UNIVERSIDAD HISPANOAMERICANA

ESCUELA DE INGENIERÍA INFORMÁTICA

ANALISIS, DISEÑO E IMPLEMENTACIÓN DE UN PROGRAMA DE CAPACITACIÓN Y ADOPCIÓN DE REDES DEFINIDAS POR SOFTWARE (SDN) DEL PORTAFOLIO DE CISCO PARA COSTA RICA Y PERÚ

Sustentante: Gustavo Aguilar Espinoza

Tutor: Yusselin Murcia Céspedes

Abril, 2020

TABLA DE CONTENIDOS

CARTA DE APROBACIÓN DEL TUTOR

CARTA DEL TUTOR

Alajuela, 02 de abril de 2020

Sra. Maria Isabel Losilla
Ingeniería Informática
Universidad Hispanoamericana

Estimada señora:

El estudiante Gustavo Aguilar Espinoza, cédula de identidad número 2-0562-0973, me ha presentado, para efectos de revisión y aprobación, el trabajo de investigación denominado **"Análisis, diseño e implementación de un programa de capacitación y adopción de redes definidas por software (SDN) del portafolio de Cisco para Costa Rica y Perú",** el cual ha elaborado para optar por el grado académico de Bachillerato.

En mi calidad de tutor, he verificado que se han hecho las correcciones indicadas durante el proceso de tutoría y he evaluado los aspectos relativos a la elaboración del problema, objetivos, justificación; antecedentes, marco teórico, marco metodológico, tabulación, análisis de datos; conclusiones y recomendaciones.

De los resultados obtenidos por el postulante, se obtiene la siguiente calificación:

a)	ORIGINAL DEL TEMA	10%	8
b)	CUMPLIMIENTO DE ENTREGA DE AVANCES	20%	18
C)	COHERENCIA ENTRE LOS OBJETIVOS, LOS INSTRUMENTOS APLICADOS Y LOS RESULTADOS DE LA INVESTIGACION	30%	28
d)	RELEVANCIA DE LAS CONCLUSIONES Y RECOMENDACIONES	20%	18
e)	CALIDAD, DETALLE DEL MARCO TEORICO	20%	20
	TOTAL		92

En virtud de la calificación obtenida, se avala el traslado al proceso de lectura.

Atentamente,

YUSSELIN TATIANA MURCIA CESPEDES (FIRMA)

Firmado digitalmente por YUSSELIN TATIANA MURCIA CESPEDES (FIRMA)
Fecha: 2020.04.02 22:41:52 -06'00'

YUSSELIN MURCIA CÉSPEDES
Cédula identidad N 205780828
Carné Colegio Profesional N 9020

CARTA DE APROBACIÓN DEL LECTOR

CARTA DE LECTOR

San José,

Universidad Hispanoamericana
Sede Llorente
Carrera

Estimado señor

La estudiante Gustavo Aguilar Espinoza, cédula de identidad 2-0562-0973, me ha presentado para efectos de revisión y aprobación, el trabajo de investigación denominado Análisis, Diseño E Implementación De Un Programa De Capacitación y Adopción De Redes Definidas Por Software (SDN) Del Portafolio De Cisco Para Costa Rica Y Perú, el cual ha elaborado para obtener su grado académico de Bachillerato de Ingeniería Informática.

He revisado y he hecho las observaciones relativas al contenido analizado, particularmente lo relativo a la coherencia entre el marco teórico y análisis de datos, la consistencia de los datos recopilados y la coherencia entre éstos y las conclusiones; asimismo, la aplicabilidad y originalidad de las recomendaciones, en términos de aporte de la investigación. He verificado que se han hecho las modificaciones correspondientes a las observaciones indicadas.

Por consiguiente, este trabajo cuenta con mi aval para ser presentado en la defensa pública.

Atte.

Randall Vargas Villalobos
1-1140-0113

DECLARACIÓN JURADA

DECLARACIÓN JURADA

Yo **Gustavo Aguilar Espinoza**, mayor de edad, portador de la cédula de identidad número **205620973** egresado de la carrera de **Ingeniería en Sistemas** de la Universidad Hispanoamericana, hago constar por medio de éste acto y debidamente apercibido y entendido de las penas y consecuencias con las que se castiga en el Código Penal el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi trabajo de tesis para optar por el título de Bachillerato en Ingeniería en Sistemas, juro solemnemente que mi trabajo de investigación titulado: **ANALISIS, DISEÑO E IMPLEMENTACIÓN DE UN PROGRAMA DE CAPACITACIÓN Y ADOPCIÓN DE REDES DEFINIDAS POR SOFTWARE (SDN) DEL PORTAFOLIO DE CISCO PARA COSTA RICA Y PERÚ**, es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 del 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte; articulo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que éstos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Asimismo, quedo advertido que la Universidad se reserva el derecho de protocolizar este documento ante Notario Público. En fe de lo anterior, firmo en la ciudad de San José, a los 03 días del mes de Abril del año dos mil 2020.

GUSTAVO ADOLFO AGUILAR ESPINOZA

Digitally signed by GUSTAVO ADOLFO AGUILAR ESPINOZA
Date: 2020.04.03 13:19:57 -06'00'

Firma del estudiante

Cédula

CARTA DE AUTORIZACIÓN DE LOS AUTORES

UNIVERSIDAD HISPANOAMERICANA
CENTRO DE INFORMACION TECNOLOGICO (CENIT)
CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DE LOS TRABAJOS FINALES DE GRADUACION

San José, Abril 03 2020

Señores:
Universidad Hispanoamericana
Centro de Información Tecnológico (CENIT)

Estimados Señores:

El suscrito (a) Gustavo Aguilar Espinoza con número de identificación 205620973 autor (a) del trabajo de graduación titulado **ANALISIS, DISEÑO E IMPLEMENTACIÓN DE UN PROGRAMA DE CAPACITACIÓN Y ADOPCIÓN DE REDES DEFINIDAS POR SOFTWARE (SDN) DEL PORTAFOLIO DE CISCO PARA COSTA RICA Y PERÚ** presentado y aprobado en el año 2020 como requisito para optar por el título de Bachillerato en Ingeniería en Sitstemas; SI autorizo al Centro de Información Tecnológico (CENIT) para que con fines académicos, muestre a la comunidad universitaria la producción intelectual contenida en este documento.

De conformidad con lo establecido en la Ley sobre Derechos de Autor y Derechos Conexos N° 6683, Asamblea Legislativa de la República de Costa Rica.

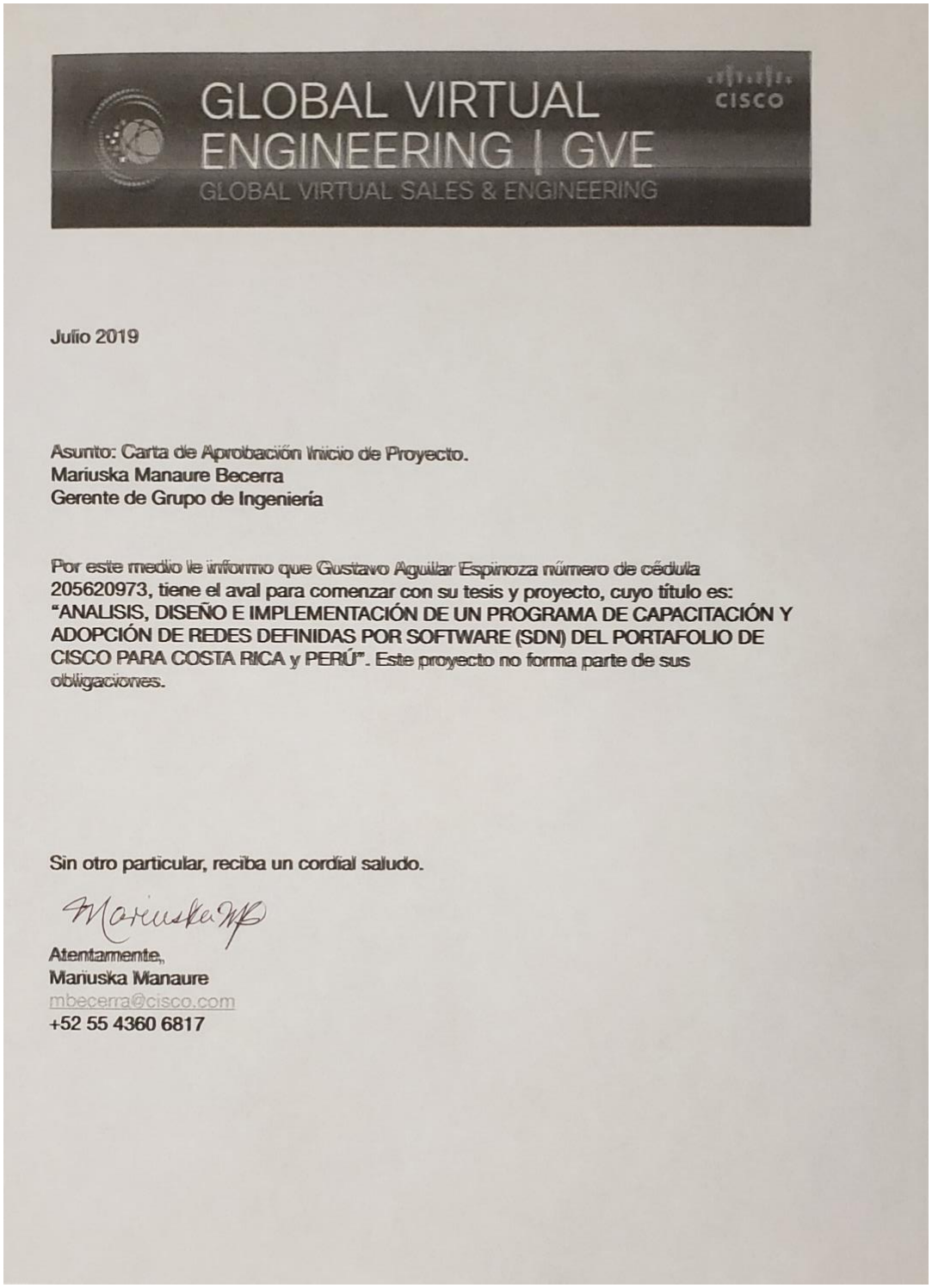
Cordialmente,

GUSTAVO ADOLFO AGUILAR ESPINOZA

Digitally signed by GUSTAVO ADOLFO AGUILAR ESPINOZA
Date: 2020.04.03 14:52:16 -06'00'

_____
Firma y Documento de Identidad

CARTA APROBACIÓN INICIO DEL PROYECTO



GLOBAL VIRTUAL ENGINEERING | GVE
GLOBAL VIRTUAL SALES & ENGINEERING
CISCO

Julio 2019

Asunto: Carta de Aprobación Inicio de Proyecto.
Mariuska Manaure Becerra
Gerente de Grupo de Ingeniería

Por este medio le informo que Gustavo Aguilar Espinoza número de cédula 205620973, tiene el aval para comenzar con su tesis y proyecto, cuyo título es: "ANALISIS, DISEÑO E IMPLEMENTACIÓN DE UN PROGRAMA DE CAPACITACIÓN Y ADOPCIÓN DE REDES DEFINIDAS POR SOFTWARE (SDN) DEL PORTAFOLIO DE CISCO PARA COSTA RICA y PERÚ". Este proyecto no forma parte de sus obligaciones.

Sin otro particular, reciba un cordial saludo.

Atentamente,
Mariuska Manaure
mbecerra@cisco.com
+52 55 4360 6817

CARTA FINALIZACIÓN DEL PROYECTO

Marzo 2020

Asunto: Carta de Conclusión Proyecto.
Mariuska Manaure Becerra
Gerente de Grupo de Ingeniería

Por este medio le informo que Gustavo Aguilar Espinoza cie número de cédula 205620973, ha concluido satisfactoriamente su tesis y proyecto, cuyo título es: "ANALISIS, DISEÑO E IMPLEMENTACIÓN DE UN PROGRAMA DE CAPACITACIÓN Y ADOPCIÓN DE REDES DEFINIDAS POR SOFTWARE (SDN) DEL PORTAFOLIO DE CISCO PARA COSTA RICA y PERÚ".

Sin otro particular, reciba un cordial saludo.

Atentamente,
Mariuska Manaure
mbecerra@cisco.com
+52 55 4360 6817

AGRADECIMIENTO Y DEDICATORIA

Este proyecto lo dedico primeramente a Dios, luego a mi esposa e hijo y después a mis padres. A Dios por que es mi razón de ser y existir; su constante ayuda es lo que me ha permitido llegar hasta acá. A mi esposa e hijo porque son la bendición mas especial que Dios me ha dado después de Él. A mis padres, porque sin su amor, cuidado y apoyo no sería el hombre que hoy soy. Los amo.

ABREVIATURAS

AAA:	Autenticación, autorización y contabilización
AD:	Active Directory
AP:	Access Point
API:	Application Programmable Interface
APNIC:	Registro regional de direcciones de Internet para la región Asia-Pacífico
ARIN:	Registro Regional de Internet para América Anglosajona
ASIC:	Application-specific integrated circuit
AVC:	Application Visibility and Control
BFD:	Bidirectional Forwarding Detection
BGP:	Border Gateway Protocol
BYOD:	Bring Your Own Device
CANSAC:	Centroamérica, Andino y Caribe
CAPEX:	Inversión de capital
CAPWAP:	Control and Provisioning for Wireless Access Point
CDP:	Cisco Discovery Protocol
CEF:	Cisco Express Forwarding
cEdge:	Cisco Edge
CLI:	Command Line Interface
CMD:	Cisco Meta Data
CPU:	Central Processing Unit
DHCP:	Dynamic Host Configuration Protocol

DNA: Digital Network Architecture

DTLS: Datagram Transport Layer Security

ECMP: Equal-cost multi-path

EID: Endpoint identifier

EVPN: Ethernet VPN

GPTW: Great Place to Work

GPO: Group Policy

GRE: Generic Routing Encapsulation

GUI: Graphical User Interface

HQ: Headquarters

HTDB: Host tracking database

IA: Inteligencia Artificial

IAAS: Infrastructure as a Service

IBM: International Business Machines

IEEE: Institute of Electrical and Electronics Engineers

IGP: Interior Gateway Protocol

IKE: Internet Key Exchange

INCOSE: International Council on Systems Engineering

IOS-XE: Internetworking Operating System Linux Kernel

IoT: Internet of Things

IPSec: Internet Protocol Security

IPv4: Internet Protocol Version 4

IPv6: Internet Protocol Version 6

ISE: Identity Services Engine

ISP: Internet Service Provider

IT: Tecnología de la información

LACNIC: Latin American and Caribbean Internet Addresses Registry

LAN: Local Area Network

LISP: Locator ID Separation Protocol

LTE: Long Term Evolution

MAC: Media Access Control

MACsec: Media Access Control Security

MAN: Metropolitan Area Network

MCO: Argentina, Chile, Colombia, Uruguay, Paraguay

MP-BGP: Multiprotocol Extensions for Border Gateway Protocol

MPLS: Multiprotocol Label Switching

MR: Map Resolver

MS: Map Server

NFV: Network Function Virtualization

NMS: Network Management Software

NSF: Nonstop Forwarding

ONF: Open Network Foundation

OPEX: Operational expenditures

OS: Operating System

OT:	Tecnología Operativa
PAN:	Policy Access Node
PNP:	Plug and Play
PoE:	Power over Ethernet
pxGrid:	Platform Exchange Grid
QoS:	Quality of Service
RA:	Realidad Aumentada
REST:	Representational State Transfer
RFC:	Request For Comments
RIB:	Routing information base
RIPE NCC:	Réseaux IP Européens Network Coordination Centre
RIR:	Registro Regional de Internet
RLOC:	Routing Locator
ROI:	Return of Investment
RP:	Redundancy Port
SaaS:	Software as a Service
SDA:	Software Defined Access
SD-WAN:	Software Defined WAN
SDLC:	Systems Development Life Cycle
SDA:	Software Defined Access
SDN:	Software Defined Networking
SGACL:	Security Group Access Control Lists

SGT:	Security Group Tag
SLA:	Service Level Agreement
SMB:	Small Business
SNMP:	Simple Network Management Protocol
SSH:	Secure Shell
SSID:	Service Set Identifier
SSO:	Stateful Switch Over
SVI:	Switch Virtual Interface
SWIM:	Software Image Management
SXP:	Security Exchange Protocol
TACACS:	Terminal Access Controller Access Control System
TCP:	Transmission Control Protocol
TCP MSS:	Transmission Control Protocol Maximum Segment Size
TLS:	Transport Layer Security
vEdge:	Viptela Edge
VLAN:	Virtual Local Area Network
VM:	Virtual Machine
VN:	Virtual Network
VNI:	Visual Networking Index
VPLS:	Virtual Private LAN Service
VPN:	Virtual Private Network

VRF: Virtual Route Forward

VRRP: Virtual Router Redundancy Protocol

VSS: Virtual Sales Specialists

VXLAN: Virtual Extensible LAN

WAN: Wide Area Network

WDM: Wavelength Division Multiplexing

WLC: Wireless LAN Controller

ZTP: Zero Touch Provisioning

5G: Quinta generación de tecnologías de telefonía móvil

INTRODUCCIÓN

La puesta en práctica de este proyecto conlleva la fusión de dos ámbitos importantes en mi desarrollo profesional: tecnología y negocios. Los conocimientos adquiridos durante la carrera no solo facultaron el desarrollo ingenieril sino también la colocación de ese conocimiento al servicio de la industria.

Mi rol principal en la empresa hoy es como consultor de corporativo. La formación como ingeniero ha brindado el abordaje granular de los sistemas, sus inter relaciones con el fin de hacer que dichas corporaciones se vean beneficiadas de la tecnología en que invierten. Tener una postura orientada a la mejora de procesos por medio de la arista tecnológica ha sido clave en mi desarrollo.

Este proyecto es una expresión de mi desarrollo profesional aportando en este caso, no a una organización externa sino a la misma para la que laboro, todo el beneficio de este trabajo minucioso y dedicado.

La finalización de lo planteado comprende la adopción de las tecnologías de Redes Definidas por Software (SDN) del portafolio de Cisco en los países de Costa Rica y Perú, con miras a otras regiones de Latinoamérica.

CAPÍTULO I: PROBLEMA DEL PROYECTO

1. ANTECEDENTES Y JUSTIFICACION DEL PROYECTO

1.1. Antecedentes del Contexto de la Empresa

Cisco es una empresa global con sede en San José, California, Estados Unidos, principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

1.1.1. Misión

La misión de Cisco es "Perfilar el futuro de Internet al crear valor y oportunidad sin precedentes para nuestros clientes, empleados, inversores y socios del ecosistema.”

1.1.2. Visión

Respecto a la visión "Cambiar la forma en que trabajamos, vivimos, jugamos y aprendemos".

1.1.3. Fundadores

La empresa fue fundada en 1984 por el matrimonio de Leonard Bosack y Sandra Lerner, quienes formaban parte del personal de computación de la Universidad de Stanford.

Al igual que San Francisco, de la cual Cisco capta su nombre, proporciona una puerta de entrada a *Pacific Rim*, Cisco proporciona la tecnología de red que es la puerta de entrada a la comunicación basada en computadora. Cisco es la empresa líder del

mercado mundial en enrutamiento, conmutación, comunicaciones unificadas, comunicación inalámbrica y seguridad.

En 1984, los fundadores Len Bosack y Sandy Lerner estaban experimentando en la Universidad de Stanford para conectar redes aisladas en dos edificios separados en el campus. Después de conectar los cables de red entre los dos edificios y conectarlos con puentes y luego con enrutadores, los dos se dieron cuenta de que para hacer que las redes dispares hablaran entre sí y compartieran información, se necesitaba una tecnología que pudiera manejar los diferentes protocolos de área local. Entonces Bosack y Lerner inventaron el enrutador multiprotocolo, que lanzaron en 1986. Para 1989, con sólo tres productos y 111 empleados, los ingresos de Cisco eran de $27 millones. (Silicon Valley Historical Association, 2008)

En los años 90 y el inicio del uso generalizado de Internet, Cisco obtuvo su primera patente para su método y equipo para enrutar la comunicación entre redes de computadoras. Treinta y tres patentes y muchos productos de vanguardia más adelante, y con oficinas en todo el mundo, en 1997 la compañía presentó sus primeros productos de voz sobre *IP* y fax sobre *IP*, así como una línea de productos de datos por cable. El año siguiente, Cisco presentó su primer cable modem para la oficina pequeña, el hogar y el teletrabajo, y el enrutamiento Gigabit Ethernet y Capa 3 en conmutadores.

Hoy, Cisco continúa concentrándose en sus áreas principales de enrutamiento y conmutación, así como en tecnologías avanzadas que incluyen comunicaciones IP, LAN inalámbrica, redes domésticas, seguridad de red, redes de área de almacenamiento y sistemas de video. A medida que las redes evolucionan de una infraestructura a otra, Cisco vuelve a estar en el centro de una nueva forma de

comunicación: con más de 14 mil millones de dispositivos que se espera que estén conectados a Internet para 2010, la compañía está creando un estado de alto rendimiento. La plataforma de comunicaciones que permitirá la convergencia segura de datos, voz, video y comunicación móvil.

A través de estos y muchos otros proyectos, y mediante una amplia investigación y desarrollo, Cisco continúa cumpliendo su promesa de transformar la forma en que las personas se conectan, se comunican, colaboran y crecen.

Figura 1 Cisco edificio corporativo

Fuente: Cisco. (2019). Cisco News Release (2009). Recuperado de https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=2033629

1.1.4. **Cisco en Latinoamérica.**

Cisco soporta muchas operaciones en Latinoamérica. Algunas de estas se encuentran divididas por tipo de mercado. Por ejemplo gobierno, mercados pequeños, comercial-empresarial, proveedores de servicio, educación, etc. Estos a su vez son organizados según el territorio teniendo tres grandes grupos, a saber: MCO, Brasil, Mexico y *CANSAC*.

El territorio de MCO comprende el cono sur de América: Argentina, Chile, Uruguay Venezuela y Colombia. Brasil y México por su tamaño cada uno conforma un territorio por aparte. CANSAC a su vez se encuentra dividido en 3 territorios: Centroamérica (Costa Rica, Honduras, Nicaragua, Panamá y Belice), Caribe (Antillas mayores y

menores) y Andino (Perú, Bolivia y Ecuador). El proyecto es desarrollado en los países de Perú y Costa Rica.

1.1.5. **Cisco en Costa Rica.**

Cisco cumple 20 años de presencia en Costa Rica, trabajando en dos ejes fundamentales: foco en el cliente y desarrollo de capital humano.

Tras el inicio de sus operaciones a nivel local en el año 1997, la compañía se ha posicionado como una de las empresas líderes de tecnología en el mercado costarricense, ofreciendo productos, servicios y soluciones de excelencia para una amplia gama de clientes, desde corporativos hasta gobierno.

“Ahora que cumplimos 20 años en Costa Rica le queremos apostar a iniciar un nuevo ciclo en el país, en el que buscamos cubrir las necesidades críticas a través de nuevas soluciones y servicios en seguridad, colaboración, *cloud*, analítica y data centers para garantizar relevancia con clientes, partners, gobierno y ciudadanos. También queremos seguir contribuyendo con la transformación del país generando nuevas y mejores oportunidades para los jóvenes con nuestros programas de formación. Creemos que la educación en IT y redes es un elemento esencial para mejorar la calidad de vida de la población y cerrar brechas sociales”, destacó Luis Carlotti, Country Manager de Costa Rica. (Revista Summa, 2017)

Cisco Costa Rica obtuvo el lugar #3 overall, #2 IT y # 7 para Centroamérica en la categoría de empresas de 20 a 100 colaboradores en el ranking de *GPTW* 2017;

reconociéndonos por cuarto año consecutivo como uno de los mejores lugares para trabajar.

Hoy más que nunca Cisco está logrando un impacto en el mundo y la sociedad. Además en su fuerza de trabajo, teniendo claro como el liderazgo y la cultura son aspectos que le distinguen.

GPTW no solo es una prioridad del negocio; representa el “People Deal” de la empresa; cómo sigue innovando para continuar posicionándose en el mercado. Siendo pioneros en el futuro del trabajo digital, fortalece su liderazgo, equipos y talento con un propósito común y valores fuertes, en un ambiente de confianza en el equipo y en el futuro. (Cisco, n.d.)

1.1.6. **Crecimiento en la región**

Cisco ha tenido un crecimiento importante desde su llegada a Costa Rica. Las soluciones de enrutamiento y conmutación son las que se posicionaron inicialmente y de manera rápida en el país. A estas se fueron sumando nuevas soluciones de voz IP, telefonía y video para optimizar aún mas las comunicaciones empresariales.

Cisco se ha abierto camino en el mercado local e incursionado en nuevos segmentos que se han sumado a los ejes principales del negocio. Algunos de estos nuevos segmentos son servicios de seguridad, analítica, datacenter y nube.

El portafolio de soluciones de Cisco también ha evolucionado e integrado con otras arquitecturas como *FlexPod* o *VBlock*, u *Openstack* en alianza con IBM. Además, cuenta con soluciones en la nube, con una estrategia llamada *Intercloud*, en donde

lidera una confederación de partners que construyen nubes híbridas para dar mayor flexibilidad, redundancia y accesibilidad a los clientes.

Un amplio listado de soluciones y servicios de seguridad, así como innovaciones en entornos de colaboración complementan su portafolio. “Cada vez sacamos un nuevo portafolio de telepresencias mas sofisticadas, con mejores herramientas, calidad de imagen que permite al final del día comunicarse desde cualquier dispositivo, en cualquier lugar y en cualquier momento”, agregó.

Cisco se proyecta mas allá de las comunicaciones empresariales. La compañía ha apostado por el crecimiento de las ciudades inteligentes ante el inminente aumento de flujo de datos en la red. “Es la oportunidad de conectar las cosas, con las personas, con los datos, con los procesos a través de sensores, y cómo a partir de esta nueva conectividad podremos transformar ciudades para hacerlas más inteligentes, generar mayor sostenibilidad y calidad de vida en los ciudadanos”, finalizó Carlotti. (Cisco, n.d.)

Actualmente las oficinas Cisco Costa Rica se encuentran en el Centro Corporativo Plaza Roble, Edificio Los Balcones A, Primer Nivel, Escazú, Costa Rica.

1.1.7. **Estrutura del grupo de ingeniería Cisco Costa Rica**

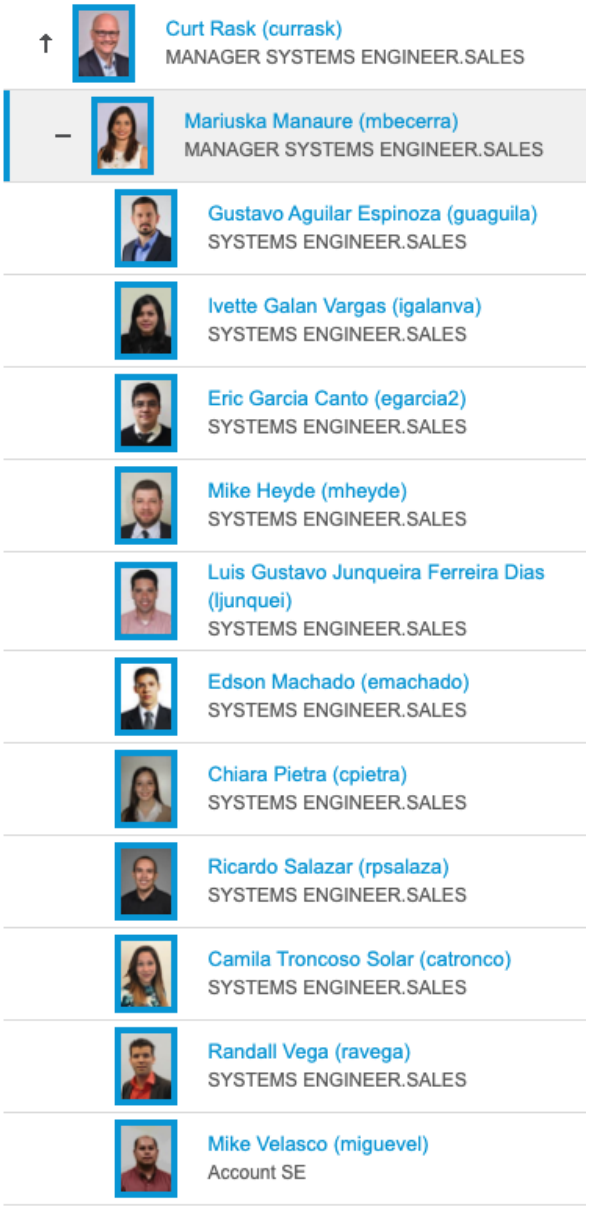


Figura 2 Cisco Ingeniería GVS-SE CANSAC

Fuente: Cisco (2019). Cisco Directory (2019). Recuperado de https://directory.cisco.com/dir/

Nota: Acceso confidencial

1.1.8. **Estrutura del grupo de ventas Cisco CANSAC**

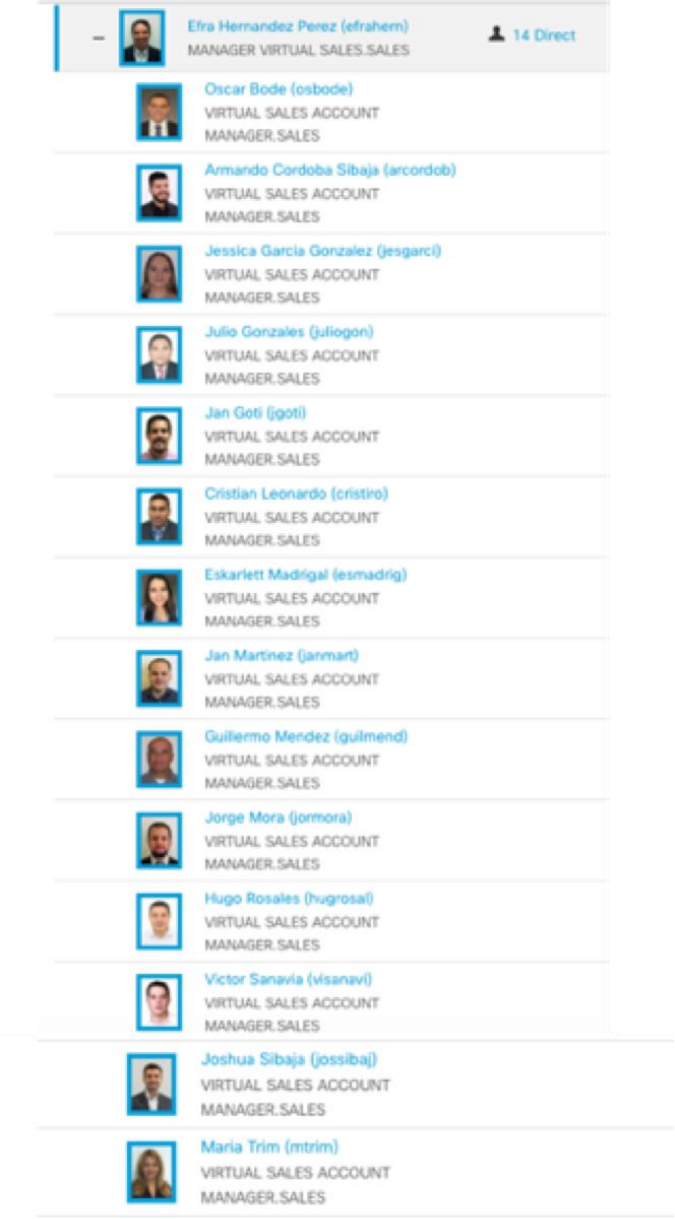


Figura 3 Cisco Ingeniería Estructura Grupo de Ventas CANSAC

Fuente: Cisco (2019). Cisco Directory (2019). Recuperado de https://directory.cisco.com/dir/

Nota: Acceso confidencial

1.1.9. **Organigrama Cisco Costa Rica**

La distribución de un mapa organizacional de Cisco en los diferentes países que opera, no sigue la típica estructura organizacional de un gerente local con una estructura que le reporte a este directamente. Lo anterior debido a que cada grupo funcional tiene directores y líderes de grupo alrededor. Cisco ha sido una de las empresas en las tecnologías de Colaboración pioneras. Siendo la empresa que popularizó el servicio de VoIP y teleconferencias, la operación de Cisco en Costa Rica tiene profesionales en diferentes áreas los cuales reportan a personas en diferentes partes del mundo. No obstante, hay operaciones locales las cuales se pueden identificar no como una jerarquía, mas si como un grupo local de trabajo.

