

Facultad de Ingenierías

202401\_001\_BIT-31\_1\_00

Inteligencia en Redes de Datos

Carlos Andrés Méndez Rodríguez

Software Defined Network (SDN)

Estudiantes:

Alonso Amador Rojas 2011017801

Daniela Castillo Madrigal 20200120519

Dennis Josué Valverde Gómez 20190111782

2024

Tabla de contenido

[Introducción 3](#_Toc2393300)

[Objetivos 4](#_Toc679345430)

[Conceptos Fundamentales de SDN 5](#_Toc1733464492)

[Arquitectura de SDN: plano de control y plano de datos 6](#_Toc1698472190)

[Componentes clave de una red SDN: controlador, switches y aplicaciones 7](#_Toc2018807946)

[Aplicaciones de SDN en Telemática 7](#_Toc994469790)

[Beneficios de SDN. 8](#_Toc2094079324)

[Desafíos de seguridad y gestión asociados con la implementación de SDN. 9](#_Toc1546962227)

[Limitaciones de SDN en cuanto a rendimiento, interoperabilidad y complejidad. 10](#_Toc1217285116)

[Soluciones Cisco 11](#_Toc1729231742)

[Soluciones de otros fabricantes. 13](#_Toc1073946493)

[Conclusiones 14](#_Toc451633862)

[Bibliografía 15](#_Toc864947657)

## Introducción

En el campo de la telemática, la evolución de las redes de comunicación es fundamental para satisfacer las crecientes demandas de conectividad, rendimiento y seguridad. Una de las tecnologías emergentes que está transformando la forma en que se diseñan y gestionan las redes es la Red Definida por Software (SDN, por sus siglas en inglés). SDN ofrece una arquitectura flexible y programable que permite una gestión centralizada y dinámica de los recursos de red. Este trabajo se centra en explorar los fundamentos, aplicaciones y beneficios de SDN en el contexto de la telemática.

## Objetivos

* Comprender los principios básicos de SDN: Explorar los conceptos fundamentales detrás de SDN, incluyendo la separación del plano de control y el plano de datos, y el papel del controlador SDN.
* Analizar las aplicaciones de SDN en telemática: Investigar cómo SDN puede ser aplicado en entornos telemáticos para mejorar la gestión de redes, optimizar el rendimiento y garantizar la seguridad de las comunicaciones.
* Evaluar los beneficios y desafíos de SDN en telemática: Examinar los beneficios potenciales de SDN en términos de flexibilidad, escalabilidad, automatización y seguridad, así como identificar los desafíos y limitaciones asociados con su implementación.

## Conceptos Fundamentales de SDN

SDN (Redes definidas por software) es un enfoque de red que permite la programación y el control centralizados de la infraestructura de la red, separando el plano de control del plano de datos. Algunos conceptos básicos de SDN incluyen:  
Control centralizado: La lógica de control SDN está centralizada en el controlador, proporcionando una visión global de la red y facilitando la programación y automatización.

Separación del plano de control y del plano de datos: en lugar de dividir el control de la red entre dispositivos, SDN separa el plano de control (donde se toman las decisiones de enrutamiento y conmutación) del plano de datos (donde se transmite el plano de datos).

Abstracción de la red: SDN crea una vista abstracta y programable de la red, lo que facilita la implementación de políticas de red y la optimización del tráfico.  
Programabilidad: con SDN, los administradores de red pueden programar el comportamiento de la red a través de interfaces programáticas, lo que permite una mayor flexibilidad y adaptabilidad.

Centralización de aplicaciones y servicios: SDN permite el despliegue centralizado de aplicaciones y servicios de red, simplificando la gestión e introduciendo nuevas capacidades.

## Arquitectura de SDN: plano de control y plano de datos

Plano de control: en una arquitectura SDN, el plano de control es el principal elemento responsable de cómo se debe manejar el tráfico en la red. Este plano consta de un controlador SDN que recopila información sobre el estado de la red, toma decisiones basadas en esa información y comunica esas decisiones a los dispositivos de red en el plano de datos. Los controladores pueden comunicarse con dispositivos de red y programar su comportamiento utilizando protocolos como OpenFlow. El controlador SDN realiza una gestión de red centralizada y unificada, facilitando la implementación de políticas de red, la detección y corrección de problemas y la adaptación a cambios en la topología de la red.

