SDN in the Cold Chain of Perishable Product Distribution in Guayaquil

Michael Cedeño
Escuela Superior Politécnica del Litoral
Guayaquil, Ecuador
Email: mijacede@espol.edu.ec

Javier Dillon
Escuela Superior Politécnica del Litoral
Guayaquil, Ecuador
Email: jdillon@espol.edu.ec

Isaac Vasco
Escuela Superior Politécnica del Litoral
Guayaquil, Ecuador
Email: ivasco@espol.edu.ec

***Abstract*—The integration of SDN into IoT networks offers numerous benefits. It provides a more complete vision of the network landscape, anticipating possible errors and failures that may arise in the system. This centralized and simplified management of IoT connectivity enables the configuration, monitoring and control of distributed devices in a network.**

In addition, previous research has highlighted the potential and opportunities of combining SDN and IoT, as well as exploring specific architectures, protocols, applications, and solutions to improve the performance and security of SDN-enabled IoT networks. These advances include integration with 5G networks, security management, cloudlet placement optimization, among others. Furthermore, the use of SDN in smart city applications and cellular networks has been proposed to improve efficiency and quality of life.

The integration of SDN and IoT is crucial for the future development of IoT technology. It enables secure and flexible communication between connected devices, provides centralized management and control, enhances network security, and offers opportunities to improve scalability and efficiency. The combination of SDN and IoT opens up new possibilities for network connectivity and innovation in various domains.

I. Introduction

La integración de redes definidas por software (SDN, por sus siglas en inglés) con dispositivos de Internet de las cosas (IoT, por sus siglas en inglés) se ha convertido en un área de creciente interés en redes y conectividad. La convergencia de estas dos tecnologías promete traer nuevas oportunidades y desafíos para conectar y comunicar dispositivos IoT en un entorno cada vez más dinámico y heterogéneo.

La Redes Definidas por Software (SDN, por sus siglas en inglés) es una alternativa enfocada en la gestión de redes que separa el plano de control y el plano de datos, permitiendo una mayor flexibilidad y agilidad en el manejo y la configuración de la red. Por otro lado, los dispositivos IoT abarcan una amplia gama de objetos físicos conectados, como sensores, actuadores y dispositivos inteligentes, que recopilan y comparten datos en tiempo real.

La integración de un red definida por software (SDN) en IoT ofrece númerosos beneficios. Entre ellos, permitir brindar un visión más completa del panorama de red anticipando asi los posibles errores y fallas que pudieran llegar a surgir en el sistema. Esta gestión centralizada y simplificada de la conectividad IoT permite la configuración, supervisión y control de los dispositivos distribuidos en una red.

Otro aspecto importante es la capacidad de poder controlar el flujo de tráfico en una red mediante la programación de un controlador basado en software. A su vez, el administrador puede seleccionar un solo protocolo de comunicación para poder comunicarse con distintos dispositivos dentro de la red a través de un controlador central, esto permite que haya una mayor libertad a la hora de seleccionar equipos en la red.

Por otro lado, la utilización de este tipo de red en dispositivos IoT brinda más ventajas en seguridad que otras alternativas de redes. Los administradores pueden segmentar la red creando niveles de seguridad y crear zonas especializadas para mantener a raya dispositivos comprometidos que puedan infectar al resto.

Por último, la integración de SDN con el internet de las cosas (IoT, por sus siglas en Ingles) es una tendencia que ofrece múltiples ventajas para mejorar la conectividad, la seguridad y la eficiencia de las redes que soportan los dispositivos IoT. Al separar el plano de control del plano de datos, se logra una mayor flexibilidad y agilidad en la gestión de la red, así como una mejor visibilidad y control del tráfico. Además, se facilita la interoperabilidad entre diferentes tipos de dispositivos y protocolos, lo que permite una mayor diversidad y escalabilidad en el ecosistema IoT. En este informe, se aborda la cuestión crucial de cómo mejorar la distribución de productos perecederos en Guayaquil, tomando como enfoque central la implementación de una Arquitectura de Red Definida por Software (SDN) en la cadena de frío. La tesis se fundamenta en la premisa de que mediante la adopción de esta innovadora infraestructura tecnológica, es posible aumentar la eficiencia operativa y la confiabilidad de todo el proceso de distribución, asegurando condiciones óptimas de almacenamiento y transporte para los productos delicados en cuestión.

II. STATE OF THE ART

La aplicación de SDN en el contexto del Internet de las cosas (IoT) ha sido objeto de investigación y se han realizado varias contribuciones. Los investigadores SK Tayyaba, MA Shah, OA Khan y AW Ahmed han discutido en su trabajo las ventajas de la combinación de SDN e IoT, y han señalado que esta combinación tiene un gran potencial y ofrece un camino prometedor hacia el futuro (Tayyaba, Shah, Khan, & Ahmed, 2017). En otro trabajo, los mismos investigadores

han realizado una predicción cualitativa para el año 2020, destacando las oportunidades y desafíos de la integración de SDN e IoT (Tayyaba et al., 2016) .