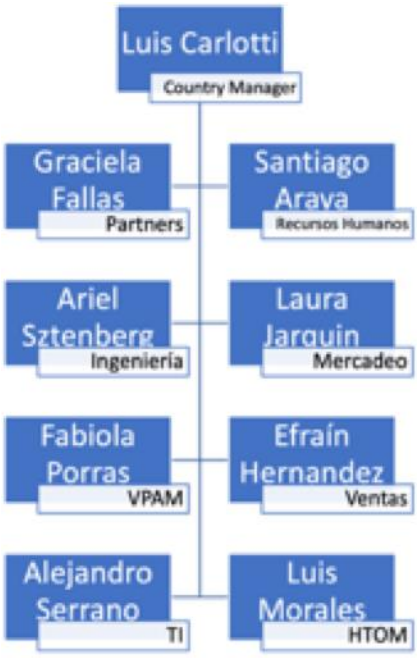


Gráfico 1 Organigrama Cisco Costa Rica

Fuente: Elaboración propia. (2019).

1.1.10. **Cisco: Cambiando la forma en que trabajamos, vivimos, jugamos y aprendemos.**

El impacto de la tecnología cómo un disruptor seguirá siendo una constante en la industria. El efecto de ésta como herramienta y eje de procesos, es vital para la prevalencia de las empresas sin importar su tamaño o enfoque. En la medida que las empresas incorporen la tecnología y sus buenas prácticas, se verán beneficiadas de la misma y así mismo el alcance de sus productos y servicios al mercado local o internacional continuará su curso regular.

El presente trabajo contempla la capacitación de los grupos de preventa técnicos de la en las tecnologías SDN. Las empresas manejan tareas y procesos repetitivos que pueden automatizarse. Desde el control de operaciones, control de inventario y ventas, hasta la generación de reportes. Haciendo uso de tecnologías como SDN muchas actividades se pueden automatizar con el beneficio colateral de ahorro de recursos y tiempo.

Según *Gartner*, una firma consultora y de investigación de las tecnologías de la información con sede en Stamford, Connecticut, Estados Unidos, las organizaciones de TI deben pasar de la automatización oportunista a la automatización sistemática de los procesos de TI. (Gartner, 2016)

Asimismo, el grupo *Forbes* ha emitido varios reportes en los últimos años que muestran cómo la automatización está transformando los entornos laborales y las actividades de primera linea. Según éste último, la automatización y la inteligencia artificial, están transformando el papel de los trabajadores de primera línea. (Forbes, 2018)

Todos los países, industrias y negocios se están involucrando en la era digital para aprovechar las oportunidades posibles que habilitan la conectividad a nivel global. La digitalización impulsa a las empresas a reevaluar sus modelos de negocios, operaciones y estrategias tecnológicas. La investigación de Cisco, junto con otros expertos en negocios en la industria, pronostica que muchos de los negocios líderes hoy en día, serán desplazados por competidores que interrumpen en el mercado con nuevos enfoques: la digitalización es un imperativo para la supervivencia de los negocios.

Según la firma *Gallup*, las dinámicas de trabajo están atravesando un proceso de transformación digital. Los principales cambios en la cultura, la tecnología y los negocios están desafiando las formas tradicionales en que las organizaciones han operado durante casi un siglo. Estos cambios incluyen:

- Compromiso de los empleados: los empleados (y otros integrantes de la fuerza laboral de la organización), el corazón de la organización y la clave de su éxito, no están interesados en sus trabajos. Según una encuesta realizada por Gallup en 142 países, en promedio, entre el 68% y el 87% de los empleados de una organización no están comprometidos o no comprometidos activamente. Los empleados no comprometidos son los que vienen a trabajar para cobrar un cheque de pago simplemente. Los empleados que no participan activamente son aquellos que expresan abiertamente una actitud negativa. Disminuyen la moral al difundir su descontento. Esto tiene un enorme impacto en el balance final, ya que más de un tercio de los salarios simplemente se desperdician.

- Fuerza laboral multigeneracional: la fuerza laboral está envejeciendo y muchas organizaciones están teniendo problemas para reclutar talentos más jóvenes. En la manufactura, por ejemplo, el 35% de los trabajadores se jubilará en cinco años, lo que deja una enorme brecha de conocimiento. Algunas empresas están desarrollando programas creativos para permitir que las personas mayores se jubilen, pero luego permanecen como contratistas remotos. Otros buscan la digitalización para automatizar tantos procesos como puedan. Los factores de compromiso de los empleados varían según la generación. Una empresa típica ahora tiene cuatro generaciones distintas: los conocidos *baby boomers*, la generación X, los millennials y generación Z. Cada una de estas generaciones tiene motivaciones, valores y estilos de trabajo distintos. La gerencia debe, hasta cierto punto, personalizar un enfoque para cada generación para mejorar el compromiso y aumentar la productividad. Para el año 2025, el 75% de la fuerza laboral estará compuesta por milenialls.
- Movilidad y flexibilidad: la proliferación de dispositivos móviles está impulsando dos cambios de comportamiento importantes en la fuerza laboral. Primero, los límites de la jornada laboral tradicional de 9 a 5 se están rompiendo. Si bien aún puede haber horas de trabajo estándar, las organizaciones ahora necesitan que los trabajadores estén disponibles casi en cualquier momento durante el día. Esto se debe en parte al creciente movimiento hacia la globalización que se encuentra en la mayoría de las empresas. En segundo lugar, dados los horarios laborales extendidos, los trabajadores ahora esperan cierta flexibilidad en su jornada laboral. Esto significa la capacidad de tomarse el tiempo para ver el juego escolar de un niño, o de apretar en algún momento para hacer ejercicio durante el día. Esto parece especialmente cierto

para las generaciones más jóvenes que dan prioridad a la flexibilidad en su vida laboral y están evaluando a los empleadores con la capacidad de apoyar esto.7

- Internet de las cosas (*IoT*): hay más de 13 mil millones de dispositivos conectados a Internet hoy en día, y se espera que crezcan a más de 50 mil millones para el año 2020. Potentes tendencias tecnológicas como el aumento de la capacidad de procesamiento, el almacenamiento y el ancho de banda. Combinados con la creciente capacidad de conexión y la reducción de los factores de forma, todos trabajan juntos para garantizar que la organización verá cambios sin precedentes en la próxima década.

El valor de los negocios se ve muy influenciado por el poder de las conexiones y, más específicamente, la capacidad de crear inteligencia a partir de esas conexiones. Las organizaciones ya no pueden confiar únicamente en las competencias básicas internas y en el conocimiento de sus empleados; en cambio, necesitan capturar la inteligencia más rápido y de muchas fuentes externas. Esto ocurrirá a través de conexiones habilitadas por la Digitalización del Trabajo.

Para abordar estos desafíos y oportunidades, las organizaciones deben adoptar un enfoque integral, estructurado y transversal que se centre en coordinar los habilitadores tecnológicos, sociales y empresariales. Las iniciativas exitosas requieren estrategias claras y multifuncionales basadas en imperativos empresariales, no en tecnología. Planes de trabajo estructurados que identifiquen y evalúen sus recursos así como una comprensión de sus necesidades. (Cisco, 2016)

1.2. JUSTIFICACIÓN DEL PROYECTO

Durante los últimos años una serie de factores han coincido para impulsar la industria de la telemática en una dirección totalmente innovadora. Se le conoce cómo Redes Definidas por Software o SDN es la última revolución en redes de computadoras y comunicaciones. Lo anterior no ha sido un salto lógico, sino la combinación de necesidades empresariales y la madurez de varias tecnologías en conjunto que han proporcionado una base estratégica para su evolución.

1.2.1. Factores que impulsan el desarrollo de SDN

Para comprender el impacto tecnológico y comercial que suponen SDN, es necesario mencionar dichos factores. (Stallings, 2015). Según Stallings los siguientes son algunos de los factores detrás de esta evolución:

1.2.1.1. Big data

Las empresas de todo tamaño y perfil dependen cada vez más del procesamiento y análisis de grandes cantidades de información. El análisis eficiente de estos grandes volúmenes suele requerir sistemas de archivos y bases de datos distribuidos, plataformas de computación en la nube, almacenamiento en Internet y otras tecnologías de almacenamiento escalables.

1.2.1.2. Computación en la nube

Hay una tendencia cada vez más clara en muchas organizaciones a trasladar una parte sustancial o incluso todas las operaciones de tecnología de la información a una

infraestructura conectada a Internet conocida como computación en la nube empresarial. Este cambio drástico en el procesamiento de datos de TI se acompaña de un cambio que impacta fundamentalmente los requisitos de la infraestructura de red.

1.2.1.3. **IoT o el Internet de las cosas**

El concepto básico detrás de *IoT* consiste en la interconexión de todos los componentes que se utilizan diariamente a la web suministrando una dirección IP a cada elemento. IoT involucra una gran cantidad de objetos que utilizan arquitecturas de comunicaciones estándar para proporcionar servicios a los usuarios finales. Miles de millones de dichos dispositivos se interconectarán en redes industriales, comerciales y gubernamentales, proporcionando nuevas interacciones entre el mundo físico y la informática, el contenido digital, el análisis, las aplicaciones y los servicios. IoT ofrece oportunidades sin precedentes para usuarios, fabricantes y proveedores de servicios en una amplia variedad de sectores. Las áreas que se beneficiarán de las capacidades de recopilación, análisis y automatización de datos de IoT incluyen salud y estado físico, atención médica, monitoreo y automatización del hogar, ahorro de energía y red inteligente, agricultura, transporte, monitoreo ambiental, inventario y gestión de productos, seguridad, vigilancia, educación, y muchos otros.

1.2.1.4. **Los dispositivos móviles**

Los dispositivos móviles son un componente indispensable de toda infraestructura de TI en las empresas, incluidos los suministrados por el empleador y los que pertenecen al empleado y son traídos al ambiente laboral. Lo que comúnmente se

conoce como el esquema *BYOD*. La gran población de dispositivos móviles genera nuevas demandas únicas en la planificación y gestión de redes.

Alta demanda: las empresas se enfrentan a un creciente número de solicitudes que centran su atención en la necesidad de diseñar, evaluar, gestionar y mantener la infraestructura de red no solo operativa, sino funcional para las metas del negocio.

1.2.1.5. **IPv6**

Otro factor importante que impulsa el desarrollo de SDN pero que Stallings no comenta es IPv6.Las redes actuales en su mayoría corren sobre IPv4 la cual proporciona un máximo de 4,29 billones de direcciones de 32 bits. Cuando IPv4 se convirtió en un estándar en 1980, este número parecía brindar suficientes direcciones. Había alrededor de 4.5 billones de personas en la Tierra en ese momento, por lo que incluso si todas las personas en el planeta necesitaran un IPv4 dirección, todo indicaba que existía suficiente cantidad para cubrir la demanda. Sin embargo, el agotamiento general ocurrió el 31 de enero de 2011. Cuatro de los cinco RIR entes encargados de la distribución mundial de dominios de direcciones agotaron la asignación de todos los bloques que no han reservado para la transición de IPv6; esto ocurrió el 15 de abril del 2011 en Asia (APNIC), el 14 de septiembre de 2012 en Europa, Medio Oriente y Asia Central (RIPE NCC), el 10 de junio de 2014 en América Latina y el Caribe (LACNIC), y el 24 de septiembre de 2015 para América del Norte (ARIN). Los proveedores de servicios individuales (ISP’s) todavía tenían grupos de direcciones IP no asignados y podían reciclar direcciones que sus suscriptores ya no necesitaban. Cada uno agotó su grupo de direcciones disponibles en diferentes momentos. (Graziani, 2017)

Cisco se encuentra en una posición especial para llevar a sus clientes a través de la transformación de las redes a SDN. Este trabajo lo hace por medio de las soluciones tecnológicas que ofrece. Sin embargo, el estado actual de la industria respecto al conocimiento de SDN es inmaduro.

Según Gartner SDN está comenzando a llamar la atención. En un estudio realizado el año pasado, el 55% de los clientes de Gartner estaban pensando en implementar SDN. Sin embargo, la misma investigación encontró que el 23% todavía no está familiarizado con la solución. Con la falta de estándares comunes y la gran variedad de enfoques, implementar SDN puede parecer desalentador a pesar de los beneficios. (Lerner, 2014)

1.3. DEFINICIÓN DEL PROBLEMA

Las tecnologías de SDN se encuentran entre los principales objetivos comerciales de Cisco. El desconocimiento generalizado de SDN, los riesgos percibidos por los clientes asociados con la tecnología entre otros factores, han impedido la adopción a gran escala hasta ahora. Estos impedimentos deben ser abordados por medio de la capacitación y el compromiso de la empresa.

Según lo comentado anteriormente, la experiencia empresarial actual alrededor de las Redes Definidas por Software es muy limitada; por tanto, puede ser difícil comprender por qué y cómo comenzar con la tecnología.

Por otro lado, Gartner recomienda que el momento para que las organizaciones se preparen para SDN es ahora. Sin embargo, la adopción empresarial sigue siendo muy limitada. Gran parte de esta adopción de SDN hasta la fecha ha sido en entornos de gran escala u organizaciones con redes de centros de datos muy grandes, como los

proveedores de servicios. Se estima que a la fecha existen entre 500 y 1,000 implementaciones principales de SDN a nivel mundial. (Lerner, 2014)

El desarrollo de las nuevas tecnologías de SDN plantea la necesidad de que los ingenieros de sistemas, analistas de sistemas, gerentes de TI, y administradores de redes tengan una comprensión firme de sus conceptos y los beneficios que conlleva. Estos profesionales deben evaluar las implicaciones de estas nuevas tecnologías y cómo se diseñan las redes SDN.

Aunque el momento tecnológico en la industria es ideal para la introducción de las tecnologías SDN, la falta de capacitación en la solución, sus componentes y funcionamiento de la misma, los beneficios que aporta, los cambios y retos que plantea y la ausencia de casos de uso en entornos empresariales, crean una barrera que impide a la fuerza de ventas de Cisco realizar un abordaje efectivo de sus clientes. Sin una comprensión profunda de la solución, resulta difícil hacer una evaluación de las necesidades del cliente y las potencialidades de la solución, porque no se comprende realmente el alcance que tiene. Lo anterior repercute en la selección de las tecnologías adecuadas, su posterior diseño y propuesta final, pero sobre todo en la poca penetración del mercado .

El mercado global de Redes Definidas por Software, que incluye infraestructura de red física, controladores y software de virtualización de red, servicios de seguridad de red y servicios profesionales relacionados con SDN, crecerá de $960 millones en 2014 a más de $8 mil millones en 2018, según IDC. (Bent, 2014)

Si bien Cisco brinda documentación como hojas de datos, fichas técnicas, documentos para resolución de problemas entre otros, la documentación se centra más en el producto. La comprensión de las necesidades, la mitigación y educación en cuanto a los riesgos percibidos, las diferentes ofertas y el perfil de la industria con el que se interactúa para llevar el producto al mercado requiere evaluación. Esto provoca una desconexión con el cliente, lo cual impide comunicar el valor que SDN plantea o realizar un diseño congruente y compatible con las necesidades de la empresa en el marco de la digitalización. No se identifican las capacidades que puede lograr con la solución. Por tanto, la empresa se encuentra en una posición compleja y apremiante; requiere una respuesta estratégica que le permita cumplir con sus objetivos comerciales y de expansión de SDN en el mercado, pero tiene un escenario inmaduro en cuanto a la comprensión de la tecnología.

Lo anterior supone la necesidad primaria de un plan de adopción y capacitación de SDN que brinde además del conocimiento de las propuestas puntuales de Cisco en éste ámbito, una visión mas amplia del origen de la tendencia tecnológica, los disparadores, los beneficios, sus matices del lado agnóstico al fabricante, los problemas que solventa para el cliente, su preponderancia de cara a tecnologías emergentes y disruptivas como *5G*, *IA* y *RA*.

1.3.1. Diagrama Ishikawa

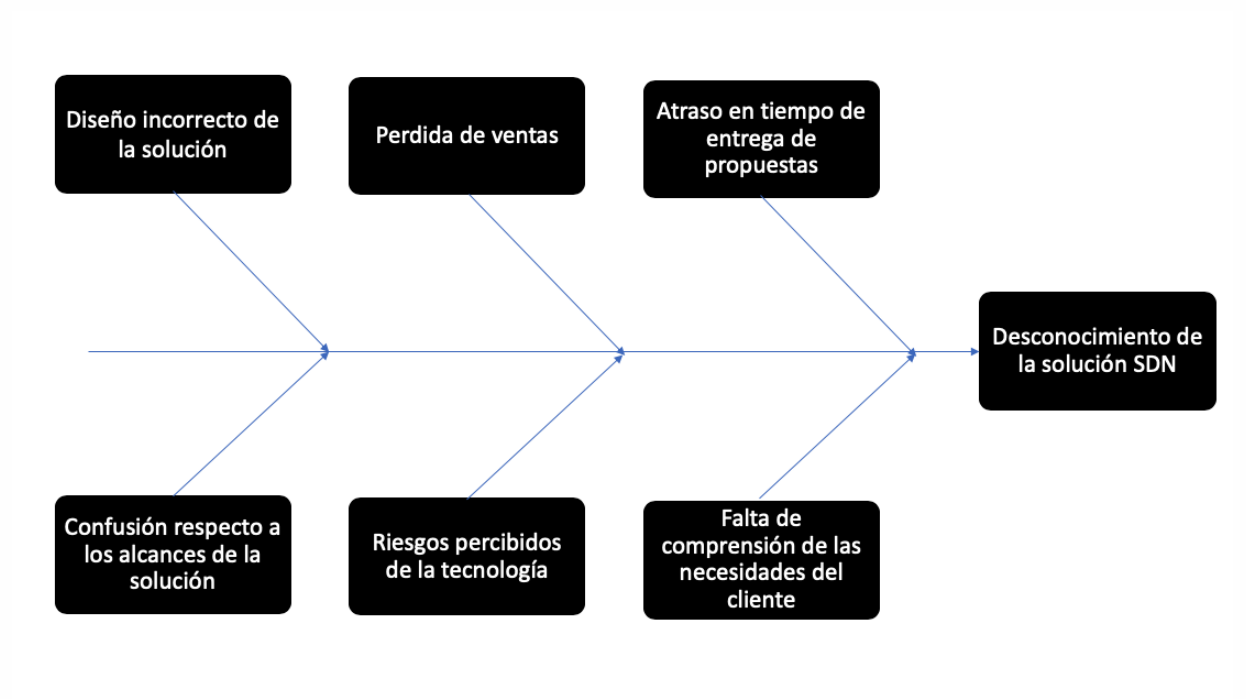


Gráfico 2 Diagrama Ishikawa enumeración de falencias

Fuente: Elaboración propia

1.3.2. **Impacto en el proceso de venta**

Un ciclo de ventas es la serie de fases predecibles necesarias para vender un producto o servicio. Los ciclos de ventas pueden variar mucho entre organizaciones, productos y servicios, y no existen dos ventas idénticas. Identificar los pasos y las etapas principales mejora la eficacia de ventas, ayuda a los vendedores a vender más y acelera el proceso de incorporación de nuevas tecnologías. El ciclo de venta se compone de 5 fases:

La primera fase contempla el descubrimiento de las necesidades del cliente. Aquí mismo de manera indirecta se obtiene visibilidad del potencial del territorio. Esta fase es vital para aterrizar los planes de venta y ejecución, detectar tecnologías en demanda para la zona, comunicar necesidades a nuestras unidades de negocio para la creación de nuevas soluciones o productos, detectar la competencia, comprender por qué y qué está necesitando la industria. Buscar nuevos clientes potenciales es un paso crucial. Una buena forma de comenzar es definir al cliente potencial ideal para el negocio y pensar cómo abordarlo.

La segunda fase del ciclo de ventas es fundamental. Se debe presentar la oferta como una solución a las necesidades del cliente potencial adaptando la propuesta con base en el dimensionamiento. Este proyecto se enfoca en esta fase del ciclo de venta para la optimización de su ejecución. Siendo ésta donde se consigue el cierre técnico por medio de la conciliación de las necesidades del cliente con el portafolio de productos, se presentan diferentes opciones con el objetivo de cubrir cada requerimiento visto.

La tercera fase del ciclo de ventas se evalúan los riesgos probables para la venta. Se debe entender las objeciones más probables, como el precio y el tiempo. Preparar al

equipo de ventas para gestionarlas de la manera correcta, aumentará la cantidad de negocios ganados y acelerará el proceso de ventas. El gráfico 3 muestra las fases del proceso de venta.

Gráfico 3 Etapas ciclo de ventas

Fuente: Elaboración propia

El alcance de las etapas 4 y 5 depende de las fases iniciales, siendo éstas las principales áreas de trabajo para el presente proyecto.

Aunque el foco del proyecto está en las fases 1 a 3 del ciclo, las fases 4 y 5 serán optimizadas en cuanto al abordaje asertivo de la oportunidad. (The 5 Steps Sales Process | A Flowchart For Success | Act!365, n.d.)

1.4. OBJETIVOS DEL PROYECTO

1.4.1. Objetivo general:

Proveer un plan de capacitación de las tecnologías SDN que permita a la fuerza de ventas hacer un análisis del estado de situación actual del cliente y desarrollar un diseño bajo tecnologías SDN acorde a su perfil.

1.4.2. Objetivos específicos:

- Identificar los vacíos de conocimiento y las áreas de capacitación del equipo de preventa técnico relacionadas a las tecnologías SDN.
- Evaluar los retos actuales y principales riesgos percibidos por parte de los clientes que impidan la adopción de las tecnologías SDN.
- Definir el formato sobre la cual se entregará la capacitación
- Proveer la capacitación al equipo de preventa técnica en las tecnologías SDN.

1.5. ALCANCES Y LIMITACIONES

1.5.1. Alcances del Proyecto

- El primer entregable consiste en un resumen de la evaluación de las necesidades de fortalecimiento en el tema de las tecnologías SDN.
- El segundo entregable consta de un análisis de las principales barreras que impiden la adopción de las tecnologías SDN.

- El tercer entregable comprende el desarrollo de una capacitación en las tecnologías SDN que incluye el origen, estándares de industria, arquitectura, componentes, beneficios, evaluación del cliente e integración de las tecnologías. Incluye además la aplicación de un laboratorio de programabilidad donde se demostrará un caso de uso de la tecnología orientado a la automatización de una red tipo SDN.
- El cuarto entregable consiste en la aplicación de la metodología al equipo de trabajo.

1.5.2. **Limitaciones del Proyecto**

- El proyecto será implementado en Costa Rica y Perú.
- A la altura del tercer entregable el proyecto se enfocará en las tecnologías de SDN de Cisco propiamente.
- Para el laboratorio de programabilidad se utilizará un ambientes virtualizado con tecnologías SDN de Cisco.

1.6. **CRONOGRAMA DE ACTIVIDADES**

Tabla 1 Resumen de actividades y tiempos

Fuente: Elaboración propia

#	Nivel 1	Nivel 2	Nivel 3	Tiempo
1	- Identificar las áreas de fortalecimiento en cuanto al conocimiento colectivo de las Redes Definidas por Software (SDN) en el departamento de preventa técnica.	-Fase de evaluación del departamento de preventa técnica.	-Evaluar el conocimiento generalizado del equipo de preventa técnico relacionadas a los estandares de industria de las Redes Definidas por Software (SDN). -Detectar los principales vacios de conocimiento en el tema. -Determinar su comprensión del alcance e impacto de las Redes Definidas por Software (SDN).	1 semana
2	- Detectar las principales barreras en la industria en la adopción de negativas relacionadas a las Redes Definidas por Software (SDN)	-**Analizar** las oportunidades perdidas y ganadas y las principales razones detrás del éxito o rechazo de la oferta	-Revisar la información capturada. -Comparar los resultados de ambas categorías. - Estudio de mercado respecto a las tecnologías de Redes Definidas por Software (SDN) -Consultar la opinión de los foros tecnológicos mas importantes -Categorizar los resultados y establecer un punto de partida	1 semana
3	- Capacitación en las tecnologías de Redes Definidas por Software (SDN)	-**Diseñar** programa de capacitación	-Comunicar objetivos -Presentar los contenidos -Identificar las audiencias -Ajustar el cronograma -Evaluar los resultados	6 semanas
4	- Demostración de casos de uso y aplicación de la capacitación de Redes Definidas por Software	-**Implementar** la capacitación a un grupo de gerencia interno para su evaluación	-Realizar una dinámica grupal para la aplicación de la capacitación -Demostrar casos de uso	2 semanas
5	-Implementar la capacitación en los territorios de Costa Rica y Perú	-Aplicar y evaluar la metodología	-Evaluar los resultados de la capacitación	2 semanas

CAPÍTULO II: MARCO TEÓRICO

2. MARCO TEÓRICO

En este capítulo se establecen los bloques conceptuales que se utilizarán a lo largo del proyecto. Cada bloque guarda estrecha relación con el análisis desde su fase de diseño hasta la ejecución del mismo.

2.1. Ingeniería de Sistemas y Sistemas

La ingeniería de sistemas y la ciencia de sistemas se han convertido en uno de los campos más importantes, completos y fundamentales, y tiene una amplia aplicación en casi todas las áreas de nuestra sociedad; desde la gestión macroeconómica del gobierno hasta la producción diaria de instalaciones de fabricación, el desarrollo de naves espaciales, diseño de productos de consumo, etc. La ingeniería de sistemas se está aplicando en todo momento, a diferentes niveles.

Liu (Liu, 2015) citando la definición de la Junta Americana de Ingeniería y Tecnología es:

> "...la profesión en la que se aplica con juicio el conocimiento de las ciencias matemáticas y naturales obtenidas mediante el estudio, la experiencia y la práctica para desarrollar formas de utilizar, económicamente, los materiales y las fuerzas de la naturaleza en beneficio de la humanidad."

Es la aplicación de lo que descubrimos de la ciencia en sistemas hechos por el hombre. La ingeniería de sistemas, de manera similar, aplica el conocimiento, las teorías, los modelos y los métodos de las ciencias de los sistemas, basados en la filosofía del pensamiento de sistemas, para orientar el diseño de sistemas creados por el hombre.

El Consejo Internacional de Ingeniería de Sistemas define la ingeniería de sistemas de la siguiente manera:

> “La ingeniería de sistemas es un enfoque interdisciplinario y un medio para permitir la realización de sistemas exitosos. Se enfoca en definir las necesidades del cliente y la funcionalidad requerida al inicio del ciclo de desarrollo, documentar los requisitos, luego proceder con la síntesis del diseño y la validación del sistema mientras se considera el problema completo: operación, desempeño, prueba, fabricación, costo y cronograma, capacitación y soporte y disposición. La ingeniería de sistemas integra todas las disciplinas y grupos de especialidad en un esfuerzo de equipo que forma un proceso de desarrollo estructurado que pasa del concepto a la producción y la operación. La ingeniería de sistemas considera el negocio y las necesidades técnicas de todos los clientes con el objetivo de proporcionar un producto de calidad que satisfaga las necesidades del usuario.”

Formalmente, los sistemas tienen los siguientes elementos menciona:

- Subsistemas y componentes: Estas son las construcciones / unidades funcionales fundamentales para los sistemas. Si se desea, los sistemas se pueden descomponer casi infinitamente, hasta el nivel del micromundo, como los electrones y los átomos. Para la mayoría de los propósitos de diseño, no es necesario descomponer un sistema a este nivel de profundidad. Como regla general, la descomposición generalmente se detiene en el nivel de ensamblaje, es decir, en el nivel en el cual los artículos comerciales disponibles pueden obtenerse externamente. El nivel más bajo

de componentes de ensamblaje y los otros niveles del sistema se denominan subsistemas. Los subsistemas se describen a través de un sistema de numeración jerárquica como 2.0, 2.1, 2.1.1; por definición, 2.1 es un subsistema de 2.0, y 2.1.1 es un subsistema de 2.1. Es importante tener en cuenta que el subsistema y los componentes a veces no son elementos de hardware tangibles. Dependiendo de la naturaleza del sistema, algunos componentes también pueden ser software, humanos o incluso información.

Los componentes de los sistemas tienen atributos. Estos atributos, a menudo llamados parámetros dependientes del diseño, definen y especifican los componentes del sistema. Por ejemplo, las dimensiones físicas de un componente, el tiempo medio entre fallos, la entrada y salida de alimentación, etc. El propósito del diseño de sistemas, en cierta medida, es derivar estos atributos cuantitativos y cualitativos de los requisitos del sistema, de modo que se puedan construir u obtener componentes específicos del sistema.

Los componentes y subsistemas de los sistemas interactúan y regulan los comportamientos del sistema a través de diferentes relaciones. Un sistema comienza con los requisitos del usuario / cliente; los requisitos son la base para las funciones de los sistemas; los requisitos de nivel superior pueden ser refinados por requisitos de nivel inferior; Las funciones de nivel superior se descomponen por funciones de nivel inferior. Cada función es realizada por uno o más componentes. Estas relaciones son esenciales para traducir con éxito los requisitos de los sistemas en atributos de componentes, proporcionar una justificación del sistema y proporcionar trazabilidad para las actividades de diseño de sistemas. (Liu, 2015)

2.2. Clasificación de temas

Dependiendo de las perspectivas desde las cuales se estudia un sistema, se puede clasificar en diferentes categorías. Comprender las categorías del sistema puede ayudarnos a limitar el alcance de los sistemas y derivar características comunes del sistema. Al categorizar el sistema, hay que tener en cuenta que ninguna de las clasificaciones es clara, y además, cualquier subsistema puede pertenecer a varias categorías diferentes; por ejemplo, un sistema hecho por el hombre podría ser dinámico y controlado en bucle cerrado. (Liu, 2015)

En términos generales, un sistema se puede clasificar en una o más de las siguientes categorías: sistema natural o artificial, sistema estático o dinámico, sistema conceptual o físico y sistema abierto o cerrado, los clasifica de la siguiente manera:

2.2.1. Sistemas naturales versus sistemas artificiales

Un sistema natural es un sistema auto-organizado que la naturaleza formó después de millones de millones de años de selección y desarrollo. Ejemplos de sistemas naturales son el planeta, los océanos y los lagos naturales. Un sistema natural se sostiene a sí mismo mediante la auto-organización a un estado de equilibrio, por ejemplo, la cadena alimenticia en un lago natural. Cualquier perturbación a este equilibrio puede ser devastadora para el sistema natural. Un sistema hecho por el hombre, por otro lado, está hecho por humanos. Los sistemas hechos por el hombre, como computadoras o automóviles, no se pueden obtener de la naturaleza, sino solo a través de los esfuerzos creativos de los seres humanos. La ingeniería de sistemas estudia los sistemas hechos por el hombre como objetos, con menos preocupación por

los sistemas naturales. Sin embargo, hay que tener en cuenta que no existe un aislamiento absoluto entre los sistemas naturales y los sistemas creados por el hombre. De hecho, los sistemas naturales y los creados por el hombre interactúan constantemente entre sí y, a veces, tienen un gran impacto entre ellos. Los sistemas hechos por el hombre a menudo necesitan insumos de la naturaleza (es decir, el automóvil necesita gasolina, que se obtiene del petróleo crudo del mundo natural) y dependen de la naturaleza para procesar los desechos generados (por ejemplo, los gases de efecto invernadero del automóvil). (Liu, 2015)

2.2.2. **Sistemas estáticos versus sistemas dinámicos**

Los sistemas también pueden ser clasificados como estáticos o dinámicos. Los sistemas estáticos son aquellos sistemas estructurales que no cambian su estado dentro de un ciclo de vida específico del sistema, como un puente, un edificio o una carretera. Un sistema dinámico es aquel en el que su estado, o el estado de sus componentes, cambia con el tiempo, de manera continua o discreta. El estado de un sistema dinámico puede considerarse una función del tiempo, su cambio se produce a una tasa más determinista. De manera similar a los sistemas naturales frente a los creados por el hombre, la distinción entre sistemas estáticos y dinámicos es relativa, no absoluta. (Liu, 2015)

2.2.3. **Sistemas conceptuales versus sistemas físicos**

Nuestro mundo comprende sistemas físicos, y los sistemas físicos consisten en objetos que se pueden ver, tocar y sentir. Los sistemas naturales como los animales,

las bacterias, los lagos y los humanos son todos sistemas físicos; Los sistemas físicos también incluyen sistemas creados por el hombre, como las computadoras, aparatos, herramientas y equipos que los humanos usamos a diario. Los sistemas conceptuales son aquellos que consisten solo en conceptos, no en objetos reales, por lo que no podemos ver o tocar físicamente estos sistemas. Los sistemas conceptuales ilustran las relaciones entre los objetos y nos permiten entender el sistema y comunicar detalles sobre las estructuras y el mecanismo del sistema. Un modelo de simulación de un proceso de operación de fábrica, un plano del ensamblaje de la máquina o el modelo de procesamiento de información de la cognición y la percepción humanas serían ejemplos de sistemas conceptuales. La ciencia y las matemáticas son los fundamentos del modo conceptual. (Liu, 2015)

2.2.4. **El Analista de Sistemas**

El analista de sistemas desempeña un papel clave en los proyectos de desarrollo de sistemas de información. El analista de sistemas asiste y guía al equipo del proyecto para que el equipo desarrolle el sistema correcto de manera efectiva. Los analistas de sistemas deben entender cómo aplicar la tecnología para resolver problemas de negocios. Además, los analistas de sistemas pueden actuar como agentes de cambio que identifican las mejoras organizativas necesarias, diseñar sistemas para implementar esos cambios y capacitar y motivar a otros a usar los sistemas. (Tegarden, Wixom, & Dennis)

2.2.5. **Habilidades del Analista de Sistemas**

Los nuevos sistemas de información introducen cambios en la organización y su gente. Liderar un esfuerzo exitoso de cambio organizacional es uno de los trabajos más difíciles que alguien puede hacer. Comprender qué cambiar, saber cómo cambiarlo y convencer a otros de la necesidad de cambio requiere una amplia gama de habilidades. Algunas de estas habilidades son técnicas, empresariales, analíticas, interpersonales, administrativas como también éticas.