Plano de datos: es donde se transmiten paquetes de datos en la red. Este plano consta de dispositivos de red, como conmutadores y enrutadores, que se encargan de reenviar paquetes según las instrucciones del controlador SDN. La separación del plano de datos y el plano de control proporciona una mayor flexibilidad y programabilidad en la gestión del tráfico de red, ya que los dispositivos de red se pueden configurar de forma dinámica y centralizada.

## Componentes clave de una red SDN: controlador, switches y aplicaciones

Controlador SDN: El controlador es el cerebro de la red SDN. Es responsable de recopilar información sobre el estado de la red, tomar decisiones de enrutamiento y configuración, y luego comunicar esas decisiones a los dispositivos de red en el plano de datos. El controlador puede utilizar protocolos como OpenFlow para comunicarse con los dispositivos de red y programar su comportamiento. Además, el controlador proporciona una interfaz centralizada para la gestión y programación de la red, lo que facilita la implementación de políticas de red, la detección y corrección de problemas, y la adaptación a cambios en la topología de la red.

Dispositivos de red (switches y routers): Estos dispositivos conforman el plano de datos de la red SDN y son responsables del reenvío efectivo de los paquetes de datos. En una red SDN, estos dispositivos son programables y pueden recibir instrucciones de reenvío del controlador SDN. Esto permite una gestión dinámica y centralizada del tráfico, lo que a su vez ofrece una mayor flexibilidad y adaptabilidad a las necesidades cambiantes de la red.

Aplicaciones SDN: Las aplicaciones SDN son programas o servicios que se ejecutan en la capa de aplicación sobre el controlador SDN. Estas aplicaciones pueden aprovechar la visibilidad y el control centralizado de la red para implementar políticas de red, optimizar el tráfico, mejorar la seguridad, entre otros. Las aplicaciones SDN pueden desarrollarse por terceros o por el equipo de operaciones de red para adaptarse a sus necesidades específicas. Algunos ejemplos de aplicaciones SDN incluyen la gestión de ancho de banda, la segmentación de red, la optimización de la entrega de contenido, entre otros.

En conjunto, estos componentes forman la base de una red SDN, permitiendo una gestión centralizada, programabilidad y una mayor flexibilidad en la gestión del tráfico de la red. La interacción entre el controlador, los dispositivos de red y las aplicaciones SDN es fundamental para la implementación exitosa de una red SDN y para obtener sus beneficios en términos de agilidad, eficiencia operativa y capacidad de adaptación.

## Aplicaciones de SDN en Telemática

Las aplicaciones SDN en el procesamiento remoto de información cubren una amplia gama de casos de uso que aprovechan la programabilidad, el control centralizado y la visibilidad de la red que ofrece SDN. A continuación, se ofrece una explicación amplia de algunos de los usos de SDN en el procesamiento remoto de información:  
  
Gestión del tráfico y calidad de servicio (QoS): en el procesamiento remoto de información, la gestión eficaz del tráfico es esencial para garantizar la entrega oportuna de datos críticos, como información de vehículos conectados o sistemas de navegación. Con SDN, se pueden implementar políticas dinámicas de QoS para priorizar ciertos tipos de tráfico sobre otros, brindando una experiencia de usuario consistente y confiable.  
Seguridad y aislamiento de la red: la seguridad es una preocupación importante en el procesamiento remoto de información, especialmente en entornos como los vehículos conectados. SDN permite implementar políticas de seguridad granulares, como segmentación de red y aislamiento de tráfico, para proteger sistemas críticos y evitar intrusiones no deseadas.  
Gestión del ancho de banda: en un entorno de procesamiento de información remoto, optimizar el uso del ancho de banda es fundamental para garantizar conexiones eficientes y confiables. SDN admite la gestión dinámica del ancho de banda, lo que significa que los recursos de la red se pueden asignar y reasignar dinámicamente según las necesidades cambiantes para un rendimiento óptimo.

## Beneficios de SDN.

Las SDN ofrecen beneficios como escalabilidad al simplificar la gestión y abstraer la infraestructura física, automatización y flexibilidad al tener una gestión centralizada y la red programada. Estos beneficios junto permiten a las organizaciones adaptarse rápido a las necesidades cambiantes de los negocios y mejorar la eficiencia operativa en la gestión de las redes de comunicación. A continuación, se detallan los beneficios con enfoque en escalabilidad, automatización y flexibilidad.

