertos
PAB_HUMANIDADES	Catalyst 3850 48T	48-port 10/100/1000BASE-T	48 puertos
PAB_CIENCIAS ADM	Catalyst 3850 48T	48-port 10/100/1000BASE-T	48 puertos
PAB_CIENCIAS DE SALUD	Catalyst 3850 48T	48-port 10/100/1000BASE-T	48 puertos

Tabla 23: Densidad de puertos por área de trabajo

Fuente: Elaboración propia

En la Tabla 23, se observa las áreas de trabajo donde se alojarán los switches propuestos con la característica definida para ello, la cantidad de puertos y la densidad de los mismos de

acuerdo al número de usuarios. Cabe mencionar que existen un total de 100 dispositivos de red, de los cuales 65 son switches y la propuesta opta por 48 switches enfocados para las áreas de trabajo mencionadas.

El ancho de banda que pueden alcanzar estos equipos de red son flujos de datos de 10 Mbps, 100 Mbps y 1 Gbps, se tratan de tasas ideales, los hilos de fibra óptica del backbone del campus universitario, se encuentra conectada a un canal de 1 Gbps, los puntos de red de los usuarios están en 100 Mbps que depende del ancho de banda obtenido. De igual manera, el modelo de switch propuesto para las capas de core, distribución y acceso cuenta con un ASIC programable que permite al dispositivo participar junto con el controlador SDN. Es decir, una plataforma que pueda darle forma al tráfico desde una consola de control centralizada sin tener que tocar los switches de manera individual (los scripts o plantillas que comprometen a esta gestión serán colocadas en la parte de Anexos).

4.8 Servidores

En la organización existen 15 servidores funcionando, brindando diferentes servicios y aplicaciones de red. Sobre estos equipos se ejecutan plataformas Windows Server o Linux como veremos enseguida.

SERVICIO	SERVIDOR	DESCRIPCION
DIRECTORIO ACTIVO	SRV2K2PDC01 SRV2K2PDC02 SRV2K2PDC03	AD, Controller, DNS, DHCP
NETWORK MANAGER	SRV2K2PDC04 SRV2K2PED01	Antivirus Server, Web Filter Server
EMAIL	SRV2K2PED02	Mail Server, Exchange Server
SERVIDOR DE ARCHIVOS	PDLOFPSVR	File Server
BASE DE DATOS	DBPPDBS01 DBPPDBS02 DPLOPDBSR	PeopleSoft, Servidor de Aplicación, DIM Technical
CyberCampus (PeopleSoft)	DPLOAS01	Serv. De Aplicación
	DPLOAS02	PeopleSoft PS
	DPLOAS03	Report Server 1
	DPLOAS04	Report Server 2
Intranet	DPLOPDBSR2	PayR Database

Tabla 24: Servidores y servicios utilizados en la UC

Fuente: Elaboración propia

En la Tabla 24, se hace hincapié a estos servidores porque sus servicios muy probablemente requerirán puertos en la capa de distribución para enrutar vlans a nivel de capa 3, lo que limitaría la cantidad de densidad de puertos disponibles en los switches de la capa mencionada. La recomendación es dejar espacio en la capa de distribución para el crecimiento o cambios futuros en el diseño.

4.9 Disponibilidad de servicios de red

Teniendo en cuenta los usuarios, los servidores y servicios de red se considera que la disponibilidad debe duplicarse en algún componente que lo requiera y cuyo fallo pueda incapacitar las aplicaciones críticas como correo, directorio activo, peoplesoft y otros que puedan utilizar los docentes, administrativos y estudiantes. Los componentes son los enlaces de un switch de distribución, para nuestro caso el área de Pab_F_Aulas que comprende a Pab_Ingeniería, Otras Ingenierías, Humanidades, Ciencias de la Administración y Salud. También, podría considerarse a los switches de acceso con los mismos nombres y que enlazan a los usuarios finales.

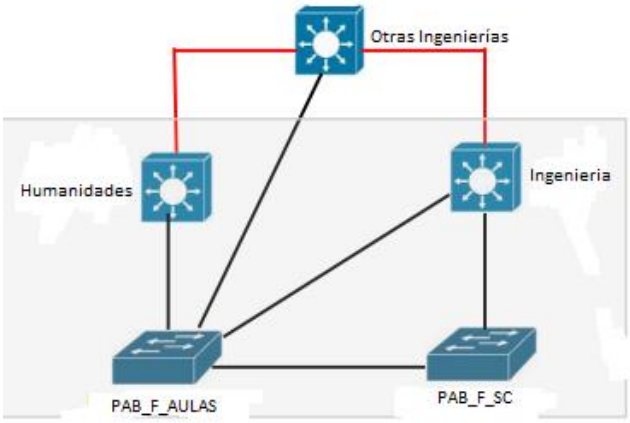


Figura 31: Disponibilidad en áreas críticas

Fuente: Elaboración propia

La Figura 31 nos indica la disponibilidad que deben tener las áreas críticas de trabajo en la organización, en donde tenemos un switch PAB_F_AULAS que contiene a 3 switches importantes y mencionados anteriormente. La idea es que no sean interrumpidos los servicios ante alguna falla y esto debe replicarse en todas las áreas donde se crea conveniente. También es posible hacer disponibilidad en el borde de la red LAN para garantizar una alta

disponibilidad de Internet. Sin embargo, estos servicios no se consideran aplicaciones críticas para el negocio de la empresa.

4.9.1 Diseño de capas de red

A nivel de capa 2 el diseño se centra en la división a grupos funcionales, por cada grupo funcional resulta una LAN virtual mostrada en la siguiente imagen.

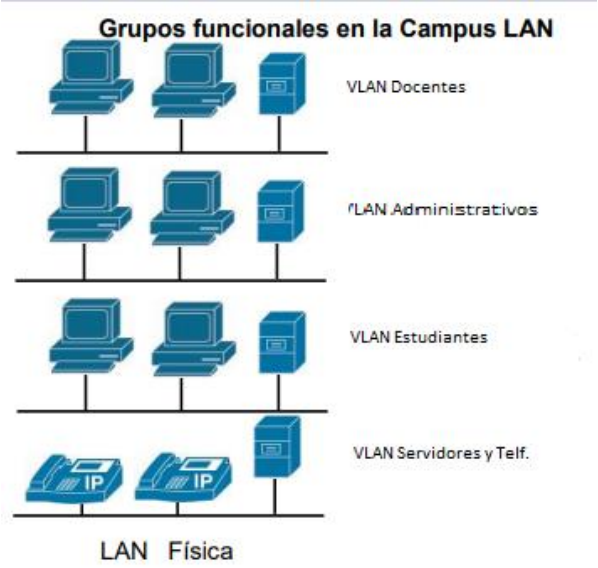


Figura 32: Grupos funcionales de la LAN

Fuente: Elaboración propia

La Figura 32 nos indica la función de los grupos funcionales propuestos en la capa 2, en donde se seleccionó ello de acuerdo al perfil de tráfico definido para cada uno de estos, con el fin de proveer a los usuarios el ancho de banda suficiente y necesario para sus labores en la empresa. Cabe mencionar que residen sobre la misma infraestructura de red y se extienden a lo largo de todos los switches mediante la propagación del nombre de dominio de la universidad

Debido a que los usuarios necesitan intercambiar información en la red LAN sea de un segmento de red a otro o de una VLAN, resulta necesario el siguiente escenario para su cometido.

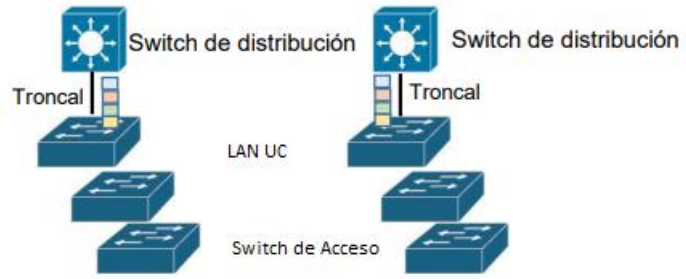


Figura 33: Conectividad entre Switch de distribución y acceso

Fuente: Reporte_SoporteTI_CU

La Figura 33 nos muestra a los switches de distribución con una conexión troncal hacia cada switch de acceso (contiene a las diferentes áreas de trabajo), ello para permitir múltiples conexiones lógicas entre los dispositivos que llevan los segmentos de red o grupo funciona definido.

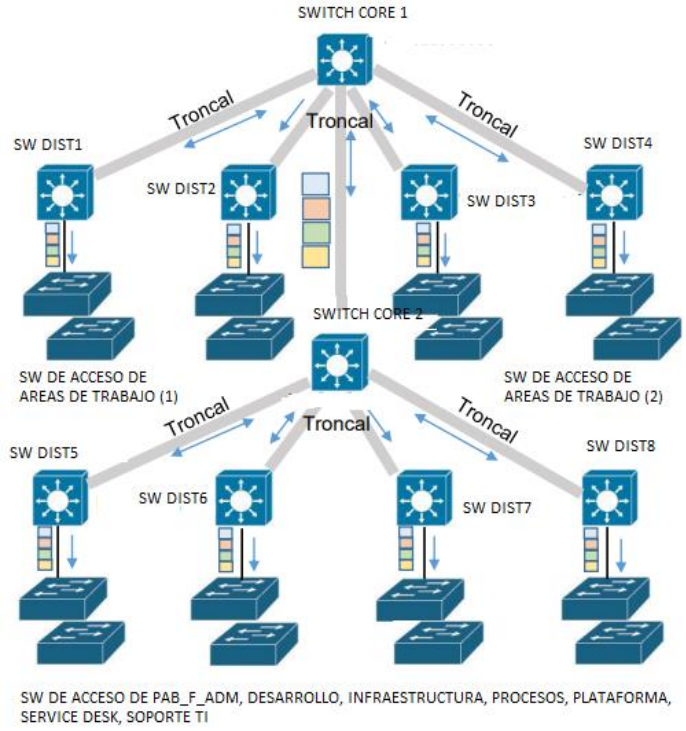


Figura 34: Diseño de switches en la red LAN del campus universitario

Fuente: Reporte_SoporteTI_UC

La Figura 34, nos indica la propagación de las capas de core, distribución y acceso propuesto a la organización (teniendo en cuenta la Figura 45 en donde se observa una red LAN totalmente inadecuada y solo con dos capas y sin redundancia alguna), a través de una infraestructura de red jerárquica establecida, contando con switches programables y con alta disponibilidad ante una caída). A continuación, se detallará el diseño propuesto para cada capa a nivel de switch.

4.9.2 Capa de Núcleo o Core

La capa de core brinda diferentes conexiones a diferentes áreas del campus universitario a través de los switches de distribución por lo que puede conmutar tráfico a gran velocidad.

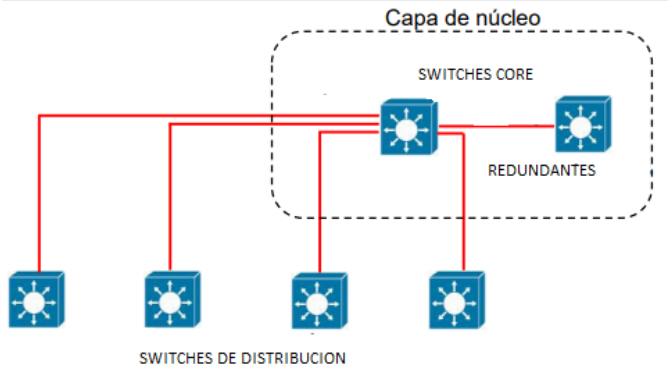


Figura 35: Ubicación de Switch Core redundantes

Fuente: Reporte_RedesTI_CU

La Figura 35 muestra a los switches core conectados entre si y que ante cualquier falla el servicio estará operativo (en la topología actual no cuenta con redundancia o algún equipo de respaldo ante algún problema). Además, lo ofrecido proporciona una óptima convergencia, fuentes de energía redundantes, cables dac (stacking de switch) y rapidez en el acceso a información en la organización. En total se proponen 4 switches de core.

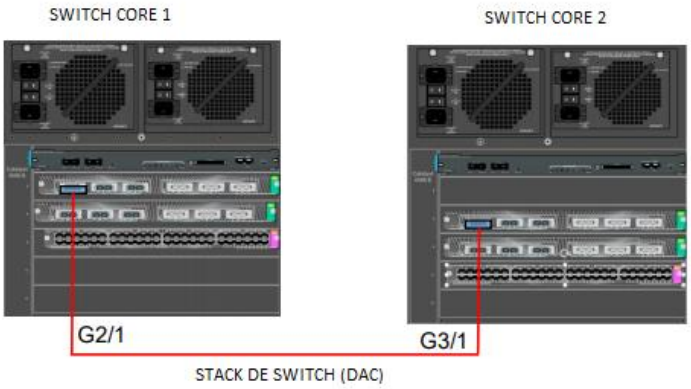


Figura 36: Switch de Core unidos por cable DAC (Stack)

Fuente: RedesTI_CU

Como se mencionaba líneas arriba, la Figura 36 nos indica como se debe realizar el stack o apilamiento de switches propuesto, ya no solo depende de tener un switch de respaldo ante un mal funcionamiento o interrupción de energía, sino de apilar los switches (en especial el Core) y que todos los que conforman esta capa sean capaz de gestionarse de manera unificada. Cabe recordar que los switches propuesto son programables y listos para ser vistos por el controlador OpenDayLight para su gestión e ingresando todos los cálculos realizados en la parte de requerimientos del proyecto.

4.9.3 Capa de Distribución

Se agrega esta capa en la topología de red propuesta para establecer las funciones de comunicar la capa de acceso con el core, poder establecer la interconexión entre estas capas es importante que los equipos dispongan de puertos de alta velocidad (considerado en el modelo propuesto) y también, deberían existir múltiples switches en esta capa por el motivo de que el campus universitario se extiende en diferentes áreas de trabajo y evitar así, la tediosa tarea de tender medios de conexión de alto precio a grandes distancias. En total se proponen 8 switches de distribución, aprovechando las ubicaciones iniciales de algunos switches que solo necesitan ser actualizados en las áreas de Desarrollo, Infraestructura, Procesos, Soporte TI y Plataforma.

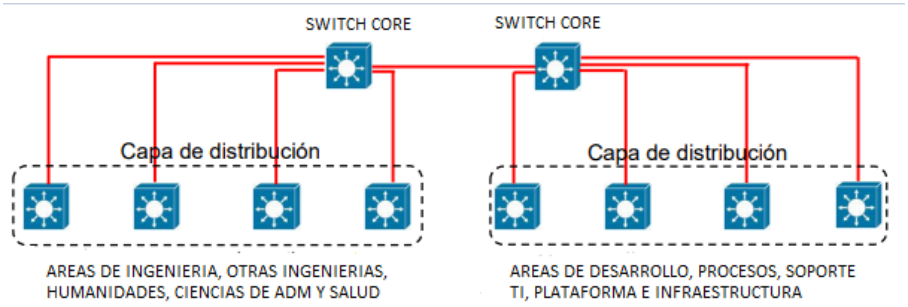


Figura 37: Switch de distribución propuestos (Esquema lógico)

Fuente: RedesTI_CU

En la Figura 37, se observa los switch de distribución de la topología diseñada, se consideran ocho switches en esta capa, de las cuales cuatro están asociadas a la alimentación de los switches de acceso (áreas de trabajo) distribuidas a lo largo del campus universitario, y también cuatro switches sobre las otras áreas de la organización.

UBICACIÓN	SWITCH
RECTORADO	Catalyst 3850-48 WS
PASTORAL	Catalyst 3850-24 WS
ESTRADO	Catalyst 3850-48 WS
PAB_F_ADM	Catalyst 3850-48 WS
PAB_F_AULAS	Catalyst 3850-48 WS
PAB_F_LABORATORIOS	Catalyst 3850-48 WS
PAB_DIRECCION	Catalyst 3850-24 WS
ENTRADA_F	Catalyst 3850-48 WS

Tabla 25: Ubicación de switches de distribución

Fuente: Elaboración propia

En la Tabla 25, se especifica los dispositivos de la capa de distribución, cuya función implica representar un alto rendimiento de procesamiento de paquete, soporte para filtro de determinados paquetes, entre otros. Siendo características que apoyan al rendimiento de la red en la entrega eficiente de datos a través de la red.

4.9.4 Capa de Acceso

Para hacer frente a los servicios de red y la demanda del usuario final, se ha realizado la elección de los switches de acceso para cada área de la empresa considerando el número de dispositivos a alimentar, la densidad del switch elegido y la criticidad del mismo, con el propósito de proporcionar un medio de conexión de dispositivos a la red.

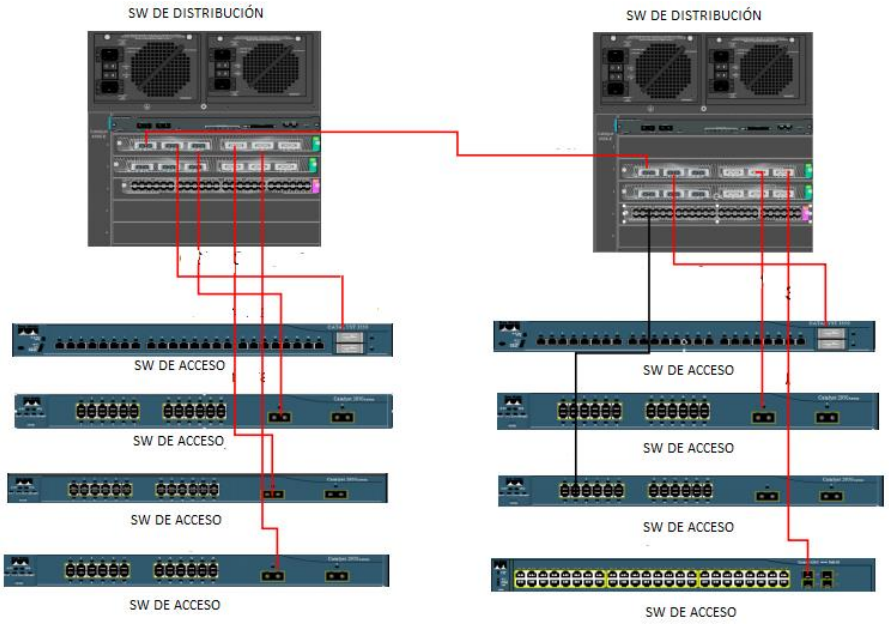


Figura 38: Switch de Acceso interconectados con switch de distribución

Fuente: Reporte_RedesTI_CU

La Figura 38 muestra la topología específica obtenida para la interconexión de los diferentes dispositivos de red (distribución), en cada conexión se establece el medio de fibra óptica según sea la necesidad. Respecto a los switches desactualizados de la Tabla 3, los que complementan a la capa de acceso son los switches juniper EX2200 que necesitan una actualización o upgrade tecnológico para que pueda cumplir con la solución propuesta y sea visible para la consola SDN.

5 CAPITULO 5

En este capítulo, se presentan las validaciones de los resultados obtenidos en el diseño del proyecto propuesto, considerando el cumplimiento de los objetivos específicos y la prueba y validación de los resultados.

5.1 Plan de pruebas

El esquema general del entorno de simulación se muestra en la Figura 67, en donde las máquinas virtuales de Mininet y OpenDayLight se ejecutarán en diferentes instancias. Se establece conectividad entre ambas máquinas virtuales dentro de una misma red de área local (LAN). Los procesos que se observaran en los planos de datos, control y aplicación de la red SDN son los siguientes:

- **Plano de datos:**
  En este plano, el encargado es Mininet quien ejecuta los switches virtuales conocidos como OpenvSwitch que permite ejecutar procesos para la conmutación de paquetes y es compatible con OpenFlow, LACP, entre otros.