Los analistas deben tener las habilidades técnicas para comprender el entorno técnico existente de la organización, la base tecnológica del nuevo sistema y la forma en que ambos pueden encajar en una solución técnica integrada. Se requieren habilidades comerciales para comprender cómo se puede aplicar la TI a las situaciones empresariales y para garantizar que la TI ofrece un valor comercial real. Los analistas aportan soluciones a los problemas continuos tanto en el proyecto como a nivel organizativo, y ponen a prueba sus habilidades analíticas con regularidad.

A menudo, los analistas necesitan comunicarse de manera efectiva, uno a uno con los usuarios y los gerentes de negocios que a menudo tienen poca experiencia con la tecnología y con los programadores que a menudo tienen más experiencia técnica que el analista. Deben poder dar presentaciones a grupos grandes y pequeños y escribir informes. No solo necesitan tener habilidades interpersonales sólidas, sino que también deben manejar a las personas con las que trabajan, y deben manejar la presión y los riesgos asociados con situaciones poco claras. (Tegarden, Wixom, & Dennis)

Finalmente, los analistas deben tratar de manera justa, honesta y ética con otros miembros del equipo del proyecto, gerentes y usuarios del sistema. Los analistas a

menudo tratan con información confidencial o información que, si se comparte con otros, podría causar daño (por ejemplo, división entre los empleados); es importante que los analistas mantengan la confianza con todas las personas.

2.3. **Redes Definidas por Software**

El concepto de SDN es un enfoque de arquitectura que optimiza y simplifica las operaciones de la red. Lo hace vinculando estrechamente la interacción (aprovisionamiento, reportes y alarmas) entre las aplicaciones, servicios y dispositivos de red, sean físicos o virtualizados. Dado que uno de los enfoques principales es la centralización, el uso de un punto de control de red centralizado lógicamente es común. Se realiza con un controlador SDN, que luego organiza, funcione como capa intermedia y facilita la comunicación entre aplicaciones que desean interactuar con los elementos de red que desean transmitir información. Luego, el controlador expone y abstrae las funciones y operaciones de la red a través de interfaces programáticas modernas, amigables con las aplicaciones y bidireccionales. (Paresh, Syed, & Chayapathi, 2016)

Lo anterior implica que las redes definidas por software, pueden ser programables vienen con un diccionario amplio que permite la interacción con las mismas por medio de lenguajes de programación. Esto es funcional para abordar los desafíos y una variedad de soluciones que se presentan hoy en día. El éxito de las tecnologías de red que precedieron a las redes definidas por software hace posible el avance de esta tecnología. Es un hecho que la mayoría de las redes del mundo (incluida Internet) funcionan sobre la base de IP, BGP, MPLS y Ethernet.

2.3.1. **SDN Origen**

El origen de las Redes Definidas por Software (SDN) se le puede atribuir a una persona: Martin Casado. Anteriormente, Casado era miembro de *VMware*, vicepresidente *senior* y gerente general de la unidad comercial de redes y seguridad de VMware. Ha tenido un profundo impacto en la industria, no solo por sus contribuciones directas (incluidas OpenFlow y *Nicira*), sino al abrir los ojos de los grandes operadores de redes y mostrar que las operaciones de red, la agilidad y la capacidad de administración deben cambiar. Echemos un vistazo a esto con un poco más de detalle.

Ha tenido un profundo impacto en la industria, no solo por sus contribuciones directas (incluidas OpenFlow y Nicira), sino al abrir los ojos de los grandes operadores de redes y mostrar que las operaciones de red, la agilidad y la capacidad de administración deben cambiar. Echemos un vistazo a esto con un poco más de detalle.

OpenFlow sirvió como el primer protocolo importante del movimiento de redes definidas por software (SDN). OpenFlow es el protocolo en el que trabajó Martin Casado mientras obtenía su doctorado en la Universidad de Stanford bajo la supervisión de Nick McKeown. OpenFlow es solo un protocolo que permite el desacoplamiento del plano de control de un dispositivo de red del plano de datos. En términos más simples, el plano de control puede considerarse como el cerebro de un dispositivo de red y el plano de datos puede considerarse como el hardware o los circuitos integrados específicos de la aplicación (ASIC) que realmente realizan el reenvío de paquetes. (Edelman, Oswalt, & Lowe, 2018)

SDN pueden considerarse como una capa de abstracción que rige cómo se comunica el plano de control en la red. SDN no es un conjunto de mecanismos, ya que SDN se puede implementar de varias maneras diferentes. Aunque gran parte de la discusión sobre SDN involucra la interfaz de OpenFlow para los conmutadores de la red física, OpenFlow debe considerarse desde un punto de vista técnico como el componente menos interesante de SDN. A diferencia de los protocolos de enrutamiento de red distribuidos de hoy en día, se puede considerar que SDN simplemente realiza una función. SDN realiza sus funciones en una vista abstracta de la red física la cual subyace bajo esta. Esto permite que SDN ignore la infraestructura física que se ha utilizado para implementar la red y que los ingenieros desde el plano de control de red administren el tráfico de ella sin verse limitados por el diseño físico de la misma. En SDN, el sistema operativo de red es responsable de tomar una función específica y asegurarse de que los resultados de la función se distribuyan a cada conmutador en la red. (Anderson & Morreale, 2014)

Hoy en día varios fabricantes tienen soluciones tipo SDN, Cisco es uno de ellos. En el ámbito de SDN existen diferentes enfoques según el ámbito de red que se pretendan llevar a SDN. Cisco cuenta con dos aplicaciones de esta tecnología una aplicada a la WAN y otra a la LAN. Se les conoce como Cisco *SD-Access* y Cisco *SD-WAN* o lo que es igual Acceso y Redes de banda ancha Definidos por Software, respectivamente.

2.3.2. **SDN Componentes**

En una red tradicional el software que implementa las funciones en los dispositivos tiene varios roles. Estos roles se pueden catalogar como planos funcionales que trabajan independientemente y que interactúan entre si mediante interfaces de Programa de Aplicación (API) patentadas o abiertas. (Paresh, Syed, & Chayapathi, 2016)

Las clasificaciones de alto nivel de estos roles son las siguientes

2.3.2.1. **Plano de Control**

Una de sus funciones es determinar y decidir las rutas que deben tomar los datos a medida que fluyen a través de la infraestructura de red. La decisión de permitir o rechazar el tránsito de datos, el comportamiento en cola de estos datos y cualquier manipulación necesaria de los mismos, etc.

2.3.2.2. **Plano de Datos**

La función de esta parte del software es implementar el reenvío, la puesta en cola y el procesamiento de los datos a través del dispositivo, según las instrucciones proporcionadas por el plano de control. Este rol se conoce como plano de reenvío o plano de datos. Por lo tanto, el plano de control facilita y decide el tratamiento de los datos que ingresan al dispositivo, mientras que el plano de datos realiza las acciones basadas en esas decisiones.

2.3.2.3. **Plano de Gestión**

Mientras que los planos de control y reenvío se ocupan del tráfico de datos, el plano de gestión tiene la responsabilidad de la configuración, el monitoreo de fallas y la gestión de recursos del dispositivo de red.

2.3.2.4. **Plano operativo**

El estado operativo del dispositivo es constantemente monitoreado por el plano operativo, que tiene una vista directa de todas las entidades del dispositivo. El plano de gestión trabaja directamente con el plano operativo y lo utiliza para recuperar información sobre el estado del dispositivo, así como para enviar actualizaciones de configuración para manipular el estado operativo del dispositivo. El gráfico 4 muestra los planos de control y datos en redes tradicionales.

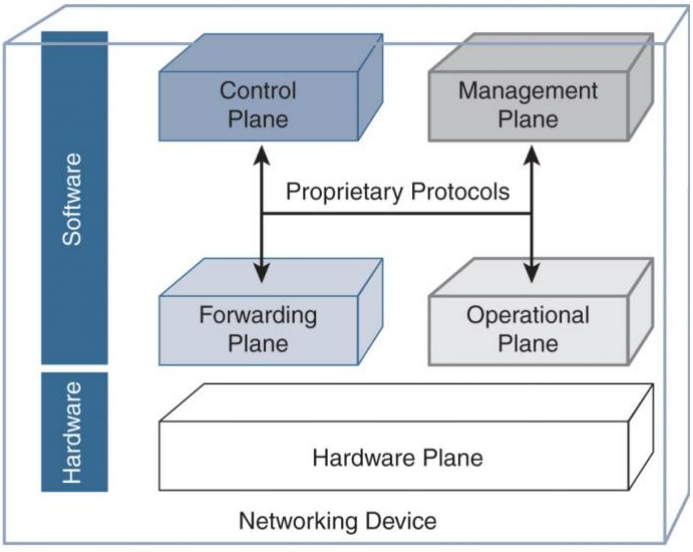


Gráfico 4 Planos de Control y Datos en redes tradicionales

Fuente: Chayapathi, R. (2017). Recuperado 12 noviembre, 2019, de https://learning.oreilly.com/library/view/network-functions-virtualization/9780134464312/graphics/05fig09.jpg

En los dispositivos de red tradicionales, estos planos se acoplan y se comunican mediante interfaces y protocolos propietarios como lo muestra el gráfico 4.

Un ejemplo de esto es la configuración de un *router*. El plano de gestión es el responsable de la configuración del enrutador, proporciona los mecanismos para definir parámetros como el nombre del equipo, la dirección IP de las interfaces que se utilizarán, la configuración de los protocolos de enrutamiento, los umbrales y las clasificaciones que se utilizarán para la calidad del servicio (QoS), etc. El plano operativo monitorea los estados de la interfaz, el consumo de CPU, la utilización de la memoria, etc. y comunica el estado de estos recursos al plano de administración para fines de monitoreo de fallas. El protocolo de enrutamiento, definido a través del plano de gestión, se ejecuta en el router, formando un plano de control y predetermina el flujo de tráfico de datos para llenar las tablas de búsqueda de rutas (denominada base de información de enrutamiento o RIB) que asigna estos datos a la interfaz de salida del router. El plano de datos utiliza esta tabla de búsqueda de rutas y programa la ruta de los datos que transitan por este router.

Dado que el plano de control está incluido en el software del dispositivo, la arquitectura de red resultante tiene un plano de control distribuido, donde cada nodo está realizando sus propios cálculos de plano de control. Estos planos de control pueden intercambiar información entre ellos, por ejemplo, el protocolo de enrutamiento que se ejecuta en cada dispositivo interactúa para determinar la topología general de la red o aprender información de enrutamiento entre sí. Aunque el plano de gestión también está localizado, los sistemas de gestión de red (NMS) han desempeñado un papel centralizado al colocar otra capa encima del plano de gestión agrupado. Los

protocolos como syslog, Simple Network Management Protocol (SNMP) y NetFlow se han utilizado tradicionalmente para realizar operaciones de monitoreo, mientras que la configuración se realiza mediante CLI, API, SNMP o scripts patentados.

2.3.3. **SDN Beneficios**

Cuando se introdujo originalmente el concepto de SDN, sus beneficios no fueron lo suficientemente convincentes como para que los vendedores y fabricantes o proveedores de servicios siguieran seriamente esta dirección. Las implementaciones a escala todavía usaban mecanismos parcialmente automatizados para el aprovisionamiento y la administración y la estrecha integración de los planos de control y datos no se consideraba un gran obstáculo para el crecimiento. Por lo tanto, SDN se consideró inicialmente como un tema académico y no como un cambio tecnológico práctico, al menos no se veían los beneficios. A medida que la industria de las redes se expandió y creció su demanda, la administración habitual de las redes comenzó a percibirse como una restricción o limitación. No tomó mucho tiempo pasar del mundo académico a las implementaciones en el mundo real. La adopción de SDN ha sido impulsada por su potencial para implementar redes flexibles, escalables, abiertas y programables. (Paresh, Syed, & Chayapathi, 2016)

A continuación algunos de los beneficios tecnológicos más importantes de SDN:

- Programabilidad y Automatización. La capacidad de controlar la red a través de aplicaciones es quizás la más importante de las ventajas de SDN. Las redes actuales exigen una mayor agilidad en la restauración de la red, escalabilidad masiva, implementación más rápida y optimización de gastos operativos. Simplemente no

pueden darse el lujo de reducir la velocidad por la falta de velocidad en los procesos impulsados por el hombre. El uso máximo de herramientas y aplicaciones automatizadas se ha convertido en una necesidad para satisfacer las demandas de la red. La capacidad de automatización y programabilidad es necesaria para admitir el aprovisionamiento de redes, el monitoreo e interpretación de los datos del dispositivo e implementar cambios en el tiempo de ejecución basados en cargas de tráfico, interrupciones, eventos conocidos y desconocidos. Los métodos disponibles a través de los proveedores han sido tradicionalmente específicos para sus dispositivos o sistemas operativos y han ofrecido soporte limitado (si lo hay) para permitir que un dispositivo externo tome decisiones basadas en la lógica y las restricciones en la red. SDN ofrece una solución al vincular las aplicaciones a la red y salvar el vacío que existía con los procesos de control y gestión manual. Dado que SDN pone la inteligencia en un dispositivo de control central (es decir, el controlador SDN), los programas y códigos que reaccionan automáticamente a los eventos esperados e inesperados se pueden construir directamente en el controlador. Ademas, las aplicaciones pueden ejecutarse en la parte superior del controlador utilizando las API hacia el norte para transmitir la lógica al controlador y, finalmente, a los dispositivos de reenvío. La aplicación puede manejar fallas y situaciones de demanda creciente, ofreciendo una reparación y restauración rápidas. Este enfoque puede minimizar los costos operativos al permitir reducir significativamente el tiempo de inactividad del servicio, mejorar el tiempo de aprovisionamiento y aumentar la proporción de dispositivos con respecto al personal operativo de la red.

- Soporte para control centralizado. La centralización del plano de control facilita la implementación de la lógica de control, ya que toda la información importante necesaria está fácilmente disponible. Esta visión consolidada de la red es posible gracias a SDN. Simplifica la lógica para controlar la red y reduce la complejidad operativa y el costo.
- Esquema multi fabricante y arquitectura abierta. SDN rompe la dependencia del control específico del proveedor al proponer protocolos estandarizados. Los métodos patentados tradicionales que los proveedores ofrecen para acceder y configurar dispositivos no son fáciles de programar y presentan un obstáculo cuando se desarrollan aplicaciones y scripts para automatizar algunos de los procesos de configuración y administración. Especialmente en un entorno de proveedor mixto (o incluso sistema operativo mixto), las aplicaciones deben tener en cuenta los cambios y las diferencias en las interfaces del dispositivo. Además, si existen diferencias en la forma en que los proveedores han implementado un protocolo estandarizado de plano de control (tal vez debido a la diferencia en la interpretación), podrían surgir problemas de interoperabilidad. (Paresh, Syed, & Chayapathi, 2016). Estos desafíos han existido en las redes clásicas, pero a medida que SDN elimina el control de los dispositivos, dejando solo el plano de datos, resuelve implícitamente los problemas de interoperabilidad del plano de control en una implementación de proveedores mixtos.
- Descargar el dispositivo de red. El plano de control de los dispositivos de red puede ocupar una cantidad significativa de recursos, especialmente cuando los dispositivos ejecutan múltiples protocolos para comunicar varios tipos de información entre ellos

(por ejemplo, rutas internas, rutas externas, etiquetas, etc.) y luego almacenar esta información localmente, así como ejecutar lógica de protocolo adicional para usar los datos para los cálculos de ruta. Esto crea una sobrecarga innecesaria para los dispositivos y limita su escalabilidad y rendimiento. El enfoque de SDN, que elimina toda esta sobrecarga de los dispositivos, les permite concentrarse en lo que están diseñados principalmente para hacer (reenviar datos) mientras liberan el proceso.

2.3.4. **Python**

Se realizó la elección de Python para las interacciones con los equipos en este proyecto por la versatilidad y aceptación en el mercado. Es un lenguaje fácil de aprender, y se puede utilizar como un punto base para luego aprender otros lenguajes de programación. Python es ampliamente utilizado, por grandes empresas como *Google, Pinterest, Instagram, Disney, Yahoo, Nokia, IBM* y otras.

Python fue creado por Guido Van Rossum, un científico informático y matemático holandés que decidió regalarle al mundo un proyecto con el que estaba participando durante la Navidad de 1989. El lenguaje apareció en algún lugar alrededor de 1991, y desde entonces ha evolucionado a ser uno de los principales lenguajes de programación utilizados en todo el mundo hoy. (Ravindran, Hillar, & Romano, 2018)
Python tiene una serie de ventajas que son convenientes mencionar:

2.3.4.1. **Portabilidad**

Python se ejecuta en todas partes, y portar un programa de Linux a Windows o Mac generalmente es solo una cuestión de corregir rutas y configuraciones. Python está diseñado para la portabilidad y se encarga de las peculiaridades específicas del sistema operativo detrás de las interfaces que lo protegen del dolor de tener que escribir código adaptado a una plataforma específica.

2.3.4.2. **Coherencia**

Python es extremadamente lógico y coherente. Se puede ver que fue diseñado por un brillante científico informático. La mayoría de las veces, solo puedes adivinar cómo se llama un método, si no lo sabes. Puede que no se dé cuenta de lo importante que es esto en este momento, especialmente si está al principio, pero esta es una característica importante. Significa menos desorden en su cabeza, así como menos revisión en la documentación y menos necesidad de mapeos en su cerebro cuando codifica.

2.3.4.3. **Productividad del desarrollador**

Un programa de Python suele ser de una quinta parte a un tercio del tamaño de un código *Java* o *C++* equivalente. Esto significa que el trabajo se hace más rápido. Y más rápido es bueno. Más rápido significa una respuesta más rápida en el mercado. Menos código no solo significa menos código para escribir, sino también menos código para leer (y los codificadores profesionales leen mucho más de lo que escriben), menos código para mantener, depurar y refactorizar. (Lutz, 2013)

Otro aspecto importante es que Python se ejecuta sin la necesidad de largos pasos de compilación y vinculación que requieran mucho tiempo, por lo que no tiene que esperar para ver los resultados de su trabajo.

2.3.4.4. **Una extensa biblioteca**

Python tiene una biblioteca estándar increíblemente amplia, se dice que viene con baterías incluidas. Si eso no fuera suficiente, la comunidad de Python en todo el mundo mantiene un cuerpo de bibliotecas de terceros, adaptadas a las necesidades específicas, a las que puede acceder libremente en el Índice de Paquetes de Python (PyPI). (Ravindran, Hillar, & Romano, 2018). Cuando codifica Python y se da cuenta de que necesita una determinada característica, en la mayoría de los casos, hay al menos una biblioteca en la que esa característica ya se ha implementado para usted.

2.3.4.5. **Calidad del software**

Python está muy enfocado en la legibilidad, la coherencia y la calidad. La uniformidad del lenguaje permite una alta legibilidad y esto es crucial en la actualidad, donde la codificación es más un esfuerzo colectivo que un esfuerzo en solitario.
Otro aspecto importante de Python es su adaptabilidad e integración intrínsecos. Puede usarse como un lenguaje de scripting, pero también para explotar estilos de programación funcionales, imperativos y orientados a objetos. Es versátil.

2.3.4.6. **Integración de Software**

Otro aspecto importante es que Python puede extenderse e integrarse con muchos otros idiomas, lo que significa que incluso cuando una compañía usa un idioma diferente como su herramienta principal, Python puede actuar como un agente de cola entre aplicaciones complejas que necesitan hablar. entre sí de alguna manera. Este es un tipo de tema avanzado, pero en el mundo real, esta característica es muy importante. (Ravindran, Hillar, & Romano, 2018)

2.3.5. **Metodología de enseñanza para capacitaciones virtuales**

Dadas las condiciones y características de la audiencia que se necesita alcanzar con la capacitación, se ha optado por un modelo de entrega virtual. Como resultado de lo anterior, surgió la necesidad de enmarcar la misma de acuerdo a las mejores prácticas para la entrega de capacitaciones bajo formatos virtuales. Se exploraron varias metodologías para esta labor:

2.3.5.1. **Dick y Carey**

Este es uno de los modelos de diseño de capacitaciones más conocidos y citados con frecuencia. El modelo de Dick y Carey ha influido en gran medida en el diseño de capacitaciones para instituciones. Describe un proceso de diseño recursivo y reiterativo que incluye 10 etapas de diseño dispuestas linealmente con bucles de retroalimentación en áreas clave que ayudan al diseñador en la mejora continua y la evaluación.

Este modelo tiene varias ventajas, ya que ilustra claramente el proceso de diseño en la capacitación y presenta un flujo claro a seguir. Sin embargo, la crítica más citada al modelo es su naturaleza lineal y la percepción de que las etapas de diseño descritas en el modelo son demasiado rígidas. Además, según el mismo autor y creador del modelo (Dick) sugiere que muchos diseñadores sienten que el modelo está desactualizado en un nivel filosófico, viéndolo como excesivamente conductista y positivista. (Kumaran & Maddison, 2016)

Si bien el modelo de Dick y Carey tiene muchos factores que lo convierten en una valiosa herramienta de diseño hasta el día de hoy, opté por no usar este modelo debido a la falta de flexibilidad percibida.

2.3.5.2. **Kemp**

El modelo de Kemp identifica e intenta ordenar nueve componentes del proceso de diseño de capacitaciones en una disposición cíclica, no lineal. Hace énfasis en la naturaleza sistémica del diseño

Idealmente, se podría ingresar al proceso de desarrollo en cualquier punto del modelo y continuar el flujo. Muchos de los pasos comparten similitudes con los modelos Dick y Carey, lo que representa un tipo de enfoque híbrido qué enfatiza tanto el proceso de desarrollo como el análisis de tareas.

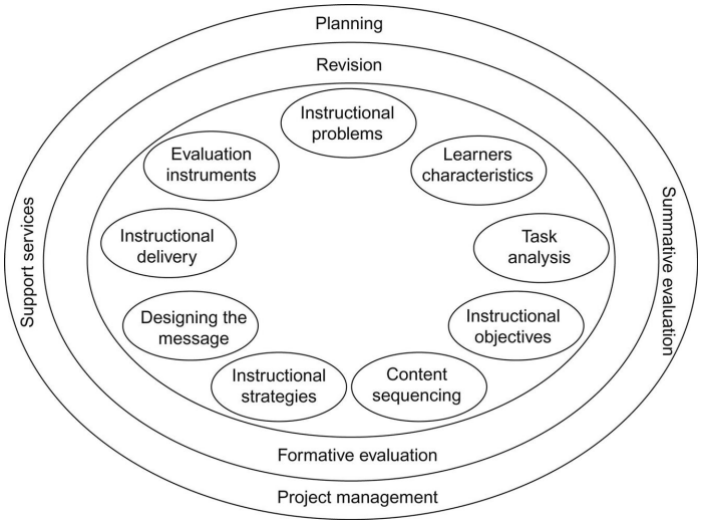


Gráfico 5 Modelo Kemp

Fuente: Maddison, T., & Kumaran, M. (2016) Recuperado 10 septiembre, 2019, de https://learning.oreilly.com/library/view/distributed-learning/9780081006092/images/F000040f04-01-9780081005989.jpg

El gráfico 5 muestra los componentes del modelo Kemp. El modelo Kemp está diseñado específicamente para su uso por múltiples grupos involucrados en el diseño y desarrollo de programas a gran escala y también tenía la intención de representar un ciclo continuo de desarrollo en el que la planificación, la revisión, la evaluación y la gestión son persistentes, concurrentes y continuamente en curso durante toda la vida del proyecto. (Kumaran & Maddison, 2016)

Hay muchos elementos que pueden ser útiles en este modelo, su énfasis en un ciclo sin puntos iniciales o finales claros lo hace innecesariamente complejo para el trabajo que me propongo desarrollar.

2.3.5.3. **ADDIE**

El modelo ADDIE —Análisis, Diseño, Desarrollo, Implementación y Evaluación— fue desarrollado por el Centro de Tecnología Educativa de la Universidad Estatal de Florida a mediados de la década de 1970. Representa un marco más genérico que sirve como guía para el proceso de diseño de capacitaciones. (Kumaran & Maddison, 2016)

El gráfico 6 ilustra las fases del modelo ADDIE. Seleccioné el modelo ADDIE por su simplicidad, flexibilidad y capacidad para organizar los contenidos de la capacitación. La siguiente es una descripción de cada fase del modelo y cómo se aplica al desarrollo de una capacitación en línea.

Gráfico 6 Fases del modelo ADDIE

Fuente: Elaboración propia

2.3.5.3.1. **A - Análisis**

En esta fase del proceso, se deben analizar todos los factores necesarios para desarrollar una capacitación oportuna.

Se deben definir los objetivos de la organización al ofrecer la capacitación. Definir el problema(s) que la organización ha identificado y se resolverá dentro de la capacitación.

Al mismo tiempo se debe determinar qué habilidades o conocimientos tienen los participantes para evitar duplicar esfuerzos o incluir información redundante.

Deben contemplarse los vínculos entre los objetivos de la capacitación y la realidad del entorno de trabajo para garantizar que los estudiantes retengan una cantidad máxima de información.

Se debe evaluar si existen barreras para usar el e-Learning como método de entrega. Por ejemplo, si todos los estudiantes designados no tienen acceso a la tecnología móvil. (Kumaran & Maddison, 2016)

Los resultados de la fase de Análisis del modelo ADDIE fueron capturados en las entrevistas realizadas a los grupos de preventa técnicos (ver anexos). El análisis de situación nos brindó evidencia acerca de la necesidad de proveer un plan de capacitación que contemple adicional a las tecnologías de SDN de Cisco, un marco general acerca de SDN en la industria.

2.3.5.3.2. **D - Diseño**

En esta fase del proceso de diseño, el objetivo es planificar y especificar los objetivos de la capacitación. Cada tema dentro de la misma que se revisará, los medios y recursos que se utilizarán para apoyar la capacitación, el contenido del curso y finalmente, como se evaluarán los estudiantes. Esencialmente, esta es la columna del desarrollo de la capacitación, donde el contenido se distribuye de manera especifica. La fase de diseño es donde se lleva a cabo gran parte del trabajo. Durante esta fase, las metas y objetivos de la capacitación se formulan y redactan, se definen las actividades de aprendizaje y se determina la selección de los medios y basados en los objetivos. Un tema a definir en la fase diseño es la disponibilidad de recursos y cómo debería entregarse la capacitación. Algunas preguntas que ayudan en la definición de esta fase son las siguientes:

- ¿Cómo se entregará la capacitación (presencial, virtual)?
- ¿El equipo tendrá acceso a la capacitación una vez finalizada la misma?
- ¿Cómo accesarán el contenido de la capacitación? ¿solo en premisas o cualquier lugar?
- ¿Cómo determinará el equipo que la audiencia meta ha adquirido los beneficios del aprendizaje deseados?

2.3.5.3.3. **D - Desarrollo**

La fase de desarrollo del modelo ADDIE consiste en establecer los planes de la fase de diseño. Durante esta fase, se trabaja en finalizar las metas y objetivos de aprendizaje, construir los materiales y contenidos de la capacitación.

En sí, esta sección es la parte más larga del modelo ADDIE. En esta se creará, probará y producirá los materiales de la capacitación, la estructura de la misma, etc. A este punto, se debe comprender cuál es el nivel de la audiencia y qué medios serían más efectivos para impulsar el contenido y facilitar el aprendizaje. (Kumaran & Maddison, 2016)

Al adaptar el modelo ADDIE para este proyecto, naturalmente los contenidos de la misma serán estructurados, desarrollados y documentados en el capítulo 5.

2.3.5.3.4. **I - Implementación**

La fase de implementación del modelo ADDIE está destinada a servir como un período de capacitación para los instructores. La intención es que puedan interactuar con los materiales que desarrollaron y el método de entrega, antes de que el material entre en funcionamiento. (Kumaran & Maddison, 2016)

Esta es también la fase en que se asegura que las herramientas, el software y la aplicación de aprendizaje o el sitio web funcionen como se necesita.

2.3.5.3.5. **E- Evaluación**

La última fase del modelo ADDIE es la evaluación. La fase generalmente consiste en evaluaciones formativas y sumativas. Una evaluación formativa se refiere a los materiales de instrucción en sí mismos y qué tan bien están facilitando el proceso de aprendizaje. La evaluación formativa se realiza en gran medida a través de la retroalimentación de los alumnos y los instructores, pero también se puede derivar de los informes de uso de la herramienta o de la observación a gran escala del

rendimiento de los estudiantes. En el último caso, los patrones de falla generalizada en la selección de respuestas correctas en las pruebas pueden indicar problemas con la prueba o con el material de instrucción. La evaluación formativa es a menudo continua y se retroalimenta en el proceso de diseño en un ciclo reiterativo y recursivo de revisión de contenido. (Kumaran & Maddison, 2016)

En el caso de este proyecto se realizaron evaluaciones formativas para determinar la calidad e integración de los contenidos de la capacitación. Con la finalización de la capacitación se realizará un taller en vivo para evaluar el alcance del proyecto.

2.3.5.3.6. **Contenidos, Áreas de Fortalecimiento y Objetivos de Aprendizaje**

Según los resultados capturados a partir de las encuestas a los grupos de preventa técnicos y el estado actual de situación actual de la tecnología SDN comentado en la definición del problema por parte de Gallup y Gartner se definieron los siguientes objetivos de aprendizaje para cada área de fortalecimiento detectada.

Tabla 2 Relación contenidos, áreas de fortalecimiento y objetivos de aprendizaje

Contenidos de la Capacitación	**Áreas de fortalecimiento**	**Objetivos de Aprendizaje**
Software Defined Networking	Ver Encuesta Grupos de Preventa Técnico. Resultados Pregunta 1.0	Al llegar al final de esta sección de la capacitación, los integrantes deberán definir el concepto de SDN.
SDN Origen	Encuesta Grupos de Preventa Técnico. Resultados Pregunta 1.0	Completando esta parte del programa, los integrantes deberán relatar el origen de las tecnologías de SDN desde una perspectiva agnóstica al fabricante.
SDN Componentes	Encuesta Grupos de Preventa Técnico. Resultados Pregunta 2.0	Al finalizar esta área del módulo, los integrantes del grupo deben mencionar los principales componentes de una solución SDN, desde una perspectiva agnóstica al fabricante..
SDN Beneficios	Encuesta Grupos de Preventa Técnico. Resultados Pregunta 5.0	Finalizando esta sección de la capacitación, los integrantes deberán explicar los beneficios técnicos y comerciales de las tecnologías SDN.
Acceso Definido por Software SDA	Encuesta Grupos de Preventa Técnico. Resultados Pregunta 6.0	Terminando esta parte del programa de capacitación, los integrantes deberán describir el concepto de SDN en las tecnologías y la manera en que Cisco lo implementa.
La Evolución de los Requerimientos en las Redes Digitales	Encuesta Grupos de Preventa Técnico. Resultados Pregunta 3.0	Al completar esta sección del programa de capacitación, los integrantes deberán explicar la Evolución de los requerimientos técnicos de las empresas y cómo Cisco los cubre.

Componentes de la Solución SDA	Encuesta Grupos de Preventa Técnico. Resultados Pregunta 2.0	Al finalizar esta área del módulo, los integrantes del grupo deben mencionar los componentes específicos de la tecnología SDA de Cisco
La Arquitectura SDA	Encuesta Grupos de Preventa Técnico. Resultados Pregunta 2.0	Terminando esta parte del programa de capacitación, los integrantes deberán relacionar los componentes de SDA discutidos en la sección anterior y explicar su acomodo dentro de la Arquitectura SDA de Cisco.
Consideraciones de diseño SDA	Encuesta Grupos de Preventa Técnico. Resultados Pregunta 4.0	Al completar esta parte del programa, los integrantes deberán enumerar las principales consideraciones al diseñar una implementación SDA .
Dimensionamiento de sitios SDA	Encuesta Grupos de Preventa Técnico. Resultados Pregunta 1.0	Finalizando esta sección de la capacitación, los integrantes deberán listar los principales aspectos del proceso de dimensionamiento de en las implementaciones de SDA.
Migración a SD-Access	Encuesta Grupos de Preventa Técnico. Resultados Pregunta 6.0	Terminando esta área de la capacitación, los integrantes deberán explicar las consideraciones pertinentes al realizar la migración de una red clásica a una red SDA.
Redes de Banda Ancha Definidas por Software: SD-WAN	Encuesta Grupos de Preventa Técnico. Resultados Pregunta 1.0	Al finalizar esta área del módulo, los integrantes del grupo deben definir el concepto de SD-WAN.
Por qué implementar SD-WAN	Encuesta Grupos de Preventa Técnico. Resultados Pregunta 5.0	Al completar esta sección del programa de capacitación, los integrantes deberán explicar la evolución de los requerimientos de las redes de banda ancha tradicionales y los beneficios de implementar redes tipo SD-WAN.