- Escalabilidad: la gestión de la red se centraliza en el controlador SDN, permite simplificar la gestión de la red eliminando la necesidad de configurar individualmente cada dispositivo de red, además da una mayor facilidad con la expansión de la red sin afectar la operación de la misma por incluir un nuevo dispositivo. Las SDN abstraen la infraestructura física de red por lo tanto las decisiones de enrutamiento y conmutación se toman en función de las políticas definidas en un nivel lógico, en vez de depender de la topología física subyacente.

- Automatización: las tareas de gestión de red se automatizan mediante la coordinación de servicios y recursos de la red, incluyendo la automatización de la configuración, aprovisionamiento y optimización de la red, reduciendo la tasa del error humano porque no hay intervención manual, genera eficiencia operativa. Las SDN proporcionan una interfaz programable y API abierta que brindan una integración con herramientas de automatización, EMS (sistemas de gestión empresarial) y NMS (sistemas de gestión de red). Con esto se logra la creación de flujos de trabajo automatizados e integrados con sistemas existentes para mejorar la entrega de servicios de red.

- Flexibilidad: al separar el plano de control del de datos se genera una arquitectura desacoplada, es decir, los dispositivos de red como routers, switches, entre otros, son gestionados de manera dinámica y centralizada por medio del controlador SDN, lo que hace flexible la configuración y gestión de red. Los dispositivos pueden ser programados y configurados mediante el software, permitiendo una implementación rápida de funcionalidades nuevas y servicios sin la necesidad de cambiar la infraestructura física subyacente.   
 Hay una mayor flexibilidad para controlar el tráfico de acuerdo con las necesidades específicas del negocio debido a la implementación de políticas de red dinámicas y granulares. Incluyendo la capacidad de priorizar ciertos tipos de tráfico, aplicar reglas de seguridad y calidad de servicios de manera más eficiente además de definir políticas de acceso basadas en identidad y contexto.

## Desafíos de seguridad y gestión asociados con la implementación de SDN.

Las implementaciones de SDN tienen desafíos en seguridad y en la gestión que se recomienda considerarlos para ofrecer una buena disponibilidad de red, garantizar la integridad y confidencialidad. En la actualidad, se está expuesto a múltiples tipos de amenazas de seguridad por esa razón es de gran importancia la protección de los controladores SDN, switches y demás dispositivos de red asociados, de esta manera evitar que el control de la red se pueda comprometer. La SDN al separar el plano de control del plano de datos, el controlador SDN llega a ser un punto crítico que se debe proteger contra ataques de denegación de servicio, secuestro de controlador y la inyección de comandos maliciosos.

Una característica de las redes definidas por software es la segmentación de la red dinámicamente, esto conlleva a garantizar un aislamiento adecuado entre cada una de las redes virtuales para prevenir la propagación de ataques. Estos se pueden realizar mediante políticas de seguridad basadas en etiquetas que se aplican a los flujos de tráfico definiendo reglas para permitir o denegar tráfico entre los segmentos de red. También con firewalls virtuales, sistemas de prevención de intrusiones o IPS, monitoreo continuo, implementación de un modelo de control de acceso basado en roles, entre otros. Como las SDN implican el uso de software, es muy importante mantener actualizados los componentes del sistema y aplicar parches de seguridad oportunamente para mitigar vulnerabilidades.

Otro punto para considerar es la gestión de identidad y acceso, debido a que los dispositivos de red pueden ser provisionados dinámicamente y los flujos de tráfico pueden redirigirse en tiempo real, es importante establecer las políticas de acceso adecuadas y mecanismos de autenticación seguros.

## Limitaciones de SDN en cuanto a rendimiento, interoperabilidad y complejidad.

Rendimiento: Debido al procesamiento y toma de decisiones de enrutamiento de manera centralizada en el controlador SDN puede haber una latencia adicional la cual afecta el rendimiento de aplicaciones que necesitan tiempos de respuesta bajos. El controlador debe dar abasto con el manejo de las cargas de trabajo requeridas por la red ya que la centralización puede ocasionar que el controlador se convierta en un punto único de fallo.