En una revisión realizada por AH Mohammed, RM Khaleefah e IA Abdulateef, se examina el uso de SDN en IoT y se discuten las ventajas y los desafíos de esta combinación (Mohammed, Khaleefah, & Abdulateef, 2020). El estudio también destaca la importancia de la optimización de la energía y la gestión eficiente del tráfico en las redes IoT habilitadas para SDN.

Otro aspecto importante es la integración de SDN y computación en la niebla en el contexto de IoT. Salman, Elhajj, Chehab y Kayssi han realizado una encuesta que proporciona una visión general de las perspectivas y los desafíos de la combinación de SDN y computación en la niebla en el ámbito de IoT (Salman, Elhajj, Chehab, & Kayssi, 2018). Esta investigación destaca la necesidad de soluciones eficientes y escalables para abordar los desafíos de conectividad y administración en las redes IoT.

En términos de arquitecturas SDN, los trabajos de Kreutz y Blial proporcionan una visión general de las arquitecturas SDN existentes y discuten sus características y opciones de diseño (Kreutz et al., 2014)(Blial, Ben Mamoun, CN Benaini, & Communications, 2016). Los autores destacan la importancia de la flexibilidad y la escalabilidad en el diseño de arquitecturas SDN para abordar los requisitos específicos de las redes IoT.

En cuanto a los protocolos y aplicaciones específicos, los estudios de Braun y Menth, Li y Medved son relevantes. Braun y Menth analizan el protocolo OpenFlow y su aplicación en redes habilitadas para SDN, incluidas las redes IoT (Braun & Menth, 2014). Li propone un marco general basado en SDN para IoT con implementación de funciones de red virtualizada (NFV) (Li, Altman, & Touati, 2015). Medved discuten el enfoque de OpenDaylight para la arquitectura de controlador SDN y su aplicabilidad en el contexto de IoT (Medved, Varga, Tkacik, & Gray, 2014).

Además, los investigadores han explorado soluciones específicas para mejorar aspectos clave de las redes IoT habilitadas para SDN. Estos incluyen la optimización de la ubicación de cloudlets para minimizar la demora de acceso (Zhao, Sun, Shi, & Liu, 2018), la habilitación de redes IoT heterogéneas sobre redes 5G mediante el uso de MEC/SDN (Ateya, Algarni, Hamdi, Koucheryavy, & Soliman, 2021), y el modelado del tráfico y la evaluación del rendimiento de la red de acceso NB-IoT basada en SDN (Chen & et al., 2020).

En términos de gestión y seguridad, los estudios de Tello y Oquendo, Kataoka, y Bedhief proponen una arquitectura basada en SDN para proporcionar conectividad confiable en sistemas IoT en el contexto de redes 5G (Tello-Oquendo, Akyildiz, Lin, & Pla, 2018). Kataoka propone un enfoque de lista de confianza para la gestión de tráfico distribuido en IoT utilizando Blockchain y SDN (Kataoka, Gangwar, & Podili, 2018). Bedhief propone una gestión autónoma de controladores SDN distribuidos para redes IoT altamente dinámicas (Bedhief, Kassar, Aguili, Foschini, & Bellavista, 2019).

Otros aspectos abordados en la literatura incluyen la gestión de datos de IoT basada en los principios de SDN (Eghbali & Lighvan, 2021), la seguridad en la computación perimetral basada en SDN en sistemas de atención médica habilitados para IoT (Li & et al., 2020), la transferencia de autenticación habilitada por Blockchain en redes 5G basadas en SDN (Yazdinejad & et al., 2019), y la arquitectura de IoT segura habilitada por SDN (Karmakar et al., 2020).

En el ámbito de las redes celulares, se ha observado un interés creciente en el uso de SDN para abordar la complejidad y optimizar la capa de enlace entre los dispositivos IoT y los sistemas basados en radio. Los estudios previos han propuesto soluciones basadas en SDN para mejorar la eficiencia energética y escalabilidad en entornos de sensores inalámbricos. Estas soluciones buscan reducir el consumo de energía y mejorar la gestión del tráfico en redes IoT. En cuanto a la gestión de IoT, se ha investigado la aplicación de SDN en la separación de SDN a escala urbana, lo que permite una gestión más eficiente y centralizada de los dispositivos IoT en entornos urbanos.