Arquitectura de la solución SD-WAN	Encuesta Grupos de Preventa Técnico. Resultados Pregunta 2.0	Terminando esta parte del programa de capacitación, los integrantes deberán relacionar los componentes de SD-WAN discutidos en la sección “SDN Componentes” y explicar su ubicación dentro de la Arquitectura SD-WAN de Cisco.
Componentes de la solución Cisco SD-WAN	Encuesta Grupos de Preventa Técnico. Resultados Pregunta 2.0	Al finalizar esta área del módulo, los integrantes del grupo deben mencionar los componentes específicos de la tecnología SD-WAN de Cisco.
Planificación de la implementación	Encuesta Grupos de Preventa Técnico. Resultados Pregunta 7.0	Al completar esta parte del programa, los integrantes deberán enumerar las principales consideraciones al diseñar una implementación SD-WAN de Cisco .

CAPÍTULO III: MARCO METODOLÓGICO

3. MARCO METODOLÓGICO

El marco de trabajo de este capítulo consiste en la presentación del diseño metodológico usado como base para el proyecto. El objetivo de la mayoría de las investigaciones, especialmente los estudios aplicados, es encontrar la respuesta a alguna pregunta o solución a algún problema y traducir esa respuesta en hallazgos o informes que puedan conducir a decisiones prácticas de un tipo u otro.

Los hallazgos de este tipo de estudios pueden presentarse en forma de palabras, números o ambos. Los números, a menudo generados como puntajes en pruebas o calificaciones en encuestas, generalmente se presentan tablas basadas en procedimientos estadísticos descriptivos o inferenciales. Cuando las palabras son el principal medio de información, generalmente es el resultado de analizar lo que se conoce como datos cualitativos (que no debe confundirse con el término investigación cualitativa), que se obtiene de métodos de recopilación tales como cuestionarios de respuestas largas, entrevistas o notas de campo. (Riemer, Quartaroli, & Lapan, 2011)

3.1. Tipo y Enfoque de la Investigación

Este proyecto esta desarrollado sobre un enfoque de investigación aplicada. Se aplicarán los conocimientos obtenidos de las investigaciones para desarrollar un programa de capacitación con miras a la adopción de las tecnologías SDN para los grupos de preventa del territorio de Perú y Costa Rica.

La investigación cualitativa es un enfoque que permite a los investigadores explorar en detalle las características propias de la organización desde el aspecto social hasta comportamientos individuales y su alcance. Para obtener esta información, los

investigadores cualitativos dependen de la recopilación de datos primarios, cara a cara, a través de observaciones y entrevistas en profundidad.

Los investigadores cualitativos también pueden elegir enfoques participativos y de colaboración que involucren a las partes interesadas en las decisiones y actividades de investigación. (Riemer, Quartaroli, & Lapan, 2011)

Por tanto, para este proyecto el enfoque de la investigación a desarrollar será de tipo cualitativo. Dado que el objetivo de fondo será la adopción de las tecnologías SDN de Cisco, la aproximación uno a uno con los diferentes equipos de preventa es medular para detectar los puntos de falencia y obtener retroalimentación de estos.

3.1.1. **Fuentes y Sujetos de la Información**

Este segmento contiene las fuentes de la información teórico y practica utilizados para desarrollar este proyecto.

3.1.1.1. **Fuentes de información primaria**

Las fuentes primarias contempladas para la elaboración de este proyecto consisten en entrevistas y opiniones capturadas de los diferentes participantes en los territorios mencionados. Esta es la data primaria utilizada para elaborar el programa de capacitación y adopción de las tecnologías SDN de Cisco.

3.1.1.2. **Fuentes de información secundaria**

Las fuentes secundarias para la documentación de este proyecto se componen de información pública y privada de Cisco Systems, libros e información en sitios de internet con su debido respaldo.

Tabla 3 Sujetos de Información

	Puesto Laboral o Descripción general	**Profesión u oficio**	**Experiencia**	**Relación con el tema**
	Encargado comercial del territorio	Gerentes de cuenta	Variable 1 a 7 años en el territorio	Encargado(a) de cumplir las metas comerciales de la empresa
	Grupo de ingeniería en preventa	Ingeniero	Mas de 12 años en las tecnologías	Responsable de asesorar técnicamente la venta
	VSS	Especialistas	Variable	Asesor comercial de la solución

3.1.2. **Técnicas y Herramientas**

Una de las características únicas de la investigación cualitativa es la naturaleza cara a cara de la recopilación de datos. Algunos investigadores cualitativos deciden involucrarse en el campo o en el entorno del estudio y participar en él. La participación implica presencia en el lugar, incluida la residencia allí; participación en las actividades de la vida diaria de individuos y familias; y asistencia a eventos especiales, rituales, ritos de paso y otros eventos puntuales o irregulares que ilustran características importantes del contexto del estudio relacionado con el tema de investigación."

En el caso de esta investigación, parte de la captura de la información se ha realizado por observación durante los viajes a los territorios en cuestión, en entrevistas uno a uno, conversaciones a lo interno con los participantes y la interacción directa con los gerentes de cuenta encargados de los territorios. (Riemer, Quartaroli, & Lapan, 2011) Se sabe entonces, que en un verdadero estudio de campo cualitativo, la observación participante (mediante la cual el investigador observa y participa al mismo tiempo) y la entrevista informal junto con la documentación fotográfica pueden ocurrir durante toda la vida del estudio, lo que permite al investigador acumular datos a nivel comunitario. Los datos recopilados a través de estos pasos proporcionan la base para una encuesta derivada cualitativamente, cuyos resultados se pueden explicar con los datos cualitativos y mediante la verificación de los miembros, revisando los resultados con los miembros de la comunidad de estudio.

Para el proyecto se han escogido las técnicas de observación y entrevista no estructurada. Producto de estos resultados se establecerán los contenidos para el programa de capacitación y adopción de las tecnologías SDN de Cisco.

3.1.3. **Variables de Investigación**

Para el proyecto se han escogido las técnicas de observación y entrevista no estructurada.

Tabla 4 Objetivos específicos y variables de investigación

Objetivos Específicos	**Variables asociadas**	**Descripción**
Definir los principales vacíos de conocimiento que impidan la colocación del portafolio de las soluciones de SDN de Cisco	Crear una encuesta con los cuestionarios necesarios para el diagnostico de las principales áreas de capacitación	El alcance de este objetivo consiste en la definición de los contenidos necesarios dentro del programa de capacitación
Crear un programa de capacitación de las tecnologías SDN de Cisco	Diseño, desarrollo del programa de capacitación de tecnologías SDN de Cisco	En esta fase se creara el programa de capacitación con su debida estructura y formato de entrega
Entrega del programa de capacitación	Impartir el programa de capacitación de tecnologías SDN de Cisco	En este punto se imparte el programa de capacitación el cual será dado en formato digital y grabado para su posterior reutilización

3.1.4. **Diseño de la investigación**

En cuanto al diseño de la investigación, nos referimos al marco de trabajo que establece una linea de ejecución nítida. Brinda visibilidad acerca del cómo las partes armonizan con el todo del proyecto, aportando coherencia y consistencia al trabajo. El gráfico 7 muestra las etapas del diseño.

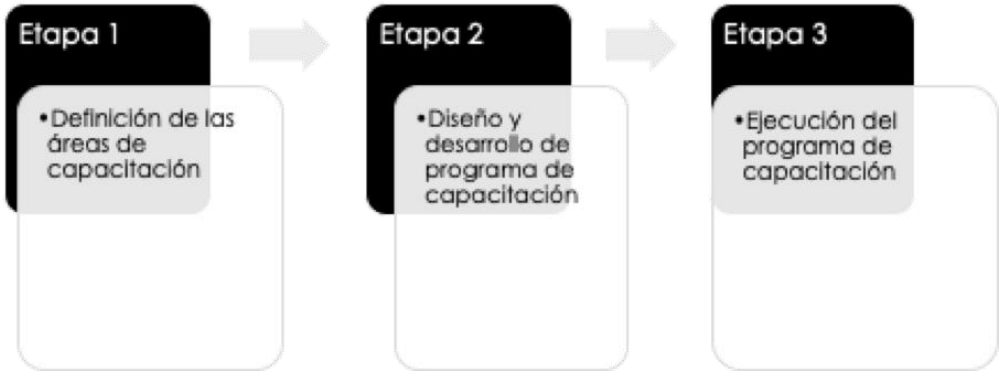


Gráfico 7 Etapas en el diseño de la investigación

Fuente: Elaboración propia

Tabla 5 Etapas del proyecto

Etapa 1	Etapa 2	Etapa 3
Se realiza el diagnóstico de las contenidos para el programa de capacitación	En esta etapa se procede con el diseño y desarrollo del programa de capacitación a partir de los criterios definidos en la etapa 1	Esta fase contempla la ejecución o entrega del programa de capacitación en tecnologías SDN

3.1.5. **Matriz de Coherencia**

La presente matriz permite la ilación de los componentes fundamentales del proyecto. Es decir, concilia los objetivos y entregables con los métodos de investigación, las etapas y temas planteados en el marco teórico del proyecto.

Tabla 6 Esquema matriz de coherencia

Objetivo	**Entregable**	**Etapa**	**Técnicas/ de recolección de datos**	**Instrumentos**	**Temas relacionados para marco teórico**
Definir los principales vacíos de conocimiento que impidan la colocación del portafolio de las soluciones de SDN de Cisco	Encuestas	Etapa 1	Observación y entrevistas no estructuradas	Viajes a la región, reuniones presenciales	Habilidades del Analista de Sistemas Análisis y definición de requisitos.
Crear un programa de capacitación de las tecnologías SDN de Cisco	Diseño y desarrollo de los contenidos del programa de capacitación	Etapa 2	Entrevistas no estructuradas Observación	Desarrollo del programa de capacitación	Análisis y definición de requisitos. SDN Sistemas conceptuales versus sistemas físicos
Entrega del programa de capacitación	Presentación prototipo inicial	Etapa 3	Entrevistas no estructuradas Observación	Material para consumo on-demand virtual o presencial	Modelos de procesos de diseño de ingeniería de sistemas

CAPÍTULO IV: DIAGNOSTICO DE LA SITUACION ACTUAL

4. DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

4.1. Diagnóstico Administrativo

Cisco tiene diferentes operaciones en Latinoamérica las cuales se encuentran segmentadas según el tipo de mercado que atienden. Por ejemplo gobierno, mercado medio, SMB, empresarial, proveedores de servicio, educación, salud, etc. Estos a su vez están organizados según el territorio que cubren, teniendo cuatro grandes grupos para la región de Latinoamérica: MCO, Brasil, Mexico y CANSAC.

El territorio de MCO comprende el cono sur de America: Argentina, Chile, Uruguay Venezuela y Colombia. Brasil y México por su tamaño cada uno conforma un territorio por aparte. CANSAC a su vez se encuentra dividido en 3 subterritorios: Centroamérica (Costa Rica, Honduras, Nicaragua, Panama y Belice), Caribe (Antillas mayores y menores) y Andino (Perú, Bolivia y Ecuador). Este proyecto está enfocado en dos países principales Costa Rica y Perú. La razón del enfoque en estos dos países es que, si bien las tecnologías de SDN precisan mayor penetración en toda Latinoamérica, mi cobertura como ingeniero actualmente está sobre estos dos territorios.

Cisco es una empresa líder a nivel mundial en software. La empresa tiene conocimiento de sus clientes, bases instaladas, soluciones y productos de primera línea además de una impecable ejecución de sus estrategias tecnológicas. Es conocido que el establecimiento de tecnologías de punta siempre es acogido en ciertas latitudes con más rapidez que en otras. Cisco cómo empresa global define estrategias tecnológicas y comerciales que deben ser seguidas por cada uno de los grupos locales. La región de Latinoamérica regularmente entra en el grupo de países que adoptan las

tecnologías emergentes o disruptivas en estados mas avanzados de maduración. Lo anterior se debe a factores como la economía, la cultura, la expectativa de resultados por los *early adopters*, etc. Como lo menciona Gartner en el estudio titulado 'Informe destacado para el análisis la adopción de NFV / SDN en los CSP llamado para los cambios estratégicos en los programas de transformación:

> "…las empresas que están haciendo inversiones en el mundo de SDN son las empresas con hiper-escala, proveedores de servicios y Telcos los que están comenzando a entrar en el abordaje y producción de las soluciones. Dentro de este grupo también se cuentan con los denominados "early adopters" como universidades y organizaciones de tecnología especializada.
>
> Existe aún mucho escepticismo en torno a SDN por parte de las empresas convencionales, particularmente de las personas de redes que tienen una gran influencia en las decisiones y el presupuesto de las mismas. Las inquietudes van en la línea de ¿por qué se necesita dicha tecnología?, ¿qué es lo que realmente puede lograr?
>
> Sin embargo, las organizaciones siguen considerando la capacidad de programación y agilidad que promete que SDN."
>
> (Gartner, 2018)

Al margen de lo anterior, las metas corporativas y el interés de introducir las tecnologías SDN en los mercados Latinoamericanos se mantienen. Si bien se visualizan algunos casos de éxito de implementaciones SDN de Cisco, la mayoría

están en países como Estados Unidos, Japón, Inglaterra y Alemania. Se cuenta con pocas implementaciones en Latinoamérica.

Como una medida que impulse el proceso de evangelización tecnológica de SDN, se plantea introducir este programa de capacitación que resultará en una comprensión cabal de dichas tecnologías, sus beneficios, impacto y habilitadores tecnológicos, logrando con esto la adopción del portafolio SDN de Cisco y cumplir así con los objetivos corporativos de la empresa.

Los históricos de ventas del portafolio de SDN de Cisco para la región muestran crecimiento mas no al paso que se requiere. Si bien el portafolio de SDN de Cisco tiene potencial y un mercado claro e identificado, se necesita equipar los actuales grupos de alcance para que puedan comunicar el valor de SDN y lograr con esto una penetración mayor en el territorio.

Se requieren entonces acciones que permitan aumentar la huella tecnológica en el territorio. El mercado presenta retos que van desde la presencia de canales poco capacitados, competencia de otros fabricantes, reducción de costos, etc. Adicional a esto Latinoamérica ha sido de los países que abraza las tecnologías emergentes en la fase meseta.

A partir de lo anterior se hace evidente y justificable la creación del programa que permite el desarrollo y adopción de la tecnología para optimizar el ingreso en el mercado.

4.2. **Diagnóstico técnico**

La empresa cuenta con la infraestructura necesaria para dar soporte al proyecto y hacerlo sostenible en el tiempo. El contenido quedará disponible para los grupos de manera digital. Dado que la calidad de las videoconferencias suele ser sensible a problemas de conectividad, se utilizará la herramienta en nube (Cisco Webex) que permite además de entrelazar las audiencias pertinentes con acceso ubicuo, funcionar como un repositorio. Este se utilizará para la colocación de los contenidos y su eventual consumo desde la nube.

La arquitectura de Webex permite conectarse al centro de datos más cercano, con la menor latencia posible a ese servidor. La red troncal de Webex conecta todos los centros de datos con rutas redundantes. Se cuenta con ubicaciones de centros de datos conectadas mediante enlaces duales de 100G. El tráfico en esta red está optimizado para los medios y eliminamos tantos puntos de estrangulamiento como sea posible sin dejar de proporcionar una red altamente segura. El contenido quedará almacenado con redundancia en 22 ubicaciones en todo el mundo en los centros de datos de Cisco existentes en los Estados Unidos de América que prestan servicios a América del Norte y al resto del mundo, Londres, Frankfurt y Amsterdam.

El proyecto cuenta con las aprobaciones necesarias para su ejecución.

4.3. **Diagnóstico de la percepción**

La elaboración del diagnostico de percepción, surge del reconocimiento de la capacitación de los grupos de preventa de Cisco. Para validar esta necesidad percibida, se realizaron encuestas no estructuradas con los grupos involucrados en el proceso de venta (ver anexo 1).

A partir de las entrevistas se logró establecer un consenso respecto a la pertinencia y beneficio que aportaría el programa de capacitación a los grupos en cuestión. Requieren una comprensión más profunda del marco tecnológico de SDN, que les permita entender las soluciones, sus beneficios, el dimensionamiento de la implementación y sus componentes para lograr demostrar el valor de las soluciones SDN de Cisco, cumplir con los objetivos de la empresa y orientar la región hacia las mejores prácticas de la industria.

4.4. **Conclusiones del diagnóstico y brechas**

En conformidad con los resultados del análisis de investigación, se concluye lo siguiente:

- La necesidad de comprensión de los estándares, orígenes, trayectoria, componentes y alcance de las soluciones SDN de industria en los grupos de preventa de Cisco para comprender las soluciones propias del portafolio SDN de Cisco y su valor en la industria.
- El conocimiento de la tecnología SDN en un marco agnóstico partiendo de su origen, el estándar, los componentes, la trayectoria y el alcance funcional, es una necesidad fundamental para los grupos de preventa técnicos de Cisco. Esto les permitirá

comprender las soluciones propias del portafolio de SDN de Cisco bajo una perspectiva más integral y el valor que aporta a la industria.

- El cumplimiento de las metas corporativas de la empresa se ve afectado cuando sus grupos no comprenden la ubicación de las soluciones SDN en la industria desde una perspectiva agnóstica al fabricante. Por lo anterior, no logran instrumentalizar estrategias técnicas y comerciales que permitan colocar a la empresa en una posición competitiva respecto a otros fabricantes. No se sienten muy seguros durante las interacciones cara a cara con los clientes.
- La industria en Latinoamérica presenta un marcado desconocimiento de la tecnología de SDN lo cual impacta de manera directa las empresas y las economías que dejan de percibir los beneficios de estas tecnologías de punta que sí están implementado los mercados mas desarrollados.

Según las brechas detectadas entre el estado actual y deseado, se detecta la viabilidad del proyecto como una pieza clave para la adopción de las tecnologías SDN. Dentro del alcance del proyecto se persigue lo siguiente:

- Brindar un programa de capacitación en las tecnologías SDN reutilizable que permita comprender el origen, estándares de industria, arquitectura, modelos de soporte y beneficios de las tecnologías SDN.
- Propiciar la penetración en los mercados Latinoamericanos a través de las tecnologías SDN de Cisco.
- Aumentar el volumen de ventas y oportunidades del portafolio SDN de Cisco.

CAPÍTULO V: PROPUESTA DEL PROYECTO

5. SDN y NFV

En el marco teórico de esta tesis se hizo referencia al concepto de SDN desde una perspectiva general. Para efectos del plan de capacitación que se desarrolla en este capítulo, se hará una explicación detallada del concepto de SDN y NFV cómo antesala a los dos principales métodos que Cisco utiliza para desarrollar estas tecnologías: SDA y SD-WAN.

Como se menciona en el planteamiento del problema, hay una serie de factores que han contribuido al desarrollo de SDN. El volumen cada vez mayor y la variedad del tráfico de red, generado por fuentes de alta demanda como big data, computación en la nube y tráfico móvil, hacen cada vez mas difícil cumplir con los requisitos de desempeño que requieren las organizaciones. Las redes deben proporcionar adaptabilidad y escalabilidad. SDN y NFV responden a esta necesidad brindando la capacidad de ser mas adaptables a las demandas crecientes. (Stallings, 2015)

5.1. SDN Redes definidas por software

Las redes definidas por software proporcionan un nivel de flexibilidad y personalización que satisface las necesidades más recientes de las redes. Las tendencias de TI, como la nube, la movilidad, las redes sociales y videoconferencias.

5.1.1. Funcionalidad SDN

Existen dos elementos que participan en el reenvío de paquetes a través de la infraestructura de red. Clásicamente estos han sido conocidos como plano de control y plano de datos. El primero se encarga de la toma de decisión respecto a la ruta que

han de seguir los paquetes. En el esquema tradicional, los equipos de red realizan estas decisiones de manera independiente. Es decir, cada equipo realiza el proceso para decidir dónde son enviados los paquetes basados en políticas y lo que se configure en el plano de control. Los protocolos de enrutamiento tradicionales como OSPF, BGP, EIGRP se encargan de estas funciones.

La propuesta de las tecnologías SDN apuntan a la centralización de estas funciones. La razón es, que si bien el esquema tradicional de enrutamiento y decisión de envío de tráfico ha sido funcional, es inflexible y requiere que todos los equipos realicen la misma función y corran prácticamente los mismos protocolos. Desde la perspectiva de SDN, se centraliza el proceso de toma de decisión en un equipo que viene a hacer las veces de un cerebro o controlador y el resto de la infraestructura de red, como el sistema nervioso; recibe ordenes del controlador. Con SDN un controlador central realiza todas las funciones complejas, incluido el enrutamiento, los nombres, la declaración de políticas y las comprobaciones de seguridad. A partir de lo anterior el proceso de toma de decisiones se vuelve más eficiente. (Stallings, 2015)

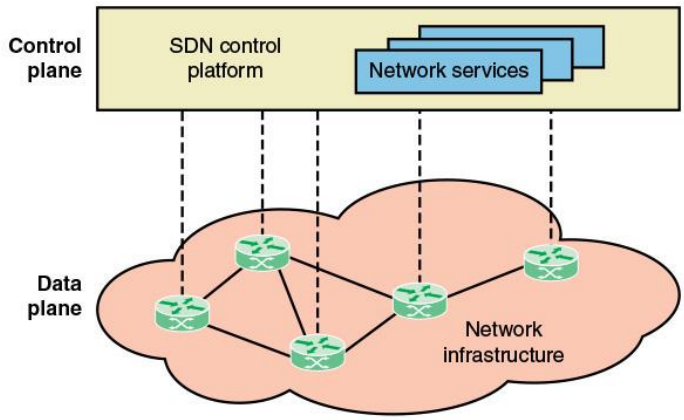


Gráfico 8 Planos en Redes Definidas por Software

Fuente: M William, S. (2015). Recuperado 9 noviembre, 2019, de https://learning.oreilly.com/library/view/foundations-of-modern/9780134175478/graphics/02fig15.jpg

El gráfico 8 muestra la distribución de los planos de control y datos en SDN. El plano de control de SDN puede tener varios controladores. El controlador SDN define los flujos de datos que ocurren en el plano de datos SDN. El controlador configura cada flujo a través de la red y verifica que la política de red permita la comunicación. Si el controlador permite un flujo en particular, calcula la ruta que tomará ese flujo e incluirá una entrada para ese flujo en cada uno de los equipos a lo largo del camino. Con todas las funciones complejas incluidas en el controlador, los conmutadores simplemente administran las tablas de enrutamiento cuyas entradas son administradas por el controlador. (Stallings, 2015)

5.1.2. **Factores clave en el desarrollo de la tecnología**

Un factor determinante para SDN es el uso cada vez más extendido de la virtualización de servidores. La virtualización del servidor enmascara los recursos del equipo, incluido el número e identidad de servidores físicos, procesadores y sistemas operativos individuales, de los usuarios del servidor.

La virtualización permite utilizar una misma maquina como si fueran varios servidores. Lo anterior brinda una utilización mas eficiente de los recursos del hardware. También permite migrar rápidamente un servidor de una máquina a otra para equilibrar la carga o para el cambio dinámico en caso de falla de la máquina. La virtualización de servidores se ha convertido en un elemento central en el manejo de aplicaciones de big data y en la implementación de infraestructuras de computación en la nube. (Stallings, 2015)

Por otra parte se tiene el incremento de dispositivos móviles de los usuarios finales como teléfonos inteligentes, tabletas y computadoras portátiles, para acceder a los

recursos de la empresa. Estos dispositivos pueden generar grandes cantidades de información rápidamente consumiendo los recursos de la empresa que deben ser utilizados para labores especificas. Los administradores de red deben responder a estos requerimientos de manera asertiva, asignando recursos según requerimientos, QoS y seguridad.

Las infraestructuras de red existentes pueden responder a este tipo de requisitos, pero el proceso puede llevar mucho tiempo si la red de la empresa es grande o involucra dispositivos de red de múltiples proveedores. El administrador de red debe configurar el equipo de cada proveedor uno a uno y ajustar los parámetros de rendimiento y seguridad por sesión y por aplicación. En una empresa grande, cada vez que se presenta una nueva VM, puede tomar horas o incluso días para que los administradores de red realicen la configuración necesaria.

5.1.3. **NFV Virtualización de funciones de red**

Mencionamos antes que un factor clave en la implementación de SDN es la necesidad de proporcionar una respuesta de red flexible al uso generalizado de servidores virtualizados. La tecnología de virtualización se ha utilizado para funciones de servidor a nivel de aplicaciones, como servidores de bases de datos, servidores en la nube, web, email, etc. Esta misma tecnología se puede aplicar de la misma manera a dispositivos de red, como enrutadores, conmutadores, firewalls y servidores *IDS / IPS*. (Stallings, 2015)

La virtualización de funciones de la red o NFV separa las funciones de red, como enrutamiento, muro de fuego, detección de intrusos y traducción de direcciones de red

de las plataformas de hardware y las implementa en software. Para lograr esto, utiliza la virtualización estándar la cual se ejecutan en servidores con alto rendimiento para entregar de manera virtualizada las funciones de red. Cualquier procesamiento o función del plano de datos y control de la infraestructura de red cableadas o inalámbricas se puede llevar a NFV.

Cómo se puede apreciar en el gráfico 9, las funciones de red de distintos tipos de equipos de red al lado izquierdo, como residen en un ambiente virtualizado (derecha).

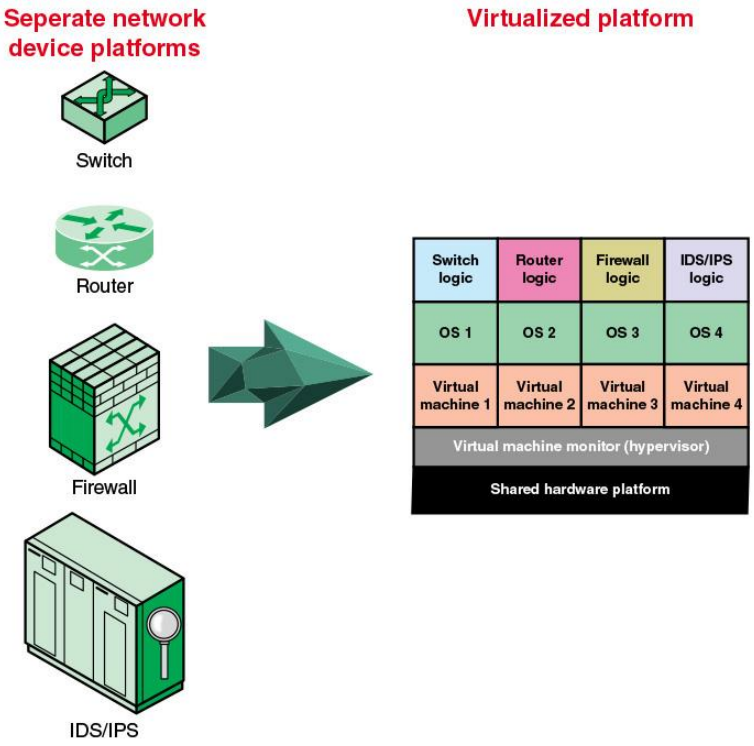


Gráfico 9 Virtualización de Funciones de Red

Fuente: Maddison, T., & Kumaran, M. (2016b). Recuperado 10 septiembre, 2019, de https://learning.oreilly.com/library/view/foundations-of-modern/9780134175478/ch02.html

SDN y NFV tienen objetivos en común. Ambos buscan mover las funcionalidades a software, utilizan API estándar o abiertas para las comunicaciones, permiten la evolución, implementación y reposicionamiento más eficientes de las funciones de red.

SDN y NFV son esquemas independientes pero complementarios. SDN desacopla los datos y los planos de control del control del tráfico de la red, lo que hace que el control y el enrutamiento del tráfico de la red sea más flexible y eficiente. NFV desacopla las funciones de red de plataformas de hardware específicas a través de la virtualización para hacer que la provisión de estas funciones sea más eficiente y flexible. La virtualización se puede aplicar a las funciones del plano de datos de los enrutadores y otras funciones de red, incluidas las funciones del controlador SDN. Por lo tanto, cualquiera se puede usar solo, pero los dos se pueden combinar para obtener mayores beneficios. (Stallings, 2015)

5.2. **Acceso Definido por Software SDA**

El acceso definido por software de Cisco (SD-Access) es la evolución de los diseños tradicionales de LAN de campus a redes que implementan directamente la intención de una organización. SD-Access se ejecuta como parte del software Cisco DNA Center y permite: diseñar, aprovisionar, aplicar políticas y facilitar la creación de una red cableada o inalámbrica en el campus inteligente con seguridad.

El Fabric es una parte integral de SD-Access, permite que la red del campus se superponga con redes virtuales y programables sobre la red física. Logra por tanto que

se alojen una o más redes lógicas según sea necesario para cumplir con los requisitos de diseño. Además de la virtualización de la red, la tecnología mejora el control de las comunicaciones, proporcionando segmentación definida por software y aplicación de políticas basadas en la identidad del usuario y la pertenencia a grupos. La segmentación definida por software se integra utilizando la tecnología Cisco *TrustSec*, proporcionando microsegmentación para grupos escalables dentro de una red virtual usando etiquetas (SGT). A partir del DNA Center se introducen la automatización en la creación de redes virtuales reduciendo los gastos operativos, reduce el riesgo y aporta seguridad integrada. (Cisco, 2019)

5.2.1. **La Evolución de los Requerimientos en las Redes Digitales**

Con la digitalización, las aplicaciones de software han evolucionado de simplemente soportar un proceso comercial, a convertirse en algunos casos en la fuente principal de ingresos. Para algunas empresas son además un punto importante de diferenciación competitiva. Las organizaciones se ven en un desafío constante de escalar la capacidad de su red para reaccionar rápidamente a las demandas y el crecimiento de las aplicaciones. En este contexto, la LAN en la empresa se vuelve un concentrador donde las personas y dispositivos acceden a las aplicaciones. Por tanto, las capacidades de la inalámbricas y cableadas de la LAN deben mejorar para adaptarse a esas necesidades cambiantes. A continuación incluimos algunos de los requisitos claves detrás de la evolución de las redes existentes:

- Implementación y automatización simplificadas: la configuración y administración de dispositivos de red a través de un controlador centralizado que utiliza API abiertas permite una implementación rápida y segura de dispositivos y servicios de red.
- Mayor ancho de banda: se requieren nuevas redes que permitan estándares de *Ethernet* de 10 Gbps, 40 Gbps o 100 Gbps.
- Mayor capacidad de los puntos de acceso inalámbrico: con la última tecnología *802.11ac Wave 2* las demandas de ancho de banda en los puntos de acceso inalámbrico (AP) ahora superan el 1 Gbps. *IEEE* ha ratificado el estándar 802.3bz que define 2.5 Gbps y 5 Gbps Ethernet. La tecnología Cisco *Catalyst Multigigabit* admite esa demanda de ancho de banda sin requerir una actualización del cableado estructurado existente.
- Requisitos de poder adicionales a través de Ethernet: los dispositivos nuevos como la iluminación, cámaras de vigilancia, terminales de escritorio virtuales, conmutadores remotos y AP's pueden requerir una mayor potencia para funcionar. Al diseñar la capa de acceso se debe tener presenta la capacidad suministrar hasta 60W por puerto. Esto se puede lograr utilizando *Cisco Universal Power Over Ethernet*. Adicionalmente contemplar la alimentación perpetua de poder (PoE) durante las actualizaciones o reinicio del conmutador. Los conmutadores de la linea Catalyst 9000 tienen la capacidad de brindar *PoE* de manera perpetua con capacidad de hasta 100W por puerto.