Interoperabilidad: las SDN tienen estándares abiertos que están en una constante evolución, puede ocasionar desafíos entre dispositivos de algunos fabricantes que utilicen versiones diferentes de esos estándares. La integración en entornos de red existentes se puede complicar por la variedad de equipos de red y tecnologías legacy, las soluciones de puente o adaptadores entre equipos no compatibles aumentan la complejidad y los puntos potenciales de fallo. OpenFlow es uno de esos estándares abiertos de SDN, sin embargo, esa falta de estandarización en áreas como la gestión de políticas y configuración dificulta la interoperabilidad en diferentes implementaciones de SDN.

Complejidad: es importante mencionar que el uso de SDN requiere de una curva de aprendizaje para los encargados de administrar las redes, cambia la forma en que se diseñan, administra e implementan las redes. La gestión centralizada trae ciertos beneficios, pero a la vez la responsabilidad de concentrar la red en el controlador SDN, una configuración incorrecta o algunos errores en el controlador generarían impactos significativos en toda la red.

## Soluciones Cisco

Cisco ACI Cisco Application Centric Infrastructure: es la solución de redes definidas por software (SDN) más segura, abierta y completa de la industria que automatiza, acelera la implementación y administración de la infraestructura, simplifica la administración y mueve fácilmente cargas de trabajo entre sistemas desde múltiples instalaciones y múltiples nubes, abordando los riesgos de manera proactiva. de donde sea. surgen. Simplifique, agilice y acelere radicalmente el ciclo de vida de implementación de aplicaciones. Los centros de datos actuales son dinámicos. Las operaciones de TI deben cumplir con los requisitos de calidad del servicio empresarial en un entorno que cambia rápidamente. Cisco ACI transforma las operaciones de TI de reactivas a proactivas a través de una serie de capacidades de software altamente inteligentes que analizan todos los elementos del centro de datos para garantizar la intención comercial, garantizar la confiabilidad e identificar problemas de rendimiento de la red antes de que ocurran.

A medida que las aplicaciones se vuelven más comunes en las redes corporativas, los profesionales de TI desean crear políticas consistentes y soluciones de cifrado desde el campus hasta la nube.

Beneficios de Cisco ACI

Para mantenerse al día con la afluencia de datos y la creciente demanda de velocidad y agilidad de la red, los profesionales de redes están aprendiendo a administrar, conectar, construir y administrar sus redes no solo en centros de datos sino también en grandes entornos de nube. Cisco ACI se creó para simplificar la infraestructura y las operaciones de TI al automatizar la red, brindar seguridad de extremo a extremo y ayudar a las empresas a acelerar su transición a entornos de nube o de múltiples nubes.

Con Cisco ACI, los clientes pueden gestionar la complejidad, aumentar los ingresos empresariales e implementar el trabajo en cualquier lugar (pequeño y grande, local y remoto) en nubes públicas y privadas, centros de datos satelitales y bordes de telecomunicaciones habilitados para 5G. Las principales ventajas de Cisco ACI son:

Acelerar las operaciones de red

Cisco ACI proporciona una red flexible y de alta disponibilidad que permite la flexibilidad de implementar aplicaciones dentro de sitios, entre sitios y en centros de datos en todo el mundo, al tiempo que elimina la necesidad de una infraestructura compleja de interconexión de centros de datos (DCI).

● Promover el desarrollo de 400G a 800G. ● Proporciona administración y visibilidad de la red centralizada con monitoreo del estado de la red en tiempo real y totalmente automatizado.

● Integración perfecta de redes centrales y superpuestas. ● Aproveche las API abiertas hacia el norte para brindar flexibilidad a los equipos de DevOps y la integración de socios del ecosistema.

● Utilizar una plataforma común para gestionar entornos físicos y virtuales. ● Automatice los flujos de trabajo de TI y permita una implementación flexible de aplicaciones.

Escala de forma segura a múltiples nubes

● Utilice una solución SDN segura basada en la nube. ● Establecer continuidad del negocio y preparación para desastres.

● Obtenga seguridad inherente con un modelo de lista blanca de confianza cero y capacidades innovadoras para la aplicación de políticas, la microsegmentación y el análisis.

● Obtenga seguridad integrada con productos de seguridad de Cisco y socios del ecosistema.

● Mantenga una postura de seguridad coherente en entornos de múltiples nubes. Proporcionar una experiencia única

● Benefíciese de la simplicidad operativa a través de políticas, gestión y modelos operativos comunes en todas las aplicaciones, redes y recursos de seguridad.