La seguridad es otro aspecto crítico en el entorno IoT, y se han propuesto marcos de seguridad basados en SDN para abordar los desafíos de seguridad en las redes IoT. Estos marcos se centran en la segmentación de red, el control de acceso granular y la detección de anomalías para proteger los dispositivos IoT y los datos transmitidos.

En el contexto de las aplicaciones de ciudades inteligentes, se han investigado soluciones basadas en SDN para mejorar la eficiencia y la calidad de vida de los ciudadanos. Estas soluciones incluyen la gestión y optimización de los servicios urbanos, como el transporte, la iluminación y la gestión de residuos, a través de la implementación de SDN en la infraestructura de la ciudad.

Se ha propuesto el uso de las arquitecturas EOPA y RNOPA en la optimización del rendimiento de acceso a las nubes, con el objetivo de reducir la latencia y mejorar la consistencia promedio en los dispositivos IoT.

Algunos de los avances que destacan en el campo son:

- La integración de redes IoT heterogéneas con las redes 5G que permiten un despliegue denso y una conectividad eficiente.
- Modelos de colas que pueden aplicarse en diferentes escenarios de casos para mejorar la escalabilidad en las redes IoT.
- Utilización de la infraestructura WSN para desarrollar un marco que permita la cooperación con entornos basados en la nube sin problemas; en colaboración con protocolos como MQTT.
- La gestión de la seguridad en las redes IoT a través de estructuras de supervisión para mejorar la escalabilidad y el control de la movilidad.
- Utilización de los controladores SDN ONOS y ODL en la gestión y administración de redes IoT.
- La computación perimetral (MEC) se empleó para desarrollar un marco que permita el acceso autorizado a

dispositivos IoT por parte de servidores Edge, eliminando la reautenticación innecesaria en los cambios repetidos entre celdas heterogéneas.

III. Field Technologies

En su tesis de grado, el Ingeniero Franklin German Placencia Camacho propuso una solución para mejorar la integración de sistemas de alarmas comunitarias utilizando arquitecturas SDN (Software Defined Networking) e IoT (Internet of Things). (Placencia Camacho, 2021)

En primer lugar, Placencia Camacho planteó la problemática de los sistemas de seguridad ciudadana y cómo la falta de políticas de gestión de tráfico y calidad de servicio en las redes computacionales que los soportan puede ocasionar problemas de saturación y cuellos de botella.

Para abordar esta problemática, propuso la utilización de dos tecnologías emergentes. En primer lugar, propuso el uso de una arquitectura de red definida por software (SDN) para separar el plano de control del plano de datos en los conmutadores de red. Esta separación permitiría una gestión más eficiente del tráfico y facilitaría la expansión, migración o actualización de redes de gran tamaño.

En segundo lugar, propuso reemplazar la infraestructura de las alarmas comunitarias activadas por dispositivos de radiofrecuencia por una arquitectura de red IoT (Internet of Things) con un protocolo de comunicaciones MQTT. Esta integración permitiría una mejor comunicación y control de las alarmas comunitarias, además de facilitar su interoperabilidad con otros dispositivos y sistemas.

La investigación también incluyó un análisis de ancho de banda de una red tradicional sin políticas de control, demostrando que los servicios de tráfico crítico (como audio digital, videovigilancia, datos y paquetes de control IoT) tienden a acaparar la mayor parte del ancho de banda de la red.

Finalmente, se evaluaron las ventajas y resultados de una topología de red definida por software diseñada para trabajar en conjunto con protocolos IoT, brindando sencillez y simplicidad en la implementación de políticas de tráfico y calidad de servicio configuradas a través de un entorno web. Esta solución podría ser implementada y replicada en entornos de red de alta demanda. Para esto, Camacho presentó una síntesis de los resultados obtenidos en la cual se englobaron las configuraciones primarias que se implementaron sobre el controlador SDN primario y replicado sobre los conmutadores definidos por software para optimizar el ancho de banda que una red tradicional dispone y evaluar los beneficios que supone la migración hacia una red basada por software. Véase la Figura 1.

"Es evidente la mejora que se genera en términos de congestión y carga de paquetes de datos al agregar un conmutador SDN entre el enrutador primario y los dispositivos de red que anteriormente solían conectarse de forma directa sin ningún tipo de política de control.