5.2.2. **Servicios Integrados y Seguridad**

Las siguientes capacidades de seguridad deben ser brindadas consistentemente si un usuario se conecta a un puerto Ethernet con cable o a través de la LAN inalámbrica:

- Analítica y ‘Calidad de Experiencia ’en toda la red: debe pronosticar de manera proactiva los riesgos relacionados con la red y la seguridad mediante el uso de telemetría de datos para mejorar el rendimiento de la red, los dispositivos y las aplicaciones, incluso con tráfico cifrado.
- Servicios de identidad: la identificación de usuarios y dispositivos que se conecten a la red brindando la información contextual necesaria para implementar políticas de seguridad en el control de acceso. La segmentación de la red mediante SGT para la asignación a grupos y redes virtuales (VN).
- Políticas basadas en grupos: la creación de políticas de acceso y seguridad de aplicaciones basadas en la información del grupo de usuarios. Por su complejidad y dependencia de los esquemas de IP, las listas de control de acceso (ACL) tradicionales deben ser automatizadas.
- Segmentación definida por software: las etiquetas de grupo asignadas a partir de políticas basadas en grupos se usarán para segmentar la red y lograr el aislamiento del plano de datos dentro de las redes físicas y virtuales.
- Virtualización de red: la capacidad de compartir una infraestructura común al tiempo que admita múltiples redes virtuales con datos aislados y planos de control permitirá que diferentes conjuntos de usuarios y aplicaciones estén aislados de forma segura aunque usen el mismo hardware.

5.2.3. **Componentes de la Solución SDA**

La solución SDA combina el software de Cisco DNA Center, los servicios del motor de identidades (ISE) y las funcionalidades de las redes cableadas e inalámbrica. La solución SD-Access cuenta con una estructura donde los equipos se les asignan roles específicos. El gráfico 10 muestra los roles de los conmutadores. A continuación se especifican:

- Nodo de control
- Edge node o nodo final
- Intermediate node o nodos intermedios (solo transporte)
- Border node o nodo barrera

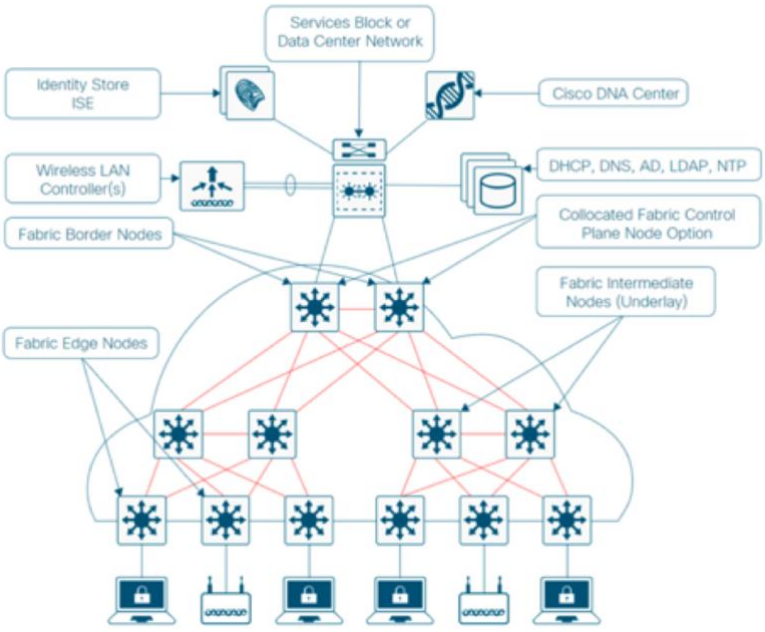


Gráfico 10 Solución SDA y componentes del Fabric

Fuente: Cisco. (2019). Recuperado 10 octubre, 2019, de https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/sda-sdg-2019oct.pdf

En cuanto a la red inalámbrica la integración al fabric general se logra asignando los WLC o controladores y AP’s como fabric WLC y fabric AP.

Luego los sitios de fabric pueden interconectarse utilizando diferentes tipos de redes: IP, SD-WAN y SD-Access para crear una estructura más grande.

En esta sección describo la funcionalidad de cada equipo según rol dentro del fabric. Los roles se asignan a la topología física del campus y los componentes necesarios para la administración de la solución, la integración inalámbrica y la aplicación de políticas. (Cisco, 2019)

5.2.3.1. **Nodo de Plano de Control**

El nodo del plano de control en el fabric de SDA se basa en la funcionalidad del protocolo LISP que usa una estructura MS o mapeo de servidores y MR o resolución de mapa combinadas en el mismo nodo. La base de datos del plano de control rastrea todos los puntos finales en el fabric y los asocia a los nodos de la estructura. Con lo anterior logra desacoplar la dirección IP del punto final o la dirección MAC de la ubicación en la red o el enrulados mas cercano. La funcionalidad del nodo plano de control puede ubicarse en un nodo de borde o puede usar nodos dedicados para la implementaciones mas grandes. Se pueden utilizar entre dos y seis nodos por temas de resistencia solo para implementaciones cableadas. Los nodos de borde y barrera se registran y usan todos los nodos del plano de control existentes, por lo que los nodos elegidos deben tenerlas mismas características para brindar rendimiento constante. (Cisco, 2019)

El nodo del plano de control habilita las siguientes funciones:

- Ubicación del host en la base de datos: la base de datos de seguimiento de host (HTDB) es un repositorio central de enlaces de nodos EID-a-fabric-edge.
- Servidor de mapas: el LISP MS se utiliza para llenar la base de datos de ubicación a partir de mensajes de registro de los dispositivos en el fabric.
- Resolución de mapas: LISP MR se utiliza para responder a las consultas de mapas de dispositivos en el fabric que solicitan información de mapeo de RLOC's para EID's de destino.

5.2.3.2. **Nodo de Plano de Borde**

Los nodos de borde en el fabric de SDA son el equivalente de un conmutador de capa de acceso en un diseño LAN de campus tradicional. Los nodos de borde implementan un diseño de acceso de Capa 3 con la adición de las siguientes funciones de fabric:

- Registro de dispositivos finales: cada nodo de borde tiene una sesión LISP con cada nodo del plano de control. Después de que un dispositivo final es reconocido por el nodo de borde, se agrega a la base de datos de seguimiento de host llamada tabla EID. El nodo de borde también crea un registro de mapa en LISP para informar al nodo del plano de control del dispositivo final y que sea agregado al HTDB.
- Mapeo de usuario a redes virtuales: los dispositivos finales se colocan en redes virtuales VLAN con su respectiva interfaz virtual (SVI) asociados con una instancia de LISP. La asignación de dispositivos finales a las VLAN se puede realizar de forma

estática o dinámica utilizando 802.1X. También se asigna un SGT, y se puede usar esta misma para proporcionar segmentación y aplicación de políticas en el fabric.

- Puerta de enlace capa 3 a *Anycast*: se puede usar una puerta de enlace común con direcciones IP y MAC en cada nodo que comparte una subred EID común que proporciona reenvío y movilidad óptimos entre diferentes RLOC.
- Reenvío de LISP: en lugar de una decisión típica basada en enrutamiento, los nodos de borde del fabric consultan al servidor de mapas para determinar el RLOC asociado con el *EID* de destino y usan esa información como el destino del tráfico. En caso de que no se resuelva el RLOC de destino, el tráfico se envía al fabric de borde predeterminado en el que se utiliza la tabla de enrutamiento global para el reenvío. La respuesta recibida en el servidor de mapas se almacena en el caché de mapas LISP, que se fusiona con la tabla *CEF* (Cisco Express Forwarding) y se instala en el hardware. Si se recibe tráfico en el borde del fabric para un dispositivo final que no está conectado localmente, se envía la solicitud de mapa LISP para activar una nueva solicitud de mapa; esto aborda el caso en el que el dispositivo final puede estar presente en otro equipo de borde en el fabric.
- Encapsulación y desencapsulación de VXLAN: los nodos de borde en el fabric utilizan el RLOC asociado con la dirección IP de destino para encapsular el tráfico con los encabezados de VXLAN. Al regresar ocurre al contrario, el tráfico VXLAN recibido en un RLOC de destino se desencapsula. La encapsulación y la desencapsulación del tráfico permite que la ubicación de un punto final cambie y se encapsule con un nodo de borde diferente y RLOC en la red, sin que el punto final tenga que cambiar su dirección dentro de la encapsulación. (Cisco, 2019)

5.2.3.3. **Nodo Intermedio**

Los nodos intermedios en el fabric son parte de la red de Capa 3 utilizada para las interconexiones entre los nodos de borde hacia los nodos de frontera. En el caso de un diseño de campus de tres niveles con equipos centrales, distribución y acceso, los nodos intermedios son el equivalente de los conmutadores de distribución, aunque el número de nodos intermedios no se limita a una sola capa de dispositivos.

Los nodos intermedios enrutan y transportan el tráfico IP dentro del fabric. No existen requisitos de encapsulación y desencapsulación de *VXLAN*, mensajes de plano de control LISP o de reconocimiento SGT en un nodo intermedio. Este solo tiene el requisito de manejar los requerimientos el máximo tamaño de paquete de IP posible en el fabric con su información VXLAN.

5.2.3.4. **Nodo Frontera**

Los nodos de frontera en el fabric sirven como puerta de enlace entre la estructura SDA y las redes externas al fabric. El nodo de borde en el fabric es responsable del funcionamiento de la virtualización de red y la propagación de SGT desde el fabric al resto de la red. La mayoría de las redes usan un equipo frontera externo para tener un punto de salida común, de la misma manera que una red empresarial hacia internet. El equipo de frontera externo es un mecanismo eficiente que ofrece un punto de salida predeterminado a todas las redes virtuales en el fabric, sin la necesidad de importar ninguna ruta externa. Un nodo de frontera en el fabric tiene la opción de configurarse como un equipo de frontera interno, que funciona como puerta de enlace para direcciones de red específicas, como servicios compartidos o centro de datos, donde

las redes externas se importan en los VN dentro del fabric en puntos de salida explícitos para esas redes. Un nodo de frontera también puede tener una función combinada interno y externo, lo cual es útil en redes con requisitos específicos que no se pueden admitir solo con equipos configurados como equipos frontera externos, donde uno de los equipos frontera externo también es una ubicación donde se deben importar rutas específicas utilizando la funcionalidad de equipo frontera interno. (Cisco, 2019)

Los nodos de frontera realizan las siguientes funciones:

- Anuncio de subredes EID: SDA configura el ‘Protocolo de Puerta de Enlace Fronterizo ’(BGP) como el protocolo de enrutamiento preferido utilizado para anunciar los prefijos EID fuera del fabric, y el tráfico destinado a las subredes EID que vienen desde fuera del fabric pasan a través de los nodos frontera. Estos prefijos EID aparecen solo en las tablas de enrutamiento en el borde; en el resto del fabric, se accede a la información EID utilizando el plano de control del fabric.
- Punto de salida del fabric: el nodo de frontera del fabric externo es la puerta de salida para los nodos de borde dentro del fabric. Esto se implementa utilizando LISP. También son posibles los nodos de frontera internos conectados a redes con un conjunto de subredes IP bien definido, con el requisito de anunciar esas subredes en el fabric.
- Asignación de la instancia de LISP a VRF: el node borde en el fabric puede extender la virtualización de la red desde el interior del fabric al exterior mediante el uso de

instancias de VRF externas con protocolos de enrutamiento compatibles con VRF para preservar la virtualización.

- Mapeo de políticas: el nodo de frontera del fabric también asigna información de SGT desde dentro del fabric para que se mantenga adecuadamente al salir del mismo. La información SGT se propaga desde el nodo de frontera en el fabric a la red externa al fabric, ya sea mediante el transporte de las etiquetas a dispositivos compatibles con Cisco TrustSec mediante el Protocolo de intercambio SGT (SXP) o mediante la asignación directa de SGT en el campo de metadatos del paquete, utilizando capacidades de etiquetado en línea implementadas para conexiones al nodo de frontera.

5.2.3.5. **Nodo Extendido**

Se pueden extender las capacidades del fabric a los conmutadores industriales del portafolio IoT de Cisco 3000, 4000 y 5000, conectándolas a un nodo de borde del fabric en SDA tipo Catalyst de la serie 9000. Lo anterior permite la segmentación de los usuarios, dispositivos finales y equipos IoT. A través de automatización en el DNA Center, los conmutadores configurados como nodo extendido acceden al en el fabric conectándose al equipo de borde a través de un enlace troncal 802.1Q de un EtherChannel con uno o varios miembros físicos y se descubren utilizando Plug-and-Play y ZTP. Los dispositivos finales, incluidos los AP de fabric, se conectan al conmutador de nodo extendido. Las VLAN y SGT se asignan mediante la incorporación de host como parte del aprovisionamiento en el fabric. La política de etiquetado se aplica en el borde del fabric. Los beneficios de extender las capacidades de del fabric

mediante nodos extendidos son: la simplicidad operativa de IoT mediante la automatización basada en el DNA Center, la consistencia de políticas en TI y OT y una mayor visibilidad de la red de los dispositivos IoT. (Cisco, 2019)

5.2.4. **Controlador Inalámbrico en el Fabric**

El controlador en el fabric se integra con el fabric del plano de control. Tanto los controladores en el fabric como los controladores que no, proporcionan gestión de imágenes y configuración de AP's, gestión de sesión de cliente y servicios de movilidad. Los controladores en el fabric proporcionan servicios adicionales para la integración en el fabric al registrar las direcciones MAC de los clientes inalámbricos en la base de datos de seguimiento del host del plano de control de fabric durante los eventos de unión de clientes inalámbricos, y al proporcionar actualizaciones de ubicación de los RLOC de borde en el fabric durante los eventos de roaming del cliente. Una diferencia clave en el comportamiento de los controladores que no están en el fabric es que los WLC fabric no son participantes activos en la función de reenvío de tráfico del plano de datos para los SSID que están habilitados para fabric: los AP de modo de fabric reenvían el tráfico directamente a los bordes del fabric para esos SSID. (Cisco, 2019)

5.2.4.1. **Puntos de Acceso en Modo Fabric**

Los AP en modo fabric son equipos Cisco preparados para *WiFi6 (802.11ax)* y 802.11ac Wave 2 y Wave 1 AP asociados con el fabric WLC que se han configurado con uno o más *SSID* habilitados para fabric. Los AP en modo fabric continúan

soportando los mismos servicios de inalámbrica que los AP tradicionales; aplican AVC, calidad de servicio (QoS) y otras políticas inalámbricas; establecen el plano de control *CAPWAP* para el fabric WLC. Los AP de Fabric se unen como AP de modo local y deben conectarse directamente al conmutador de nodo de borde del Fabric para habilitar los eventos de registro de Fabric, incluida la asignación de RLOC a través del WLC de Fabric. Los nodos de borde en el fabric utilizan CDP para reconocer los AP como hosts especiales cableados, aplicando configuraciones de puertos especiales y asignan los AP a una red de superposición (overlay) única dentro de un espacio EID común a través del fabric. Esta asignación permite la simplificación de la administración mediante el uso de una subred única que engrana la infraestructura de los AP's en el sitio del fabric. (Cisco, 2019)

5.2.5. **ISE o Motor de Servicios de Identidad**

El Cisco ISE es una plataforma que permite el control absoluto de los accesos y consistencia para los usuarios y dispositivos que acceden a la red en la organización. El ISE es un componente integral de SDA necesario para la implementación de políticas, lo que permite el mapeo dinámico de usuarios y dispositivos a grupos escalables y simplifica la aplicación de políticas de seguridad de extremo a extremo. Dentro de ISE, los usuarios y dispositivos se muestran en una interfaz simple y flexible. El ISE se integra con el *DNA Center* mediante el uso de *pxGrid*, *API* y *REST* para el intercambio de información de clientes y la automatización de configuraciones relacionadas el fabric en ISE. La solución SDA se integra con *TrustSec* para admitir políticas basadas en grupos en toda la red, incluida la información de SGT en los

encabezados de *VXLAN* para el tráfico del plano de datos. Además soporta múltiples VN que utilizan asignaciones únicas de VNI. Los grupos, las políticas, los servicios de AAA (autenticación, autorización y trazabilidad) y la creación de perfiles de dispositivos finales están controlados por el ISE y se engranan a los flujos de trabajo creados a través de las políticas del DNA Center.

5.2.6. **Cisco DNA Center**

Como toda solución SDN, el cerebro orquestador de la automatización en SDA de Cisco es el DNA Center. SDA contiene un paquete de aplicaciones que se ejecutan como parte del software del DNA Center y permiten: diseñar, aprovisionar, aplicar políticas y facilitan la creación de una red cableada y/o inalámbrica en un marco seguro.

Desde el DNA Center se gestionan los flujos de trabajo, configuraciones y operaciones. A continuación incluyo sus funciones principales:

- Diseño: configura las características globales, perfiles del sitio, inventario de dispositivos físicos, DNS, DHCP, direccionamiento IP, administración y repositorio de imágenes de software, plantillas de dispositivos y acceso de usuarios.
- Políticas: los aspectos críticos del negocio se definen internamente, incluida la creación de redes virtuales, la asignación de puntos finales a redes virtuales, las definiciones de contratos de políticas para grupos y la configuración de políticas de aplicaciones.
- Aprovisionamiento: aprovisiona dispositivos y los agrega al inventario para administración, Cisco *Plug and Play*, crea dominios en el *fabric*, nodos de plano de

control, nodos de borde, nodos de frontera, fabric para inalámbrica, los aspectos de la red inalámbrica, tránsito y conectividad externa.

- Calidad de Experiencia: permite el monitoreo proactivo y evaluación para garantizar que la experiencia del usuario cumple con la parámetros definidos utilizando paneles de control de salud de red, cliente y aplicación, gestión de problemas y pruebas basadas en sensores.
- Plataforma: permite el acceso por medio de programación abierta a la red y la integración del sistema con equipos de terceros que utilizan API's, configuraciones, un panel de tiempo de ejecución y un kit de herramientas para programadores.

El DNA Center permite la integración mediante API's. Por ejemplo, la administración de direcciones IP a través de Infoblox y Bluecat y la integración de cumplimiento de políticas con el ISE están disponibles a través del DNA Center. Un conjunto completo de API's REST en sentido 'Norte 'permite la automatización, integración e innovación. (Cisco, 2019)

- Toda la funcionalidad del DNA Center está accesible a través de las API REST en sentido norte.
- Las organizaciones y socios de negocio pueden crear fácilmente nuevas aplicaciones.
- Todas las solicitudes de API REST en sentido norte se rigen por el mecanismo RBAC del DNA Center.

El DNA Center es clave para permitir la automatización de las implementaciones de dispositivos en la red, proporcionando la velocidad y la coherencia necesarias para la eficiencia operativa. Las organizaciones que utilizan el Cisco DNA Center obtienen beneficios como un menor costo y riesgos al implementar y gestionar sus redes. (Hucaby, Garza, & Edgeworth, 2019)

5.2.7. **Servicios Compartidos**

El diseño para la virtualización de una red de extremo a extremo requiere una planificación detallada para garantizar el funcionamiento de las redes virtuales. En la mayoría de los casos, es necesario tener algún tipo de servicios compartidos que puedan reutilizarse en múltiples redes virtuales. Es importante que esos servicios compartidos se implementen correctamente para preservar el aislamiento entre diferentes redes virtuales que comparten esos servicios. El uso de un enrutador de fusión directamente conectado al fabric proporciona un mecanismo para la redistribución de rutas y prefijos de servicios compartidos a través de múltiples redes.

El uso de uno varios firewall proporciona una capa adicional de seguridad y monitoreo del tráfico entre redes virtuales. Algunos ejemplos de servicios compartidos incluyen:

- Infraestructura inalámbrica: el desempeño de la radiofrecuencia y costo operativo se ven beneficiados mediante el uso de redes inalámbricas comunes (SSID únicas) frente a las estrategias ineficientes (aún muy utilizadas) de configurar múltiples SSID’s para separar la comunicación de los dispositivos finales. La segregación del

tráfico se logra mediante la asignación de VLAN dedicadas en el WLC y mediante la asignación dinámica de VLAN’s mediante autenticación de 802.1X para asignar los dispositivos finales inalámbricos en sus VN correspondientes.

- DHCP, DNS y administración de direcciones IP: el mismo conjunto de servicios de infraestructura se puede reutilizar si tienen soporte para redes virtualizadas. Este soporte incluye capacidades especiales tales como criterios avanzados de selección dentro DHCP, alcance al todo el set de opciones de DCHP, dominios múltiples y soporte para direcciones superpuestas para que los servicios se extiendan más allá de una sola red.
- Acceso a Internet: se puede usar el mismo conjunto de firewalls de Internet para múltiples redes virtuales. Si las políticas de firewall deben ser únicas para cada red virtual, se recomienda el uso de un firewall que soporte contextos múltiples.
- Servicios de colaboración de voz y video en IP: cuando los teléfonos IP y otros dispositivos de comunicaciones unificadas están conectados en múltiples redes virtuales, la señalización de control de llamadas al equipo administrador de comunicaciones y el tráfico IP entre esos dispositivos debe poder atravesar múltiples VN en la infraestructura. (Cisco, 2019)

5.2.8. **La Arquitectura SDA**

La arquitectura SD-Access es compatible con la tecnología fabric implementada para el campus, lo que permite el uso de redes virtuales (redes superpuestas o superposición de fabric) que se ejecutan en una red física creando topologías alternativas para conectar dispositivos. Las redes superpuestas en las estructuras de

centros de datos u overlay se usan comúnmente para proporcionar redes lógicas de Capa 2 y 3 con movilidad de máquinas virtuales (ejemplos: *VXLAN, EVPN* y *FabricPath*). Las redes de superposición u *overlay* también se utilizan en redes de área amplia para proporcionar túneles seguros desde sitios remotos (ejemplos: *MPLS, DMVPN y GRE*). En esta sección proporcionaremos información sobre los elementos de la arquitectura SDA de la mano con recomendaciones de diseño. (Hucaby, Garza, & Edgeworth, 2019)

5.2.9. **Underlay o Red Subyacente**

La red subyacente está definida por los conmutadores y enrutadores físicos que se utilizan para implementar la red SDA. Todos los elementos de red en el underlay deben establecer conectividad IP mediante el uso de algún protocolo de enrutamiento. En lugar de utilizar topologías y protocolos de red arbitrarios, el *underlay* en SDA utiliza la base de capa 3 que incluye los conmutadores de borde del campus para garantizar el rendimiento, la escalabilidad y la alta disponibilidad de la red.

En SDA los conmutadores en el underlay admiten la conectividad física de los dispositivos de los usuarios. Sin embargo, las subredes y los dispositivos finales del usuario final no son parte del underlay; son parte de una red overlay de Capa 2 o Capa 3 accesible por lenguajes de programación.

La solución de SDA es compatible con redes underlay IPv4 y overlays en IPv4 o IPv6. (Hucaby, Garza, & Edgeworth, 2019)

5.2.10. **Consideraciones de diseño para el underlay o red subyacente**

El diseño del underlay es vital para asegurar la estabilidad, el rendimiento y la utilización eficiente de la red SDA. La automatización para implementar la capa overlay es posible a través del DNA Center.

Las redes de underlay para el fabric tienen los siguientes requisitos de diseño:

- Capa 3 para el diseño de acceso: el uso de una red enrutada de Capa 3 proporciona al fabric el mayor nivel de disponibilidad sin la necesidad de utilizar protocolos para evitar bucles interminables o técnicas de agrupamiento de interfaces.
- Aumente el MTU predeterminado: el encabezado VXLAN agrega 50 y opcionales hasta 54 bytes adicionales a la encapsulación. Algunos conmutadores admiten un máximo de transmisión (MTU) de 9216, mientras que otros pueden tener 9196 o menor. Dado que las MTU en los servidores suelen subir a 9,000 bytes, habilitar un MTU de 9100 en toda la red asegura que las tramas gigantes de Ethernet se puedan transportar sin ninguna fragmentación dentro y fuera del fabric.
- Utilice enlaces punto a punto: los enlaces punto a punto proporcionan los tiempos de convergencia más rápidos porque eliminan la necesidad de esperar los tiempos de espera de un protocolo en la capa superior como se usa regularmente en las topologías más complejas. La combinación de enlaces punto a punto con el diseño de la topología física recomendada proporciona convergencia rápida después de una falla del enlace. La convergencia rápida es un beneficio de la detección rápida de fallas de enlace que activa el uso inmediato de entradas de topología alternativas ya existentes en la tabla de enrutamiento. Implemente los enlaces punto a punto

utilizando tecnología óptica no cobre. La razón es que las interfaces ópticas ofrecen los tiempos de detección de fallas más rápidos para mejorar la convergencia.

- El enrutamiento de múltiples rutas de igual costo o ECMP es una estrategia de enrutamiento donde el reenvío de paquetes para el siguiente salto a un solo destino puede ocurrir en múltiples rutas categorizadas como las mejores. El equilibrio en las cargas entre estas rutas ECMP se realiza automáticamente mediante Cisco Express Forwarding (CEF). Los protocolos de enrutamiento o IGP's compatibles con ECMP deben usarse para aprovechar los enlaces con costos paralelos y proporcionar rutas de reenvío redundantes brindando resiliencia.
- La detección de reenvío bidireccional o BFD se debe utilizar para mejorar la detección de fallas y las características de convergencia de los protocolos de tuteo. El reenvío sin interrupción provisto por NSF funciona con SSO para proporcionar el reenvío continuo de paquetes en caso de un fallo del procesador de rutas (RP). Los protocolos de enrutamiento o IGP's compatibles con NSF deben usarse para minimizar la cantidad de tiempo que una red no está disponible después de un fallo en el conmutador.
- IGP dedicados para el fabric: la red de underlay en el fabric solo requiere accesibilidad IP desde el borde del fabric hasta el nodo de borde. En una implementación tipo fabric, se puede implementar un diseño con IGP's con una sola área y un proceso dedicado dentro del fabric de SDA. Generalmente se utiliza un protocolo de estado de enlace, como IS-IS, para obtener las ventajas del rendimiento. Ahora, si bien IS-IS se utiliza para la automatización de LAN, otros protocolos de

enrutamiento como OSPF y EIGRP pueden utilizarse y ambos son compatibles con ECMP y NSF.

- Propagación de interfaces de bucle invertido: las direcciones de bucle invertido asignadas a los dispositivos en el underlay deben propagarse fuera del fabric para establecer la conectividad con los servicios de infraestructura, como los nodos del plano de control del fabric, DNS, DHCP y AAA. Se necesitan usar máscaras de 32 bytes para los *host* y hacerlos visibles en los RLOC, la ruta predeterminada no se puede usar para este propósito. Aplique etiquetas a las rutas de host a medida que se introducen en la red. Haga referencia a las etiquetas para redistribuir y propagar solo las rutas de loopback etiquetadas. Esta es una manera fácil de propagar selectivamente rutas fuera del fabric y evitar mantener listas de prefijos.
- Accesibilidad al WLC: la conectividad al WLC debe tratarse como las direcciones de *loopback*. Los AP no pueden utilizar una ruta predeterminada en el underlay para llegar a los WLC. Debe existir una ruta de IP específica para el WLC en la tabla de enrutamiento global en cada conmutador donde los AP están físicamente conectados.
- Automatización de LAN: la configuración del underlay se puede automatizar utilizando los servicios de automatización de LAN del DNA Center. En casos de implementaciones donde ya existe ciertas configuración, se puede crear manualmente la capa del underlay. Las configuraciones manuales del underlay permiten variaciones a la implementación automatizada. Podría elegirse un IGP diferente por ejemplo, pero los principios de diseño para el underlay se mantienen. La automatización de LAN en el DNA Center es una alternativa a las implementaciones

manuales de underlay para redes nuevas y utiliza un diseño de acceso por enrutamiento en IS-IS. Aunque hay muchos protocolos de enrutamiento alternativos, IS-IS ofrece ventajas operativas como la conexión con equipos laterales sin dependencias del protocolo IP, la capacidad de asociaciones basados netamente en en loopbacks y el tratamiento agnóstico del tráfico IPv4, IPv6 o no IP.

- En las últimas versiones de Cisco DNA Center, la automatización de LAN utiliza las funciones de Cisco Network Plug and Play para implementar la configuración de enrutamiento de unidifusión y de multidifusión específica de la fuente en el underlay, lo que ayuda a la eficiencia a la hora de la entrega de tráfico para los servicios integrados en la parte superior.
- El uso de la automatización de la LAN en el underlay proporciona la homogeneidad de *MTU's*, enlaces punto a punto enrutados, *ECMP, NSF, BFD* y acceso enrutado, al tiempo que propaga las direcciones loopback para los nodos del fabric. También puede proporcionar las credenciales de *CLI* y *SNMP* asi como SWIM para actualizar el software de los equipos a las versiones deseadas.
- Para automatizar la implementación del fabric, DNA Center utiliza PnP para acceder a un dispositivo conectado directamente al underlay. Se accede a los dispositivos restantes mediante el descubrimiento via CDP hop-by-hop. (2019). Software-Defined Access. El gráfico 11 muestra como queda la conexión en capa 2:

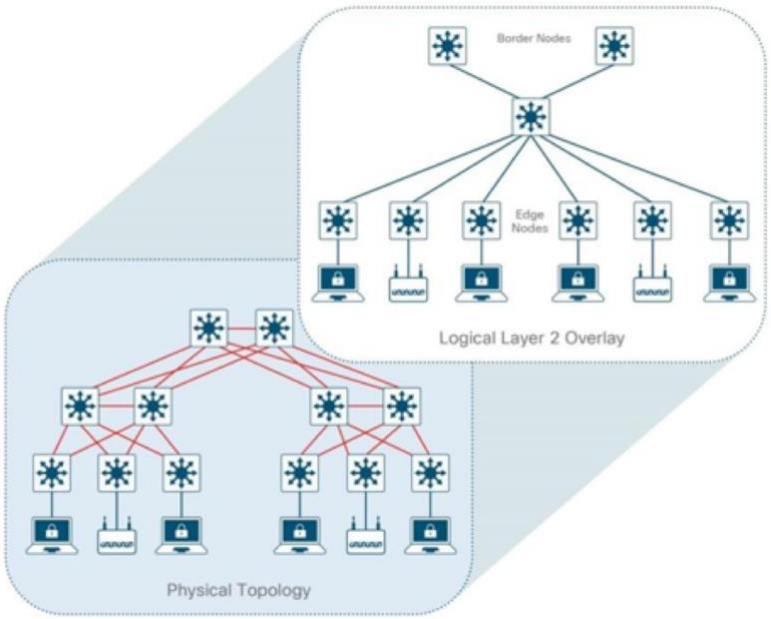


Gráfico 11 Conexión de Capa 2 con la Red Superpuesta

Fuente: Cisco. (2019b). Recuperado 10 octubre, 2019, de https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/sda-sdg-2019oct.pdf

5.2.11. **El Overlay o Red Superpuesta**

Se crea una red superpuesta sobre el underlay o red subyacente para crear una red virtualizada. El tráfico del plano de datos y la señalización del plano de control están contenidos dentro de cada red virtualizada, manteniendo el aislamiento entre las redes y la independencia del underlay. La estructura SDA implementa la virtualización encapsulando el tráfico de usuarios en redes overlay utilizando paquetes IP que se obtienen y terminan en los límites del fabric. ASi mismo los limites del fabric incluyen sus entradas y salidas, los conmutadores de borde del fabric para usuarios cableados y AP’s de fabric para clientes inalámbricos. Las redes tipo overlay pueden ejecutarse en todos o un subconjunto de los dispositivos de la red underlay. Se pueden ejecutar varias redes overlay en el mismo underlay para soportar multi inquilino o asignación de

recursos de almacenamiento a varios administradores independientes mediante la virtualización. Cada red overlay aparece como una instancia virtual de enrutamiento y reenvío (VRF) para la conectividad a redes externas. Se mantiene la separación de overlays cuando se extienden las redes fuera del fabric utilizando VRF-lite, manteniendo la separación de la red dentro de los dispositivos conectados al fabric y en los enlaces entre los dispositivos habilitados para VRF.