- **Plano de control y aplicación:**
  El controlador OpenDayLight será quien administre la red simulada en Mininet a través de OpenFlow y ejecutará instrucciones sobre las aplicaciones que permitan la conmutación de paquetes de inicio a fin.

En referencia a Mininet, este sistema creará los dispositivos de red que permitirán la integración con la topología SDN. Estos dispositivos de red incluyen (hosts, switches, controlador y enlaces. En la simulación propuesta con Mininet, el controlador OpenDayLight se ejecutará en la red de simulación siempre y cuando la máquina virtual que contiene el switch pueda comunicarse con el controlador. El listado de dispositivos de red usados para esta simulación, serán mencionados a continuación:

- **Controlador:**
  Para el entorno de simulación se propone un controlador OpenDayLight (Controller) quien será el encargado de gestionar a los dispositivos de red.

- **Switches:**
  Se utilizará un total de 15 switches que simularán el entorno de red del campus y según la topología de red propuesta.

- **Enlaces:**
  Los enlaces (links) suman un total de 30 y para esto, se toma en cuenta las conexiones entre los switches, hosts y controlador.

- **Hosts:**
  En total son usados 16 hosts/terminales que serán los clientes y en donde están asociados directamente a los switches.

Asimismo, la versión de Mininet propuesta es 2.2.1 instalada en una máquina virtual y utilizando la herramienta de virtualización llamado VMware Workstation versión 15. Adicionalmente, la versión de OpenvSwitch es 1.4.0 y se usó la versión 1.1 de OpenFlow.
Por otro lado, se utiliza el controlador OpenDayLight para el entorno de simulación de red SDN a través de su distribución Lithium 0.3.0 al tener mayor compatibilidad con protocolos y versiones de los elementos de red utilizados en la topología SDN. Cabe mencionar que este controlador está alojado en otra máquina virtual por medio de VMware Workstation versión 15. Entonces para establecer la comunicación y un ambiente de prueba concreto, se incluye las máquinas virtuales creadas en una misma red y también, pueda permitir asociar la red SDN con los dispositivos de red tradicionales de manera virtualizada.

5.1.1 Pruebas de tráfico para ancho de banda y resultados

Esta prueba consiste en establecer tráfico entre un host/terminal y otro host/servidor que permita medir el rendimiento de ancho de banda (basado en los cálculos obtenidos en la parte del diseño). Para ello, es necesario contar con una herramienta adicional que permita crear

flujos de datos para medir el rendimiento propuesto y se propone la herramienta IPERF en el cual, los resultados arrojados contienen el ancho de banda utilizado, la transferencia de datos, el tiempo transcurrido, entre otros valores. A continuación, se mostrarán las pruebas realizadas basado en dos tipos de tráfico: TCP para ancho de banda y UDP para otros valores obtenidos.

- **Tráfico TCP (Ancho de banda)**

  En esta parte, se realizaron pruebas con IPERF utilizando el protocolo TCP con un tamaño de 85.3 Kbyte (utilizado por defecto en el controlador ODL). Entonces, se configuró el host h16 como servidor utilizando el puerto 8080, y entre los hosts h1, h2, h3, h6, h10 y h13 como clientes para enviar datos al puerto 8080 mencionado. Los resultados son los indicados a continuación:

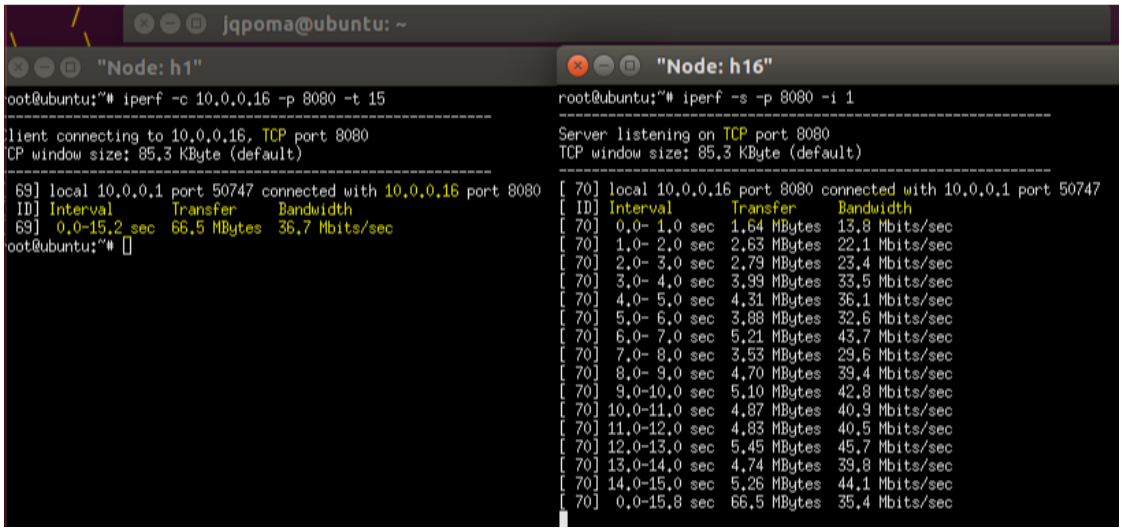


Figura 39: Prueba y resultado TCP del host h1 al host 16 de la red SDN

Fuente: Elaboración propia

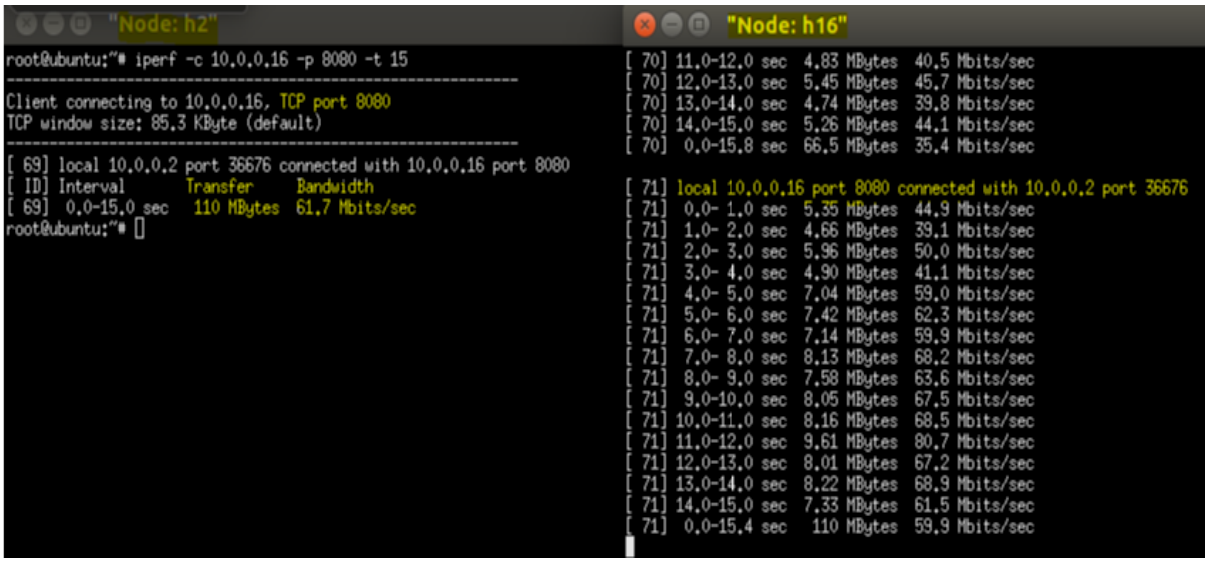


Figura 40: Prueba y resultado TCP del host h2 al host 16 de la red SDN

Fuente: Elaboración propia

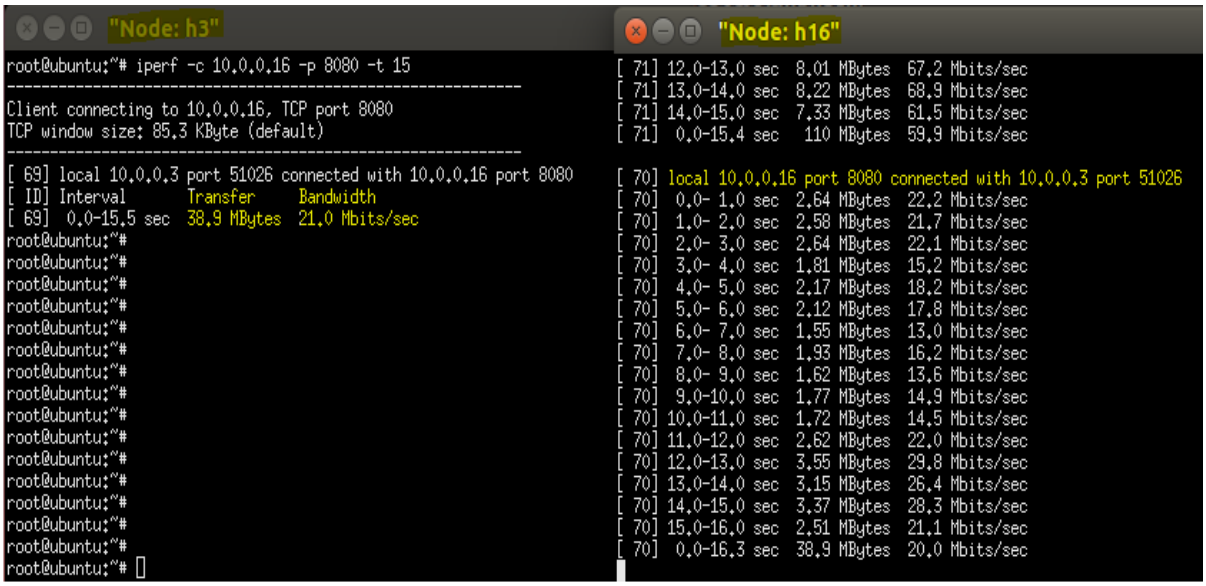


Figura 41: Prueba y resultado TCP del host h3 al host h16 de la red SDN

Fuente: Elaboración propia

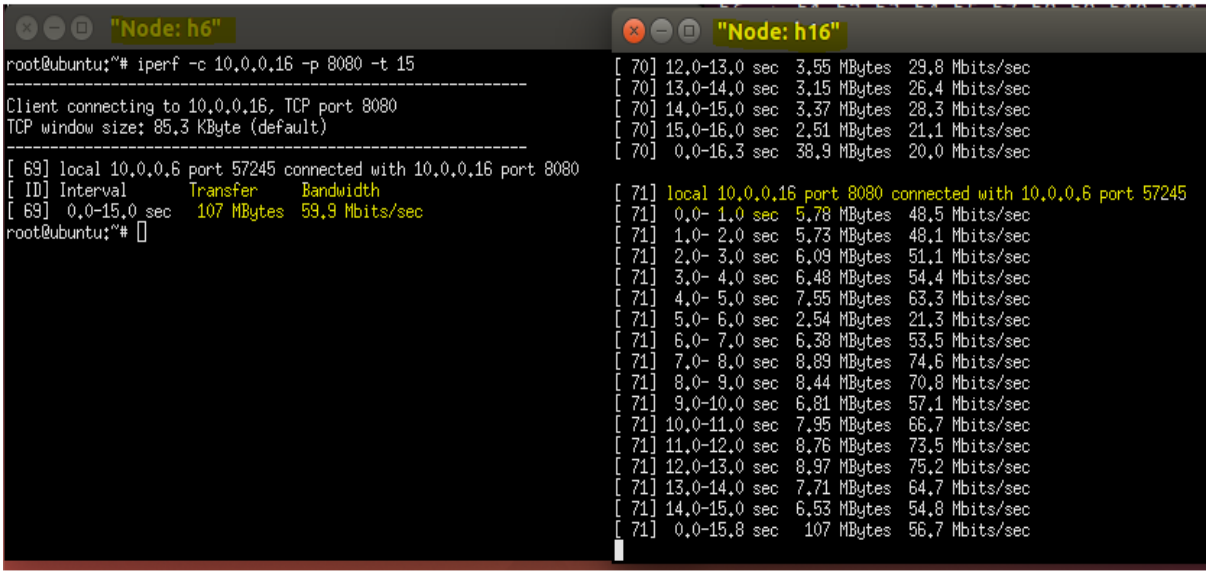


Figura 42: Prueba y resultado TCP del host h6 al host h16 de la red SDN

Fuente: Elaboración propia

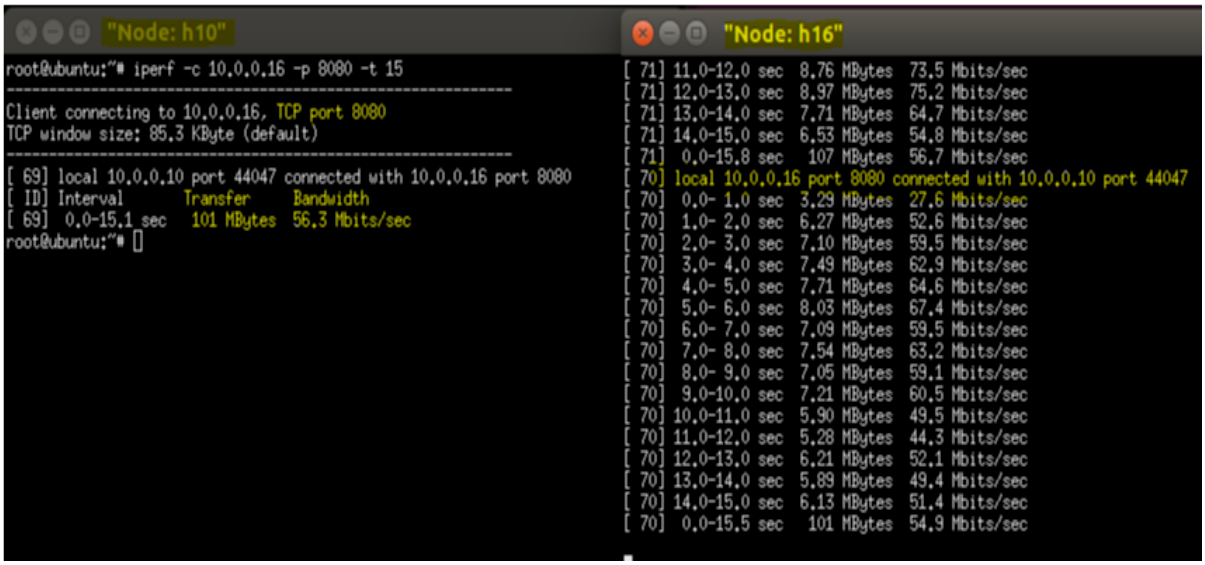


Figura 43: Prueba y resultado TCP del host h10 al host h16 de la red SDN

Fuente: Elaboración propia

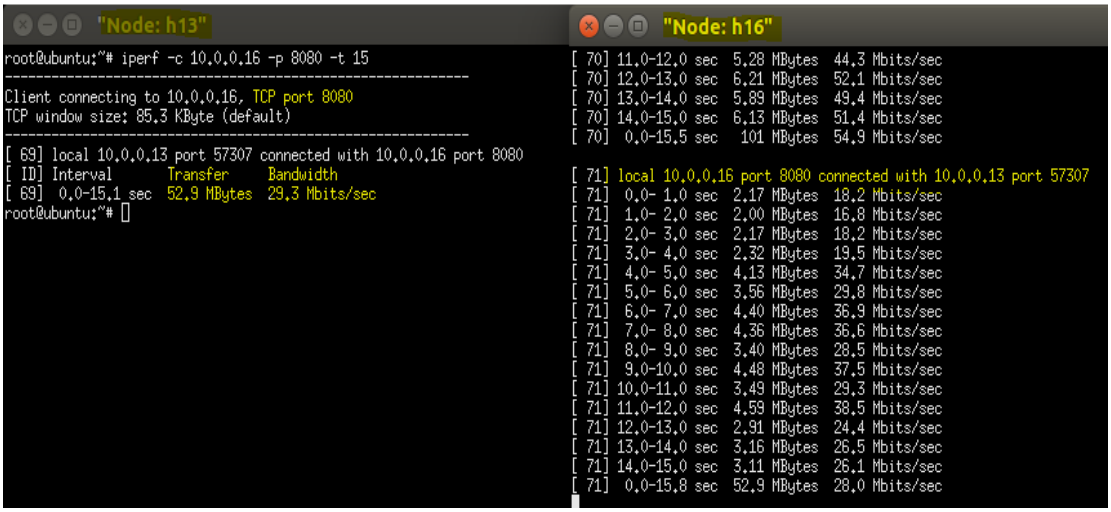


Figura 44: Prueba y resultado TCP del host h13 al host h16 de la red SDN

Fuente: Elaboración propia

Los resultados de estas pruebas a nivel TCP (es usado por varios servicios de red como web, correo, ftp, entre otros), nos arrojan un ancho de banda determinado para los hosts de la red SDN. y que hace referencia al OE1 del proyecto.

REGLAS DE ANCHO DE BANDA	INTERVALO DE TIEMPO	TRANSFERENCIA	ANCHO DE BANDA TOTAL	TIPO DE TRAFICO
H1	0-15 seg.	66.5 Mbps	36.7 Mbits/seg.	TCP
H2	0-15 seg.	110 Mbps	61.7 Mbits/Seg.	TCP
H3	0-15 seg.	38.9 Mbps	21.0 Mbits/seg.	TCP
H6	0-15 seg.	107 Mbps	59.9 Mbits/seg.	TCP
H10	0-15 seg.	101 Mbps	56.3 Mbits/seg.	TCP
H13	0-15 seg.	52.9 Mbps	29.3 Mbits/seg.	TCP

Tabla 26: Reglas de ancho de banda a nivel TCP en la red SDN

Fuente: Elaboración propia

Con estos resultados, simplemente se asocia el Host al tipo/perfil de usuario que maneja el campus universitario quedando de la siguiente manera:

USUARIO	PERFIL/TIPO
H1	DOCENTE
H13	

USUARIO	PERFIL/TIPO
H2	ESTUDIANTE
H6	

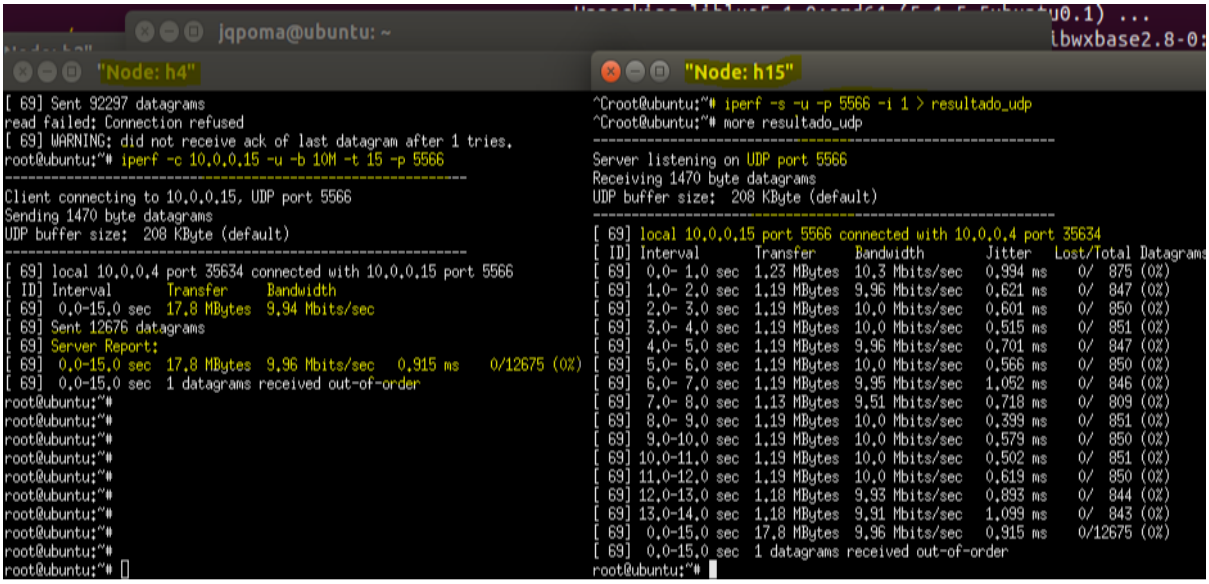
USUARIO	PERFIL/TIPO
H3	ADMINISTRATIVO
H10	

Tabla 27: Host y perfiles de usuario del campus universitario

Fuente: Elaboración propia

- **Tráfico UDP (Jitter)**

  Lo mismo sucede para UDP, en donde se realizaron pruebas con IPERF con un tamaño de buffer de 208 Kbyte (por defecto de la herramienta). Entonces, se configuró al host h15 como servidor utilizando el puerto 8081, y los hosts h4, h8, h11 y h12 como clientes para enviar datos al puerto mencionado.