Tomando como punto referencial la información de la tabla 1 y sintetizando el análisis de resultados previamente expuesto

Arquitectura	Servicios en demanda	Política	Retardo en IoT	AB Intranet	AB Global
Tradicional	Navegación WEB (normal)	Por defecto	-	< 4Mbps	18 Mbps / 20 Mbps
Tradicional	Navegación WEB (pico)	Por defecto	-	< 2Mbps	12 Mbps / 20 Mbps
Tradicional	Navegación WEB (pico), VoIP local, tráfico de dispositivos IoT locales	Por defecto	< 2 seg	< 2Mbps	5.4 Mbps / 20 Mbps
Tradicional	Navegación WEB (pico), VoIP local, tráfico de dispositivos IoT locales, CCTV local y remoto	Por defecto	< 2 seg	< 2Mbps	1.3 Mbps / 20 Mbps
SDN + IoT	Navegación WEB (pico), VoIP local, tráfico de dispositivos IoT locales y remotos	- FW inhabilitado - sin políticas QoS	-	< 20Kbps	0 Mbps / 20 Mbps
SDN + IoT	Navegación WEB (pico), VoIP local, tráfico de dispositivos IoT locales, CCTV local y remoto	- FW habilitado - todo tráfico a través de FW habilitado - sin políticas QoS	< 1 seg	< 4Mbps	6 Mbps / 20 Mbps
SDN + IoT	Navegación WEB (pico), VoIP local, tráfico de dispositivos IoT locales, CCTV local y remoto	- FW Habilitado - habilitación de tráfico TCP Y UDP - bloqueo de paquetes ICMP interno - Limitación de ancho de banda a través de política de QoS	< 1 seg	7Mbps < AB < 10 Mbps	14.6 Mbps / 20 Mbps
Tradicional (Segmento de prueba remoto)	Navegación WEB (pico), VoIP local, tráfico de dispositivos IoT locales, CCTV local y remoto	Por defecto	< 2 seg	< 4 Mbps	1.1 Mbps / 10 Mbps
SDN + IoT (Segmento de prueba remoto)	Navegación WEB (pico), VoIP local, tráfico de dispositivos IoT locales, CCTV local y remoto	- FW Habilitado - habilitación de tráfico TCP Y UDP - bloqueo de paquetes ICMP interno - Limitación de ancho de banda a través de política de QoS	< 1 seg	< 7 Mbps	9.2 Mbps / 10 Mbps

Fig. 1. Resultados Globales Obtenidos

durante el desarrollo de este capítulo, las políticas por defecto de un enrutador propietario no priorizan el tráfico de información de ningún tipo, es decir: se tratan a toda la información por igual y genera cuellos de botella y problemas significativos en el ancho de banda para transmisión y recepción de datos en una red; sin embargo, únicamente con agregar un dispositivo intermediario completamente programable, se habilita una extensa gama de funcionalidades técnicas que permiten clasificar, limitar e inclusive obstruir directamente el tráfico de red local y saliente.

Con base en dicho análisis, se ha demostrado que varios segmentos de red SDN controlados a través de un nodo centralizado, contribuye en gran medida a la replicación de políticas de bajo nivel que anteriormente requerían ser implementadas de forma manual por parte de los administradores de red, esto ha permitido reducir el tiempo de implementación, despliegue de red y actualización de políticas de control sobre redes de gran magnitud; y adicionalmente, se ha proporcionado un marco de control completamente adaptable y configurable con el afán de descongestionar segmentos saturados que dependen de la cantidad de políticas de control e ingeniería de tráfico que un único administrador desarrolle"

IV. Methodology

La Internet de las Cosas (IoT) es un paradigma que permite conectar dispositivos inteligentes a través de redes inalámbricas, generando una gran cantidad de datos que pueden ser procesados y analizados para obtener información

útil. Sin embargo, la gestión de estas redes requiere de una adaptación dinámica a las condiciones cambiantes del entorno. Por ello, se propone el uso de las Redes Definidas por Software (SDN), que permiten separar el plano de control del plano de datos, y así facilitar la configuración, el monitoreo y la optimización de la red. En este trabajo se presenta una solución que integra IoT con SDN, mediante la creación de una red virtual que abstrae los recursos físicos y ofrece una interfaz unificada para el despliegue y la gestión de servicios IoT. Véase la Figura 2

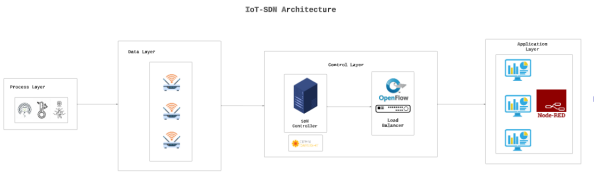

Fig. 2. Esquemático de la Estructura de Red

Para llevar a cabo la gestión de la Red Definida por Software (SDN), implementamos un enfoque que involucra varios componentes clave. En primer lugar, implementamos un controlador OpenDayLight, el cual se encuentra alojado en un contenedor de Docker en un entorno Ubuntu. La versión específica del controlador que utilizamos es Carbon. Este controlador desempeña un papel central en la orquestación y administración de la red virtualizada.