Las redes overlay de capa 2 emulan un segmento LAN para transportar tramas de capa 2, transportando las subredes a través del underlay en la capa 3. En el gráfico 12 se observa su conexión:

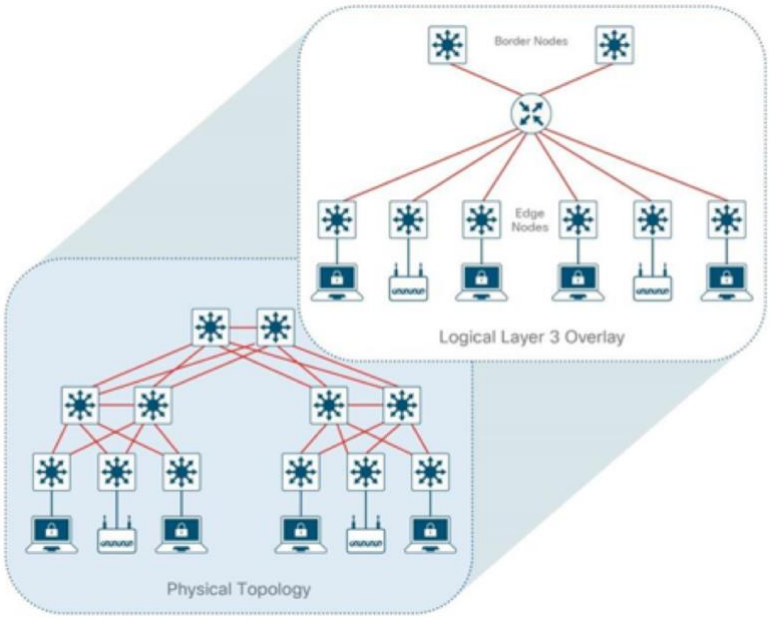


Gráfico 12 Conexión de Capa 3 a Nivel Lógico

Fuente: Cisco. (2019c). Recuperado 10 octubre, 2019, de https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/sda-sdg-2019oct.pdf

Las redes overlay de capa 2 son útiles para emular topologías físicas y según el diseño pueden estar sujetas a difusiones de la capa 2. Las redes tipo overlay de capa 3 abstraen la conectividad basada en IP de la conectividad física y permiten múltiples redes IP como parte de cada red virtual. (Cisco, 2019)

5.2.12. **El Fabric para el Plano de datos y el Plano de Control**

SDA configura la red de overlay para la encapsulación del plano de datos del fabric utilizando VXLAN. VXLAN encapsula tramas completas de capa 2 para el transporte a través del underlay con cada red de overlay identificada con un identificador de red tipo VXLAN (VNI). El encabezado VXLAN también lleva los SGT's necesarios para la microsegmentación. La función de mapeo y resolución de las direcciones de los dispositivos finales requiere un protocolo del plano de control. SDA usa LISP o Protocolo de separación de localizadores para esta tarea. LISP ofrece la ventaja del enrutamiento basado no solo en la dirección IP o la dirección MAC como el identificador de dispositivo final (EID) para un dispositivo, sino también una dirección IP adicional que se utiliza como un localizador de enrutamiento o RLOC para representar la ubicación de red de ese dispositivo. La combinación EID y RLOC proporciona toda la información necesaria para el reenvío de tráfico, incluso si un dispositivo final utiliza la misma dirección IP pero aparece en una ubicación de red diferente. La capacidad de desacoplar la identidad del dispositivo final de su ubicación permite que direcciones IP que pertenecen a la misma subred estén disponibles en múltiples gateways de Capa 3. Esto es un claro contraste y ventaja en comparación con la relación uno a uno que se hace convencionalmente en una subred IP con su respectivo gateway en las redes

tradicionales. El siguiente diagrama muestra un ejemplo de dos subredes que forman parte de un red overlay. Las subredes se extienden a través de dispositivos de capa 3 físicamente separados. La interfaz RLOC es la única dirección enrutable que se requiere para establecer la conectividad entre los dispositivos finales de la misma o diferente subred.

5.2.13. **Consideraciones de diseño para las políticas de seguridad**

Las políticas de seguridad varían según la organización; no es posible definir un diseño de seguridad único para todos. Los diseños de seguridad se rigen por las políticas de seguridad de la información y márgenes de cumplimiento legal. La fase de planificación para un diseño de seguridad es clave para garantizar el equilibrio correcto en la seguridad y experiencia del usuario.

Se deben considerar los siguientes aspectos al diseñar una política de seguridad para una red SDA:

- Apertura de la red: algunas organizaciones solo permiten dispositivos del corporativo en la red mientas que otras admiten el esquema BYOD o “Traiga su propio dispositivo". Se puede lograr un equilibrio entre ambas mediante la implementación del modelo BYOD en el que se ofrezca una lista de dispositivos finales aprobados por TI a los usuarios para uso comercial. También es posible un enfoque basado en la identidad en el que las políticas de seguridad de la red se pueden implementar según la propiedad del dispositivo. Por ejemplo, los dispositivos de corporativo pueden obtener acceso basado en grupos, mientras que los dispositivos personales pueden obtener solo acceso a Internet.

- Gestión de identidades: en la forma mas simple, la gestión de identidad puede ser un nombre de usuario y una contraseña que se utilizan para autenticar a los usuarios. Agregar funciones de seguridad integradas y visibilidad de las aplicaciones en los dispositivos de red proporciona telemetría de datos para la definición de políticas avanzadas que pueden incluir datos de contexto adicional como pueden ser la ubicación física, dispositivo utilizado, tipo de red de acceso, aplicaciones utilizadas y hora del día.
- Autenticación, Autorización y Trazabilidad o AAA: la autenticación es el proceso de establecer y confirmar la identidad de un dispositivo o usuario qué solicita acceso a la red. La autorización es el proceso de autorizar ese usuario o dispositivo final a un conjunto de recursos de red. Las políticas de segmentación no necesariamente tienen que aplicarse en la capa de acceso, y pueden implementarse en múltiples ubicaciones. Las políticas se aplican con el uso de SGACL para la segmentación dentro de las redes virtuales y la asignación dinámica de VLAN's para asignar dispositivos y usuarios finales a redes virtuales en los nodos de borde del fabric. Los registros de eventos, los contadores de visitas de ACL y herramientas de trazabilidad están disponibles para mejorar la visibilidad.
- Seguridad de dispositivos finales: los dispositivos finales pueden infectarse con malware, comprometer los datos y crear interrupciones en la red. La detección de malware, la gestión de dispositivos finales y las exportaciones de datos desde los dispositivos de red proporcionan información sobre el comportamiento de los dispositivos finales. Es necesario mantener una estrecha integración de la red con los dispositivos de seguridad y plataformas de análisis que le permitan obtener la

inteligencia necesaria para poner en cuarentena y ayudar a remediar los dispositivos si se ven comprometidos en algún momento.

- Integridad y confidencialidad de los datos: la segmentación de la red mediante VN's permite controlar el acceso a las aplicaciones así como separar las transacciones de los empleados del tráfico de IoT; el cifrado de la ruta de datos a través de la capa de conmutadores utilizando IEEE 802.1AE MACsec se utiliza para proporcionar encriptación en la capa 2, evitar intromisiones y garantizar que los datos no puedan modificarse. (Cisco, 2019)
- Seguridad de los dispositivos de red: fortalecer la seguridad de los dispositivos de red es esencial porque son objetivos comunes en los ataques de seguridad. El uso de las opciones de administración de dispositivos más seguras, como habilitar la autenticación de dispositivos usando TACACS + y deshabilitar servicios innecesarios, son las mejores prácticas para garantizar que los dispositivos de red estén seguros. La habilitación de la segmentación basada en grupos dentro de cada red virtual permite políticas de red jerárquicas simplificadas. Los políticas de seguridad que permiten el aislamiento de los planos de datos y control se logran utilizando virtualización de redes. Las políticas por grupos se integran a partir de SGT en las VN's lo que permite la aplicación de políticas comunes en todo el fabric cableado e inalámbrico. Los SGT proporcionan la capacidad de etiquetar el tráfico de dispositivos finales en función de un rol o función dentro de la red y sujeto a políticas basadas en roles o SGACL definidas centralmente en ISE. En muchas implementaciones, Active Directory se utiliza como almacén de identidad para cuentas de usuario, credenciales e información de membresía de grupos. Al pasar la fase de autorización, los

dispositivos finales pueden clasificarse en función de esa información y son asignados en el grupo que les corresponde. Estos grupos escalables se pueden usar para crear políticas de segmentación y reglas de asignación de red virtual.

La información SGT se transporta a través de la red de varias maneras:

- Dentro de la red SDA: el encabezado de la estructura SDA transporta información de los SGT. Los nodos de borde pertenecientes al fabric o no pueden aplicar SGACL para hacer cumplir las políticas de seguridad.
- Fuera de fabric en un dispositivo con capacidad Cisco TrustSec: los dispositivos que soportan TrustSec llevan la información SGT en un encabezado CMD en capa 2. Este es el modo recomendado fuera de SDA.
- Fuera del fabric a través de dispositivos que no soporten Cisco TrustSec: SXP permite el transporte de SGT a través de una conexión TCP. Esto se puede utilizar para dar el pase a dispositivos de red que no soportan SGT. (Hucaby, Garza, & Edgeworth, 2019)

5.2.14. **Gestión de la solución SDA**

No se requiere una comprensión profunda de LISP y VXLAN para la implementación de una solución SDA. Tampoco es necesario conocer los detalles de cómo configurar cada componente y función de red individual para lograr la operación coherente de extremo a extremo que ofrece. Cisco brinda el controlador de SDN llamado Cisco DNA Center, un sistema de administración centralizado e intuitivo, para el diseño, aprovisionamiento y aplicación de políticas a través de la red cableada e inalámbrica.

Además de la automatización para SDA, el DNA Center ofrece aplicaciones tradicionales para mejorar con eficiencia la organización. Por ejemplo la administración de imágenes de software, paneles de estado de dispositivos y una función llamada 360 que brinda información contextual del equipo de red o dispositivo final. El DNA Center es un componente fundamental de SDA, permite la automatización de las implementaciones de dispositivos en la red y proporciona la velocidad y coherencia necesarias para mantener la eficiencia operativa. Uno de los mayores beneficios para las organizaciones al contar con el DNA Center es la reducción de costos y riesgos al implementar y mantener sus redes. La gestión de políticas con servicios de identidad se integra en las redes SDA utilizando un repositorio externo alojado en el ISE. Este se asocia con el DNA Center para realizar el mapeo dinámico de los usuarios y dispositivos a sus grupos respectivos, simplificando la administración y aplicación de políticas de seguridad de extremo a extremo en la red, lo cual supera las implementaciones de red tradicionales que se basan en listas de acceso IP.

5.2.15. **Modelos de Sitios Referenciales para Redes SDA**

El diseño de un fabric SDA es flexible y puede adaptarse a muchos entornos, lo que significa que no hay una propuesta de diseño única. La escala de un fabric puede ser tan pequeña como un solo conmutador, un grupo o tan grande como una implementación de campus de tres niveles. Las topologías SDA deben seguir los mismos principios de diseño y mejores prácticas asociadas con un diseño jerárquico dividiendo la red en grupos modulares.

Se puede crear elementos de diseño que se puedan replicar en toda la red usando esquemas modulares. En general, las topologías SDA deben implementarse con esquemas jerárquicos donde el nodo de borde en el fabric sea el punto de salida para las redes vinculadas. A medida que las redes se hacen mas grandes, se utilizan topologías físicas más variadas para acomodar los requisitos para la implementación de servicios de red especializados. (Cisco, 2019)

5.2.15.1. **Dimensionamiento de sitios SDA**

Un objetivo práctico en el diseño de los sitios SDA es maximizar el tamaño del fabric dentro de los límites que el DNA Center soporte y dentro de los parámetros necesarios para sostener la alta disponibilidad del sitio. Al mismo tiempo se busca minimizar el número total de sitios. En el gráfico 13 se observan los tamaños de sitios para el dimensionamiento:

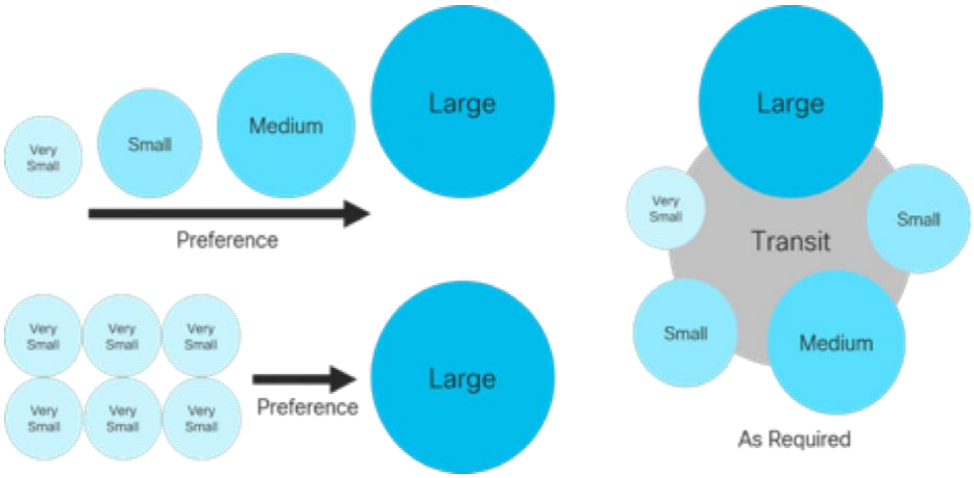


Gráfico 13 Dimensionamiento y tamaño de sitios

Fuente: Cisco. (2019d). Recuperado 10 octubre, 2019, de https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/sda-sdg-2019oct.docx/_jcr_content/renditions/sda-sdg-2019oct_7.png

5.2.15.2. **Consideraciones de diseño de SD-Access**

Cuando se diseña una red para SD-Access, más allá de las necesidades y los intereses del negocio, se deben considerar varios factores técnicos, y los resultados de estas consideraciones crean el marco de topología y equipos utilizados en la red. Estos factores no son unidimensionales, son elementos multidimensionales que deben considerarse como un conjunto, no como grupos aislados:

- ¿Es una implementación nueva o una mejora tecnológica?
- Cantidad de usuarios
- Ubicación geográfica
- Ubicación de servicios
- Tipo de tráfico
- ¿Se cuenta con enrutadores de fusión?
- ¿Cuentan con política unificadas?
- Niveles de supervivencia del sitio(s)
- ¿Se require alta disponibilidad?

5.2.15.2.1. **Implementación nueva o mejora tecnológica**

Los escenarios de mejoras tecnológicas se dimensionan de acuerdo a SDA realizando un análisis 1 a 1 de la infraestructura actual para determinar sus capacidades de cara a SDA. Se logra a través de uno de los siguientes enfoques:

- Automatización de fronteras y entrega de capa 2: esta característica de SDA conecta una red tradicional con una red de SD-Access agregando efectivamente los equipos detrás de la red convencional al fabric de SDA. Este diseño es un caso de uso temporal mientras se toma el segundo enfoque.
- Edificio por edificio o piso por piso: las áreas de la red existente se convierten a SD-Access. Esto se hace comúnmente rack por rack, piso por piso o edificio por edificio. La migración se realiza, como mínimo, un cambio a la vez. No se admite una VLAN a la vez, ya que la VLAN puede abarcar varios conmutadores tradicionales. (Cisco, 2019)

5.2.15.2.2. **Número de usuarios**

El factor mas importante en el diseño del sitio es el número total de clientes cableados e inalámbricos en todas sus ubicaciones, sitio central y sucursales. Esto determina la cantidad de puertos por conmutadores físicos y puntos de acceso requeridos, lo que en última instancia puede resultar en la necesidad de diseños de red de dos o tres niveles. El número de clientes puede ser lo suficientemente pequeño como para que la red esté compuesta por una pila de conmutadores.

5.2.15.2.3. **Geografía**

La geografía física afecta el diseño de la red. No tiene un impacto directo en la topología dentro del sitio en sí, pero la geografía debe considerarse en relación con los tipos de tránsito, ubicaciones de servicios, capacidad de supervivencia y alta

disponibilidad. Las ubicaciones que se encuentran dentro de una misma área metropolitana (*MAN*) o campus con varios edificios cercanos o con fibra directa pueden beneficiarse del diseño de una red SDA en campus distribuido. Esto permite una política unificada nativa en todas las ubicaciones además de poder brindar un solo bloque para servicios. Las ubicaciones conectadas a través de la WAN o Internet también deben tener en cuenta los servicios y la política así como la infraestructura de enrutamiento fuera del overlay del fabric utilizado para conectarlos.

5.2.15.2.4. **Servicios compartidos**

Los servicios como DHCP, DNS, ISE y WLC son elementos necesarios para los clientes en una red SDA. Los servicios se implementan comúnmente en una de tres formas. En SDA para campus distribuido y en ubicaciones distribuidas a través de la WAN, los servicios a menudo se implementan data centers locales. Estos centros de datos usualmente se conectan comúnmente a las capas centrales o de distribución en una ubicación centralizada tipo HQ o sitio central. El tráfico se envía desde los sitios remotos y sucursales de regreso al HQ y luego se dirige hacia los servicios necesarios. Los servicios pueden ser locales a la ubicación. Para fines de supervivencia, se puede establecer un bloque de servicios en cada ubicación del fabric. Los servicios locales aseguran que estos servicios críticos no se envíen a través de la WAN / MAN y garantizan que los puntos finales puedan acceder a ellos, incluso en caso de congestión o enlaces inactivos en la WAN. Sin embargo, esto también requerirá la necesidad de un enrutador de fusión por ubicación para proporcionar acceso a los servicios compartidos.

5.2.15.2.5. **Tipos de tránsito**

Los tránsitos son simplemente las conexiones físicas entre los sitios del fabric. Esta conectividad puede ser MAN, WAN o Internet. La WAN podría ser MPLS, IWAN u otras variaciones de WAN. Dentro de Cisco DNA Center, los tránsitos se denominan tránsitos SDA, basados en IP o SD-WAN. Los tránsitos de SDA se utilizan en SDA para campus distribuido. Usando el tránsito SDA los paquetes se encapsulan entre sitios usando encapsulación de fabric tipo VXLAN que transporta las construcciones de políticas a nivel macro y micro.

5.2.16. **Enrutadores de Fusión**

El término genérico enrutador de fusión proviene de MPLS de capa 3 por VPN. El concepto básico es que el enrutador de fusión conoce los prefijos disponibles dentro de cada VPN (VRF), ya sea debido a la configuración de enrutamiento estático o a través del emparejamiento de rutas, y por lo tanto puede fusionar estas rutas juntas. Las responsabilidades del enrutador de fusión genérico son enrutar el tráfico entre VRF separadas (difusión de VRF) o enrutar el tráfico hacia y desde un VRF a un grupo compartido de recursos como pueden ser servidores DHCP y DNS de la tabla de enrutamiento global (difusión de rutas). Ambas tareas implican mover rutas de una tabla de enrutamiento a una tabla de enrutamiento de VRF separada.

En una implementación de SDA, el enrutador de fusión tiene una única responsabilidad: proporcionar acceso a servicios compartidos para los puntos finales en el *fabric*. Hay dos formas principales de realizar esta tarea dependiendo de cómo se implementen los servicios compartidos. La primera opción se usa cuando las rutas de

servicios compartidos están en la tabla de enrutamiento global. En el enrutador de fusión las listas de prefijos IP se utilizan para hacer coincidir las rutas de servicios compartidos, los mapas de ruta hacen referencia a las listas de prefijos IP y las configuraciones VRF hacen referencia a los mapas de ruta para garantizar que solo se filtren las rutas que coinciden específicamente. La segunda opción es colocar servicios compartidos en un VRF dedicado en el enrutador de fusión. Con los servicios compartidos en un VRF y los dispositivos finales del fabric en otros VRF, se aplican filtros para las rutas deseadas. (Cisco, 2019)

Un enrutador de fusión puede ser enrutador convencional, un conmutador de 3 o un firewall. En este último caso debe cumplir con varios requisitos, debe soportar:

- Múltiples VRF
- Etiquetado 802.1q (etiquetado VLAN)
- Subinterfaces (cuando se usa un enrutador o firewall) o interfaces virtuales conmutadas (SVI) (cuando se usa un conmutador de Capa 3)
- BGPv4 y específicamente las extensiones MP-BGP (RFC 4760 y RFC 7606) para atributos de comunidades extendidas

5.2.17. **Conectividad WAN e Internet**

La conectividad WAN e Internet para un sitio del fabric tiene varias opciones y va a depender del diseño del underlay. El factor común entre estas opciones es que el nodo de borde generalmente está conectado a un dispositivo que se atravesará para acceder

a Internet y la WAN debido a la información de enrutamiento que posee. Esta infraestructura de enrutamiento podría ser un enrutador de perímetro, un enrutador del ISP o incluso un enrutador de fusión que realiza múltiples funciones. El aspecto clave del diseño es garantizar que dicha infraestructura de enrutamiento tenga la conectividad física y el rendimiento necesarios para conectar el sitio del fabric al exterior. (Cisco, 2019)

5.2.18. **Políticas Unificadas**

Las políticas unificadas son de los elementos principales en la solución SDA. Al lograr unificar las políticas, el tráfico cableado e inalámbrico se manejan como una sola capa de acceso (nodo de borde en el fabric) y los usuarios, dispositivos y aplicaciones tienen la misma política donde sea que se conecten en la red.

Dentro de un sitio de fabric, la política unificada se habilita y se lleva a cabo a través de los campos ID de segmento (ID de política de grupo) y VXLAN-GPO. Esto permite que la información de segmentación VRF (macro) y SGT (micro) se lleve dentro del sitio de la estructura. (Cisco, 2019)

5.2.19. **Macro Segmentación de Extremo a Extremo**

SDA utiliza redes virtuales o VRF para la macro segmentación. Las VRF mantienen una instancia del enrutamiento y conmutación separadas para los dispositivos, interfaces y subredes dentro de ella. En el fabric el DNA Center proporciona la configuración para los VRF definidos por el usuario.

La segmentación mas allá del fabric tiene múltiples variaciones según el tipo de tránsito. En SDA para campus distribuido y tránsitos SD-WAN, la información de las VN se transporta de forma nativa dentro del paquete.

En el tránsito basado en IP, debido al proceso de desencapsulación, esa información de política puede perderse. Existen dos enfoques para llevar la información de las VN entre los sitios del fabric un tránsito basado en IP. El mas sencillo, aunque menos implementado debido a que el equipo de los ISP's esta fuera del control administrativo del ingeniero, es configurar VRF-lite hop-by-hop entre cada sitio del fabric.

Una segunda opción al diseño es utilizar direcciones VPNv4 del multiprotocolo de BGP para transportar la información de la macro segmentación. Debido a que BGP es una sesión TCP de punto a punto entre pares, las construcciones de políticas pueden atravesar la red WAN del proveedor de servicios usándola simplemente como una ruta de reenvío de IP entre la infraestructura de enrutamiento BGP en cada sitio del fabric. (Cisco, 2019)

5.2.20. **Micro Segmentación de Extremo a Extremo**

SDA utiliza etiquetas SGT para la microsegmentación. Los SGT usan metadatos en forma de etiquetas únicas para asignar equipos a grupos y aplicar políticas basadas en esos grupos. Dentro de la estructura del overlay, los nodos de borde y los nodos de frontera usan SGACL suministrados por el ISE para tomar decisiones basadas en estos SGT.

Al igual que la macro segmentación, la segmentación fuera del fabric tiene múltiples variaciones según el tipo de tránsito. En SDA para campus distribuido y tránsitos SD-WAN, la información VN se transporta de forma nativa dentro del paquete.

En el tránsito basado en IP, debido a la desencapsulación, esa información de política puede perderse. Existen dos enfoques para transportar información SGT entre los sitios del fabric utilizando tránsito basado en IP. Una opción es configurar el etiquetado en línea (CMD) salto por salto entre cada sitio de la estructura. La segunda opción de diseño es usar SXP para transportar los enlaces de IP a SGT entre sitios. Usando SXP, estos enlaces pueden transportarse a través de circuitos GRE, IPsec, DMVPN y GETVPN entre sitios.

SXP tiene implicaciones en cuanto a los puntos de aplicación y escala que deben considerarse. Entre los sitios del fabric, SXP se puede utilizar para aplicar los SGT en los nodos fronterizos o en la infraestructura de enrutamiento en sentido norte. Si la ejecución se realiza en la infraestructura de enrutamiento, CMD se utiliza para transportar la información de los SGT en línea desde el nodo de borde. (Cisco, 2019)

5.2.21. **Modelos de referencia para el Fabric**

Para comprender mejor los diseños de sitios se utilizan categorías de referencia. Los números se usan solo como pautas y no necesariamente coinciden con ningún límite específico para dispositivos dentro de un diseño.

5.2.21.1. **Sitios muy pequeños**

Aquí se utiliza el concepto ‘Fabric in a Box ’donde un solo closet brinda resiliencia y capacidad de apilamiento para los conmutadores. Las funciones de borde, plano de control, frontera e inalámbrico son colocadas en una única plataforma redundante.

Tabla 7 Referencia sitios muy pequeños

Criterios dimensionamiento	**Valores**
Dispositivos finales, proyecte menos de:	2,000
Nodos Fabric, máximo	1
Nodos de plano de control	1
Nodos de borde	1
Redes virtuales, calcular menos de	8
Grupos de direcciones IP menos de	8
Puntos de Acceso, menos de	100

Debido al número de dispositivos finales soportadas, la alta disponibilidad y la capacidad de supervivencia del sitio no son requisitos comunes aquí. Los servicios locales del sitio de DHCP, DNS, WLC e ISE brindan resistencia y capacidad de supervivencia, aunque a expensas de una mayor complejidad y equipo, incluido un enrutador de fusión. Si los servicios compartidos se implementan localmente, un enrutador de fusión podría colocarse en un conmutador conectado directamente al Fabric en modo ‘Fabric in a Box ’con servicios implementados como máquinas virtuales en equipos serie C de un UCS conectado al enrutador fusion. Una alternativa es implementar un servidor blade UCS serie E en la infraestructura de enrutamiento WAN o enrutadores del fabric para virtualizar los servicios compartidos.

La alta disponibilidad en este diseño se proporciona a través de StackWise-480, que combina múltiples conmutadores físicos en un solo conmutador lógico y StackPower para proporcionar redundancia de energía entre los miembros de la pila de conmutadores. Si se usa un conmutador modular tipo 9400, se proporciona alta disponibilidad a través de módulos supervisores y fuentes de alimentación redundantes.

Los controladores de LAN inalámbrica pueden implementarse como unidades físicas conectadas directamente al ‘Fabric in a box ’o implementarse como el controlador Catalyst 9800 que viene embebido. Cuando se utiliza el Catalyst 9800 embebido con una pila de conmutadores o un supervisor redundante, el AP y el SSO del cliente se proporcionan automáticamente.

Cuando se usa una pila de conmutadores, los enlaces a la infraestructura de enrutamiento que se conectan a las capas superiores se deben conectar desde diferentes miembros en la pila. Con los conmutadores tipo chasis, los enlaces deben conectarse a través de cada supervisor. Para preparar el proceso de automatización en los nodos fronterizos, además de tener la visibilidad inicial a nivel de IP, los SVI y los enlaces troncales se configuran entre los conmutadores de los sitios pequeños y la infraestructura de enrutamiento en las capas superiores.

Los equipos Serie Catalyst 9300 configurados de pila con controlador inalámbrico Catalyst 9800 embebido son una opción óptima en este tipo diseños. La serie Catalyst 9500 tienen más opciones de conectividad física, pero sin la opción de utilizar StackWise-480 y StackPower.

5.2.21.2. **Sitios pequeños**

Estos cubren una sola oficina o edificio; el nodo de borde se coloca con el plano de control en uno o dos dispositivos y un controlador inalámbrico separado con configuración HA opcional.

Tabla 8 Referencia sitios pequeños

Criterios dimensionamiento	**Valores**
Dispositivos finales, proyecte menos de:	10,000
Nodos Fabric, máximo	25
Nodos de plano de control	2
Nodos de borde	2
Redes virtuales, calcular menos de	32
Grupos de direcciones IP menos de	100
Puntos de Acceso, menos de	200

Regularmente en un sitio pequeño, se proporciona alta disponibilidad en los nodos del fabric colocando el nodo de borde y la funcionalidad del nodo del plano de control en los conmutadores de capa centrales. Tanto para la resiliencia como para las rutas de reenvío alternativas en el overlay y underlay, los conmutadores de capa central deben conectarse directamente entre sí.

Debido a la cantidad de dispositivos finales, los sitios pequeños generalmente no integran la parte inalámbrica en SDA. Siempre que haya menos de 200 puntos de acceso y 4.000 clientes, la conexión inalámbrica integrada se puede implementar en el nodo de borde y las funciones del nodo del plano de control en los conmutadores de capa central.

Para admitir una mayor cantidad de clientes o puntos de acceso, se puede colocar un WLC físico. Para habilitar la alta disponibilidad en el dispositivo utilizando un par HA-SSO o mediante conectividad física, se implementa un bloque de servicios. Los WLC están conectados al conmutador que brinda el bloque de servicios a través de canales de puerto de capa 2 para proporcionar interfaces redundantes. El bloque de servicios es comúnmente una pequeña pila de conmutadores que está conectada a ambos conmutadores centrales. Este bloque de servicios se puede usar como un enrutador de fusión si los servidores DHCP y DNS son locales. (2019). Software-Defined Access.

5.2.21.3. **Sitios medianos**

Cubren un edificio con múltiples closets o edificios; diseñado para admitir menos de 25,000 dispositivos finales, menos de 64 VN y menos de 1,000 AP; el nodo de borde se distribuye desde el plano de control utilizando dispositivos redundantes, y un controlador inalámbrico separado tiene una configuración HA.

Tabla 9 Referencia sitios medianos

Criterios dimensionamiento	**Valores**
Dispositivos finales, proyecte menos de:	25,000
Nodos Fabric, máximo	250
Nodos de plano de control	2-4
Nodos de borde	2
Redes virtuales, calcular menos de	64
Grupos de direcciones IP menos de	300
Puntos de Acceso, menos de	1000

En un sitio medio, se proporciona alta disponibilidad en los nodos del fabric al dedicar dispositivos como nodos de borde y nodos de plano de control de manera dedica en vez de colocar las funciones en un dispositivo.

Tanto para la resiliencia como para las rutas de reenvío alternativas en el overlay y underlay, los conmutadores de capas centrales deben conectarse directamente.
Los nodos de plano de control dedicados generalmente están conectados a los conmutadores capas centrales del sitio. Para obtener un reenvío y redundancia óptimos, deben tener conectividad a través de ambos conmutadores principales.
Los sitios medianos no pueden utilizar la conexión inalámbrica embebida en SDA debido a la cantidad de dispositivos finales, los nodos del plano de control y los nodos fronterizos; por tanto, se implementan WLC físicos.

Para habilitar la alta disponibilidad, se despliega un par HA-SSO con conectividad física redundante a un bloque de servicios utilizando canales de puerto de capa 2.
El WLC debe estar conectado entre sí a través de su puerto RP. El bloque de servicios se compone usualmente de conmutadores de que operan en VSS o StackWise Virtual que están conectados a ambos conmutadores principales. Estos conmutadores de bloque de servicios se pueden usar como un enrutador de fusión si los servidores DHCP y DNS son locales.

5.2.21.4. **Sitios grandes**

Por lo general cubren un edificio grande con múltiples closets o varios edificios; diseñado para admitir menos de 50,000 dispositivos finales, menos de 64 VN y menos de 2,000 AP; múltiples salidas de borde se distribuyen desde el plano de control en

dispositivos redundantes, y un controlador inalámbrico separado tiene una configuración HA. Cada sitio del fabric incluye un conjunto de nodos de control, nodos de borde, nodos de frontera y controladores de LAN inalámbrica acordes con el tamaño de las categorías enumeradas.

Los nodos de políticas de ISE también se distribuyen a través de los sitios para cumplir con los requisitos de supervivencia. En una sola red física, se pueden implementar varios fabrics. En este caso, se deben especificar los elementos del fabric para cada una (nodos del plano de control, nodos de borde, nodos de frontera y WLC). Estos números sirven como pautas al diseñar sitios de tamaños similares, no necesariamente deben coincidir con límites especificados.

Tabla 10 Referencia sitios grandes

Criterios dimensionamiento	**Valores**
Dispositivos finales, proyecte menos de:	50,000
Nodos Fabric, máximo	1,000
Nodos de plano de control	2-6
Nodos de borde	2-4
Redes virtuales, calcular menos de	64
Grupos de direcciones IP menos de	500
Puntos de Acceso, menos de	2,000

El modelo de referencia de sitio grande cubre un edificio con múltiples closets o edificios. La red física suele ser una red de 3 niveles con equipos centrales, distribución y acceso, y está diseñada para admitir menos de 50,000 dispositivos finales. Por su tamaño esta red requiere puntos de salida de servicios dedicados, como un centro de datos dedicado, un bloque de servicios compartidos y servicios de Internet.

Este tamaño de sitio es comúnmente el sitio central o casa matriz en una implementación con varios fabric. El cortafuegos o firewall de perímetro generalmente se implementa en esta ubicación y el tráfico de Internet de los sitios remotos se atrae por medio de túneles a este sitio para ser procesado a través del firewall antes de ser enviado a Internet. El Cisco DNA Center y el módulo PAN primario del ISE generalmente se implementan en esta ubicación.

Los nodos del plano de control y los nodos fronterizos deben ser equipos dedicados desplegados como pares redundantes. Los nodos del plano de control deben conectarse a cada conmutador central para proporcionar resistencia y rutas de reenvío redundantes. (Cisco, 2019)

Un par de controladores inalámbricos en HA-SSO con conectividad física redundante despliega un bloque de servicios utilizando canales de puerto de capa 2. Los WLC’s deben estar conectados entre sí a través del puerto RP. El bloque de servicios suele formar parte de la red de centros de datos en estas instalaciones. Este bloque de servicios puede estar lejos del centro de datos, este último suelo estar conectado al equipo central y los conmutadores de distribución para proporcionar accesibilidad sin latencia. La ubicación del dispositivo de servicios del enrutador de fusión puede variar dado que se tienen múltiples dispositivos entre el bloque de servicios y los conmutadores centrales.