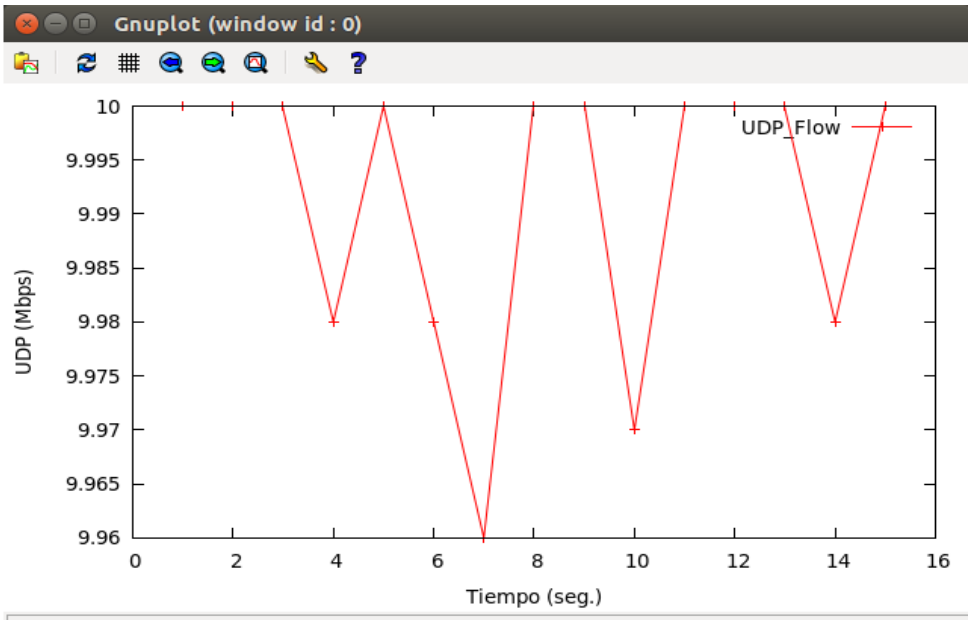
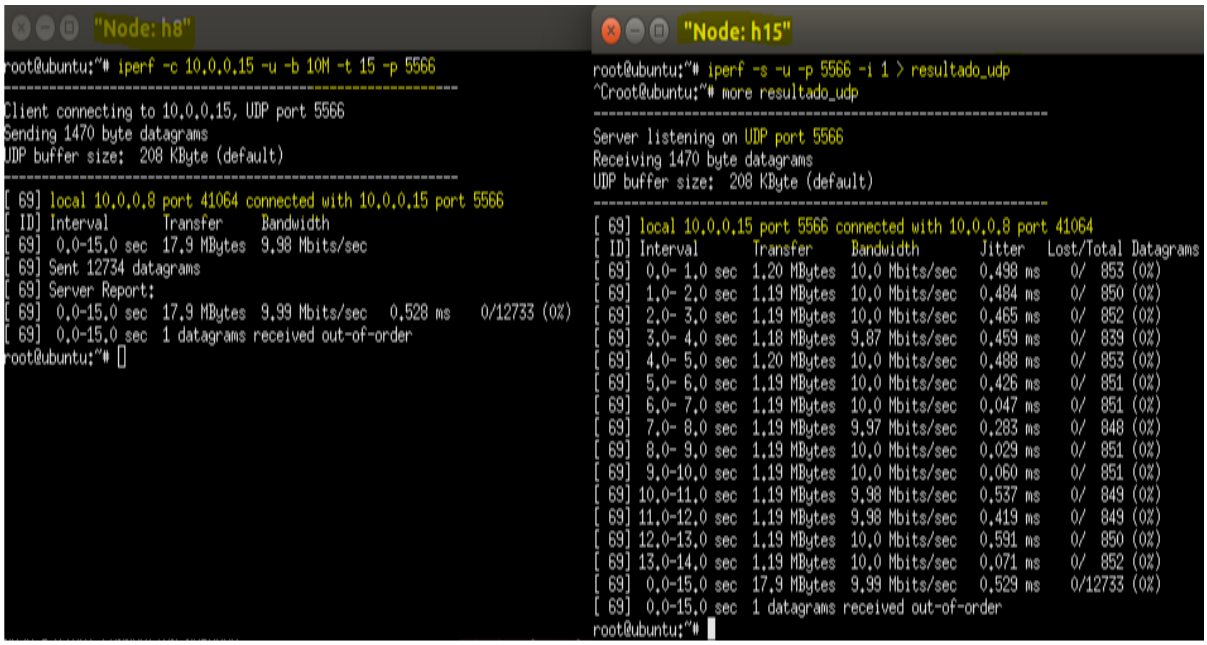


Figura 45: Prueba y resultado UDP del host h4 al host h15 de la red SDN

Fuente: Elaboración propia



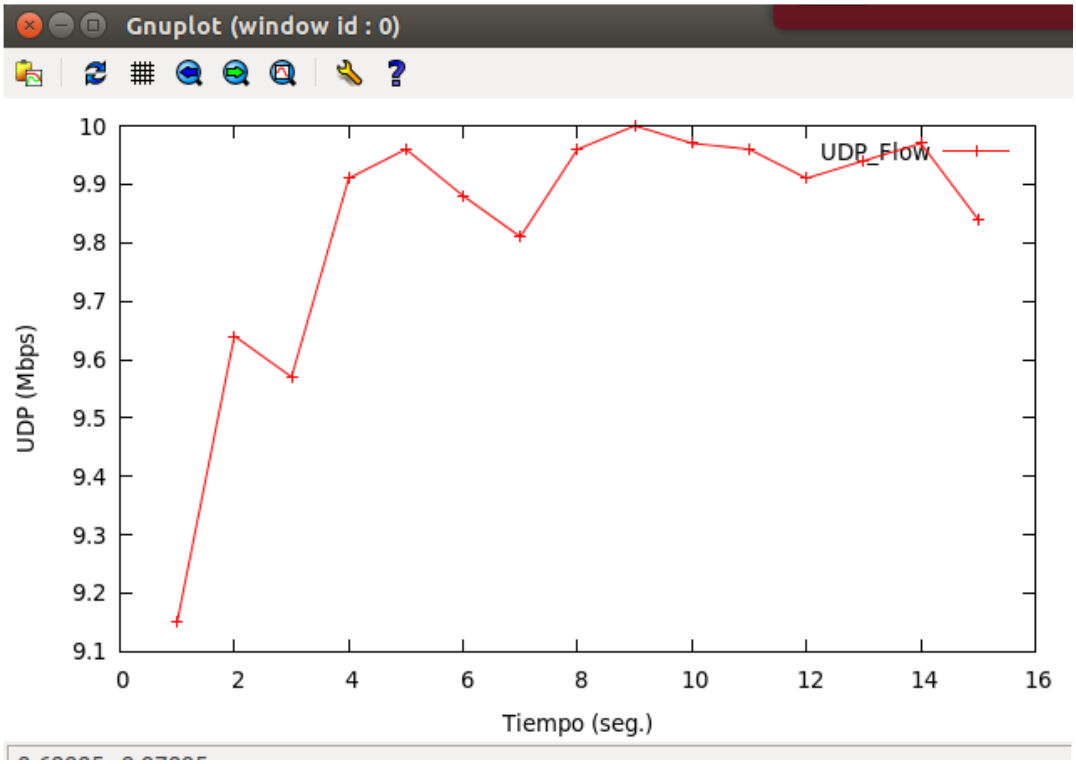
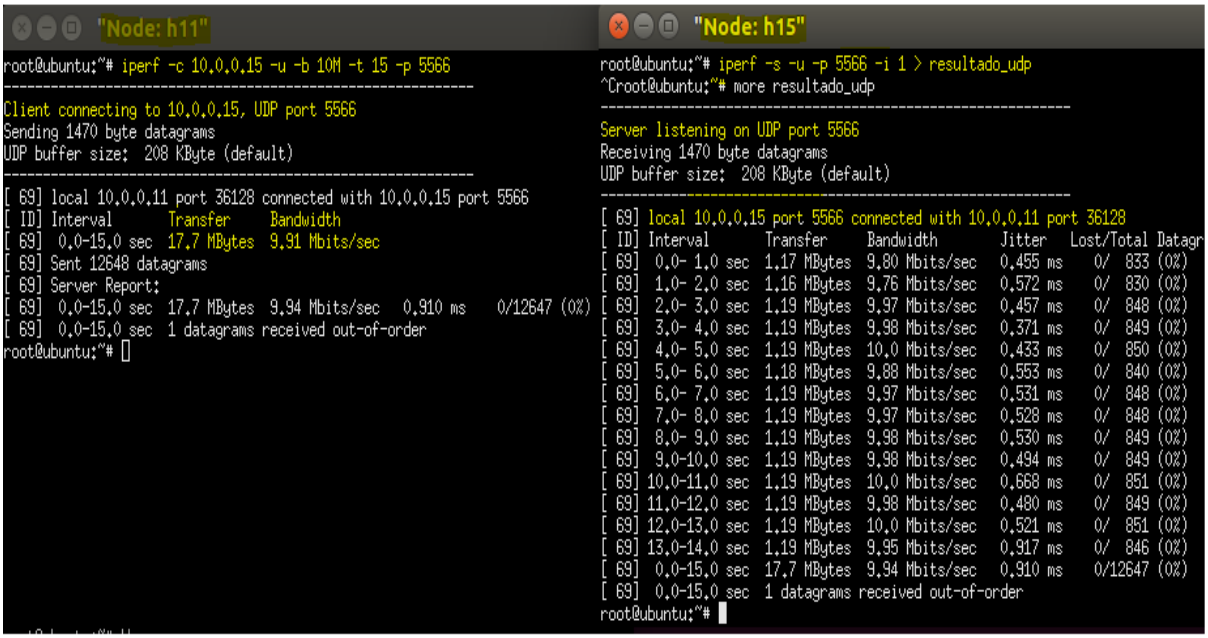


Figura 46: Prueba y resultado de UDP del host h8 al host h15 de la red SDN

Fuente: Elaboración propia



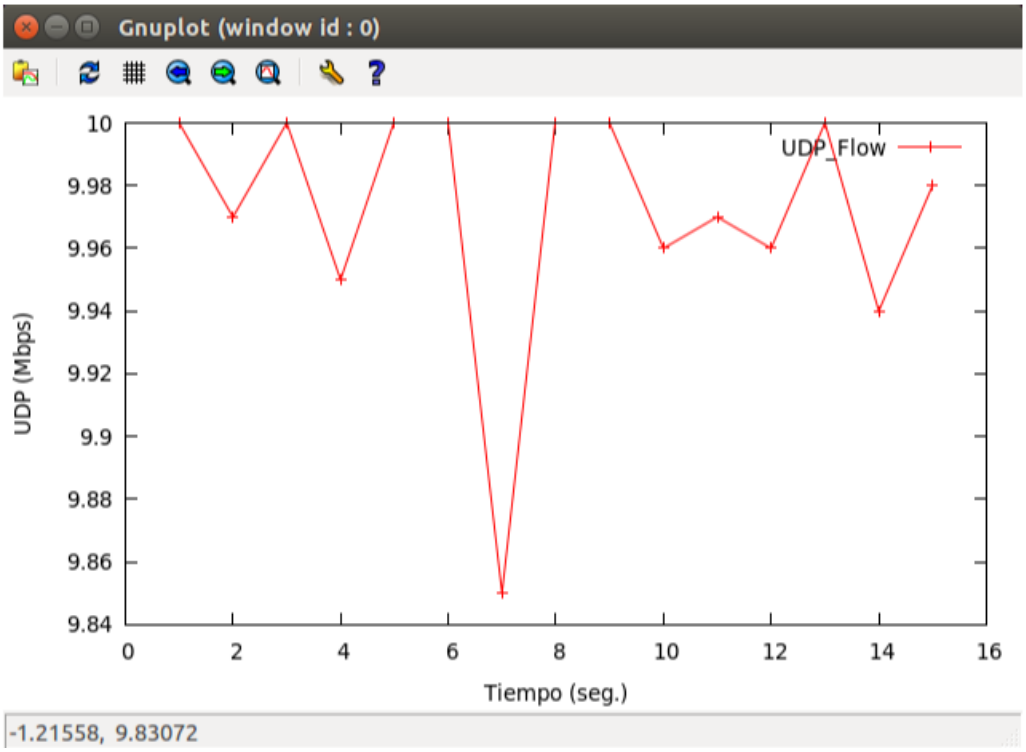
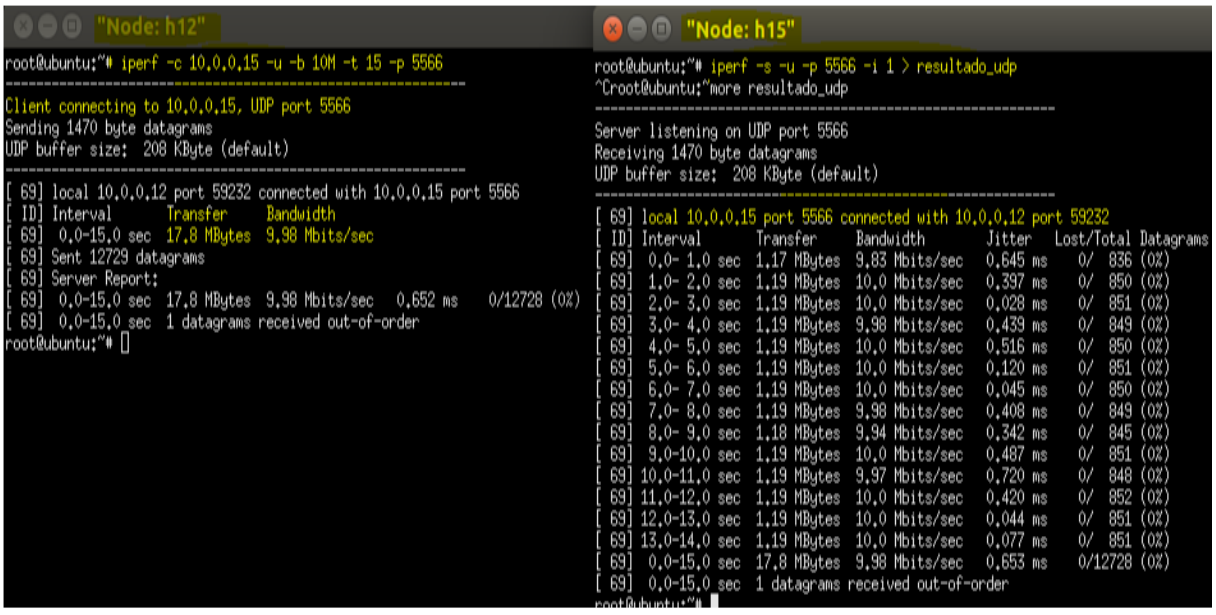


Figura 47: Prueba y resultado de UDP del host h11 al host h15 de la red SDN

Fuente: Elaboración propia



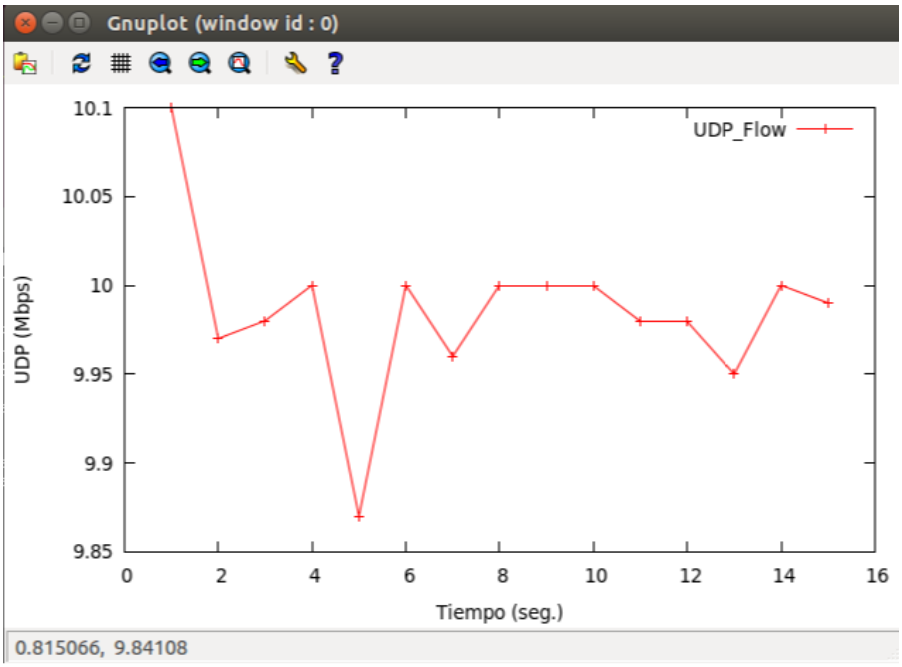


Figura 48: Prueba y resultado de UDP del host h12 al host h15 de la red SDN

Fuente: Elaboración propia

En las Figuras 45, 46, 47 y 48, se pueden apreciar que cada uno de los hosts conectan hacia el servidor h15 y tienen un promedio de ancho de banda entre 17 y 20 Mbps, por lo cual se puede mencionar que la red SDN propuesta puede manejar tráfico UDP con jitter menores a 0.10 mseg. A través de UDP se pueden hacer transmisiones de voz sobre IP (VoIP) y a manera de resumen, se presenta la siguiente Tabla 29.

REGLAS DE ANCHO DE BANDA	INTERVALO DE TIEMPO	JITTER	ANCHO DE BANDA TOTAL	TIPO DE TRAFICO
H4	0-15 seg.	0.915 mseg.	9.94 Mbits/seg.	UDP
H8	0-15 seg.	0.528 mseg.	9.98 Mbits/Seg.	UDP
H11	0-15 seg.	0.910 mseg.	9.91 Mbits/seg.	UDP
H12	0-15 seg.	0.652 mseg.	9.98 Mbits/seg.	UDP

Tabla 28: Reglas de ancho de banda a nivel UDP en la red SDN

Fuente: Elaboración propia

Con estos resultados, simplemente se asocia el Host al tipo/perfil de usuario que maneja el campus universitario quedando de la siguiente manera:

USUARIO	PERFIL/TIPO		USUARIO	PERFIL/TIPO		USUARIO	PERFIL/TIPO
H11	DOCENTE		H8	ESTUDIANTE		H4	ADMINISTRATIVO
			H12				

Tabla 29: Host y perfiles de usuario del campus universitario

Fuente: Elaboración propia

Cabe mencionar que se utilizó la opción GNUPLOT para la visualización a nivel estadístico de los resultados obtenidos en las pruebas. La instalación de esta herramienta se puede observar en el Anexo 3.