Para administrar las interfaces de red de dos switches virtuales presentes en la simulación, optamos por utilizar OpenvSwitch. Esta herramienta nos proporciona la capacidad de gestionar eficientemente las conexiones y configuraciones de red de estos switches virtuales.

En lo que respecta a la comunicación de datos, elegimos el protocolo MQTT como medio para enviar información hacia un broker de Mosquitto. Dado que el intercambio de datos es fundamental en la SDN, MQTT se revela como una elección adecuada para esta tarea, proporcionando una comunicación eficaz y escalable.

A nivel de la capa de aplicación, utilizamos node-red para diseñar un gráfico que representa el flujo de datos generado por un sensor presente en la simulación. Node-red nos permite crear visualmente el flujo de procesamiento de datos, lo que facilita la configuración y gestión de la información generada en la red.

El broker de Mosquitto y la aplicación node-red, están alojados en un contenedor Docker que residen en el servidor denominado ”Services” dentro del entorno de simulación. Esta elección arquitectónica permite una administración eficiente de estos servicios, garantizando su disponibilidad y aislamiento en el entorno virtual. Véase la Figura 3.

V. Analysis of Results

La presente ilustración corresponde a la configuración de la tabla de interfaces del switch OpenVSwitch-1. Se muestra

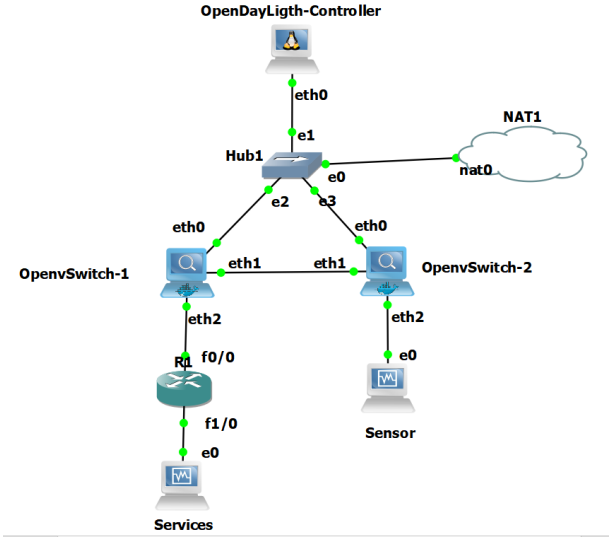

Fig. 3. Arquitectura General de la Red a implementar

la asignación del controlador OpenDaylight-Controller con IP 192.168.122.57 al bridge br0. De esta manera confirmamos la operatividad del controlador de la red sobre el dispositivo. Véase la Figura 4.

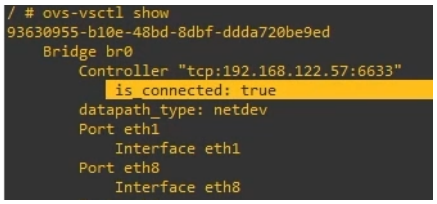

Fig. 4. Visualización de interfaces activas

La imagen ilustra la relación de conectividad entre dos componentes esenciales en la red: el OpenVSwitch1 y una máquina de servicios(Mosquitto y Node-RED) identificada por la dirección IP 172.16.0.1. Un aspecto destacado en esta representación visual es la medición precisa de los tiempos de respuesta, los cuales se sitúan en un intervalo específico, oscilando entre 10 y 13 milisegundos. Véase la Figura 5.

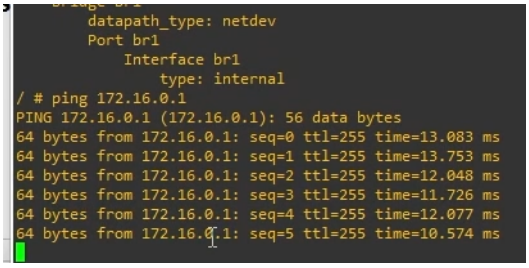

Fig. 5. Ping desde OpenVswitch1 hacia la máquina de servicios

La imagen presenta la conectividad entre el Open-vswitch2 y el controlador OpenDayLight con la dirección IP 192.168.122.57, destacando significativamente la variabilidad

en los tiempos de respuesta, los cuales fluctúan entre 0.8 milisegundos y 138.722 milisegundos. Esta representación visual es esencial para comprender la relación y los tiempos de respuesta entre estos elementos críticos en la red, y ofrece una valiosa evaluación de la eficiencia y la latencia en su comunicación. Véase la Figura 6.