Se usan comúnmente nodos de borde interno dedicados para conectar al núcleo del centro de datos, mientras que los nodos de borde externo dedicados se usan para conectar el sitio a MAN, WAN e Internet. La infraestructura de enrutamiento redundante dedicada y los cortafuegos se usan para conectar este sitio a recursos externos, y los

nodos fronterizos deben estar completamente relacionados entre sí. Aunque la topología representa el borde en el núcleo de un campus, el borde en un sitio grande a menudo se configura por separado de los conmutadores centrales en otro punto de agregación.

Un sitio grande puede tener nodos de borde y nodos de plano de control dedicados para cuentas de invitados. Estos dispositivos generalmente se implementan con los roles de fabric distribuidos y acceden físicamente a la DMZ. Esto proporciona un plano de control y datos separados entre el tráfico Guest y Enterprise y optimiza el tráfico Guest que se enviará directamente a la DMZ sin la necesidad de un Anchor WLC.

5.2.22. **Modelo de referencia SDA para campus distribuido**

SDA para campus distribuido es una solución que conecta varios sitios de fabric independientes entre sí y mantiene las construcciones de políticas de seguridad (VRF y SGT) de estos sitios. Si bien los entornos e implementaciones de múltiples sitios han sido compatibles con SDA hace tiempo, no ha habido una forma automatizada y simple de mantener las políticas entre sitios. En el nodo de borde del fabric de cada sitio los paquetes de fabric se desencapsulan en IP nativa. En combinación con SXP, la política podría llevarse a cabo entre sitios utilizando encapsulación nativa. Sin embargo, esta configuración de política era manual y requería el uso de SXP para extender la política entre sitios e implicaba asignaciones complejas de enlaces IP a SGT dentro del ISE. SDA en campus distribuido, no requiere SXP, las configuraciones son automáticas y las asignaciones complejas ya no se necesitan. Esta solución permite la comunicación

entre sitios utilizando automatización y políticas consistentes de extremo a extremo en toda la red.

El acceso definido por software (SDN) para campus distribuido utiliza la señalización del plano de control del protocolo LISP y mantiene los paquetes en la encapsulación VXLAN del fabric entre los sitios. Esto mantiene las construcciones de política de macro y microsegmentación de VRF y SGT, respectivamente, entre los sitios del fabric. El encabezado Ethernet original del paquete se conserva para habilitar el servicio de overlay de capa 2 de SDA inalámbrico. El resultado es una red que no depende de la dirección porque la política se mantiene a través de la pertenencia a grupos.

5.2.23. **Tránsito de SDA**

Los tránsitos de SDA se utilizan para el campus distribuido. La consideración clave para el diseño del campus distribuido utilizando el tránsito SDA es que la red entre los sitios del fabric y el DNA Center debe crearse con una conectividad similar a la del campus. Las conexiones deben proveer buen ancho de banda , baja latencia (menos de 10 ms como guía general) y deben acomodar la configuración de los MTU para SDA en la red del campus (generalmente 9100 bytes). La conectividad física puede ser conexiones directas de fibra, fibra oscura en alquiler, Ethernet sobre longitudes de onda en un sistema WDM o sistemas Metro Ethernet (VPLS, etc.) que admiten capacidades similares de ancho de banda, velocidad de puerto, retrasos y especificidad en el MTU. Los paquetes se encapsulan entre sitios usando la encapsulación VXLAN del fabric. (Cisco, 2019)

5.2.24. **Nodos del Plano de Control de Tránsito**

Los nodos del plano de control de tránsito rastrean todas las rutas agregadas para el fabric y asocian estas rutas a los demás sitios del fabric. Cuando el tráfico de un punto final en un sitio necesita enviar tráfico a un punto final en otro sitio, se consulta el nodo del plano de control de tránsito para determinar a qué nodo fronterizo del sitio se debe enviar este tráfico. La función de los nodos del plano de control de tránsito es aprender qué prefijos están asociados con cada sitio del fabric y dirigir el tráfico a estos sitios a través del tránsito de acceso SDA mediante la señalización del plano de control.

5.2.25. **Consideraciones de los roles y capacidades de las plataformas**

Se deben seleccionar las plataformas para la red SDA en función de las capacidades requeridas por la red, teniendo en cuenta los roles funcionales recomendados.

Para obtener los detalles más actualizados sobre qué plataformas y software son compatibles con cada versión de Cisco SDA se debe consultar la matriz de compatibilidad de hardware y software de SDA según la versión. Los requisitos de diseño de la red física determinan las plataformas y el software.

Las siguientes son algunas de las capacidades de las plataformas que se deben considerar en una implementación de SDA:

- La mayoría de equipos del portafolio Cisco Catalyst 9000 cableados e inalámbricos y los Catalyst 3850 y 3650 con compatibles con SDA. Sin embargo, solo algunos

soportan los roles de nodo de borde, frontera y plano de control en el fabric. Además estos roles pueden crecer en alcance de funciones a medida que se lanzan nuevas versiones Cisco DNA Center y IOS-XE.

- Los equipos de generaciones anteriores como los Catalyst 4500 y 6800 Series y Cisco Nexus 7700 Series también son soportados. Han de revisarse sus características porque puede haber requisitos específicos para los módulos supervisores, las tarjetas o algunas interfaces particulares respecto al fabric. Además, los roles pueden no tener el alcance requerido. Por ejemplo, el software del Nexus 7700 puede restringir la función SDA para que se use solo cómo borde externo, lo que también requiere un nodo de plano de control separado.
- La mayoría de los equipos de enrutamiento integrados como los Cisco ISR 4400 y 4300, los de servicios de agregación ASR 1000-X y 1000-HX son soportados como plano de control y nodos fronterizos. Sin embargo, ninguno puede fungir como nodo de borde en el fabric. El Cisco Cloud Services Router 1000V también es compatible, pero solo como un nodo de plano de control.
- Los controladores de LAN inalámbricos Cisco Catalyst 9800 (independientes e integrados) de la familia 8540, 5520 y 3504 tienen requisitos de software específicos para su soporte. Del mismo modo, los AP Cisco Catalyst 9100 y Cisco Aironet Wave 2 y Wave 1 requieren versiones de software específicas.
- El Cisco ISE debe implementarse con una versión compatible con Cisco DNA Center.

5.2.26. **Migración a SD-Access**

Se pueden crear de manera relativamente fácil redes en implementaciones nuevas con SDA incluyendo los componentes para la infraestructura necesaria y utilizando las funciones Plug and Play del DNA Center para automatizar el aprovisionamiento de la arquitectura de red desde cero. Por otro lado, la migración de una red existente requiere planificación adicional. A continuación se incluyen algunas consideraciones:

- Las migraciones generalmente asumen que ya se tiene una red de underlay. De ser así, ¿contiene dicha red los elementos necesario para una red underlay (ver la sección Underlay o red subyacente mas arriba en la tesina)? ¿Caso contrario, se tiene que volver a configurar la red en un modelo de acceso de Capa 3?
- ¿Tienen los actualmente componentes la capacidad necesaria para soportar la implementación de SDA o deben incluirse plataformas adicionales?
- ¿Está la organización lista para hacer cambios en el esquema de direccionamiento IP y la gestión DHCP?
- Si planean habilitar múltiples overlays, ¿cuál es la estrategia para integrar estas redes con los servicios comunes (Internet, DNS, DHCP y las aplicaciones del centro de datos)?
- ¿Se tiene actualmente configurado SGT y dónde están los puntos de aplicación de estas políticas? Si se utilizan SGT con múltiples overlays para segmentar y virtualizar dentro del fabric, ¿qué requisitos existen para extenderlos más allá del fabric? ¿Existe una infraestructura lista para soportar Cisco TrustSec, VRF-Lite, MPLS, enrutadores de fusión u otras tecnologías necesarias para extender y admitir la segmentación y la virtualización?

- ¿Se puede actualizar la cobertura inalámbrica dentro de un dominio roaming o necesita apalancarse en estrategias *over-the-top*?

Al migrar una red existente a SDA hay dos enfoques principales. Si se van a reemplazar muchas de las plataformas existentes y si se cuenta con suficiente poder eléctrico, espacio y ventilación, entonces construir la red SDA en paralelo es una opción que permita la transición fácil de los usuarios. Construir una red paralela que esté integrada con la red existente es similar a construir una red nueva. Otro enfoque es realizar las migraciones de los equipos conmutadores de acceso al fabric de SDA en fases. Esta estrategia es apropiada para redes que cuentan con equipos que soportan SDA pero de pronto tienen algunas limitaciones físicas en los laboratorios.

Para ayudar con la migración de la red, SDA admite una configuración de borde de capa 2 temporal que se puede usar durante la fase de transición. Se debe crear una configuración de borde de capa 2 que sirva como traspaso utilizando un solo nodo de borde conectado a la red de acceso de capa 2 existente. Las VLAN's existentes se asignan a los overlays de SDA. Se puede proveer redundancia de enlaced entre el borde de Capa 2 y la red de acceso externa existente utilizando EtherChannels. La redundancia del chasis en la red de acceso existente puede usar pilas de conmutadores con StackWise también. El número de dispositivos finales admitidos en un borde de Capa 2 varía según las versiones de SDA, las versiones iniciales están limitadas a 4.000 equipos. Se deben tomar en cuenta los servicios DHCP para soportar tanto los dispositivos del fabric como los que no lo son al momento de la migración. (Cisco, 2019)

5.2.27. **El fabric para el Plano de control**

Tanto el RFC 6830 como otros definen LISP como una arquitectura de red, un conjunto de protocolos que aportan una nueva semántica para el direccionamiento y reenvío de tráfico IP. En las redes IP tradicionales, la dirección IP se usa para identificar tanto el dispositivo como su ubicación física como parte de una pertenencia en una subred en un enrutador. En una red configurada con LISP, la dirección IP o MAC fungen como identificadores de dispositivos finales; una dirección IP adicional se usa como un RLOC para representar la ubicación física de ese dispositivo (generalmente una dirección *loopback* del enrutador en el cual ese dispositivo final está conectado, con su respectiva EID). La combinación EID y RLOC brinda toda la información necesaria para el reenvío del tráfico. La dirección RLOC es parte del underlay y el EID se puede asignar independientemente de la ubicación.

La arquitectura LISP requiere un sistema de mapeo que almacene y resuelva los EID a los RLOC. Esto es similar al uso de DNS para resolver las direcciones IP a los nombres de host. Los prefijos EID (IPv4 con máscaras de 32 bits o direcciones MAC) se registran en el servidor de mapas junto con sus RLOC asociados. Cuando se envía tráfico a un EID, el RLOC de origen consulta el sistema de mapeo para identificar el RLOC de destino para la encapsulación del tráfico. Al igual que con DNS, un nodo local probablemente no tiene toda la información de una red, sino que solicita la información solo cuando los hosts locales la necesitan para comunicarse (modelo pull), y la información se almacena en caché para mayor eficiencia.

Aunque no se requiere una comprensión completa de LISP y VXLAN para implementar el fabric de SDA, es útil comprender cómo estas tecnologías respaldan los objetivos de

la implementación. Algunos de los beneficios proporcionados por la arquitectura LISP son los siguientes:

- Virtualización de red: se utiliza una ID de instancia LISP para mantener topologías VRF independientes. Desde una perspectiva de plano de datos, el ID de instancia de LISP se asigna al VNI.
- Optimización de subredes: se puede extender una única subred para que exista en múltiples RLOC. La separación de EID de RLOC permite la capacidad de extender subredes a través de diferentes RLOC. El RLOC en la arquitectura LISP se usa para encapsular el tráfico EID a través de una red de Capa 3. Como resultado de la disponibilidad de la puerta de enlace anycast en varios RLOC, la configuración del cliente EID (dirección IP, subred y puerta de enlace) puede permanecer sin cambios, incluso cuando el cliente se mueve a través de la subred extendida a diferentes puntos físicos.
- Tablas de enrutamiento más pequeñas: solo los RLOC deben ser accesibles en la tabla de enrutamiento global. Los EID locales se almacenan en caché en el nodo local, mientras que los EID remotos se aprenden a través del intercambio de tráfico. Es aprendizaje es el proceso que llena las tablas de reenvío únicamente con dispositivos finales que se comunican a través del nodo. Esto permite el uso eficiente de las tablas de reenvío.

5.3. **Redes de Banda Ancha Definidas por Software: SD-WAN**

Conforme la industria evoluciona existe una mayor demanda de tráfico por parte de los dispositivos móviles, el esquema IoT, aplicaciones SaaS y la adopción de topologías de nube. Además, las necesidades de seguridad están aumentando y las aplicaciones requieren trabajar bajo prioridades. A medida que esta complejidad crece, existe una presión constante por reducir los costos y gastos operativos mientras que la alta disponibilidad y la capacidad de crecimiento siguen siendo importantes. (Hucaby, Garza, & Edgeworth, 2019)

Las arquitecturas WAN tradicionales enfrentan grandes desafíos en este panorama. Lo anterior se debe a que estás generalmente se componen de múltiples transportes MPLS, o un MPLS acompañado con un enlace de Internet o LTE utilizados de manera activa / pasiva. La mayoría de las veces con tráfico de Internet en un esquema SaaS enviado a un centro de datos central o regional para su debido acceso a Internet. Existen varios problemas relacionados con estas arquitecturas, desde insuficiente ancho de banda, costos altos, el tiempo de inactividad de las aplicaciones críticas, bajo rendimiento de SaaS, operaciones complejas, flujos de trabajo complejos para la conectividad en la nube, largos tiempos de implementación y cambios en las políticas, visibilidad limitada de la aplicación y dificultad para asegurar la red. (Cisco SD-WAN Design Guide, 2018)

En los últimos años, las soluciones de Redes Definidas por software (SDN) aplicadas a la WAN o SD-WAN han provisto soluciones a estos desafíos. SD-WAN es un derivado de la tecnología SDN. Como se ha visto, SDN es un enfoque centralizado para la administración de redes que abstrae la infraestructura de red de underlay de

sus aplicaciones. Esta separación del plano de datos y el plano de control permite centralizar la inteligencia de la red e introducir con esto automatización, simplificación de operaciones y aprovisionamiento, monitoreo y resolución de problemas centralizados. SD-WAN aplica estos principios de SDN a la WAN.

5.3.1. **Por qué implementar SD-WAN**

La solución de Cisco SD-WAN es un overlay que habilita la transformación digital y en la nube para las empresas. Integra completamente el enrutamiento, la seguridad, el manejo de políticas centralizadas y la orquestación de las redes en gran escala. Tiene la capacidad de suministrar administración para esquemas multi-inquilino desde la nube, totalmente automatizado, seguro, escalable y además brinda analítica exhaustiva a las aplicaciones.

La tecnología SD-WAN de Cisco aborda y resuelve los problemas y desafíos de las implementaciones de WAN tradicionales. Algunos de los beneficios incluyen:

- Administración centralizada de políticas y simplicidad operativa. Lo que resulta en un mejor control de cambios y tiempos de implementación.
- Capacidad de realizar combinaciones de MPLS y banda ancha de bajo costo a través de cualquier tipo de transporte de manera activa-activa, optimizando la distribución del tráfico y reduciendo los costos de ancho de banda.
- Introduce una red tipo overlay independientemente del tipo de transporte que se use que se extiende hasta el centro de datos, sucursal o en la nube.
- Flexibilidad de implementación. Debido a la separación del plano de control y el plano de datos, los controladores se pueden implementar en el sitio físico propiamente, en

la nube, o una combinación de ambos. La colocación del enrutador Cisco vEdge puede ser física o virtual y puede implementarse en cualquier lugar de la red.

- Seguridad robusta e integral, que incluye cifrado de datos, segmentación de red de extremo a extremo, identidad de certificado de enrutador y controlador con modelo de seguridad Zero-Trust, protección del plano de control, firewall de aplicaciones e inserción de Cisco UmbrellaTM, cortafuegos y otros servicios de red.
- Conectividad optimizada y directa a la nube pública desde las sucursales.
- Visibilidad y reconocimiento de las aplicaciones y políticas para garantizar el cumplimiento en los acuerdos de niveles de servicio (SLA) en tiempo real.
- Optimización dinámica de aplicaciones SaaS, lo que resulta en rendimiento optimizado de la aplicación para los usuarios.
- Análisis exhaustivo con visibilidad de las aplicaciones y la infraestructura, brindando resolución rápida de problemas para una planificación eficaz de los recursos.

5.3.2. **Arquitectura de la solución SD-WAN**

La solución Cisco SD-WAN se compone de orquestación, administración, control y planos de datos separados.

- El plano de orquestación provee la incorporación automática de los enrutadores SD-WAN en el overlay de SD-WAN.
- El plano de gestión es responsable de la configuración central y el monitoreo.
- El plano de control construye y mantiene la topología de la red y toma decisiones sobre dónde fluye el tráfico.

- El plano de datos es responsable de reenviar los paquetes basados en las decisiones del plano de control.

En el gráfico 14 muestra una descripción general de la arquitectura de la solución SD-WAN de Cisco

Gráfico 14 Arquitectura Solución SD-WAN

Fuente: Cisco. (2018) Recuperado 10 noviembre, 2019, de https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/CVD-SD-WAN-Design-2018OCT.pdf

5.3.3. **Componentes de la solución Cisco SD-WAN**

La solución Cisco SD-WAN tiene cuatro componentes principales y un servicio de análisis opcional:

- vManage Network Management System (NMS): este es un solo panel de vidrio (GUI) para administrar la solución SD-WAN.
- Controlador vSmart: este es el cerebro de la solución.
- Enrutadores SD-WAN: SD-WAN involucra enrutadores vEdge y cEdge.

- vBond orchestrator: esto autentica y organiza la conectividad entre los enrutadores SD-WAN y los controladores vSmart.
- vAnalytics: este es un servicio opcional de análisis y aseguramiento.

5.3.4. **vManage NMS**

VManage NMS brinda un único panel para la administración de la solución de manera gráfica. Este se utiliza para configurar y administrar la solución SD-WAN completa. Permite el aprovisionamiento centralizado y facilita los cambios de red.

5.3.5. **Controlador vSmart**

Los controladores vSmart (son los cerebros de la solución SD-WAN) utilizados certificados que van previamente instalados los cuales permiten autenticar cada enrutador SD-WAN que se conecta. Estos certificados garantizan que solo los dispositivos autenticados tengan acceso a la estructura SD-WAN. Después de una autenticación exitosa, cada controlador vSmart establece un túnel DTLS permanente para cada enrutador SD-WAN en la estructura SD-WAN y usa estos túneles para establecer relaciones de OMP con cada enrutador SD-WAN. OMP es un protocolo de enrutamiento patentado similar a BGP que puede anunciar rutas, próximos saltos, claves e información de políticas necesarias para establecer y mantener la estructura SD-WAN.

El controlador vSmart procesa las rutas OMP aprendidas de los enrutadores SD-WAN (u otros controladores vSmart) para determinar la topología de la red y calcular las mejores rutas a los destinos de la red. Luego, anuncia la información de

accesibilidad obtenida de estas rutas a todos los enrutadores SD-WAN en la estructura SD-WAN.

Los controladores vSmart también implementan todas las políticas del plano de control que se crean en el vManage, como el encadenamiento de servicios, la ingeniería de tráfico y la segmentación por topología VPN. Por ejemplo, cuando se crea una política en vManage para una aplicación (como YouTube) que no requiere más del 1% de pérdida y 150 ms de latencia, esa política se descarga al controlador vSmart. vSmart convierte la política en un formato que todos los enrutadores SD-WAN de la estructura pueden comprender, e implementa automáticamente la política en todos los enrutadores SD-WAN sin la necesidad de confiar en una CLI. El controlador vSmart también funciona junto con el orquestador vBond para autenticar los dispositivos a medida que se unen a la red y para organizar la conectividad entre los enrutadores SD-WAN.

5.3.6. **Enrutadores para SD-WAN (vEdge y cEdge) de Cisco**

Los enrutadores Cisco SD-WAN ofrecen las capacidades esenciales de WAN, seguridad y multinube. Están disponibles en opciones con hardware, nube y como enrutadores virtualizados. Estos usualmente se colocan en el perímetro de un sitio, como un control remoto a oficina, sucursal, campus o centro de datos.

Los enrutadores SD-WAN admiten características estándar como OSPF, BGP, ACL, QoS y políticas de enrutamiento, además del control de superposición SD-WAN y las funciones del plano de datos. Cada enrutador SD-WAN establece automáticamente una conexión segura tipo DTLS con el controlador vSmart y establece una conexión a

través de OMP para intercambiar información de enrutamiento. También establece sesiones IPsec estándar con otros enrutadores SD-WAN en la estructura. Los enrutadores SD-WAN tienen inteligencia local para tomar decisiones locales sobre el enrutamiento, la alta disponibilidad (HA), las interfaces, la administración de ARP y las ACL. El controlador vSmart proporciona rutas remotas del sitio y la información de accesibilidad necesaria para construir la estructura SD-WAN.

Hay dos opciones diferentes de enrutadores SD-WAN en el portafolio de Cisco:

- vEdge: las plataformas originales de Viptela que ejecutan el software Viptela.
- cEdge: software Viptela integrado con Cisco IOS-XE. Este es compatible con los equipos CSR, ISR, ASR1K, ENCS y las plataformas CSRv e ISRv especiales para la nube.

La imagen SD-WAN basada en el software Cisco IOS XE no es una versión estándar de Cisco IOS XE. Es un conjunto seleccionado de características de IOS XE que se adapto para SD-WAN en la imagen de IOS XE SD-WAN. vManage permite el aprovisionamiento, la configuración y la resolución de problemas de los enrutadores SD-WAN IOS XE exactamente de la misma manera que los enrutadores vEdge.

5.3.7. **Orquestador vBond**

vBond es el orquestador de la solución que autentica los controladores vSmart y los enrutadores SD-WAN y organiza la conectividad entre ellos. Es el único dispositivo que debe tener una dirección IP pública para que todos los dispositivos SD-WAN de la red puedan conectarse. Un vBond orchestrator es un enrutador SD-WAN que solo realiza funciones de vBond orchestrator.

Los componentes principales del vBond orchestrator son:

- Conexión del plano de control: cada orquestador vBond tiene una conexión de plano de control permanente sobre un túnel DTLS con cada controlador vSmart. Además, el orquestador vBond usa conexiones DTLS para comunicarse con los enrutadores SD-WAN cuando se conectan, para autenticarlos y facilitar su capacidad de unirse a la red. La autenticación básica de un enrutador SD-WAN se realiza mediante certificados y criptografía RSA.
- Recorrido NAT: el orquestador vBond facilita la orquestación inicial entre los enrutadores SD-WAN y los controladores vSmart cuando uno o ambos están detrás de dispositivos NAT. Se utilizan técnicas estándar de igual a igual para facilitar esta orquestación.
- Equilibrio de carga: en un dominio con múltiples controladores vSmart, vBond orchestrator realiza automáticamente el equilibrio de carga de los enrutadores SD-WAN a través de los controladores vSmart cuando los enrutadores se conectan.

5.3.8. **vAnalytics**

vAnalytics es un servicio opcional de análisis y calidad de experiencia que contiene capacidades avanzadas, como las siguientes:

- Visibilidad de aplicaciones e infraestructura a través de la WAN
- Pronósticos y análisis hipotéticos
- Recomendaciones inteligentes

Estas capacidades pueden aportar beneficios a SD-WAN que no son posibles desde la consola regular. Por ejemplo, si una sucursal está experimentando latencia o pérdida en su enlace MPLS, vAnalytics lo detecta y compara esa pérdida o latencia con información sobre otras organizaciones en el área que también está monitoreando para ver si también están teniendo esa misma pérdida y latencia en sus circuitos. Si lo son, vAnalytics puede informar el problema a los proveedores de servicio. vAnalytics también puede ayudar a predecir cuánto ancho de banda se requiere realmente para cualquier ubicación, y esto es útil para decidir si un circuito puede reducirse a un ancho de banda menor para reducir costos.

Entre los componentes SD-WAN, los enrutadores SD-WAN y el orquestador vBond están disponibles como equipos físicos y máquinas virtuales, mientras que vManage y vSmart solo están disponibles como máquinas virtuales.

Todas las máquinas virtuales, incluidos los enrutadores en la nube CSRv, ISRv y vEdge, se pueden alojar localmente utilizando ESXi o KVM, o se pueden alojar en AWS y Microsoft Azure.

5.3.9. **Cisco SD-WAN Cloud OnRamp**

Cómo se comentada al inicio de la sección de SD-WAN, las arquitecturas WAN tradicionales no fueron diseñadas para los esquemas de nube. A medida que las organizaciones adoptan más aplicaciones como servicio, por ejemplo Office 365 e infraestructuras de nube pública como AWS o Microsoft Azure, la infraestructura de red actual experimenta problemas importantes relacionados con el nivel de complejidad, seguridad y la experiencia del usuario final. (Hucaby, Garza, & Edgeworth, 2019)

La solución Cisco SD-WAN incluye un conjunto de funcionalidades que abordan el acceso óptimo a las aplicaciones en la nube y la conectividad a esquemas de infraestructura como servicio o IaaS. Este funcionalidad se llama Cloud *OnRamp*. Cloud OnRamp ofrece la mejor calidad de experiencia de aplicación para aplicaciones SaaS al monitorear continuamente el rendimiento de las mismas a través de diversas rutas y seleccionar la que cuenta con mejor rendimiento en función de las métricas importantes para el negocio (fluctuación, pérdidas y retrasos). Además, simplifica la conectividad de la nube híbrida y la nube múltiple de IaaS al extender la estructura de datos de SD-WAN a la nube pública y al mismo tiempo aumenta la alta disponibilidad y capacidad de crecimiento.

5.3.10. **Cloud OnRamp para software como servicio**

Las aplicaciones que funcionan bajo un esquema de Software como Servicio residen principalmente en Internet, y para poder lograr un rendimiento óptimo de estas, se debe seleccionar el punto de salida de Internet con mejor rendimiento. (Hucaby, Garza, & Edgeworth, 2019)

Si se tiene un sitio remoto con dos circuitos de acceso directo a Internet hacia dos proveedores de servicio diferentes con Cloud OnRamp configurado para priorizar las aplicaciones SaaS desde el vManage, el enrutador de SD-WAN en el sitio remoto comienza envia paquetes tipo sondas a través de HTTP a través de ambos circuitos para medir la latencia y la pérdida. Según los resultados, el enrutador de SD-WAN sabrá qué circuito funciona mejor y envía el tráfico de la aplicación en cuestión a través del circuito con mejor desempeño. El proceso de sondeo continúa, y si se produce un

cambio en las características de rendimiento del circuito, el enrutador de SD-WAN del en el sitio remoto toma las decisiones de reenvío adecuadas.

5.3.11. **Cloud OnRamp para infraestructura como servicio**

El esquema multinube es la tendencia que esta dominando las empresas. Con multinube, ciertas flujos de tráfico permanecen dentro de los límites de los centros de datos privados, mientras que otras se alojan en entornos de nube pública, como AWS y Microsoft Azure. Este enfoque proporciona a las empresas mayor flexibilidad en el consumo de infraestructura informática como servicio, donde haga sentido. (Hucaby, Garza, & Edgeworth, 2019)

Con la solución Cisco SD-WAN, la conectividad desde cualquier punto, la seguridad bajo un esquema de cero confianza, la segmentación de extremo a extremo y las políticas de QoS conscientes de las aplicaciones en tiempo real, se pueden extender a los entornos IaaS mediante el uso de enrutadores en la nube SD-WAN. Adicionalmente brinda la capacidad de utilizar cualquier tipo de transporte. SD-WAN permite el uso de una variedad de métodos de conectividad al extender de manera segura la estructura de datos de SD-WAN en el entorno de la nube pública a través de cualquier red de transporte subyacente. Estos pueden ser Internet, MPLS, 3G / 4G LTE, satélite y circuitos dedicados como el DX de AWS y el ER de Microsoft Azure.

5.3.12. **Protocolo de gestión Overlay (OMP) de SD-WAN**

El protocolo de enrutamiento OMP que gestiona la red de overlay en SD-WAN, es muy similar a BGP. El protocolo corre entre los controladores vSmart y los enrutadores vEdge donde la información del plano de control, como prefijos de ruta, rutas de próximo salto, claves criptográficas e información de políticas, se intercambia a través de una conexión segura DTLS o TLS. El controlador vSmart se parece mucho a un reflector de rutas; recibe rutas de enrutadores vEdge, procesa y aplica cualquier política a estas, y luego las anuncia a otros enrutadores vEdge en la red overlay. Si no hay una política definida, el comportamiento predeterminado es una topología de malla completa, donde cada vEdge puede conectarse directamente a un vEdge en otro sitio y recibir información absoluta del enrutamiento de cada sitio. (2018). Cisco SD-WAN Design Guide

OMP anuncia tres tipos de rutas:

- Las rutas OMP son prefijos que se aprenden del sitio local, o del lado del servicio, de un enrutador vEdge. Los prefijos se originan como rutas estáticas o conectadas, o desde el protocolo OSPF o BGP, y se redistribuyen en OMP para que puedan transportarse a través del overlay. Las rutas OMP comparten atributos como la ubicación de transporte (TLOC), que es similar a una dirección IP de siguiente salto de BGP para la ruta y otros atributos como el origen, fuente, preferencia, ID de sitio, etiquetas y VPN. Una ruta OMP solo se instala en la tabla de reenvío si el TLOC al que apunta está activo.

- Las rutas TLOC son los puntos de terminación del túnel lógico en los enrutadores vEdge que se conectan a una red de transporte. Una ruta TLOC se identifica de manera única y se representa mediante una tupla de tres campos que consiste en la dirección IP del sistema, el color del enlace y la encapsulación (GRE o IPSec). Además las rutas TLOC también llevan atributos como las direcciones IP privadas y públicas de cada TLOC, operador, preferencia, ID de sitio, etiqueta y pesos. Para que un TLOC se considere en estado activo en un vEdge particular, se debe asociar una sesión BFD activa con su respectivo vEdge TLOC.
- Las rutas de servicio (firewall, IPS, optimización de aplicaciones, etc.) representan servicios que están conectadas a la red local donde se encuentra el vEdge y están disponibles para otros sitios realizando la respectiva inserción de estos. Además, estas rutas también incluyen VPN; las etiquetas de VPN se envían en este tipo de actualización para indicar a los controladores vSmart qué VPN’s reciben servicio en un sitio remoto. (Unicast Overlay Routing Overview , 2016)

5.3.13. **Redes privadas virtuales (VPN)**

En el overlay de SD-WAN, las VPN proporcionan segmentación, al igual que las instancias de VRF con las que ya estamos familiarizados. Cada VPN está aislada entre sí y cada una tiene su propia tabla de reenvío. Una interfaz o subinterfaz se configura explícitamente en una sola VPN y no puede formar parte de mas de una. Las etiquetas se utilizan en los atributos de ruta OMP y en la encapsulación de paquetes que identifica la VPN a la que pertenece.

El número de VPN es un entero de cuatro bytes con un valor de 0 a 65530. Hay dos VPN presentes de forma predeterminada en los dispositivos y controladores vEdge, VPN 0 y VPN 512.

- VPN 0 es la VPN de transporte. Contiene las interfaces que se conectan a los transportes WAN. Las conexiones DTLS / TLS seguras a vSmart o entre los controladores vSmart y vBond se inician desde esta VPN. Las rutas estáticas o predeterminadas o un protocolo de enrutamiento dinámico deben configurarse dentro de esta VPN para obtener información adecuada del siguiente salto para que se pueda establecer el plano de control y los túneles IPSec puedan conectarse a sitios remotos.
- VPN 512 es la VPN de gestión. Transporta el tráfico de administración por un canal aparte y desde los equipos SD-WAN. Esta VPN no se transporta a través de la red overlay.

Además de las VPN predeterminadas, es necesario crear una o más VPN’s del lado del servicio que contendrán interfaces que se conectarán a la red del sitio local y transportarán el tráfico de datos del usuario. Estas VPN se pueden habilitar para funciones como OSPF o BGP, VRRP, QoS, modelado de tráfico o vigilancia. El tráfico de usuarios se puede dirigir a través de los túneles IPSec a otros sitios redistribuyendo las rutas OMP recibidas de los controladores vSmart en el sitio en el protocolo de enrutamiento VPN del lado del servicio. A su vez, las rutas desde el sitio local pueden anunciarse a otros sitios al publicar las rutas VPN del servicio en el protocolo de enrutamiento OMP, que se enviará a los controladores vSmart y se redistribuirá a los otros enrutadores vEdge en la red.

5.3.14. **Colocación del vEdge en el Overlay**

Para colocar vEdge en el overlay se necesita establecer una conexión segura con el vManage y pueda recibir la configuración. Adicionalmente se debe establecer una conexión segura con el controlador vSmart para que pueda participar en el overlay. El descubrimiento del vManage y vSmart ocurre automáticamente, pero primero debe establecerse una conexión segura con el orquestador vBond.