5.1.2 Pruebas de conectividad y obtención de tablas de flujo (Módulo L2-Switch)

Para cumplir este ítem, es necesario crear una red SDN bajo el enfoque de OpenDayLight y con la herramienta Mininet para poder realizar las pruebas de conectividad y obtener las tablas de flujo. A través de Mininet, se ofrece la posibilidad de personalizar los hosts para realizar pruebas en la red SDN. Para tal efecto, se tomaron los tiempos de respuesta de cada host/terminal de un switch hacia los otros hosts/terminal de otro switch para crear flujos de datos y medir el rendimiento entre los extremos de la red. En esta prueba, las direcciones IP y MACs de los hosts son los presentados a continuación:

HOST/TERMINAL PC=h	DIRECCION IP	MAC ADDRESS
h1	10.0.0.1	00:00:00:00:01
h2	10.0.0.2	00:00:00:00:02
h3	10.0.0.3	00:00:00:00:03
h4	10.0.0.4	00:00:00:00:04
h5	10.0.0.5	00:00:00:00:05
h6	10.0.0.6	00:00:00:00:06
h7	10.0.0.7	00:00:00:00:07
h8	10.0.0.8	00:00:00:00:08
h9	10.0.0.9	00:00:00:00:09
h10	10.0.0.10	00:00:00:00:10
h11	10.0.0.11	00:00:00:00:11
h12	10.0.0.12	00:00:00:00:12
h13	10.0.0.13	00:00:00:00:13
h14	10.0.0.14	00:00:00:00:14
h15	10.0.0.15	00:00:00:00:15
h16	10.0.0.16	00:00:00:00:16

Tabla 30: Direccionamiento IP/MAC de los hosts/terminales

Fuente: Elaboración propia

Como indica la Tabla 30, los hosts junto con su dirección IP y MAC son vitales para la prueba de ICMP y tener como resultado el flujo de OpenFlow reconocido por el controlador OpenDayLight. Por ello, es sumamente importante la prueba de ICMP ya que caso contrario no habría valores o flujos por evaluar en la topología de red SDN propuesta. Veamos a continuación, la prueba de conectividad rápida y ejecutada con el comando “pingall” en Mininet.

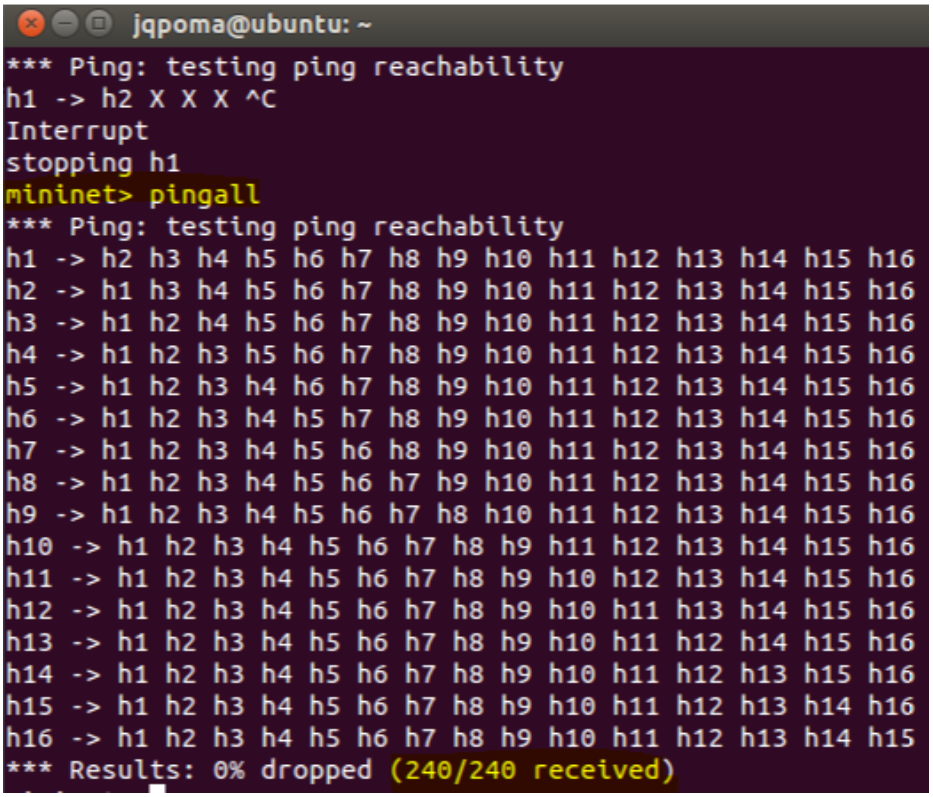


Figura 49: Prueba de ICMP exitosa

Fuente: Elaboración propia

La Figura 49, nos indica que las pruebas a nivel ICMP y por el comando “pingall” son correctas y desde el controlador OpenDayLight tiene visibilidad con los hosts ubicados debajo de la capa de acceso. Lo que sigue es probar la conectividad entre los hosts que son alojados por los diferentes switches de acceso y con ello, podemos crear la tabla de flujo o filtro de red para cada subred local. Es necesario hacer pruebas de manera individual entre todos los hosts y luego proceder con la comparación de tiempos de respuesta con el fin de determinar el rendimiento de una red SDN en comparación con una red tradicional.

Hasta este punto, se demuestra la conformación de la estructura SDN, lo que sigue a continuación son los resultados obtenidos en base esta estructura SDN propuesta.

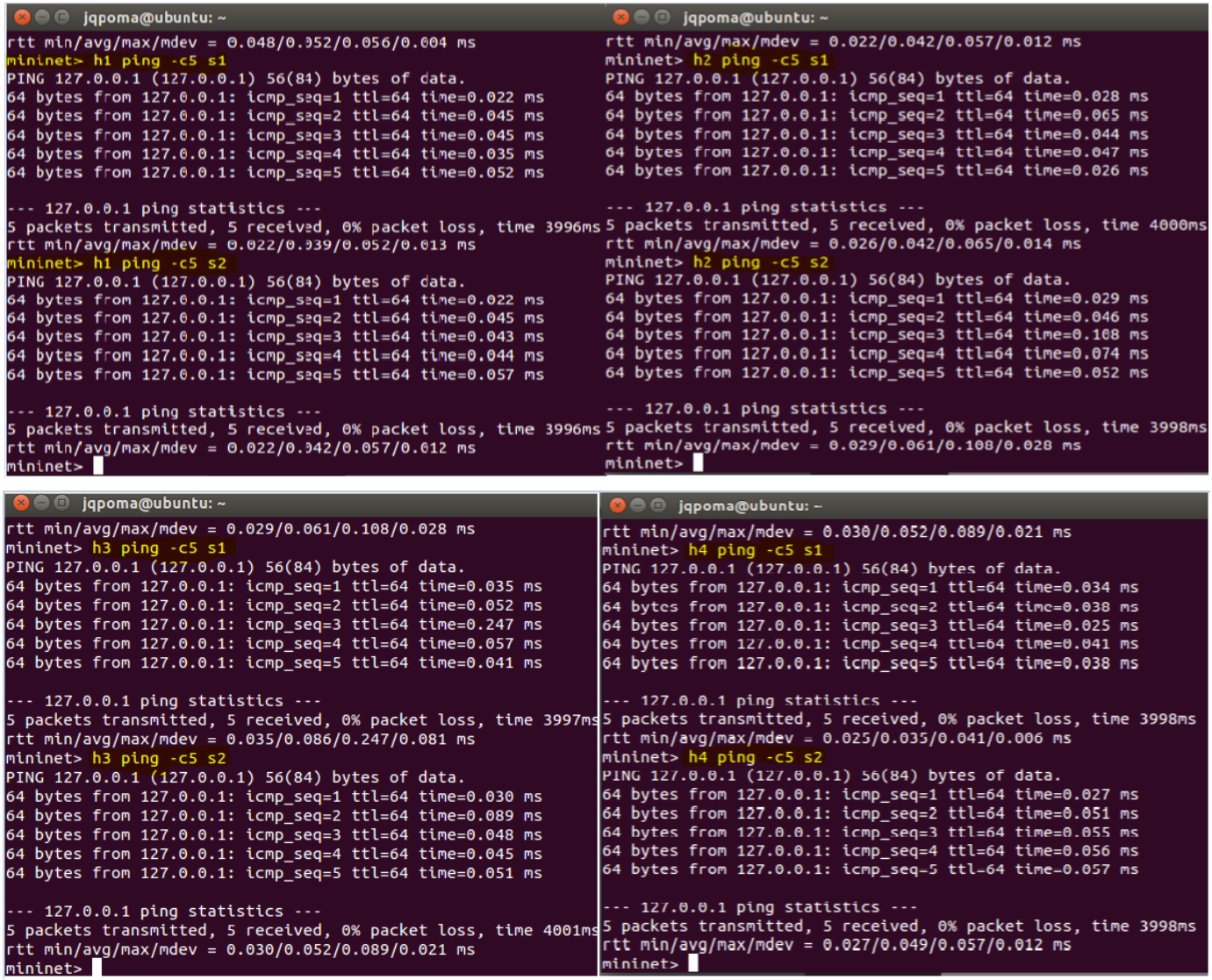


Figura 50: Prueba de ICMP exitosa desde los hosts h1, h2, h3, h4 hacia switches de core

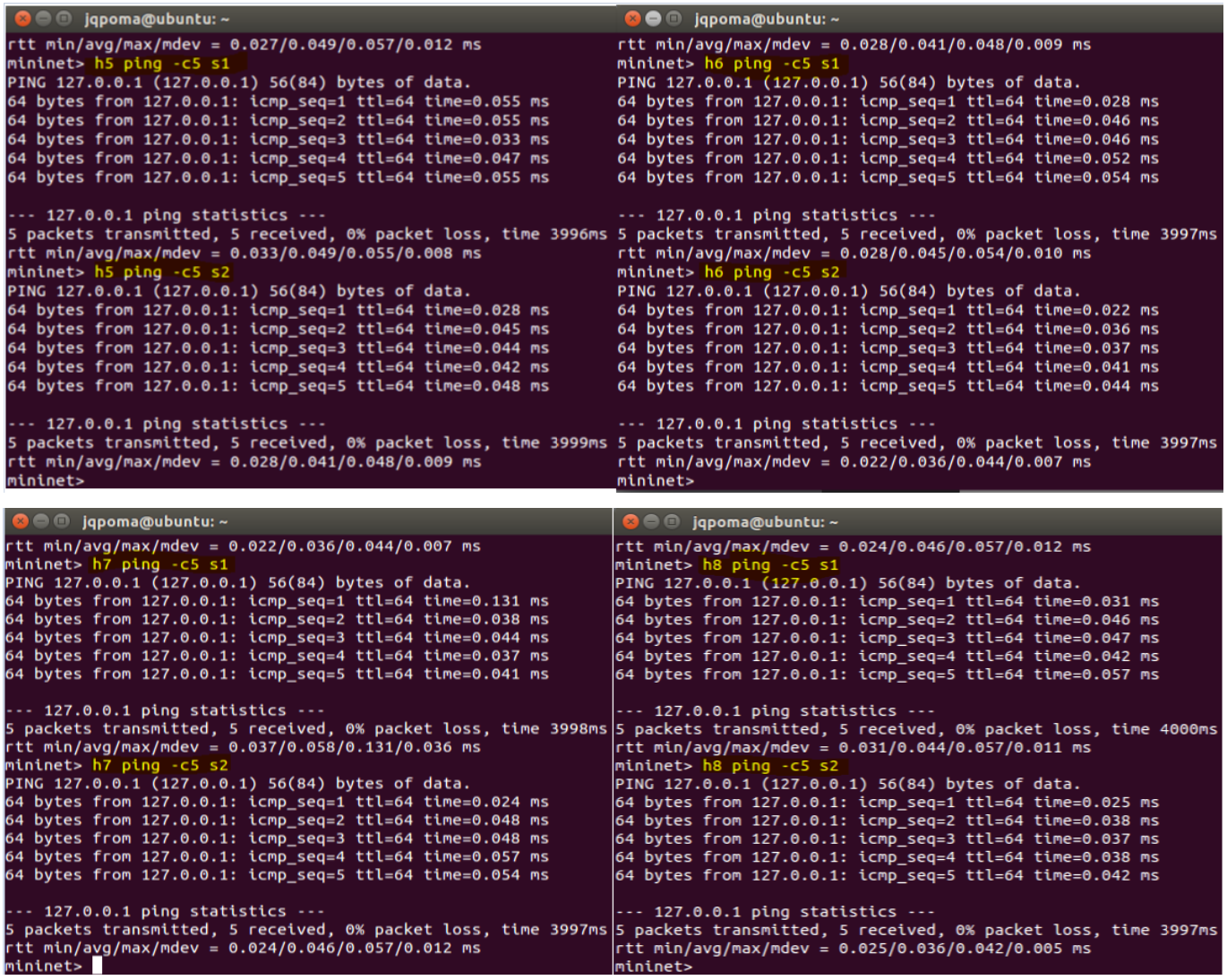


Figura 51: Prueba de ICMP exitosa desde los hosts h5, h6, h7, h8 hacia switches de core

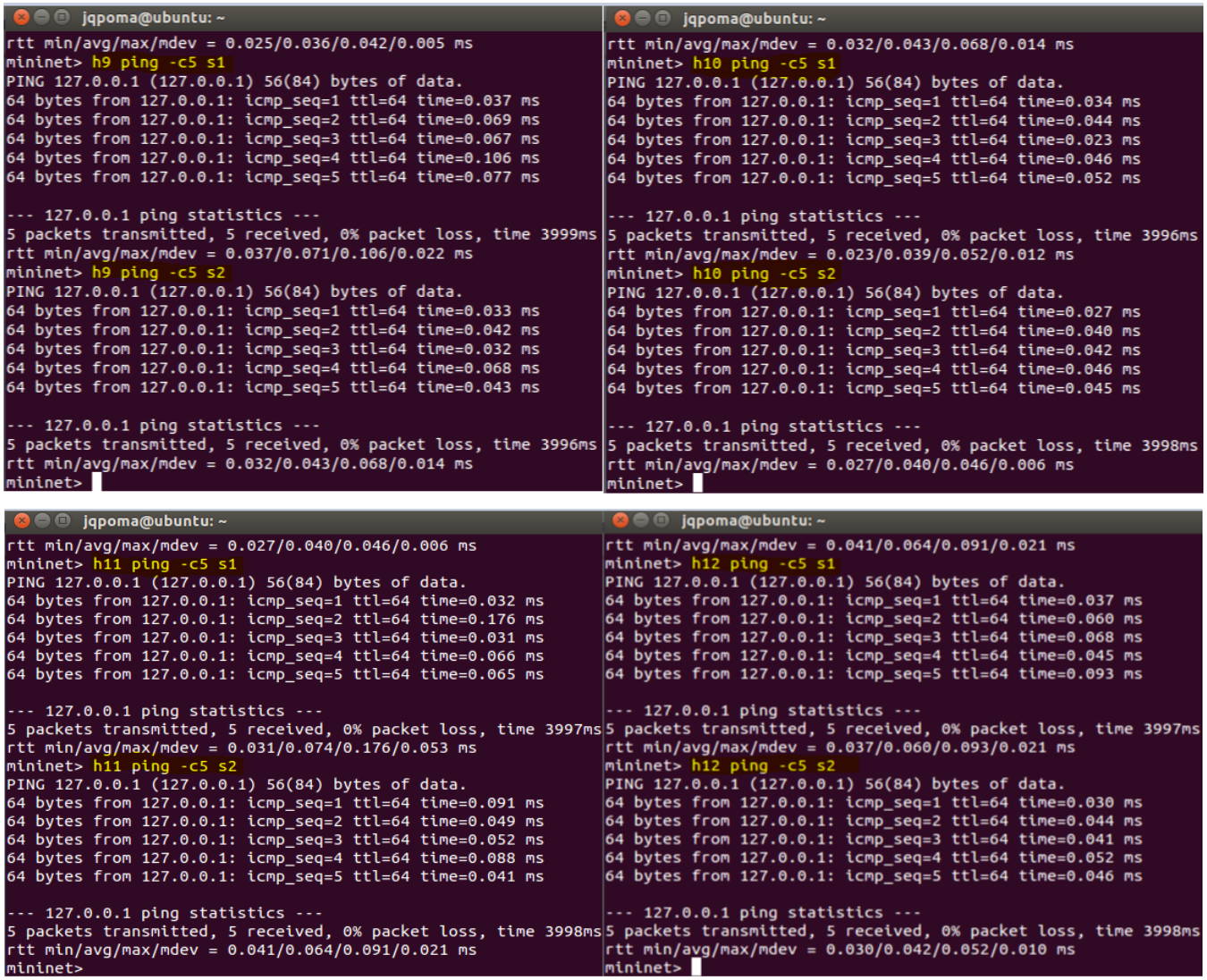


Figura 52: Prueba de ICMP exitosa desde los hosts h9, h10, h11, h12 hacia switches de core

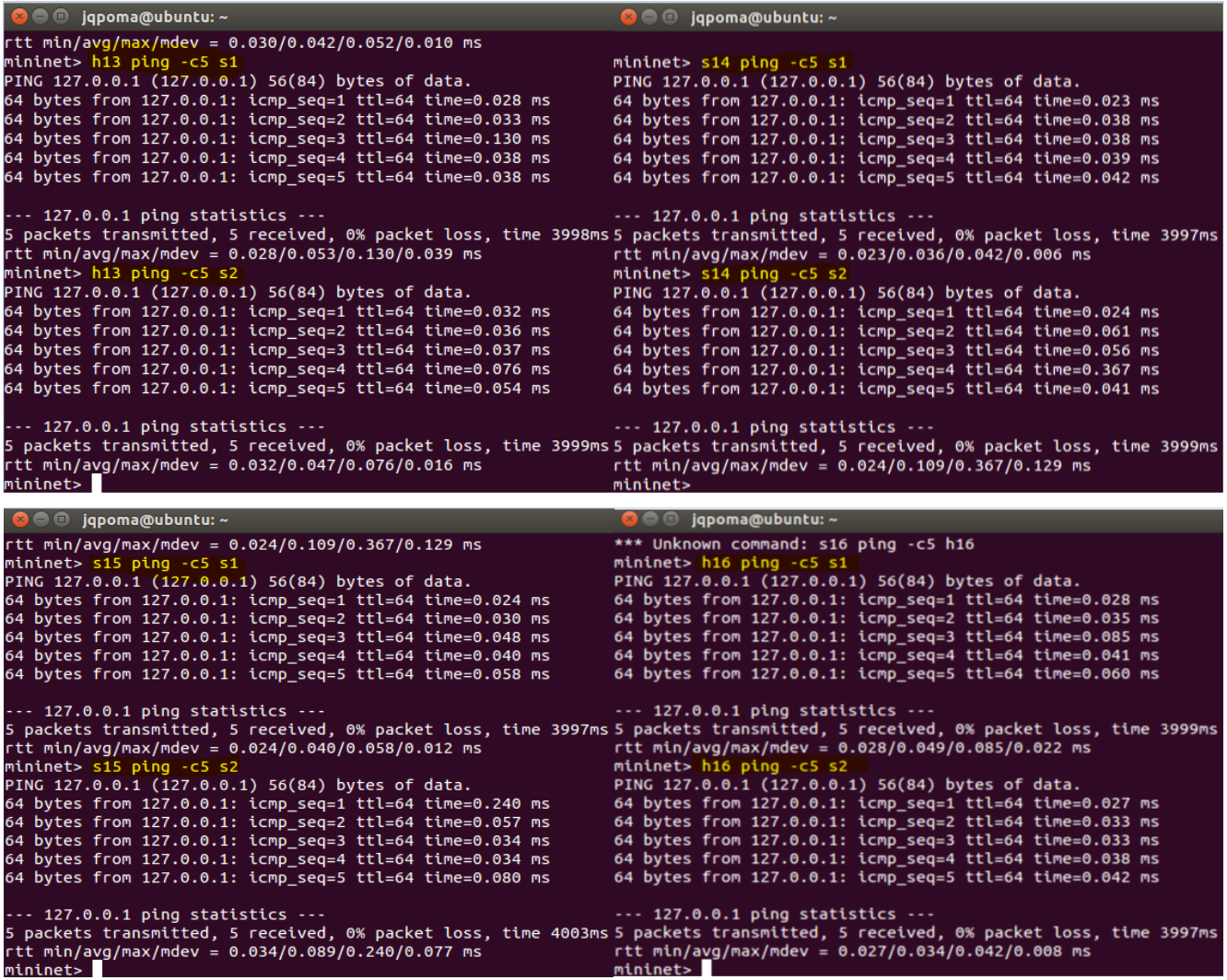


Figura 53: Prueba de ICMP exitosa desde los hosts h13, h14, h15 y h16 hacia switches de core