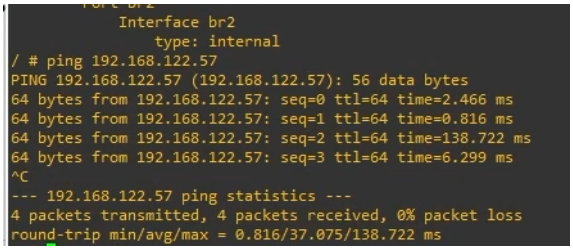

Fig. 6. Ping desde OpenVswitch2 hacia el controlador virtual (OpenDaylight)

La ilustración muestra la tabla de contendores activos en dentro del servidor Services. Se muestra el servicio de Mosquitto y Node-red funcionando correctamente. Véase la Figura 7.

Fig. 7. Visualización del contenedor levantado (Node-RED)

La imagen muestra algunas pruebas de envío de datos, desde la máquina Sensor, hacia Services. Enviando valores publicados en el tópico ”/sensor” para luego ser tomados desde Node-red para mostrarlos en un dashboard. Véase la Figura 8 y 9.

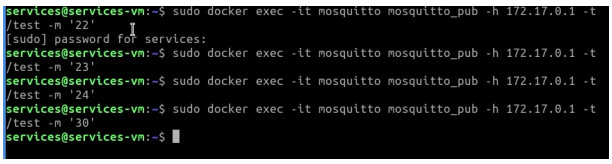

Fig. 8. Visualización del contenedor levantado (Mosquitto)

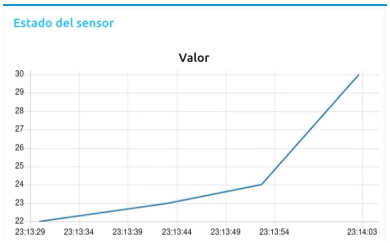

Fig. 9. Gráfico del flujo de datos en Node-Red

VI. Discussion

La gestión adecuada de dispositivos IoT es muy relevante a la hora de establecer una cadena de frío en el transporte de alimentos, puesto que el conjunto de operaciones logísticas se encarga de la correcta preservación, almacenamiento y transporte de los alimentos perecederos. En este ensayo se argumentará a favor de la implementación de una red SDN para la gestión de dispositivos IoT en la cadena de frío para la distribución de productos alimenticios perecederos en Guayaquil. Los argumentos principales son los siguientes:

- Permite una mejor monitorización y control de las condiciones de temperatura y humedad de los alimentos, lo que mejora la calidad y la seguridad alimentaria.
- Facilita la adaptación y la optimización de la red a las necesidades cambiantes del mercado y del entorno, lo que reduce los costos operativos y aumenta la competitividad.
- Ofrece una mayor protección frente a posibles ataques cibernéticos o fallos técnicos, lo que garantiza la continuidad del servicio y la confianza de los clientes.

La gestión de la cadena de frío con dispositivos IoT se mejora al implementar una red SDN, ya que facilita el seguimiento, la regulación de la temperatura y la humedad de los productos alimenticios. Esto se debe a que una red SDN tiene la capacidad de recoger y procesar los datos que envían los sensores IoT instalados en los equipos de frío, como cámaras, contenedores o vehículos, y enviar instrucciones para regular dichas condiciones según los parámetros establecidos. De esta manera, se puede asegurar que los alimentos se mantienen en el rango óptimo de temperatura y humedad durante todo el proceso logístico, desde que salen del productor hasta que llegan al consumidor.

Sin embargo, también hay que tener en cuenta algunas posibles desventajas o limitaciones de este sistema. Por ejemplo, se requiere una inversión inicial para adquirir e instalar los dispositivos IoT y los equipos SDN, así como un mantenimiento periódico para asegurar un óptimo funcionamiento. Además, se debe garantizar una buena conectividad entre los dispositivos IoT y la red SDN, lo cual puede ser difícil en zonas remotas o con mucha interferencia.

Por otro lado, la implementación de este tipo de red permite modificar la configuración, el enrutamiento y el ancho de banda de forma dinámica y centralizada, sin necesidad de intervenir físicamente en los dispositivos. Esto aportaría mucho valor a cualquier empresa que desee usar este tipo de tecnología en el manejo de sus servicios. Ya que, con las configuraciones adecuadas, se podría llegar a ajustar la capacidad de la red, regulando así la carga de trabajo según la demanda de los clientes o las condiciones climáticas.

Para llevar esto a cabo es necesario contar con el personal adecuado para la correcta gestión de la red, puesto que un manejo no adecuado de la topología podría a llegar a afectar toda la cadena de trabajo. Esto sin contar que una estructura virtual centralizada es muy vulnerable a ataques cibernéticos, lo cual dificulta en gran manera la seguridad y privacidad de los datos que pueden llegar a circular por la red.