● Utilice un modelo de implementación flexible.

● Obtenga políticas consistentes y conectividad perfecta en cualquier centro de datos y nube pública.

● Adopte redes de contenedores habilitadas mediante la integración con VMware vRealize, Azure Pack, OpenStack, OpenShift, Kubernetes y Cisco UCS ® Director. ● Tiene una API abierta y un marco SDN programable con más de 65 socios del ecosistema, incluida la infraestructura como código (IaC).

● Hay margen para la expansión.

Cisco SD-WAN (red de área amplia definida por software) es una tecnología que simplifica la gestión y operación de redes de área amplia (WAN) al separar el hardware de red de los mecanismos de control. Proporciona gestión centralizada del tráfico de red y ofrece la capacidad de enrutar dinámicamente el tráfico en función de condiciones en tiempo real. Las soluciones Cisco SD-WAN están diseñadas para mejorar la experiencia del usuario, aumentar la seguridad y reducir los costos para las empresas con sucursales distribuidas y ubicaciones remotas.

## Soluciones de otros fabricantes.

Existen otros fabricantes que ofrecen soluciones de SDN a continuación se detallan algunas soluciones:

-VMware, tiene una plataforma de virtualización llamada NSX y ayuda en la segmentación de red dirigida a centros de datos. Además, tiene otra opción como lo es SD-WAN para empresas con sucursales en múltiples ubicaciones y que deseen mejorar el rendimiento, seguridad y confiabilidad de su red WAN. Otra opción que tiene este fabricante es VMware Tanzu, es una plataforma de Kubernetes para organizaciones que adoptan contenedores y Kubernetes para desarrollo de aplicaciones modernas y que requierean una plataforma integral para administrar cargas de trabajo.  
-Huawei Cloud Fabric, virtualización de red, gestión centralizada, automatización de servicios y está enfocada en centros de datos y también redes empresariales.  
-Juniper, tiene una plataforma llamada Contrail que brinda una orquestación de red para entornos de centros de datos en nubes.  
- Arista Networks, proporciona soluciones de SDN para la visibilidad y automatización de la red a escala.  
- Nuage Networks, virtualización y automatización, enfocada para cualquier infraestructura de centros de datos y pertenece a Nokia, establece una buena conectividad con máquinas virtuales, contenedores, servidores, entre otros.

## Conclusiones

La Red Definida por Software (SDN) ofrece un enfoque innovador para diseñar y gestionar redes de comunicación, con aplicaciones prometedoras en el campo de la telemática. A través de la centralización del control y la programabilidad de la infraestructura de red, SDN puede mejorar la eficiencia operativa, optimizar el rendimiento y fortalecer la seguridad en entornos telemáticos. Sin embargo, su implementación plantea desafíos en términos de seguridad, interoperabilidad y complejidad, que deben ser abordados con precaución.

Es una tecnología que cambia la manera de diseñar, administrar e implementar una red, cada vez su uso es más común debido a la facilidad que le brinda al usuario en la gestión de la red de manera centralizada. Las redes van migrando hacia lo digital dejando atrás las topologías físicas y simplificando los procesos.

Existen diferentes fabricantes que ya tienen soluciones de SDN las más conocidas como Cisco y VMware pero también hay otras opciones de Juniper, Nokia, Arista, entre otras, que aunque no sean tan conocidas se puede encontrar en ellas soluciones que se ajusten al requerimiento de cada cliente y muchas veces ahorrar costos en sobreprecios, de esta manera le permite al usuario tener diferentes opciones para elegir y no cerrarse a uno o dos fabricantes que dominen el mercado.

## Bibliografía

Feamster, N., Rexford, J., & Zegura, E. (2014). The Road to SDN: An Intellectual History of Programmable Networks. ACM SIGCOMM Computer Communication Review, 44(2), 87–98.

Kreutz, D., Ramos, F., Verissimo, P., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-Defined Networking: A Comprehensive Survey. Proceedings of the IEEE, 103(1), 14–76.

McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S., & Turner, J. (2008). OpenFlow: Enabling Innovation in Campus Networks. ACM SIGCOMM Computer Communication Review, 38(2), 69–74.

Shirazipourazad, S., Bouillet, E., & Tovar, E. (2016). A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. IEEE Communications Surveys & Tutorials, 18(4), 2683–2712.