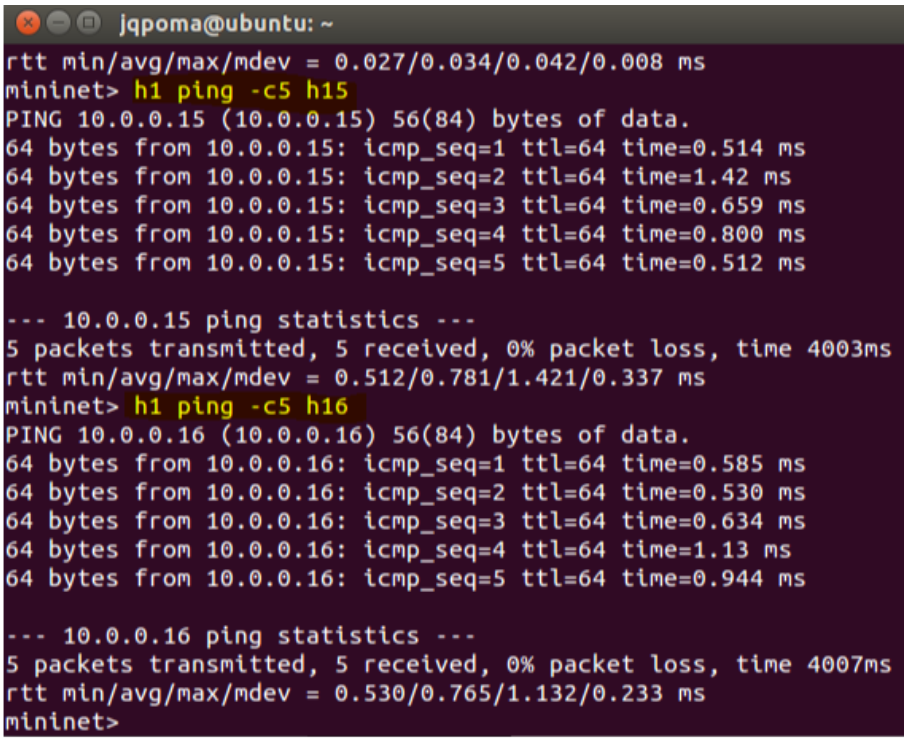


Figura 54: Prueba de ICMP exitosa desde el host h15 hacia h1

Fuente: Elaboración propia

De acuerdo a lo observado desde la Figura 51 a la 54, se visualiza la comunicación de tipo ICMP existente entre todos los hosts mencionados hacia los switches de core. En la Figura 77, se muestra la comunicación ICMP entre los hosts de cada extremo de la topología de red SDN propuesta (se toma estos puntos porque en los hosts del h1 al h10 son usuarios finales y del h14 al h16 porque son servidores y por ello la conectividad entre uno y otro host). Cabe indicar, el resultado de la prueba de ping no solo aplica a los hosts extremos, sino también entre todos los hosts interconectados debajo de los switches de acceso como muestra la topología de red SDN. Para verificar los tiempos de respuesta de los demás hosts (Ver Tabla 31).

Partiendo de estas pruebas, lo que continua es elaborar algunas tablas que permitan determinar el tiempo de respuesta tanto de los hosts hacia los switches de core y también, el tiempo de respuesta entre los hosts de los extremos de la red SDN.

HOST/TERMINAL	TIEMPO DE RESPUESTA - PRUEBA ICMP HACIA SW CORE 1				
	1ro	2do	3ro	4to	5to
h1	0.022	0.045	0.045	0.035	0.052
h2	0.028	0.065	0.044	0.047	0.026
h3	0.035	0.052	0.247	0.057	0.041
h4	0.034	0.038	0.025	0.041	0.038
h5	0.055	0.055	0.033	0.047	0.055
h6	0.028	0.046	0.046	0.052	0.054
h7	0.131	0.038	0.044	0.037	0.041
h8	0.031	0.046	0.047	0.042	0.057
h9	0.037	0.069	0.067	0.106	0.077
h10	0.034	0.044	0.023	0.046	0.052
h11	0.032	0.176	0.031	0.066	0.065
h12	0.037	0.06	0.068	0.045	0.093
h13	0.028	0.033	0.13	0.038	0.038
h14	0.023	0.038	0.038	0.039	0.042
h15	0.024	0.03	0.048	0.04	0.058
h16	0.028	0.035	0.085	0.041	0.06
TOTAL	0.607	0.87	1.021	0.779	0.849

Tabla 31: Resultados de tiempo de respuesta (ms) hacia Sw Core 1

Fuente: Elaboración propia

HOST/TERMINAL	TIEMPO DE RESPUESTA - PRUEBA ICMP HACIA SW CORE 2				
	1ro	2do	3ro	4to	5to
h1	0.022	0.045	0.043	0.044	0.057
h2	0.029	0.046	0.108	0.074	0.052
h3	0.03	0.089	0.048	0.045	0.051
h4	0.027	0.051	0.055	0.056	0.057
h5	0.028	0.045	0.044	0.042	0.048
h6	0.022	0.036	0.037	0.041	0.044
h7	0.024	0.048	0.048	0.057	0.054
h8	0.025	0.038	0.037	0.038	0.042
h9	0.033	0.042	0.032	0.068	0.043
h10	0.027	0.04	0.042	0.046	0.045
h11	0.091	0.049	0.052	0.088	0.041
h12	0.03	0.044	0.041	0.052	0.046
h13	0.032	0.036	0.037	0.076	0.054
h14	0.024	0.061	0.056	0.367	0.041
h15	0.24	0.057	0.034	0.034	0.08
h16	0.027	0.033	0.033	0.038	0.042
TOTAL	0.711	0.76	0.747	1.166	0.797

Tabla 32: Resultados de tiempo de respuesta (ms) hacia Sw Core 2

HOST/TERMINAL	TIEMPO DE RESPUESTA - PRUEBA ICMP ENTRE HOSTS				
	1ro	2do	3ro	4to	5to
h1	0.022	0.045	0.045	0.035	0.052
h2	0.028	0.065	0.044	0.047	0.026
h3	0.035	0.052	0.247	0.057	0.041
h4	0.024	0.061	0.056	0.367	0.041
h5	0.24	0.057	0.034	0.034	0.08
h6	0.027	0.033	0.033	0.038	0.042
h7	0.024	0.048	0.048	0.057	0.054
h8	0.025	0.038	0.037	0.038	0.042
h9	0.033	0.042	0.032	0.068	0.043
h10	0.023	0.038	0.038	0.039	0.042
h11	0.024	0.03	0.048	0.04	0.058
h12	0.028	0.035	0.085	0.041	0.06
h13	0.022	0.045	0.045	0.035	0.055
h14	0.028	0.065	0.044	0.047	0.038
h15	0.035	0.052	0.247	0.057	0.056
h16	0.055	0.055	0.033	0.047	0.049
TOTAL	0.673	0.761	1.116	1.047	0.779

Tabla 33: Resultados de tiempo de respuesta (ms) entre hosts/terminales

Fuente: Elaboración propia

En las Tablas 32 y 33, se pueden observar el tiempo de respuesta total por conteo de 5 en la prueba ICMP de todos los hosts hacia el switch core 1 y 2, respectivamente. Esto nos indica que el paquete enviado en el 3er intento de la Tabla 51, posee un tiempo de respuesta mayor a 1ms porque el OpenFlow aún no determina las tablas de flujos o filtros necesarios para dejar seguir al paquete de datos. Dicho paquete es enviado por el host de manera encapsulada hacia el switch de acceso y a su vez, enviado al controlador OpenDayLight a través de un mensaje ARP (solo hasta el switch de acceso) y luego genera un mensaje de envío (Packet In).

Entonces el controlador recibe el paquete y usa el módulo L2-Switch para procesar la solicitud enviada. El controlador nuevamente envia un mensaje de tipo “Packet Out” para emitir o difundir un mensaje de tipo broadcast por todos los puertos del switch (con excepción del puerto por el cual recibió el paquete). Seguidamente, con la trama completa, el host/terminal origen envía los paquetes ICMP con las direcciones IP asignadas del destino y el switch con OpenFlow los encapsula nuevamente para enviarlo al controlador

OpenDayLight a través del mensaje “Packet In”. El controlador ODL vuelve a recibir el paquete y realiza la búsqueda en su base de datos o denominado “Address Tracker” del módulo L2 Switch para ubicar al host destino dentro de la topología de red SDN.

De esta manera, las tablas de flujo quedan agregadas en el switch con OpenFlow y los siguientes paquetes ICMP enviados tienen un tiempo de respuesta menor a 1 ms. El módulo L2 Switch actualizará las tablas de flujo de acuerdo a los eventos que sucedan en la red SDN como por ejemplo el estado de un puerto, un enlace inactivo o la agregación de un nuevo host/terminal en la red. Para validar lo mencionado a continuación se presenta las tablas de flujo de los switches de core y distribución en el controlador OpenDayLight.

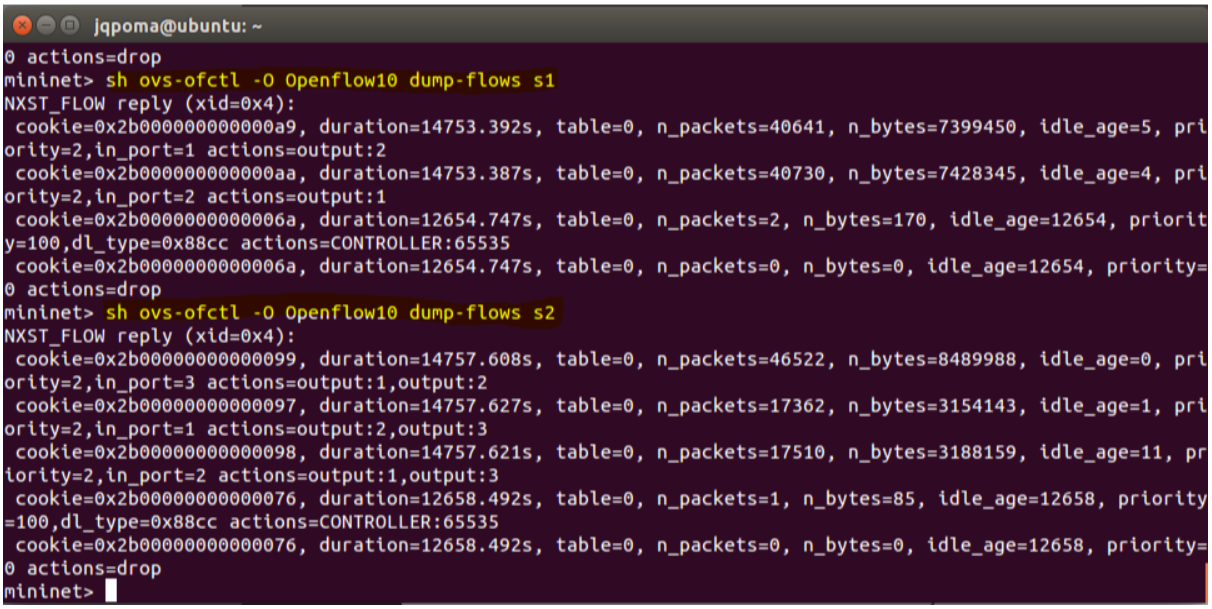


Figura 55: Entradas de flujo en el controlador ODL y switch core 1 y 2

Fuente: Elaboración propia

En la Figura 5, se puede validar que el controlador OpenDayLight instaló de manera correcta las entradas de flujo en los switches y a través del protocolo OpenFlow, esto de forma automática y sin alguna petición de un dispositivo de red en la topología propuesta. Lo mismo sucede para los switches de distribución s3, s4, s5 y s6 como se muestra a continuación.

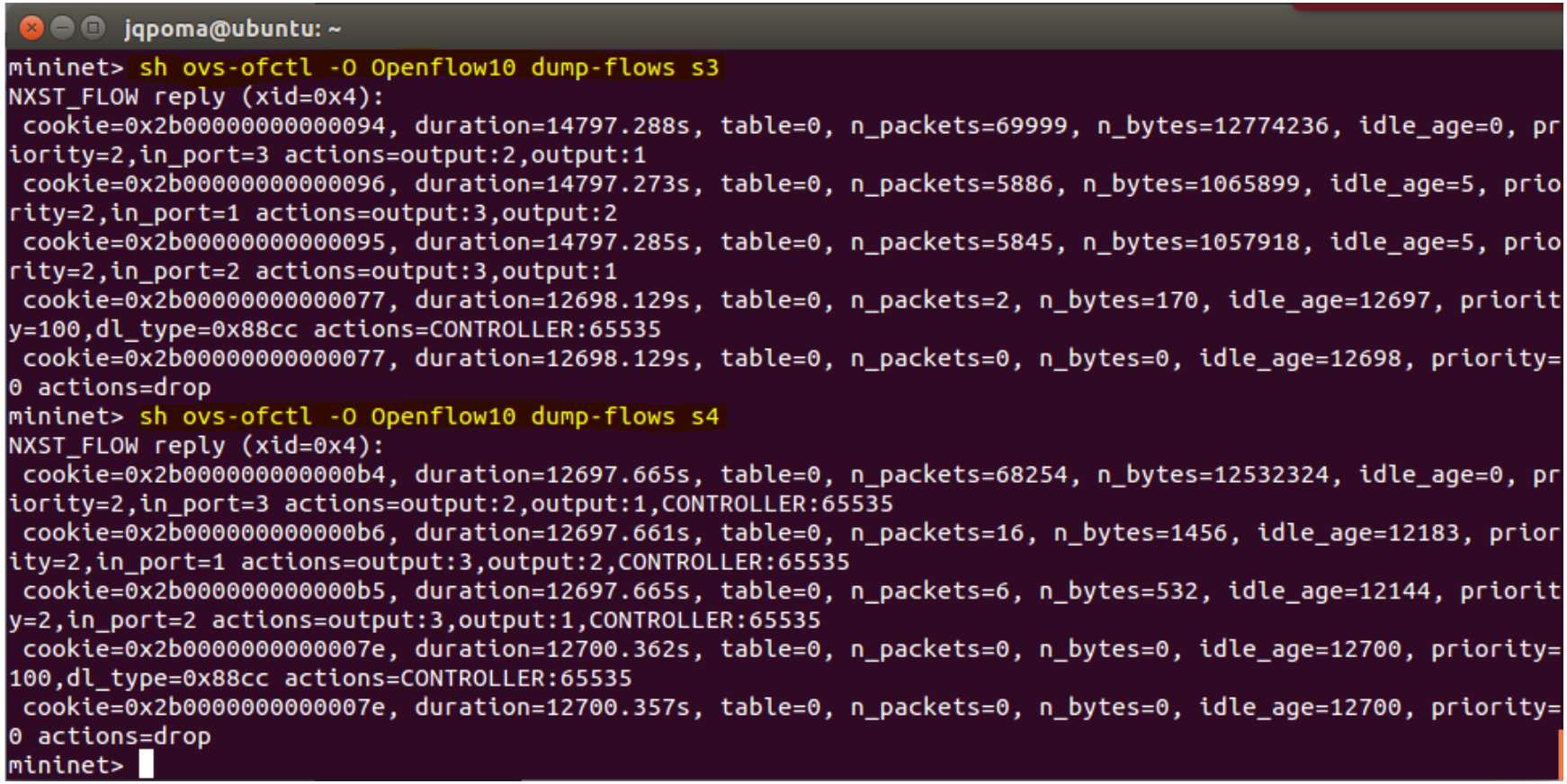


Figura 56: Entradas de flujo en el controlador ODL y switches s3 y s4

Fuente: Elaboración propia

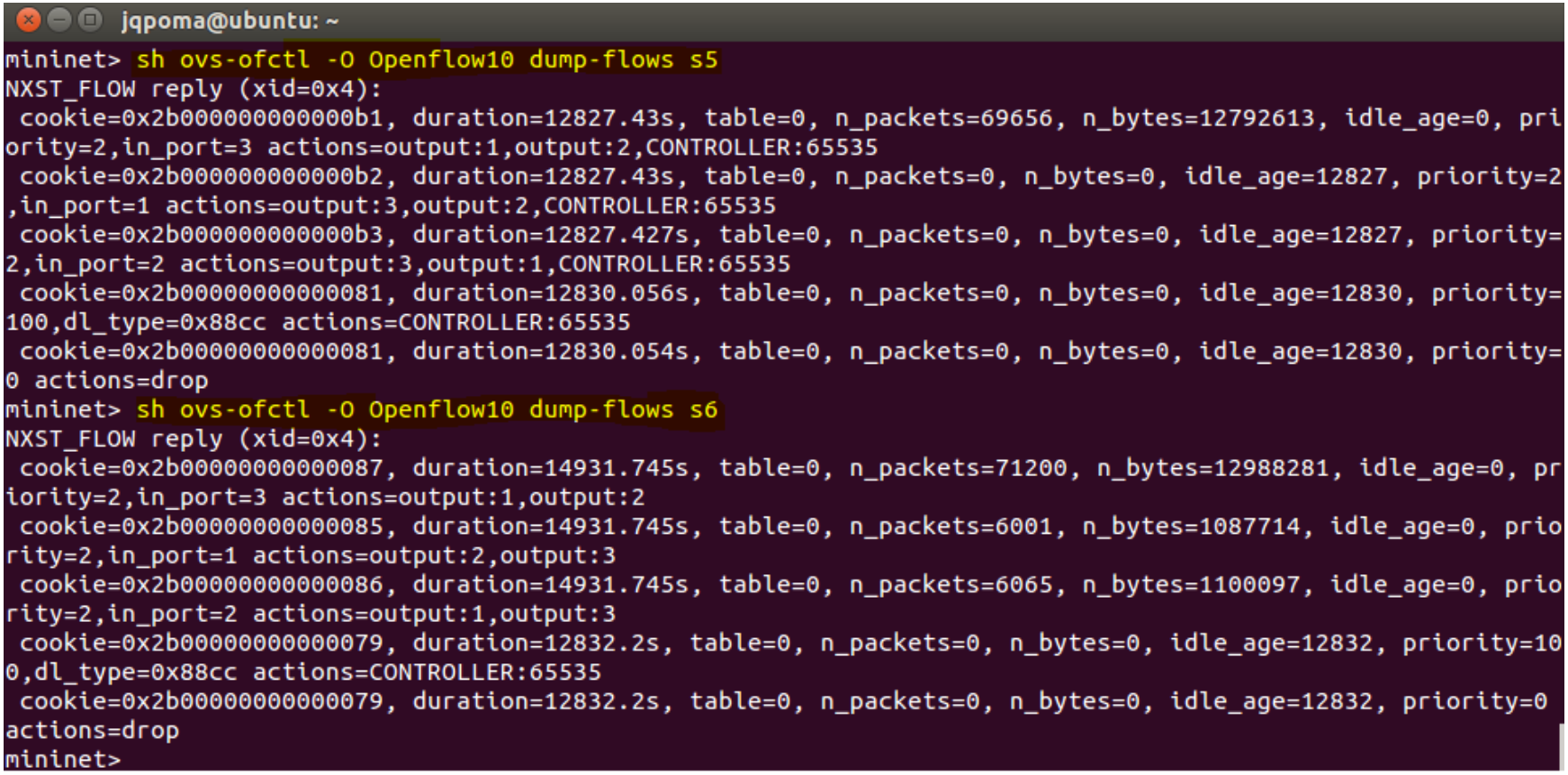


Figura 57: Entradas de flujo en el controlador ODL y switches s5 y s6

Fuente: Elaboración propia

El resultado de estas tablas de flujo (Ver Anexo 1) brinda datos del tráfico de la red desde el controlador ODL centralizado y sin tocar conmutadores individuales de la topología de red SDN. Ahora si entramos en detalle, se puede utilizar segmentos de red variados y siguiendo la misma secuencia de los puntos anteriores, es decir, el nombre del host/terminal no cambia y solo se modifican las direcciones IP para continuar. Cabe indicar, que el módulo L2-Switch es quien instala las entradas de flujos para determinar si hay conectividad o no entre los hosts de diferentes segmentos de red (usando variables específicas de cookies puede identificar, registrar y descartar peticiones basado en la duración de flujo y límites de conexión).