Por último, una red SDN bien configurada permite brindar medidas de seguridad y protección de datos más avanzadas y eficaces que una red tradicional, al centralizar el control y supervisión de la red, al mismo tiempo que se aísla el tráfico sensible del resto. Sabiendo esto, se puede tener una mejor comprensión de la capacidad de la red ante posibles amenazas.

Los controladores SDN son capaces de identificar los diversos atributos de paquetes y flujos, y aplicar políticas de seguridad dinámicas. Esto permite el bloqueo automático o la descarga de tráfico en ataques de denegación de servicio (DoS). Además, una red SDN puede aprovechar la programabilidad y la flexibilidad para implementar sistemas de monitoreo, detección y prevención de intrusiones (IDS/IPS), que pueden detectar y mitigar una serie de ataques a la red, como las inundaciones SYN, los escaneos de puertos o las inyecciones SQL. De esta forma, una red SDN puede proteger la integridad, disponibilidad y confidencialidad de los datos que circulan por la cadena de frío, evitando su alteración, interrupción o robo por parte de agentes maliciosos.

La implementación de una red SDN para la cadena de frío en el transporte de productos alimenticios perecederos es una opción viable, beneficiosa y necesaria para mejorar la seguridad, la calidad y la eficiencia de este sector. Una red SDN permite una gestión más flexible, dinámica y segura de la red que soporta la cadena de frío, adaptándose a las necesidades y demandas del tráfico y respondiendo ante situaciones imprevistas o amenazas maliciosas. Así, se garantiza la continuidad del servicio y la confianza de los clientes, que reciben productos frescos y saludables. Por lo tanto, se recomienda a los actores involucrados en la cadena de frío que adopten esta tecnología innovadora y aprovechen sus ventajas competitivas.

VII. Conclusion

La adopción de la tecnología de red definida por software (SDN) en el ámbito del transporte refrigerado se presenta como una oportunidad prometedora para mejorar significativamente la eficiencia y la calidad de este sector crucial. La capacidad de controlar de manera centralizada y dinámica los dispositivos y recursos de la red, ajustándose a las demandas y condiciones específicas de cada etapa de la cadena de frío, abre la puerta a una serie de ventajas notables.

En primer lugar, la SDN permite una optimización precisa de los recursos, incluyendo la energía, el espacio, el tiempo y el personal involucrado en el proceso de transporte refrigerado. Esto conlleva una reducción significativa de los costos operativos y, al mismo tiempo, minimiza los riesgos de pérdida o deterioro de los productos perecederos durante el viaje. La capacidad de monitorear, rastrear y gestionar datos en tiempo real sobre los productos contribuye aún más a mejorar la conservación y la calidad de los mismos, al tiempo que proporciona información valiosa y fomenta la confianza del consumidor final.

Sin embargo, es importante destacar que la implementación de la SDN en este contexto no está exenta de desafíos. La inversión inicial requerida para adoptar esta tecnología puede ser considerable, y la capacitación del personal en su uso eficiente es esencial para aprovechar al máximo su potencial. Además, la interoperabilidad con otros sistemas existentes, la seguridad cibernética y el cumplimiento de las normativas vigentes son aspectos críticos que deben abordarse de manera cuidadosa y sistemática.

Por tanto, se recomienda a las empresas que consideren la implementación de la SDN en el transporte refrigerado realicen un estudio exhaustivo de factibilidad técnica, económica y legal. Este estudio proporcionará una base sólida para la toma de decisiones informadas y ayudará a identificar los posibles obstáculos y oportunidades en el camino. Además, la planificación de una implementación gradual y una evaluación continua son esenciales para asegurar el éxito y la rentabilidad de este proyecto a largo plazo.

En última instancia, si se abordan adecuadamente los desafíos y se gestionan eficazmente los recursos, la SDN tiene el potencial de transformar la industria del transporte refrigerado, brindando beneficios sustanciales tanto a las empresas como a los consumidores finales. La optimización de los recursos y la mejora en la calidad de los productos son objetivos loables que pueden lograrse mediante la adopción de esta tecnología innovadora.

References

Ateya, A., Algarni, A., Hamdi, M., Koucheryavy, A., & Soliman, N. (2021). Enabling heterogeneous iot networks over 5g networks with ultra-dense deployment: Using mec/sdn. *Vol. 10, No. 8*, 910.

Bedhief, I., Kassar, M., Aguili, T., Foschini, L., & Bellavista, P. (2019). Self-adaptive management of sdn distributed controllers for highly dynamic iot networks. In *2019 15th international wireless communications mobile computing conference (iwcmc)* (pp. 2098–2104).

Blial, O., Ben Mamoun, M., CN Benaini, R., & Communications. (2016). An overview of sdn architectures with multiple controllers. *Vol. 2016*.