HOST/TERMINAL PC=h	DIRECCION IP	MAC ADDRESS
h1	192.168.1.100/24	00:00:00:00:01
h5	10.10.10.15/24	00:00:00:00:05
h14	192.168.1.101/24	00:00:00:00:14

Tabla 34: Direccionamiento IP para prueba de filtros

Fuente: Elaboración propia

Continuando, el módulo L2-Switch es quien instala las entradas de flujo para la comunicación entre los hosts (para la prueba, se utiliza h1 y h14 como parte del segmento 192.168.1.0/24 y h5 como parte del segmento 10.10.10.0/24).

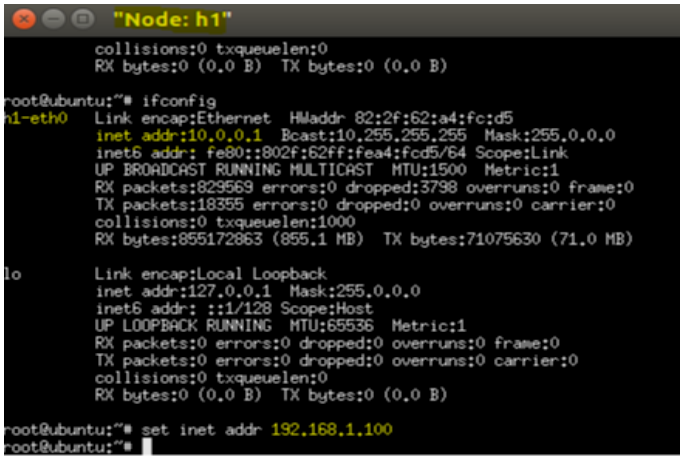


Figura 58: Cambio de dirección IP a host h1

Fuente: Elaboración propia

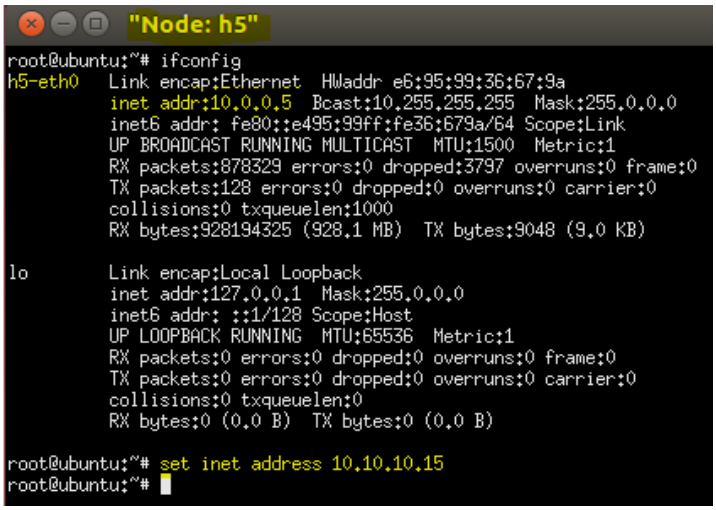


Figura 59: Cambio de dirección IP a host h5

Fuente: Elaboración propia

Con la información completa de la prueba, el módulo L2-Switch actualizará las tablas de flujos de acuerdo a los eventos de la red (en este caso, por la inclusión de un nuevo host ante el cambio de dirección ip y mac).


```
-<flow-statistics>
    <byte-count>0</byte-count>
  -<duration>
      <second>698</second>
      <nanosecond>720000000</nanosecond>
    </duration>
    <packet-count>0</packet-count>
  </flow-statistics>
  <cookie>3026418949592973369</cookie>
  <idle-timeout>1800</idle-timeout>
  <hard-timeout>3600</hard-timeout>
</flow>
```


Figura 60: Repositorio h1 “Address-tracker” del módulo L2-Switch

Fuente: Controlador ODL

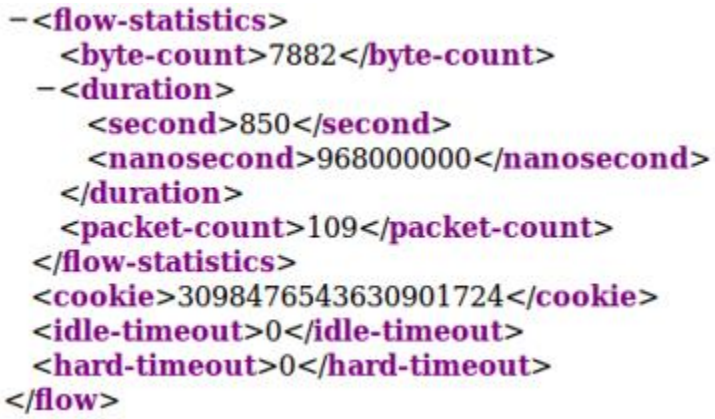


Figura 61: Repositorio h5 "Address-tracker" del módulo L2-Switch

Fuente: Controlador ODL

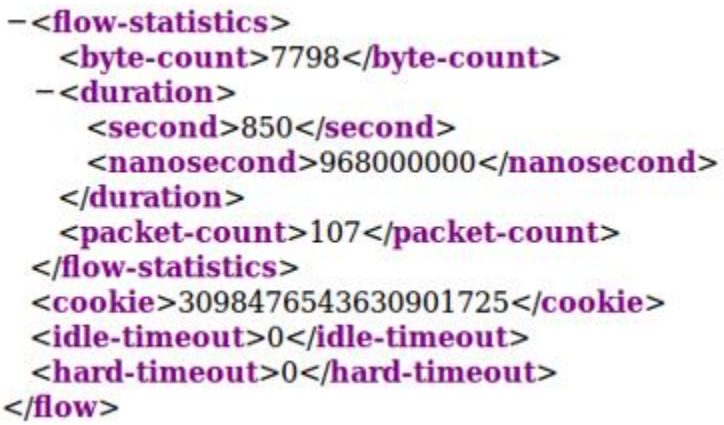


Figura 62: Repositorio h14 "Address-tracker" del módulo L2-Switch

Fuente: Controlador ODL

Los resultados obtenidos son los observados en la parte de duración, cookies y timeout de las tablas de flujos del repositorio de módulo L2-Switch. Si bien nos muestra algo más de información, lo que nos interesa son los tres ítems mencionados ya que una variación mínima en alguno de ellos, y automáticamente el módulo no procesa la solicitud de respuesta de otro elemento de la red y ejecuta una acción.

FILTROS (TABLAS DE FLUJO)	COOKIES	DURACION	TIMEOUT	Packet Count
H1 - Aulas	3026418949592970000	698 seg.	1800-3600 seg.	0
H5 - Pab F	309847654360901000	850 seg.	0 seg.	109
H14 - Administrativos	3098476543672590000	850 seg.	0 seg.	107

Tabla 35: Resultado de los filtros en base a las tablas de flujo

Fuente: Elaboración propia

Para observar todas las tablas de flujo, estas se encuentran en la parte de Anexo 2 y tener un mayor detalle de otros segmentos de red. En esta prueba, se consideró y nombró a Pabellón F, Aulas y Administrativos del campus universitario y en donde, el controlador OpenDayLight instaló correctamente las entradas sobre OpenFlow de forma automática y sin ayuda o soporte de algún dispositivo de red.

5.1.3 Topología de red y equipamiento tecnológico para la red LAN

En referencia a la topología de red, esta fue dada en un inicio como la topología de red actual. Sin embargo, se propone una nueva propuesta para la organización en donde se basa en Mininet, por temas de un mejor entendimiento se plantea la topología de una manera más exacta y como sigue a continuación:

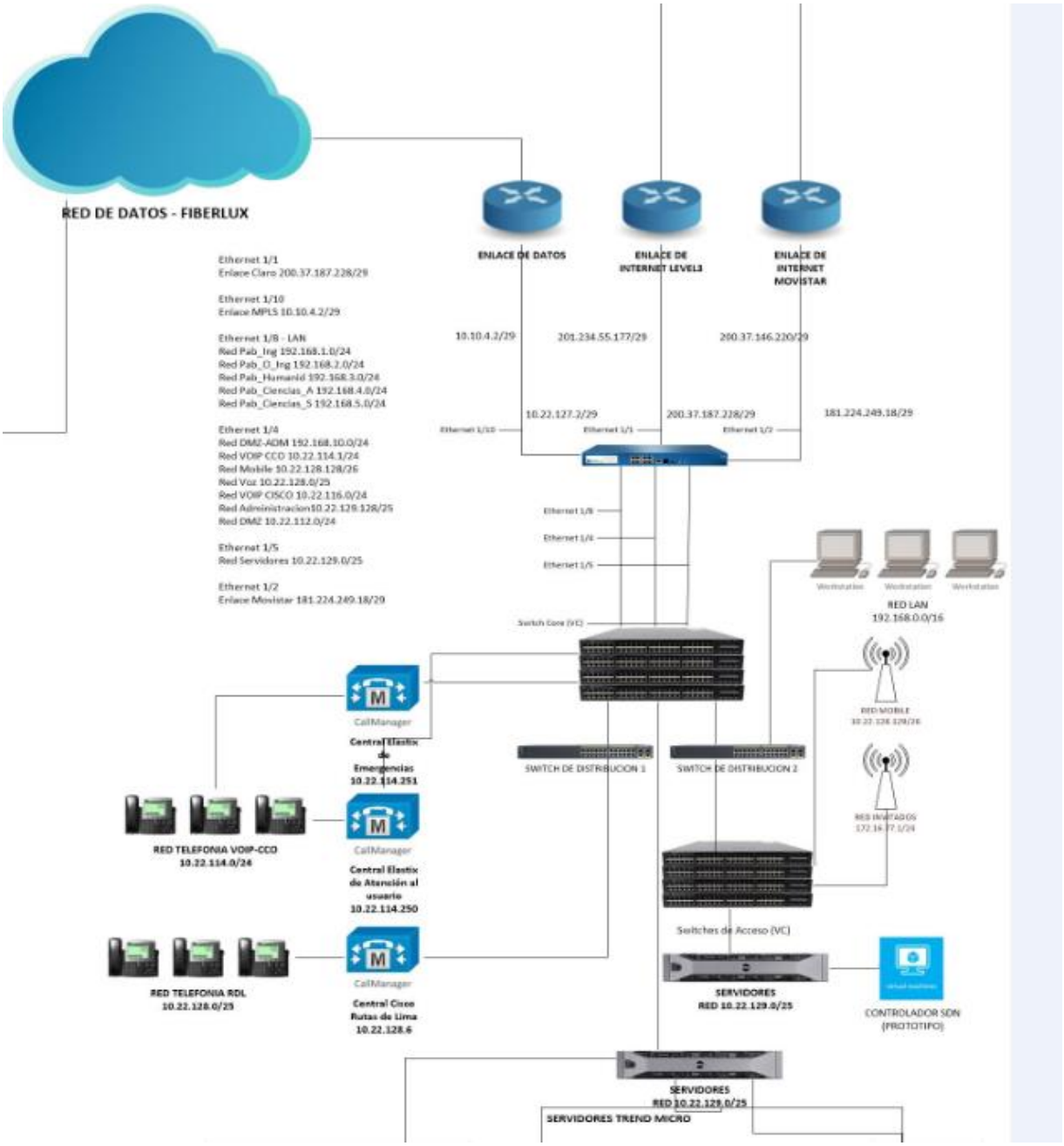


Figura 63: Topología de red LAN propuesta (Parte 1)

Fuente: Elaboración propia

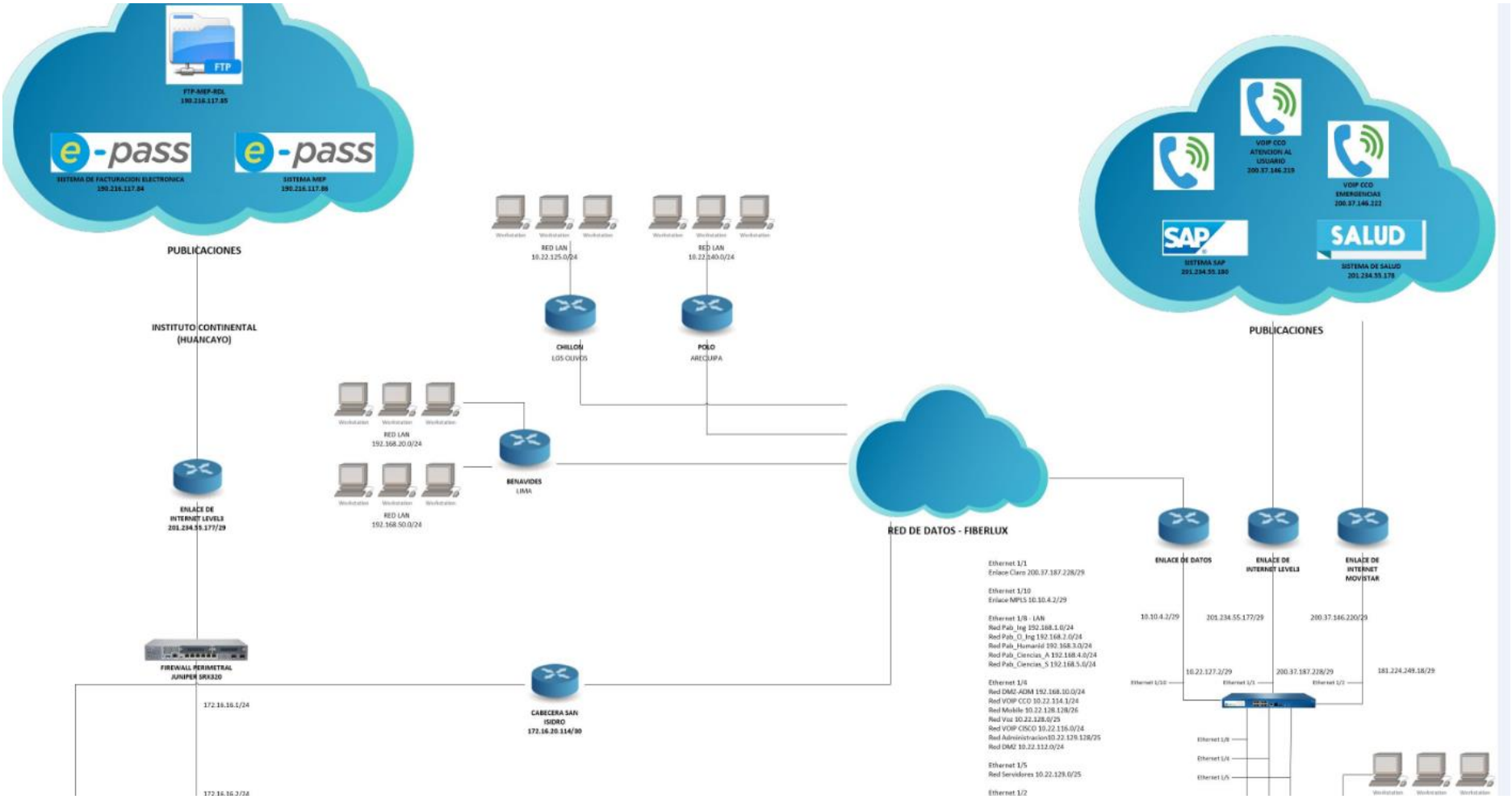


Figura 64: Topología de red LAN propuesta – Vista General (Parte 2)

Fuente: Elaboración propia (Visio-Mininet)

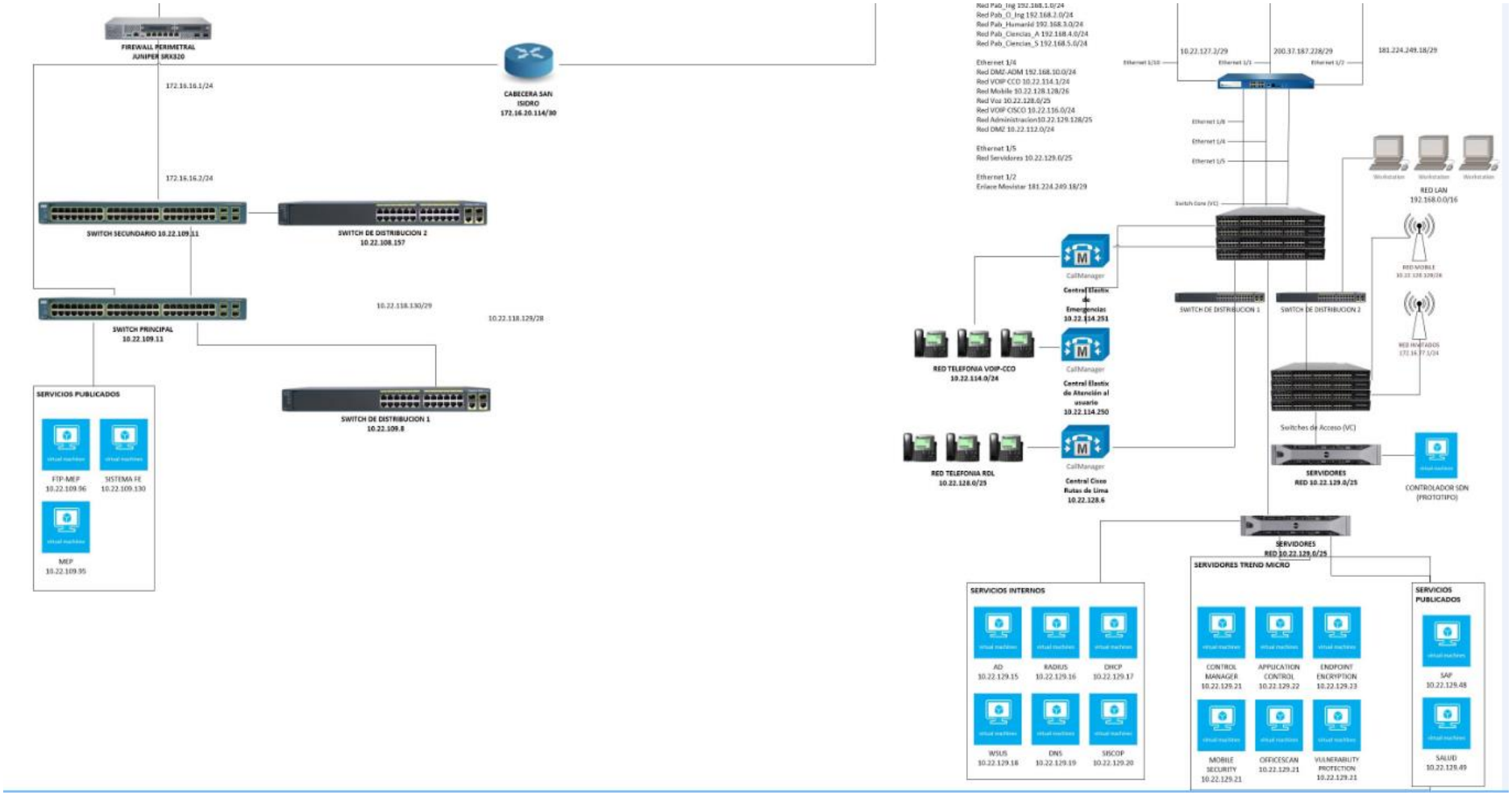


Figura 65: Topología de red LAN propuesta – Vista General (Parte 3)

Las Figuras 64 al 65 comprende una sola topología de red, la idea es mostrar la diferencia que existe con la topología actual que tiene el campus univesitario. Por ejemplo, se agregaron switches de core, distribución y acceso para la red LAN, se introdujo un servidor adicional que soporte el prototipo SDN sobre la misma red LAN, se establecen los segmentos de red, los enlaces de internet mencionados en el análisis del problema (Capìtulo 03). En referencia a la descripción de cada uno de ellos y si los dispositivos de red cumplen el diseño con la solución propuesta, lo veremos a continuación:

Como se mencionó anteriormente, existen varios switches obsoletos y desactualizados siendo su rol muy importante para soportar el tráfico de gran tamaño (docentes, administrativos y estudiantes). El desempeño de los servicios de red se ve afectado directamente a la falla de estos dispositivos de red y por generación de dominios de broadcast (segmentos de red sin uso, que ocasionan tráfico de red y probabilidad de paralizar los servicios utilizados por los usuarios). La topología de red propuesta, ofrece conectividad a los usuarios finales por dispositivos como computadoras, impresoras, switches, servidores, estaciones de trabajo, teléfonos y cámaras IP de la LAN corporativa a través de cableado o conexión inalámbrica 10/100/1000 Mbps. Al proponerse esta topología de red, se requiere de una segmentación agrupados por usuarios o áreas de trabajo (Capa 2) y el enrutamiento debe habilitarse en los switches para proporcionar la capacidad de poner a los usuarios en diferentes redes o su filtrado respectivo por categorías.