Braun, W., & Menth, M. (2014). Software defined networking using openflow: Protocols, applications and architectural design considerations. *Vol. 6, No. 2*, 302–336.

Chen, X., & et al. (2020). Traffic modeling and performance evaluation of nb-iot access network based on sdn. *Vol. 32, No. 16*, e5145.

Eghbali, Z., & Lighvan, M. (2021). A hierarchical approach to accelerate iot data management process based on sdn principles. *Journal of Network and Computer Applications*, *181*, 103027.

Karmakar, R., et al. (2020). Sdn enabled secure iot architecture. *Wireless Personal Communications*, *110*, 873–892.

Kataoka, K., Gangwar, S., & Podili, P. (2018). Whitelist: Distributed and internet-wide traffic management for iot via blockchain and sdn. In *2018 ieee 4th world forum on internet of things (wf-iot)* (pp. 296–301).

Kreutz, D., Ramos, F., Verissimo, P., Rothenberg, C., Azodolmolky, S., & Uhlig, S. (2014). Software-defined

networking: A comprehensive survey. *Vol. 103, No. 1*, 14–76.

Li, J., Altman, E., & Touati, C. (2015). A general iot framework based on sdn with nvf implementation. *Vol. 13, No. 3*, 42–45.

Li, J., & et al. (2020). A secure framework for sdn-based edge computing in iot-enabled healthcare system. *IEEE Access*, *8*, 135479–135490.

Medved, J., Varga, R., Tkacik, A., & Gray, K. (2014). Opendaylight: Towards a model-driven sdn controller architecture. In *Proceedings of the international ieee symposium on a world of wireless, mobile and multimedia networks* (pp. 1–6).

Mohammed, A., Khaleefah, R., & Abdulateef, I. (2020). A review software defined networking for internet of things. In *International congress on human-computer interaction, optimization, and robotic applications (hora)* (pp. 1–8).

Placencia Camacho, F. G. (2021). *Alarmas comunitarias basadas en arquitecturas sdn e iot* (Tesis de grado). Universidad Técnica de Ambato, Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

Salman, O., Elhajj, I., Chehab, A., & Kayssi, A. (2018). Iot survey: A sdn and fog computing perspective. *Vol. 143*, 221–246.

Tayyaba, S., Shah, M., Khan, N., Asim, Y., Naeem, W., & Kamran, M. (2016). Software defined networking (sdn) and internet of things (iot): A qualitative prediction for 2020. *Vol. 7, No. 11*.

Tayyaba, S., Shah, M., Khan, O., & Ahmed, A. (2017). Software defined networking (sdn) based internet of things (iot): A road ahead. In *Proceedings of the international conference on future distributed systems and networks* (pp. 1–8).

Tello-Oquendo, L., Akyildiz, I., Lin, S., & Pla, V. (2018). Sdn-based architecture to provide reliable internet of things connectivity in 5g systems. In *2018 17th annual mediterranean ad hoc networking workshop (med-hoc-net)* (pp. 1–8).

Yazdinejad, H., & et al. (2019). Blockchain-enabled privacy-preserving authentication transfer in sdn-based 5g networks. *IEEE Transactions on Network and Service Management*, *16*(1), 297–311.

Zhao, L., Sun, W., Shi, Y., & Liu, J. (2018). Optimal cloudlet placement for access delay minimization in sdn-based internet of things networks. *IEEE Internet of Things Journal*, *5*(2), 1334–1344.

APPENDIX

Contribuciones:

- Isaac Vasco (33,3 %): Encargado de realizar la investigación sobre el estado del arte de la integración de IoT y SDN, lo que implica analizar bases de datos académicas, investigaciones científicas y documentos técnicos relacionados con el tema. Después de recopilar la información, se procedió a examinar y seleccionar las fuentes más relevantes y fiables. Además, contribuyó al diseño esquemático de la estructura de la red, detallando las tecnologías y los dispositivos que se emplearán. Asimismo, colaboró en parte de la simulación de la red virtualizada, lo que permitió agilizar y mejorar la eficiencia del trabajo.
- Michael Cedeño (33,3 %): Encargado de la redacción y síntesis de la información a partir de la implementación realizada para la integración de la tecnología. Además, desempeño un papel fundamental al proporcionar una visión crítica y creativa en la estructuración del diseño de red, lo que llevo a una mejor comprensión a la hora de implementar todas las tecnologías.
- Javier Dillon (33,3 %): Encargado de la búsqueda de herramientas para facilitar la implementación de la topología de red planteada. Aporto con conocimientos previos de otras asignaturas, en la solución de errores que se presentaron durante la integración de las tecnologías. Además, fue de vital importancia al encaminar la búsqueda de información práctica en el desarrollo de las actividades planteadas.