- **Evaluación y selección de recursos**

Se debe realizar una evaluación de alternativas de solución que se tiene en el mercado. Para ello, se determina determina OpenDayLight como el controlador principal de la red LAN y el cual se evalúa teniendo como criterio el cumplimiento de las especificaciones y sus características técnicas detalladas con anterioridad.

- **Controlador SDN:**

La elección del controlador SDN se otorga a través de ODL (OpenDayLight) el cual ofrece su propio lenguaje de programación, interfaz REST API y su modo de virtualización.

	Beacon	Floodlight	NOX	POX	Trema	Ryu	ODL
Soporte OpenFlow	OF v1.0	OF v1.0	OF v1.0	OF v1.0	OF v1.3	OF v1.0, v1.2, v1.3 y extensiones Nicira	OF v1.0
Virtualización	Mininet y Open vSwitch	Mininet y Open vSwitch	Mininet y Open vSwitch	Mininet y Open vSwitch	Construcción de una herramienta virtual de simulación	Mininet y Open vSwitch	Mininet y Open vSwitch
Lenguaje de desarrollo	Java	Java	C++	Python	Rudy/C	Python	Java
Provee REST API	No	Si	No	No	Si (Básica)	Si (Básica)	Si
Interfaz Gráfica	Web	Web	Python+, QT4	Python+, QT4, Web	No	Web	Web
Soporte de plataformas	Linux, Mac OS, Windows y Android para moviles	Linux, Mac OS, Windows	Linux	Linux, Mac OS, Windows	Linux	Linux	Linux, Mac OS, Windows
Soporte de OpenStack	No	Si	No	No	Si	Si	Si
Multiprocesos	Si	Si	Si	No	Si	No	Si
Código Abierto	Si	Si	Si	Si	Si	Si	Si

Tabla 36: Comparativa de controladores SDN

Fuente: Comparativa_Controller_SDN.asp

La Tabla 36 nos indica la comparativa de los controladores a nivel de código abierto. Por nuestro parámetro de calidad OpenDayLight, y se considera a este último como un paquete de software que se despliega en un servidor por medio de una máquina virtual. Las plantillas o script que puedan haber dentro de esta solución estarán referenciadas en la parte de Anexo para saber un poco más su entorno de simulación.

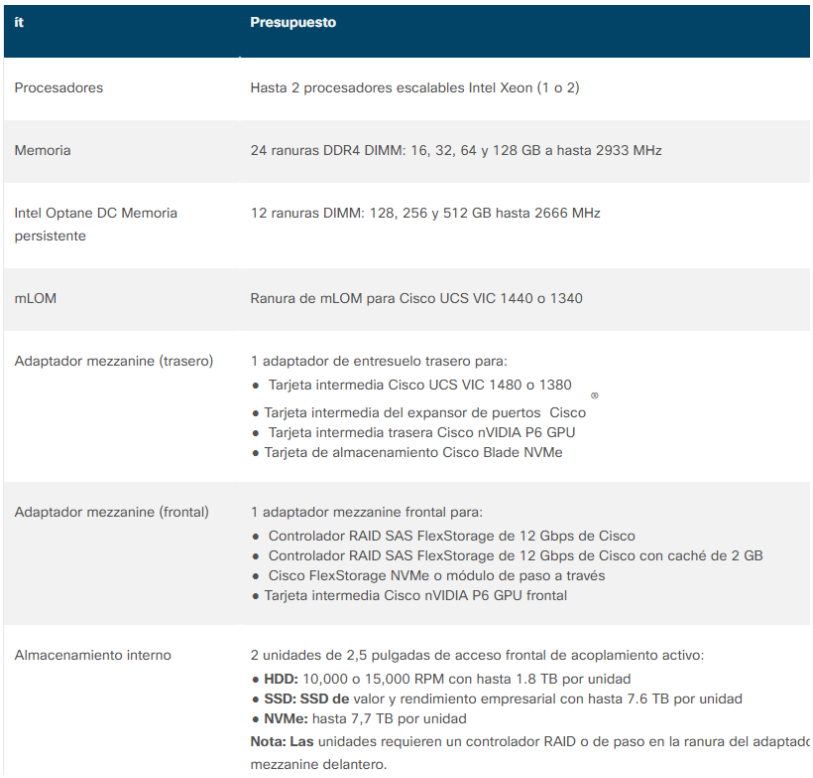
- **Servidor y Máquina Virtual**

En cuanto al servidor en donde se alojará el OpenDayLight, se propone el servidor Cisco UCS B200 M5. El controlador virtual no demanda muchos recursos de hardware (basta con instalarlo y posea suficiente capacidad de almacenamiento para los scripts o configuraciones realizadas por lo que este servidor solo tendrá la función de alojar al controlador.

Figura 67: Servidor Cisco propuesto para el paquete de software ODL

Fuente: cisco.com/products/servers

En la Figura 67, se puede observar el servidor propuesto para el alojamiento de OpenDayLight. Se propone este servidor porque tiene compatibilidad con el monitoreo a nivel UCS, es decir, tiene una función netamente programable y enfocado a una infraestructura de red virtual.



ít	Presupuesto
Procesadores	Hasta 2 procesadores escalables Intel Xeon (1 o 2)
Memoria	24 ranuras DDR4 DIMM: 16, 32, 64 y 128 GB a hasta 2933 MHz
Intel Optane DC Memoria persistente	12 ranuras DIMM: 128, 256 y 512 GB hasta 2666 MHz
mLOM	Ranura de mLOM para Cisco UCS VIC 1440 o 1340
Adaptador mezzanine (trasero)	1 adaptador de entresuelo trasero para: • Tarjeta intermedia Cisco UCS VIC 1480 o 1380 • Tarjeta intermedia del expansor de puertos Cisco • Tarjeta intermedia trasera Cisco nVIDIA P6 GPU • Tarjeta de almacenamiento Cisco Blade NVMe
Adaptador mezzanine (frontal)	1 adaptador mezzanine frontal para: • Controlador RAID SAS FlexStorage de 12 Gbps de Cisco • Controlador RAID SAS FlexStorage de 12 Gbps de Cisco con caché de 2 GB • Cisco FlexStorage NVMe o módulo de paso a través • Tarjeta intermedia Cisco nVIDIA P6 GPU frontal
Almacenamiento interno	2 unidades de 2,5 pulgadas de acceso frontal de acoplamiento activo: • **HDD:** 10,000 o 15,000 RPM con hasta 1.8 TB por unidad • **SSD: SSD de** valor y rendimiento empresarial con hasta 7.6 TB por unidad • **NVMe:** hasta 7,7 TB por unidad **Nota: Las** unidades requieren un controlador RAID o de paso en la ranura del adaptadc mezzanine delantero.

Figura 68: Características técnicas del servidor propuesto

Fuente: cisco.com/products/servers

Como indica la Figura 68, el servidor Cisco posee interesantes características de hardware respecto a escalabilidad. En nuestro caso, este servidor será dedicado únicamente al prototipo SDN sin alguna otra función (es un blade de gama regular). Se puede incluir opciones de almacenamiento a la par que se trabaja con el controlador SDN y sobre todo tiene la funcionalidad de hot swap (retiro en caliente de la fuente), para casos en que no se pierda la disponibilidad en el servidor o las cuchillas que pueda alojar. Recomendación dada por el mismo fabricante en su documentación si es que se usa algún paquete de software.

- **Switch de red**

Mencionamos este dispositivo porque será una parte esencial en el desarrollo e integración de la solución SDN. El equipo elegido es el Cisco Catalyst 3850 Series (dependiendo si es de core, distribución o acceso, los puertos serán de 48, 24 o 12 puertos según los datos obtenidos). La ventaja es que cuentan con interfaz programable ASIC a diferencia de sus

competidores que lo poseen, pero en una línea de switches más avanzados, lo cual no aplica en un entorno de campus universitario.

Trend	Feature	Installed-base access switches				Benefits
		3560-X, 3750-X Series	3750G Series	3850 Series	Cisco Catalyst 9300 Series	
Scale and performance	Bandwidth per stack	No stacking/ 64 Gbps	32 Gbps	480 Gbps	480 Gbps	Support Multigigabit access growth for wired and wireless, 802.11ac
	Uplinks	2x 10G[1]	4x 1G	4x1G, 2x10G, 4x10G (all models)	4x1G, 8x10G, 2x25G, 2x40G	
	Multigigabit technology	–	–	✔	✔	Support speeds above 1G in traditional cabling environments
Advanced security	Native Flexible NetFlow	–	–	✔	✔	
	Cisco TrustSec® and SGT[2] for wired and wireless	Wired	–	✔	✔	Orchestrate role-based access to corporate resources
	Trustworthy Systems	–	–	✔	✔	AES-256, MACsec-256
	Native MACsec-256 encryption	–	–	Multigigabit, 10G models	✔	
	Encrypted Traffic Analytics	–	–	–	✔	Detect malware hiding in encrypted traffic without decrypting it
Simplicity and automation	x86 CPU	–	–	–	✔	Accelerate innovation
	Cisco IOS® XE OS	–	–	✔	✔	Single common network OS across switching, routing, wireless, and IoT
	KVM and container-based hosting environments	–	–	–	✔	App hosting in the network
	Guest shell	–	–	✔	✔	On-box Python scripting
	Model-driven programmability	–	–	✔	✔	Standards-based programmable interfaces
	Streaming telemetry	–	–	✔	✔	Rich contextual insights
	SD-Access[3] programmability	–	–	Optional subscription	✔	

Figura 69: Lista de Switches Cisco Series

Fuente: cisco.com/products/sw/series

La Figura 69 nos muestra la comparativa de los switches Cisco en cuanto a capacidad y rendimiento. En nuestro caso y tal como lo indicamos en líneas anteriores, se considera el modelo 3850 Series porque posee características similares a los switches actuales del campus universitario y también, porque otra solución es aplicar la línea de switches Nexus 9000 (no siendo nuestro caso porque esto aplicaría para un centro de datos, con el modelo 3850S es suficiente para soportar la carga de la red LAN). La función de los switches en la capa de acceso y distribución es soportar el APIC programable mediante una actualización de firmware.

- **Licenciamiento y elementos adicionales**

En el caso del controlador OpenDayLight solo es necesario ingresar al repositorio de descargas de la página oficial de ODL e inmediatamente se puede descargarse el instalador en formato ova o .img. Por otro lado, en los switch que conformarán la red LAN su licencia

viene incluida en el paquete de software, solo es necesario activarla en los switches propuestos (licencia base), mediante una actualización; siempre y cuando seamos socios o clientes de Cisco.

En referencia al servidor, se necesita VirtualBox o VMware, incluso se puede montar el paquete de software de ODL sobre el servidor propuesto de manera directa. Los simuladores son libres y no tienen costo alguno. Por otra parte, se puede utilizar la herramienta Mininet para el diseño de la topología (por temas de mejor visibilidad y mayor detalle, se considera como una herramienta opcional para su uso). Si hablamos de recursos humanos, esto se encarga la misma universidad en asignar personal para que sea capacitado y se dedique a la gestión del controlador SDN, junto con el proveedor pueden planificar una capacitación de ser necesaria y adquirir conocimiento para las operaciones pertinentes.

Por último, se cuenta con un aproximado sobre el costo del hardware (dispositivos de red) tal como indica la siguiente imagen. (Ver Figura 70)

Item	Descripción	Cantidad	P. Unitario $.	P. Total $.	Tiempo Entrega
	MARCA: JUNIPER NETWORKS				
1	Cisco Catalyst 3850 48P-24P EX4300, 48-Port 10/100/1000BaseT PoE-plus + 1100W AC PS	12	62,124.46	62,124.46	40 días calendarios
2	PA3-ND-Cisco Catalyst 3850 48P-24P Operate Specialist 3Yr Next Day Support for EX4300-48P	12	18,324.87	18,324.87	40 días calendarios
3	Cisco Catalyst 3850 24P 12P 385012 Compact, Fanless, 12-Port 10/100/1000 BaseT (12-Ports PoE+) with 2 Dual-Purpose (10/100/1000 BaseT or SFP) Uplink Ports	36	46,404.66	46,404.66	40 días calendarios
4	PA3-ND-Catalyst 3850 24P 12P Operate Specialist 3YR Prepaid Next Day Support for EX2200-C-12P	36	9,935.64	9,935.64	40 días calendarios
5	EX-SFP-10GE-DAC-3M SFP+ 10 Gigabit Ethernet Direct Attach Copper (Twinax Copper Cable), 3M	1	261.07	261.07	40 días calendarios
			Subtotal	S/ 137,050.71	
			IGV (18%)	S/ 1,535.79	
			TOTAL (SOLES)	S/ 138,586.49	
Observaciones:			Condiciones Comerciales:		
Tiempo de entrega: 40 días calendarios			Forma Pago:	FACTURA A 30 DIAS	
Garantía de fabrica Doce (36) meses de fábrica			Lugar Entrega:	Oficinas del Cliente	
Impuestos: Los precios incluyen IGV (18%)			Validez Oferta:	30 días calendarios	

Figura 70: Costo de equipamiento de hardware (aproximado)

Fuente: Proveedor_de_UC

En la Figura 70, se observa un aproximado en el costo de equipamiento de hardware siendo algo referencial y tener un estimado en cuanto gastaría el campus universitario. Esta cotización corresponde al proveedor mencionado en el Registro de Interesados y que ya trabajo en otros proyectos con la organización. Entre los datos podemos observar la cantidad de switches de 48, 24 y 12 puertos, el cable dac para realizar el stack en los switches de core, PAR-ND hace referencia a la garantía sobre los equipos principales como el core y distribución.

5.1.3.1 Prueba de visibilidad de la topología de red en OpenDayLight

La topología de red simulada sigue la infraestructura de la red LAN del campus universitario, el cual está constituido por los siguientes componentes:

- Switch Core
- Switches de distribución y acceso
- Servidor virtual/Terminal

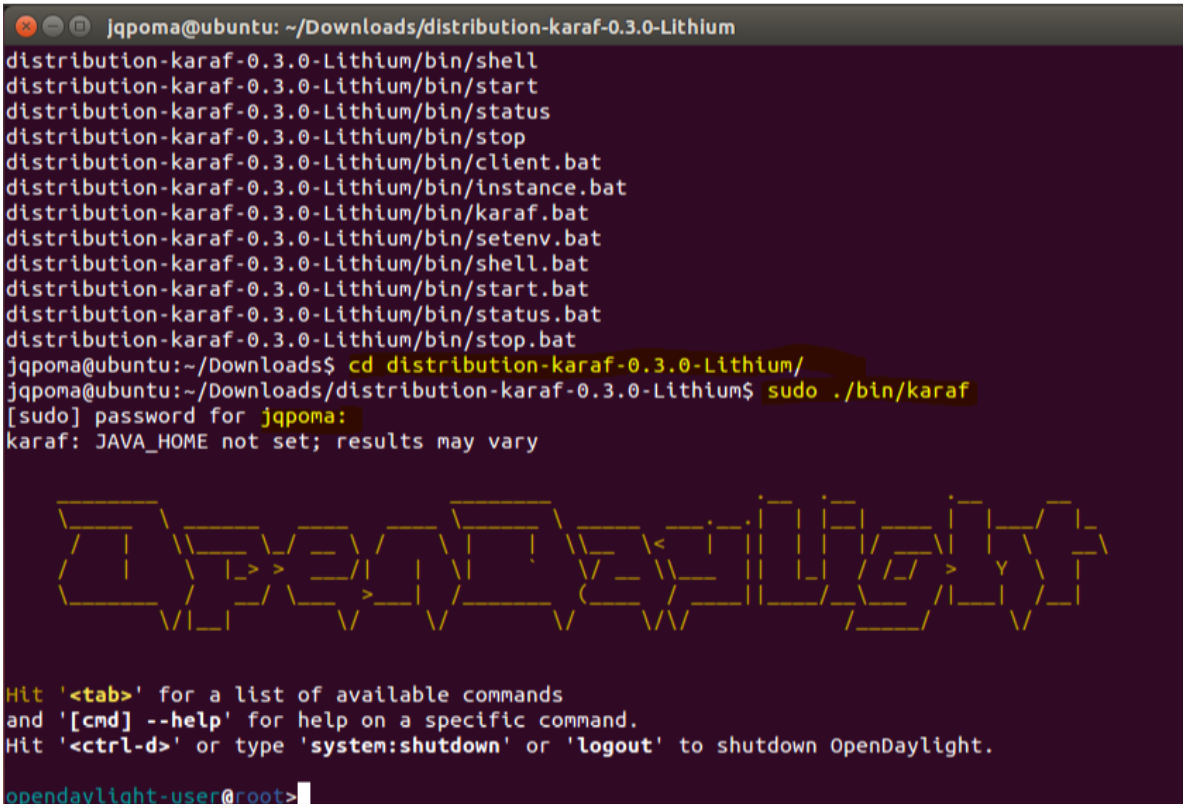


Figura 71: Controlador OpenDayLight

Fuente: Elaboración propia

Según la Figura 71, se menciona al controlador ODL porque desde aquí parte el éxito de la prueba con la topología propuesta. La distribución Lithium permite mayor compatibilidad de APIs en comparación de otras distribuciones que ofrece el proyecto OpenDayLight. Una vez dentro del controlador lo que hacemos es cargar los módulos (los cuales permite visualizar la topología personalizada y la edición del mismo), logrando mostrar la red y los hosts/terminales conectados en cada switch mencionado anteriormente. Veamos cuales son los otros módulos también importantes para el desarrollo de la prueba. (Ver Tabla 40).

MODULO	Descripción
ODL-RESTCONF	Conjunto de biblioteca multimedia para ODL
ODL-OPENFLOWPLUGIN	Permite la establecer sesion con otros protocolos
ODL-L2SWITCH	Asegura la comunicación con otro conmutador por medio de OpenFlow
ODL-YANGTOOLS	Complemento entre la comunicación del controlador con las aplicaciones
ODL-MDSAL	Encargado de la sincronizacion ODL y Mininet
ODL-DLUX	Interfaz gráfica web donde se observa la configuración ODL

Tabla 37: Módulos utilizados por el controlador OpenDayLight

Fuente: Elaboración propia

En la Tabla 37, se mencionan los módulos que serán habilitados junto con el controlador OpenDayLight. Si bien son varios módulos que trae consigo el controlador, solo es necesario los 6 módulos que se proponen ya que son los principales y que son suficientes para llevar a cabo las pruebas y resultados de la simulación propuesta.

En esta parte de la habilitación del controlador ODL, es necesario mencionar que la dirección IP 192.168.231.134 hace referencia a la máquina virtual donde está alojado el controlador ODL. Para culminar, se necesita la integración con el Mininet y para ello es donde creamos previamente la topología propuesta (mediante una sentencia de comandos que refleje un árbol).

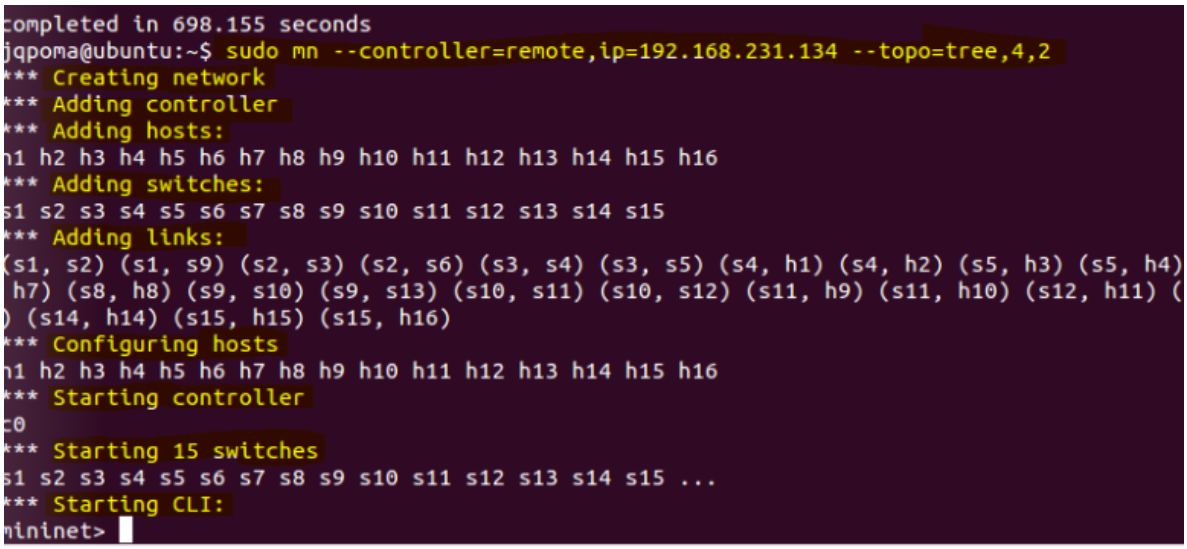


Figura 72: Creación de la topología SDN en Mininet

Fuente: Elaboración propia

Como se observa en la Figura 72, se crea la red con el controlador SDN (controller), los hosts/terminales (h1 al h16 que representan las áreas de trabajo o usuarios del entorno universitario), los enlaces (links) y los conmutadores que simulan la red propuesta.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- De acuerdo a la problemática identificada de la parte 3.2 del capítulo 03, se debe abordar con cautela al presentar varias situaciones encontradas en donde no solo basta un diagnostico de lo reportado, sino se trata de proponer una matriz donde se realiza una comparativa del problema, impacto y valoración que podrían proponer mejores medidas de solución a dicho problema.

- Se concluye que la solución diseñada (red SDN) en el capítulo 04, permitirá ahorrar tiempo en la gestión de los equipos de red debido a la programación de la red propuesta a través del controlador OpenDayLight.

- En la parte 5.1.2 del capítulo 05, se logró evidenciar la integración del controlador OpenDayLight junto con la herramienta Mininet. Con el fin de obtener resultados de los tiempos de respuesta de los dispositivos de red y crear flujos de datos.

- En el entorno de simulación de la parte 5.1.3.1 en el capítulo 05, se observó los elementos de la red SDN y los terminales de comunicación (Controlador OpenDayLight), que permitió crear la red SDN basado en el esquema actual de la organización.

Recomendaciones

- Es altamente recomendable que la empresa encargada de realizar este tipo de diseño de red SDN, sea una empresa con amplia experiencia o especialista en el tema. Con el fin de evitar retrasos en el proyecto, todo siga en buen camino y no tener errores.

- Es importante evaluar una topología de red en alta disponibilidad, el cual considere un enlace adicional u otro controlador SDN con la finalidad de no depender de un solo equipo o enlace para toda la infraestructura de red (incluso puede ubicarse en alguna sucursal si tuviese la universidad).

- De seguir con otros proyectos de mejoramiento de la red en un campus universitario, se recomienda la renovación de los dispositivos de comunicaciones, cambio o adecuación de gabinetes de red en aulas y pabellones, monitoreo constante y en tiempo real. Todas estas mejoras podrán contribuir en tener una red de calidad, con buen rendimiento que soporte cualquier proyecto relacionado al core del negocio.

- Para entender mejor las características de las redes definidas por software en todo su ámbito, se recomienda probar otros controladores SDN con el fin de obtener resultados y poder evaluarlos según la necesidad de la organización que lo requiera. En nuestro caso, se optó por OpenDayLight al tener mayor compatibilidad con el escenario propuesto de ancho de banda y tráfico de datos.

6 REFERENCIAS

Alvarez Pinilla, Raúl (2015). *Estudio de las redes definidas por software mediante el desarrollo de escenarios virtuales basados en el controlador OpenDaylight. (Tesis de grado).* Recuperado el 17 de agosto de 2018. Universidad Politécnica de Madrid, España.

Cisco Systems Inc. (2018). *Customers Stories – Full listing.* Recuperado el 17 de agosto de 2018 de https://www.cisco.com/c/en/us/about/case-studies-customer-success-stories/customer-stories-listing.html?flt1_general-table0=Education

CIO Perú (2017). *SDN resuelve muchos problemas de red.* Recuperado el 20 de agosto de agosto de 2018 de https://cioperu.pe/articulo/23244/sdn-resuelve-muchos-problemas-de-red/

Citrix Systems, Inc. (2014). *SDN 101: Introducción a software defined networking*. Recuperado el 3 de agosto de 2018 de https://www.citrix.com/content/dam/citrix/en_us/documents/oth/sdn-101-an-introduction-to-software-defined-networking-es.pdf

Colomés, P. (2016). *Conceptos básicos de redes definidas por software (SDN).* Recuperado el 3 de agosto de 2018 de http://www.redescisco.net/sitio/2016/12/12/conceptos-basicos-de-redes-definidas-por-software-sdn/

España Tarapuez, Nataly. (2016). *Diseño y simulación de una red definida por software (SDN). (Tesis de grado).* Recuperado el 3 de agosto de 2018. Universidad Central del Ecuador.

ETSI (2014). *Open Networking Foundation y ETSI anuncian la colaboración estratégica para el soporte de SDN*. Recuperado el 4 de agosto de 2018 de https://www.etsi.org/news-events/events/9-news-events/news/764-2014-03-onf-and-etsi-announce-strategic-collaboration-for-sdn-support-of-nfv

Felipe, A. (2014). *Estado del Arte: Redes Definidas por Software*. Recuperado el 3 de

agosto de 2018 de http://repositorio.ucp.edu.co:8080/jspui/bitstream/10785/2788/2/CDMIST97.pdf

Hernández Sampieri, R., Fernández, C., y Baptista, P. (2014). *Metodología de la Investigación (6a ed.).* México: Interamericana Editores.

Hernao Ramírez, J. L. (2015). *Informe Guía Teórico-Práctica sobre redes definidas por software.* Pereira, Colombia: Universidad Tecnológica de Pereira - Tesis de pregrado.

Information Systems Audit and Control Association – ISACA (2016). *Beneficios y Riesgos de Seguridad de las Redes definidas por Software.* Recuperado el 3 de agosto de 2018 de https://www.isaca.org/Journal/archives/2016/volume-4/Pages/benefits-and-the-security-risk-of-software-defined-networking-spanish.aspx

Internet Research Task Force - IRTF (2015). *Software-Defined Networking (SDN): Layers and Architecture Terminology, RFC 7426.* Recuperado el 4 de agosto de 2018 de https://tools.ietf.org/html/rfc7426

ISACA Journal (2016). *Beneficios y riesgos de seguridad de las redes definidas por software.* Recuperado el 17 de agosto de 2018 de https://www.isaca.org/Journal/archives/2016/volume-4/Pages/benefits-and-the-security-risk-of-software-defined-networking-spanish.aspx

Murillo Nogales, Pablo (2015). Análisis y evaluación de las redes definidas por software. (Tesis de grado). Recuperado el 4 de agosto de 2018. Universidad de Extremadura de Mérida, España.

OpenDayLight (2018). *The Linux Foundation projects: Casos de Uso en Nube y NFV.* Recuperado el 21 de setiembre de 2018. https://www.opendaylight.org/use-cases-and-users/by-function/cloud-and-nfv

Open Networking Foundation (2015). *Framework for SDN: Scope and Requirements.* Recuperado el 3 de agosto de 2018 de https://3vf60mmveq1g8vzn48q2o71a-

wpengine.netdna-ssl.com/wp-content/uploads/2014/10/Framework_for_SDN_-Scope_and_Requirements.pdf

Revista Cloud Computing (2015). *Tendencias que marcarán la evolución del mercado SDN*. Recuperado el 3 de agosto de 2018 de https://www.revistacloudcomputing.com/2015/01/5-tendencias-que-marcaran-la-evolucion-del-mercado-de-redes-sdn-para-el-ano-2015/

7 ANEXOS

Anexo 1: Script de la topología de red SDN propuesta (Mininet)

Este script está basado en lenguaje de programación Python y con el nombre "RedSDN_UC", el cual se ha desarrollado bajo el entorno de simulación en Mininet con la finalidad de simular la topología de red para la UC.

```
"""Topologia de red SDN propuesta – UC
---Red SDN - Sede Central---
---Core---
---Distribucion---
---Acceso---
"""
from mininet.topologia import Topologia
from mininet.net import Mininet
from mininet.util import dumpNodeConnections
class redSDN( Topologia ):
"Topologia"
def build( self ):
# host Red Pabellon F
h1 = self.addHost( 'h1')
h2 = self.addHost( 'h2')
h3 = self.addHost( 'h3')
h4 = self.addHost( 'h4')
h5 = self.addHost( 'h5')
h6 = self.addHost( 'h6')
h7 = self.addHost( 'h7')
h8 = self.addHost( 'h8')
h9 = self.addHost( 'h9')
# host Red Servidores
h14 = self.addHost( 'h14')
h15 = self.addHost( 'h15')
h16 = self.addHost( 'h16')
# host Prueba
h10 = self.addHost( 'h10')
# switch Core
s1 = self.addSwitch( 's1' )
s2 = self.addSwitch( 's2' )
# switch nodos distribucion
s3 = self.addSwitch( 's3' )
```

```
s4 = self.addSwitch( 's4' )
s5 = self.addSwitch( 's5' )
s6 = self.addSwitch( 's6' )
# switch acceso
# switch nodo1-uc
s7 = self.addSwitch( 's7' )
s8 = self.addSwitch( 's8' )
s9 = self.addSwitch( 's9' )
s10 = self.addSwitch( 's10' )
# switch nodo2-uc
S11 = self.addSwitch( 's11' )
S12 = self.addSwitch( 's12' )
S13 = self.addSwitch( 's13' )
S14 = self.addSwitch( 's14' )
# switch nodo3-uc
S15 = self.addSwitch( 's15' )
s16 = self.addSwitch( 's16' )
s17 = self.addSwitch( 's17' )
s18 = self.addSwitch( 's18' )
# links entre cores
self.addLink( s1, s2)
# links distribucion a core1
self.addLink( s3, s1)
self.addLink( s4, s1)
self.addLink( s5, s1)
self.addLink( s6, s1)
# links distribucion a core2
self.addLink( s11, s2)
self.addLink( s10, s2)
self.addLink( s12, s2)
self.addLink( s7, s2)
self.addLink( s9, s2)
# link acceso
# link nodo1-uc
self.addLink( s7, s3)
self.addLink( s8, s3)
self.addLink( s9, s3)
self.addLink( s10, s3)
# link nodo2-uc
self.addLink( s11, s4)
self.addLink( s12, s4)
self.addLink( s13, s4)
self.addLink( s14, s4)
# link nodo3-uc
self.addLink( s15, s5)
self.addLink( s16, s5)
self.addLink( s17, s5)
self.addLink( s18, s5)
```

Anexo 2: Tabla de flujo de los elementos de red en el controlador OpenDayLight

El controlador OpenDayLight tiene un repositorio de base de datos de todos los switches y hosts de la red SDN. Mediante esto se obtuvo las tablas de flujo instaladas en el switch core bajo el controlador ODL a través del módulo RestConf en código XML.


192.168.231.134:8181/restconf/operational/opendaylight-inventory:nodes
<priority>100</priority>
<table_id>0</table_id>
<match>
<ethernet-match>
<ethernet-type>
<type>35020</type>
</ethernet-type>
</ethernet-match>
</match>
<flow-statistics>
<byte-count>18096</byte-count>
<duration>
<second>1032</second>
<nanosecond>114000000</nanosecond>
</duration>
<packet-count>208</packet-count>
</flow-statistics>
<cookie>3098476543630901506</cookie>
<idle-timeout>0</idle-timeout>
<hard-timeout>0</hard-timeout>
</flow>
<flow>
<id>#UF$TABLE*0-984</id>
<priority>0</priority>
<table_id>0</table_id>
<match/>
<flow-statistics>
<byte-count>0</byte-count>
<duration>
<second>1032</second>
<nanosecond>114000000</nanosecond>
</duration>

```
        <packet-count>0</packet-count>
      </flow-statistics>
      <cookie>3098476543630901506</cookie>
      <idle-timeout>0</idle-timeout>
      <hard-timeout>0</hard-timeout>
    </flow>
  -<flow>
      <id>#UF$TABLE*0-1049</id>
    -<instructions>
      -<instruction>
          <order>0</order>
        -<apply-actions>
          -<action>
              <order>0</order>
            -<output-action>
                <output-node-connector>2</output-node-connector>
                <max-length>65535</max-length>
              </output-action>
            </action>
          </apply-actions>
        </instruction>
      </instructions>
      <priority>10</priority>
      <table_id>0</table_id>
    -<match>
      -<ethernet-match>
        -<ethernet-destination>
            <address>D6:A1:2E:A4:56:8B</address>
          </ethernet-destination>
        -<ethernet-source>
            <address>CE:FD:BC:CF:64:49</address>
          </ethernet-source>
```



```
        </ethernet-source>
      </ethernet-match>
    </match>
  -<flow-statistics>
      <byte-count>0</byte-count>
    -<duration>
        <second>698</second>
        <nanosecond>720000000</nanosecond>
      </duration>
      <packet-count>0</packet-count>
    </flow-statistics>
    <cookie>3026418949592973369</cookie>
    <idle-timeout>1800</idle-timeout>
    <hard-timeout>3600</hard-timeout>
  </flow>
-<flow>
    <id>#UF$TABLE*0-1031</id>
  -<instructions>
    -<instruction>
        <order>0</order>
      -<apply-actions>
        -<action>
            <order>1</order>
          -<output-action>
              <output-node-connector>2</output-node-connector>
              <max-length>65535</max-length>
            </output-action>
          </action>
        -<action>
            <order>2</order>
          -<output-action>
              <output-node-connector>CONTROLLER</output-node-connector>
```

```
        </action>
       -<action>
          <order>0</order>
         -<output-action>
            <output-node-connector>3</output-node-connector>
            <max-length>65535</max-length>
          </output-action>
        </action>
      </apply-actions>
    </instruction>
  </instructions>
  <priority>2</priority>
  <table_id>0</table_id>
 -<match>
    <in-port>openflow:12:1</in-port>
  </match>
 -<flow-statistics>
    <byte-count>7882</byte-count>
   -<duration>
      <second>850</second>
      <nanosecond>968000000</nanosecond>
    </duration>
    <packet-count>109</packet-count>
  </flow-statistics>
  <cookie>3098476543630901724</cookie>
  <idle-timeout>0</idle-timeout>
  <hard-timeout>0</hard-timeout>
 </flow>
-<flow>
  <id>#UF$TABLE*0-1050</id>
 -<instructions>
   -<instruction>
      <order>0</order>
     -<apply-actions>
       -<action>
          <order>0</order>
         -<output-action>
            <output-node-connector>1</output-node-connector>
            <max-length>65535</max-length>
          </output-action>
        </action>
      </apply-actions>
    </instruction>
  </instructions>
  <priority>10</priority>
  <table_id>0</table_id>
 -<match>
   -<ethernet-match>
     -<ethernet-destination>
        <address>CE:FD:BC:CF:64:49</address>
      </ethernet-destination>
     -<ethernet-source>
        <address>D6:A1:2E:A4:56:8B</address>
      </ethernet-source>
    </ethernet-match>
  </match>
 -<flow-statistics>
    <byte-count>0</byte-count>
   -<duration>
      <second>698</second>
      <nanosecond>720000000</nanosecond>
    </duration>
    <packet-count>0</packet-count>
  </flow-statistics>
```

```
    <hard-timeout>3600</hard-timeout>
  </flow>
- <flow>
    <id>#UF$TABLE*0-1032</id>
  - <instructions>
    - <instruction>
        <order>0</order>
      - <apply-actions>
        - <action>
            <order>1</order>
          - <output-action>
              <output-node-connector>1</output-node-connector>
              <max-length>65535</max-length>
            </output-action>
          </action>
        - <action>
            <order>2</order>
          - <output-action>
              <output-node-connector>CONTROLLER</output-node-connector>
              <max-length>65535</max-length>
            </output-action>
          </action>
        - <action>
            <order>0</order>
          - <output-action>
              <output-node-connector>3</output-node-connector>
              <max-length>65535</max-length>
            </output-action>
          </action>
        </apply-actions>
      </instruction>
    </instructions>
```



```
    - <match>
        <in-port>openflow:12:2</in-port>
      </match>
    - <flow-statistics>
        <byte-count>7798</byte-count>
      - <duration>
          <second>850</second>
          <nanosecond>968000000</nanosecond>
        </duration>
        <packet-count>107</packet-count>
      </flow-statistics>
      <cookie>3098476543630901725</cookie>
      <idle-timeout>0</idle-timeout>
      <hard-timeout>0</hard-timeout>
    </flow>
  - <flow>
      <id>#UF$TABLE*0-1030</id>
    - <instructions>
      - <instruction>
          <order>0</order>
        - <apply-actions>
          - <action>
              <order>1</order>
            - <output-action>
                <output-node-connector>2</output-node-connector>
                <max-length>65535</max-length>
              </output-action>
            </action>
          - <action>
              <order>0</order>
            - <output-action>
                <output-node-connector>1</output-node-connector>
```

Anexo 3: Instalación de GNUPLOT a través de Mininet

Para la visualización de los gráficos obtenidos de los resultados de ancho de banda y jitter, es necesario instalar el módulo GNUPLOT, este se realiza haciendo uso de un terminal en donde está alojado el mininet.

jqpoma@ubuntu: apt-get install gnuplot-x11

Ejecutamos este comando e inmediatamente procede la instalación hasta mostrar su validación como se observa en las siguientes imágenes.