En el gráfico 15 muestra la secuencia de eventos que ocurre al llevar el vEdge al overlay:

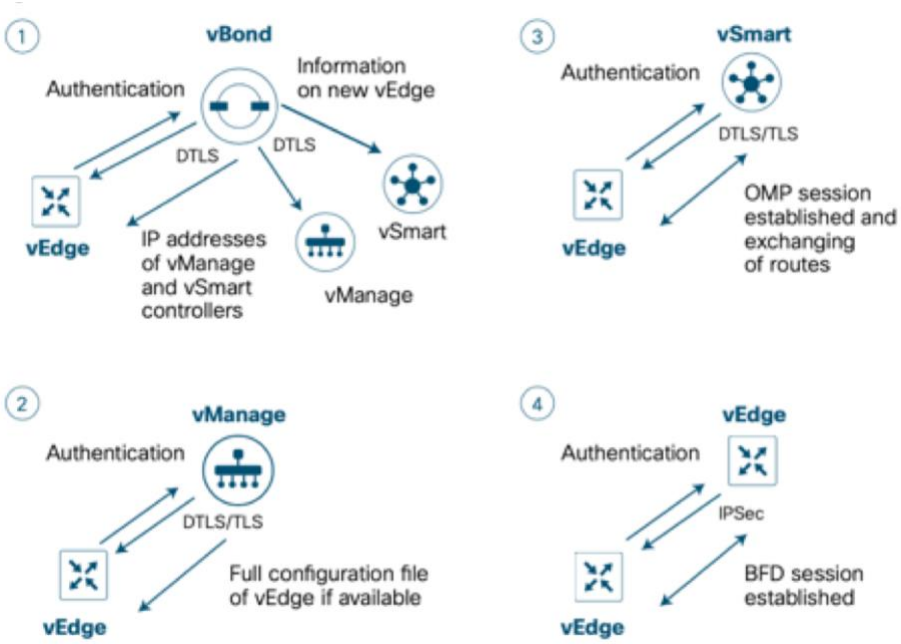


Gráfico 15 Secuencia de eventos en la incorporación del vEdge

Fuente: Cisco. (2018b). Recuperado 10 noviembre, 2019, de https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/CVD-SD-WAN-Design-2018OCT.pdf

- Luego que el equipo levanta mediante el proceso ZTP, el vEdge primero intentará autenticarse con el orquestador vBond a través de una conexión DTLS encriptada. Una vez autenticado, el vBond envía al vEdge las direcciones IP del vManage y vSmart. El vBond también informa al vSmart y vManage del nuevo vEdge que desea unirse al dominio.
- El vEdge comienza a establecer sesiones DTLS o TLS seguras con el vManage y los controladores vSmart y deshace la sesión con el vBond. Una vez que el vEdge se autentica con el vManage, el vManage envía la configuración completa al vEdge si está disponible.
- El vEdge intenta establecer conexiones DTLS / TLS con los vSmart a través de cada enlace de transporte. Cuando se autentica en un vSmart, establecerá una sesión OMP y luego aprenderá las rutas, incluidos los prefijos, los TLOC y las rutas de servicio, las llaves de cifrado y las políticas.
- El vEdge intentará establecer un túnel IPSec para los TLOC en cada transporte. Un TLOC en un color de transporte privado intenta conectarse a los TLOC en colores públicos y privados, y un TLOC en un color público intenta conectarse a otros TLOC en colores públicos de forma predeterminada. La llave de encriptación en el túnel solo construirá túneles entre TLOC del mismo color. Una vez vinculados, BFD correrá sobre las conexiones establecidas. (Cisco SD-WAN Getting Started Guide , 2020)

5.3.15. **Inicialización del enrutador vEdge**

La inicialización del vEdge ocurre automáticamente. Con el método de configuración bootstrap, la idea es configurar lo mínimo de identificación en el equipo solamente la

dirección IP o el nombre de host del vBond. El vEdge intentará conectarse al vBond y descubrirá los otros controladores de red desde allí. Para que el vEdge sea activado, se debe tomar en cuenta lo siguiente:

- Configure una dirección IP y una dirección de puerta de enlace en una interfaz conectada a la red o configure DHCP para obtener las direcciones dinámicamente. El vEdge debe tener conectividad hacia el vBond a través de la red.
- Configure la dirección IP o el nombre de host del vBond. El vEdge necesita poder localizar el servidor DNS para resolver. Para ello, configure una dirección de servidor DNS en VPN 0.
- Configure el nombre de la organización, la dirección IP del sistema y la identificación del sitio. Opcionalmente, configure el nombre del host.

5.3.16. **Proceso de aprovisionamiento ZTP**

ZTP es un procedimiento de aprovisionamiento automático que comienza cuando el vEdge se enciende por primera vez. VEdge intentará conectarse a un servidor ZTP con el nombre de host ztp.viptela.com, donde obtendrá la información del orquestador vBond. Una vez que se obtiene la información del orquestador vBond, posteriormente puede realizar conexiones a los controladores vManage y vSmart para obtener su configuración completa y unirse al overlay.

Existen algunos requisitos para el aprovisionamiento de ZTP. En los equipos vEdge solo algunos puertos están preconfigurados para ser una interfaz cliente DHCP y usarse para ZTP. Los siguientes deben conectarse a la red para que ZTP funcione:

- El gateway del vEdge en la red debe tener acceso a los servidores DNS públicos y poder llegar al controlador de Viptela.
- El vManage, debe tener una plantilla de configuración del dispositivo para el vEdge conectado al dispositivo vEdge.
- La dirección IP del equipo y la ID del sitio deben incluirse en esta plantilla para que el proceso funcione. (Cisco SD-WAN Design Guide, 2018)

5.3.17. **Plantillas de configuración**

Las configuraciones y políticas se aplican a los vEdge y los controladores vSmart que permiten que el tráfico fluya entre el centro de datos y las sucursales. Se pueden habilitar configuraciones y políticas a través del CLI, SSH o de forma remota a través de la interfaz gráfica del vManage.

Para configurar un dispositivo o controlador vEdge en la red utilizando la GUI del vManage, se debe aplicar una plantilla al vEdge. Estas plantillas pueden estar basadas en CLI o en funciones. Se pueden crear plantillas basadas en CLI, sin embargo se recomienda utilizar plantillas basadas en características porque son modulares, más escalables y menos propensas a errores. Cada plantilla está compuesta por varias características que describen las configuraciones de interfaz, túnel y el comportamiento de enrutamiento local.

5.3.18. **Plantillas de dispositivos**

Las plantillas de dispositivo son específicas para un modelo de vEdge, pero es posible crear varias plantillas del mismo tipo y modelo según su ubicación y función en

la red. Cada plantilla hace referencia a una serie de características que conforman toda la configuración del equipo. Una plantilla de equipo no se puede compartir entre varios modelos de vEdge, pero una plantilla de funciones puede utilizarse en varios modelos. (2018). Cisco SD-WAN Design Guide

La siguiente imagen ilustra los componentes de una plantilla de dispositivo. La plantilla del dispositivo está compuesta por plantillas de funciones agrupadas según las siguientes secciones:

- Información básica plantillas de sistema, registro, AAA, OMP, BFD, seguridad, archivo y NTP.
- VPN de transporte y administración: incluye las plantillas utilizadas para configurar VPN 0 y VPN 512, BGP, OSPF, interfaz VPN, VPN celular, VPN GRE y plantillas de funciones de interfaz VPN PPP.
- VPN de servicio: incluye las plantillas utilizadas para configurar las VPN de servicio, BGP, IGMP, Multicast, OSPF, PIM, interfaz VPN, puente de interfaz VPN, interfaz VPN GRE, interfaz VPN IPSec, interfaz VPN Natpool y DHCP.
- Plantillas adicionales: incluye avisos de sistema, SNMP, políticas localizadas y plantillas de funciones celulares.

5.3.19. **Plantillas de funciones**

A continuación se incluye una breve descripción de algunas de las diferentes plantillas de funciones y una breve descripción que cada una le permitirá configurar.

- Sistema: configura la información básica del sistema, ID del sitio, IP del sistema, zona horaria, nombre de host, los grupos de dispositivos, las coordenadas GPS y puertos.
- Registro: configura el registro en el disco y/o en un servidor de registro remoto.
- AAA: especifica el método y orden de autenticación, configuración de Radius, TACACS o autenticación local, incluidos los grupos de usuarios locales con diferentes permisos de lectura o escritura.
- BFD: especifica el multiplicador de rutas BFD y el intervalo de sondeo así como el mensaje saludo y BFD para cada transporte.
- OMP: cambia los tiempos de reinicio, anuncios y retención del equipo; ajusta la cantidad de rutas anunciadas; configura el número de AS para el overlay; elige qué protocolos locales se anunciarán en OMP y cambia la cantidad de rutas de igual costo instaladas en el enrutador vEdge.
- Seguridad: cambia el tiempo de generación de llaves, la ventana anti-repetición y los tipos de autenticación para IPSec.
- Archivo (opcional): archiva la configuración completa en ejecución en un servidor de archivos dentro de un período de tiempo especificado.
- NTP (opcional): configura los servidores de NTP y autenticación si es necesario.
- VPN: cambia el tiempo de entrega en los paquetes ECMP, agrega servidores DNS, anuncia protocolos (BGP, estáticos, conectados, externos OSPF) de la VPN a OMP y agrega rutas estáticas IPv4 o v6, rutas de servicio y rutas GRE.

- BGP (opcional): configura el número AS, ID de enrutador, distancia, rutas máximas, vecinos, redistribución de protocolos en BGP, tiempo de espera y temporizadores de mantenimiento.
- OSPF (opcional): configure la ID del enrutador, distancia, áreas, interfaces OSPF, ancho de banda de referencia, origen de la información predeterminada, métricas, tipo de métrica y los temporizadores SPF.
- Configuración de la interfaz VPN: configura el nombre de interfaz, estado de la misma, direcciones IPv4 y v6 estáticas o dinámicas, DHCP, NAT, VRRP, QoS, ACL para IPv4 y 6, vigilancia,ARP, 802.1x, dúplex, dirección MAC, IP (MTU), tamaño de segmento máximo del protocolo de control de transmisión (TCP MSS), extensión TLOC y más. En el caso de la VPN de transporte, configura el túnel, el color de transporte, los protocolos permitidos para la interfaz, encapsulación, preferencias, peso y más.
- Puente de interfaz VPN (opcional): configura las características de la capa 3 de una interfaz de puente, incluida la dirección IPv4, DHCP, ACL, VRRP, MTU y TCP MSS.
- Servidor DHCP (opcional): configura las características del servidor DHCP, como el grupo de direcciones, tiempo de concesión, concesiones estáticas, nombre de dominio, puerta de enlace predeterminada, servidores DNS y los servidores TFTP.
- Banner (opcional): configura el banner de inicio de sesión o el banner del mensaje del día.
- Política (opcional): adjunta una política localizada.

- SNMP (opcional): configura los parámetros de SNMP, incluidos el nombre y la ubicación del dispositivo SNMP, versión, las vistas y las comunidades de SNMP y los grupos de captura.
- Puente (opcional): define las características de capa 2 de un puente, incluida la ID de VLAN, el envejecimiento de la dirección MAC, las direcciones MAC máximas y las interfaces físicas para el puente. Las plantillas de protocolo de enrutamiento, como BGP u OSPF, y las plantillas de interfaz VPN se configuran bajo una VPN. Las plantillas de funciones del servidor DHCP se configuran bajo una interfaz VPN.

5.3.20. **Configuración de parámetros**

vManage es la consola para configurar plantillas de dispositivos y funciones, especificando variables donde sea necesario ya que las plantillas pueden aplicarse a múltiples dispositivos vEdge que tienen configuraciones únicas. (2018). Cisco SD-WAN Design Guide

Al configurar valores de parámetros dentro de las plantillas de funciones, a menudo se desplegara un cuadro que brinda tres tipos diferentes de valores:

- Global: cuando especifica un valor global, se aplicará a todos los dispositivos a los que se aplique la plantilla.
- Específico del dispositivo: cuando especifica un valor específico del dispositivo, el valor de esta variable se aplicará a la plantilla del dispositivo.
- Predeterminado: cuando especifica un valor predeterminado, se aplicará el valor a todos los dispositivos relacionados a esa plantilla.

5.3.21. **Políticas**

Las políticas son una parte importante de la solución SD-WAN de Cisco y se utilizan para influir en el flujo del tráfico de datos entre los enrutadores vEdge en la red overlay. Las políticas se aplican tanto al plano de control como al tráfico del plano de datos y se configuran centralmente en los controladores vSmart (política centralizada) o localmente (política localizada) en los enrutadores vEdge.

Las políticas de control centralizado operan en la información de enrutamiento y TLOC y permiten personalizar las decisiones de enrutamiento y determinar las rutas de enrutamiento a través de la red overlay. Estas políticas se pueden usar para configurar la ingeniería de tráfico, afinidad de rutas, inserción de servicios y los diferentes tipos de topologías VPN (malla completa, concentrador y radio, malla regional, etc.). Otra política de control centralizado es el enrutamiento consciente de la aplicación, que selecciona la ruta óptima en función de las características de rendimiento de ruta en tiempo real para diferentes tipos de tráfico. Las políticas de control localizado le permiten afectar la política de enrutamiento en un sitio local, específicamente a través de mapas de rutas OSPF o BGP y listas de prefijos.

Las políticas de datos influyen en el flujo de tráfico de datos a través de la red en función de los campos en los encabezados de paquetes IP y grupo de VPN. Las políticas de datos centralizadas se pueden usar para configurar firewalls de aplicaciones, encadenamiento de servicios, ingeniería de tráfico, calidad de servicio (QoS) y Cflowd. Las políticas de datos localizadas le permiten configurar cómo se maneja el tráfico de datos en un sitio específico, como ACL, QoS, reenvío por monitoreo y vigilancia. Algunas políticas de datos centralizadas pueden afectar el

manejo en el vEdge, como en el caso de las políticas de ruta de aplicaciones o una política de clasificación de QoS. En estos casos, la configuración aún se descarga directamente a los controladores vSmart, pero cualquier información de política que deba transmitirse a los enrutadores vEdge se comunica a través de OMP. (Configuring Localized Data Policy for IPv4, 2016)

5.3.22. **Planificación de la implementación**

Es importante planificar cuidadosamente las implementaciones de SD-WAN para facilitar la configuración, operaciones diarias y el mantenimiento. Las siguientes son algunas consideraciones:

5.3.22.1. **Numeración de puertos**

Se recomienda tener un esquema de numeración de puertos que sea consistente en toda la red. La consistencia ayuda a facilitar la configuración y la resolución de problemas.

Además, la configuración predeterminada de fábrica de un enrutador vEdge especifica ciertos puertos en VPN 0 para DHCP para que vEdge pueda obtener automáticamente una dirección DHCP, resolver DNS y comunicarse con el servidor ZTP. Por lo tanto, si utiliza ZTP, asegúrese de que este puerto tenga acceso a los servidores DHCP y DNS al conectarlos al lugar más apropiado de la red.

5.3.22.2. **IP del sistema**

System IP es una dirección IPv4 persistente a nivel de sistema que identifica de forma exclusiva el dispositivo independientemente de las direcciones de la interfaz. Actúa como una ID de enrutador, por lo que no es necesario que se anuncie o se conozca en el underlay. Sin embargo, una mejor práctica es anunciar esta dirección IP del sistema en el servicio VPN y usarla como una dirección IP de origen para SNMP y registro, lo que facilita la correlación de los eventos de red con la información de vManage. Es necesario configurar una dirección IP del sistema para que los controladores autentiquen un enrutador vEdge y lo traigan a la red overlay.

Se recomienda un esquema lógico para las direcciones IP de sistema para que los sitios sean más fácilmente reconocibles.

5.3.22.3. **Identificación del sitio**

Una ID de sitio es un identificador único de un sitio en la red overlay de SD-WAN con un valor numérico del 1 al 4294967295. Esta ID debe ser la misma para todos los dispositivos vEdge que residen en el mismo sitio. Un sitio podría ser un centro de datos, una sucursal, un campus o algo similar. Es necesario configurar un ID de sitio para que los enrutadores puedan autenticar un enrutador vEdge y llevarlo a la red overlay. De manera predeterminada, los túneles IPSec no se forman entre enrutadores vEdge dentro del mismo sitio.

Se debe elegir cuidadosamente un esquema de identificación del sitio, ya que esto facilita la aplicación de la política. Cuando aplica la política, aplica la política a una lista o rango de ID de sitios (ej. 100,200-299), y no hay soporte de comodines.

Aunque hay varias formas diferentes de organizar un esquema de ID de sitio, la siguiente tabla proporciona un ejemplo de un esquema que usa nueve dígitos. (Cisco SD-WAN Design Guide, 2018)

La agrupación de acuerdo con la geografía es útil en los casos en que desee preferir un centro de datos regional sobre otro para el acceso centralizado a Internet o para la conectividad a centros en otros países y regiones.

Los tipos de sitio deben crearse de acuerdo con los tipos de políticas aplicadas para facilitar la aplicación de la política.

Cuando se crea un nuevo sitio, con solo crear una ID que se encuentre dentro del rango automáticamente hará que la política se aplique a él. Algunos ejemplos de cómo es posible agrupar sucursales según su categoría son los siguientes:

- Sucursales que usan un firewall ubicado en el centro u otro servicio ubicado en el centro
- Sucursales que usan acceso directo a Internet
- Según ancho de banda y topologías. Los sitios de ancho de banda bajo podrían usar una topología de concentrador y radio para ahorrar ancho de banda, mientras que los sitios de mayor ancho de banda usan una topología de malla completa.
- Diferentes requisitos de SLA y transporte, MPLS para tráfico crítico, voz y video. Todo lo demás a través del circuito de Internet, y quizás algunos sitios que usan MPLS solo para voz. Se puede tener tipos superpuestos, pero la idea es ponerlos en categorías que faciliten la aplicación de políticas desde una perspectiva de configuración. Es útil pensar en los requisitos y políticas requeridos antes de asignar ID de sitio.

5.3.22.4. **Dimensionamiento de la solución Cisco SD-WAN**

El dimensionamiento de la solución de SD-WAN consta de 2 pasos: determinar el nivel de licenciamiento y la selección de los equipos.

El licenciamiento de SD-WAN (premisas o nube) se maneja en subscripciones con periodos de 3 años en adelante. Se puede seleccionar el tipo de licencia según las funciones que se necesiten. Cada licencia habilita las siguientes capacidades:

- Cisco DNA Essentials, habilita conectividad básica, SD-WAN, seguridad y visibilidad de aplicaciones.
- Cisco DNA Advantage brinda conectividad flexible, SD-WAN y seguridad avanzados, y calidad de servicio en aplicaciones orientado a políticas.
- Cisco DNA Premier brinda SD-WAN y seguridad avanzados, administración de aplicaciones por políticas , analítica de red y optimización de WAN.

Una vez seleccionado el nivel de licenciamiento se procede a a determinar el equipo necesario para cada sede y sitio central. Las siguientes preguntas orientan el proceso:

- ¿Cuentan actualmente con routers de la familia ISR, ASR o ISR G2 desplegados?
- ¿Se requieren políticas de SLA dinámicas, segmentación, circuitos diversos o características más profundas?
- ¿Se está utilizando múltiples tipos de servicios en la nube como 0365, AWS?
- ¿Necesita cumplir con los requisitos reglamentarios y de cumplimiento de estas herramientas?

- ¿Requieren un dispositivo SD-WAN para terminar conexiones físicas de Ethernet, LTE, T1 o DSL?
- ¿Existe algún requisito de segmentación y seguridad de extremo a extremo a través de la WAN?
- ¿Cuentan con algún requerimiento de implementar topologías dinámicas por VPN? ¿cuántas?
- ¿Existe algún requerimiento de que la solución pueda determinar automáticamente la mejor ruta a las aplicaciones SaaS a través de las rutas overlay de Internet y VPN?
- ¿Necesita una solución que descubra automáticamente las cargas de trabajo en la nube y aprovisione dinámicamente los túneles entre ellos?

Una vez capturada la información anterior, se debe proceder a llenar la siguiente tabla para realizar la relación uno a uno de los sitios y velocidades para terminar de determinar los equipos.

Tabla 11 Dimensionamiento de solución SD-WAN

Site	Tipo de transporte	Mbps	# of devices	Device model
Sitio central				
Sucursal 1				
Sucursal 2				
Sucursal N				
DC 1				
Cloud on Ramp				

Si el cliente cuenta con mas de un tipo de transporte por sitio, entonces se debe incluir dos columnas adicionales a la tabla (tipo de transporte y Mbps) para especificar cada proveedor que tiene. (Cisco DNA Software for SD-WAN and Routing, 2020)

El ancho de banda seleccionado por el cliente es la suma total de todos los enlaces entrantes y salientes. Para cada enrutador se elige el ancho de banda.
Una vez determinado el equipo y el ancho de banda requerido se puede seleccionar el dispositivo y licencias adecuados.

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Cada hito tecnológico que la sociedad ha alcanzado, se acompaña de una curva de adopción la cual no solo retrasa el acceso a los beneficios tecnológicos, sino a los procesos y habilitadores comerciales, los cambios culturales y las oportunidades profesionales y empresariales que para la sociedad supone.

En un mundo cada vez mas globalizado y digital, la capacidad de impactar positivamente a través de la innovación tecnológica, es una responsabilidad invisible que recae sobre los hombros de la ingeniería.

La presente tesis tuvo como objetivo proveer un plan de capacitación que permite a los grupos de preventa técnicos realizar un análisis concienzudo del estado de madurez tecnológico y situación actual de sus clientes, con miras a la implementación de tecnologías SDN en la región de Latinoamérica. Esto quiere decir que, el abordaje del proceso de venta debe evolucionar para adquirir tanto habilidades consultivas, como una comprensión de los orígenes, beneficios y disparadores comerciales de las tecnologías SDN, de cara a la implementación de los proyectos.

Para realizar esto, primero se realizo un análisis de la situación actual de los grupos de preventa técnicos. Se pudo observar que el nivel de las capacidades ingenieriles de los grupos en cuestión en lo que a las tecnologías SDN se refiere, es bajo. Ante este escenario, se concluye que es necesaria la implementación de un plan de capacitación tecnológica rápido, eficiente, que concientice acerca de la oportunidad de mercado que

supone, pero que también sea replicable y accesible de manera ubicua, por los grupos de interés en la organización.

La implementación del programa de capacitación en los grupos de preventa técnica, tuvo un impacto tanto a nivel de los objetivos organizacionales que supone para Cisco; puntualmente, la penetración del mercado. Así también para la región latinoamericana en lo que se refiere a una preparación, para los cambios fortísimos que se avecinan en la industria.

En relación con los resultados de la encuesta aplicada a los grupos de preventa técnica y al nivel de penetración de las tecnologías SDN de Cisco en el territorio, se concluye que existe un desbalance en el conocimiento fundamental de la soluciones. Lo anterior queda demostrado a partir de los hallazgos encontrados en las encuestas, los cuales translucen que un 40% del grupo no está familiarizado con las tecnologías SDN de Cisco; por otra parte solo el 20% conoce el alcance funcional de las mismas. Además, un 60% del grupo se percibe incapaz de demostrar el valor integral de las tecnologías SDN de Cisco en sus interacciones con los clientes.

En virtud de lo anterior, se puede concluir que la capacitación no debe limitarse solamente al conocimiento de las tecnologías SDN propias de Cisco, sino que se debe ampliar y propiciar una base de comprensión de los estándares, los beneficios y los factores detrás del impulso de las tecnologías SDN en la industria. Esto les permitirá detectar la oportunidad, la solución adecuada y comentar el valor de las tecnologías SDN de Cisco.

Como se afirmo anteriormente, existe un desbalance generalizado en el mercado en lo que respecta al conocimiento de las tecnologías SDN de Cisco en la región. Lo dicho hasta aquí pone en perspectiva barreras que impiden la adopción de las tecnologías SDN en el mercado. Así mismo los estudios recopilados de las firmas Gartner, Gallup y Forbes evidencian que el mercado de la región latinoamericana experimenta un reto principal de cara a la adopción de tecnologías SDN: su estado de inmadurez tecnológico.

Por lo anterior se concluye que, el desconocimiento de las soluciones infunde dilaciones innecesarias que impiden la penetración y la adopción de las tecnologías SDN de Cisco del mercado como se espera.

Asociado al desconocimiento de las soluciones se encuentran riesgos percibidos por parte de los clientes. Las inquietudes relacionadas al tema, giran en torno a: las necesidades puntuales que ameritan la inclusión de tecnologías SDN en la compañía. Por otra parte, se evalúa muy de cerca, cuáles sean los beneficios o facilidades que las soluciones aportan, qué es lo que realmente pueden lograr o cómo podría impactar la empresa la colocación de las tecnologías SDN. Estas barreras intelectuales propician una extensión innecesaria del ciclo de ventas, el cual a su vez impacta las metas organizacionales y el desarrollo tecnológico de la región latinoamericana.

Dado el impacto de la digitalización y la presencia de colaboradores en distintos países de la región la capacitación se brindará en un formato 100% digital, seguro y en nube a través de la plataforma Cisco WebEx. El material está colocado en la nube y el acceso al mismo puede realizarse en cualquier momento y lugar.

Como resultado de lo anterior, se concluye que el trabajo de fondo, la evangelización y capacitación de la tecnología, tanto en la industria como con los grupos de preventa técnica y ventas, resultan fundamentales para la comprensión de los beneficios tangibles e intangibles que las tecnologías SDN aportan y por consiguiente la adopción de las mismas en la región.

Adicionalmente, en vista del resultado de las evaluaciones de los grupos de preventa técnicos y el estado de condición del mercado en lo que a las tecnologías SDN se refiere, se concluye que la implementación del plan de capacitación tecnológica de las tecnologías SDN, brinda las bases necesarias para que los grupos de preventa técnicos de Cisco puedan articular el valor de las soluciones, alcanzar el mercado de la región y propiciar la adopción de las mismas.

Lo anterior tendrá un impacto además en el crecimiento de la región en los próximos momentos tecnológicos que la digitalización supone.

En conclusión, la capacitación en las tecnologías SDN permitirá reducir los riesgos y retos percibidos por parte del mercado. Al mismo tiempo brinda las herramientas necesarias para cubrir las áreas de capacitación identificadas a partir de los vacíos de conocimiento de los equipos de preventa técnicos de Cisco registradas y abordadas a partir de la metodología ADDIE en la sección 2.3.5.3.6 ‘Contenidos, Áreas de Fortalecimiento y Objetivos de Aprendizaje’. Para garantizar el éxito del plan de capacitación, se realizará un taller en vivo con el grupo implicado en el cual se validara el alcance y los resultados de la misma.

La capacitación les permitirá comprender el estado actual del cliente y desde esa perspectiva, ejercer un rol consultivo que les faculte comunicar los beneficios, así como seleccionar las soluciones y equipos puntuales para el posterior dimensionamiento de las tecnologías de SDN de Cisco en el mercado.

Recomendaciones

El desarrollo de este proyecto implicó la exposición a diferentes campos del saber adicional a la ingeniería para conducirlo con éxito. Por tanto, mis recomendaciones se apoyan en tres ejes: académico de cara a la universidad, metodológico en lo que a la investigación se refiere y práctico pensando en los casos de uso de la tecnología a nivel país.

Lo anterior como una preparación de cara a la inclusión de tecnologías emergentes como 5G, la inteligencia artificial y el aprendizaje automatizado, las cuales tienen un acople fundamental en los mecanismos de SDN. Como región, minimizaremos el desempleo tecnológico y estaremos mejor posicionados para la apertura de nuevas fuentes de empleo, oportunidades comerciales y el emprendedurismo estratégico, -que a su vez demandan la comprensión de las tecnologías SDN- para maximizar el aprovechamiento y colocación de los recursos donde se requiere.

La fase inicial de evaluación de los grupos de preventa técnicos con respecto al alcance y penetración de las tecnologías SDN, requirió profundizar criterios en torno a la conducción de proyectos, la creación de contenido digital de calidad, así como la conducción y entrega de capacitaciones en formato digital.

Lo anterior desde una perspectiva docente cumpliendo con los objetivos de aprendizaje definidos. Esto es algo que no se encuentra necesariamente dentro del perfil de un ingeniero. Por esta razón, mi recomendación académica se encuentra dentro de la visión de la ingeniería en un mundo cada vez mas digitalizado; donde las ideas fluyen con rapidez y la comunicación efectiva es altamente deseable. Es necesario que los

ingenieros sean capacitados para capacitar y comunicarse asertivamente. Que sepan articular el valor de una solución tecnológica a cada uno de los diferentes interlocutores en una audiencia particular, adhiriéndose a metodologías de enseñanza validadas como lo fue ADDIE en este proyecto. Considero importante fortalecer las materias que hagan énfasis en las áreas de la comunicación y desarrollo de capacitaciones. Metodologías como Design Thinking, estrategia corporativa y ADDIE podrían resultar muy útiles en el arsenal del ingeniero de hoy.

El impacto de las tecnologías SDN en la economía de las corporaciones es evidente. Lo mismo ocurre a mayor escala con los países. Tiene la capacidad de maximizar sus recursos y la masificación de servicios. Por tanto, la recomendación práctica referente a las tecnologías SDN, es para que a nivel país se hagan análisis de condición con miras a la inclusión de las tecnologías SDN desde los proveedores de servicio, gobierno, universidades, entre otros que faculten la comprensión de la tecnología y la adopción de la misma. Conviene realizar estudios de viabilidad, de impacto, de riesgo y económicos que permitan hacer proyecciones de los beneficios a mediano y largo plazo ante una eventual implementación -o ausencia- de SDN en la región.
Por la experiencia, trayectoria, casos de éxito e integración con otras tecnologías dominantes, se recomienda contar con Cisco como fabricante y aliado tecnológico en la asesoría e implementación de dichas tecnologías.

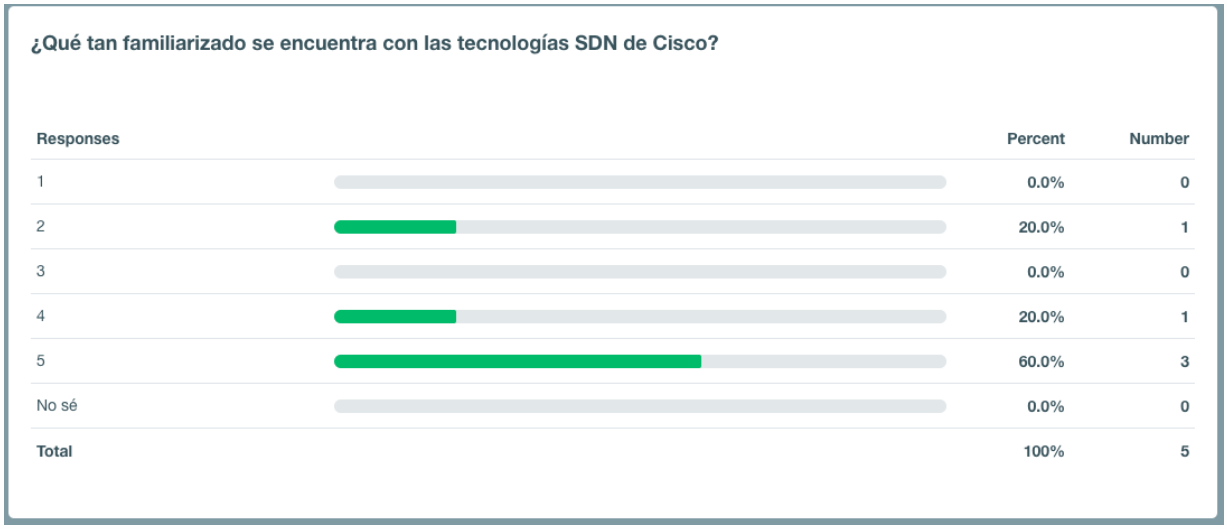
A nivel de recomendación en cuanto a herramientas para la entrega de clases en formatos 100 digitales, es altamente sugerido seguir utilizando Cisco Webex para

realizar la implementación de las capacitaciones ya que esta cumple a cabalidad con los estándares de seguridad mas alto a nivel de protección de la información privada y propiedad intelectual de sus participantes.

El físico y matemático británico William Thomson dijo lo siguiente “Lo que no se define no se puede medir. Lo que no se mide, no se puede mejorar. Lo que no se mejora, se degrada siempre”. Dado que el cambio en los ambientes tecnológicos es la norma, la recomendación metodológica para este proyecto plantea una revisión constante. Se recomienda revisar esta capacitación al inicio de cada cuatrimestre para contemplar las mejoras tecnológicas de la mano con la evolución de las tendencias en la industria y los particulares del mercado para cada vertical. Por otra parte, se considera apropiado incluir estudios FODA y comparativos de las soluciones de SDN de Cisco contra la de otros fabricantes para contrastar los resultados, beneficios y desventajas de cada uno.

CAPÍTULO VII ANEXOS

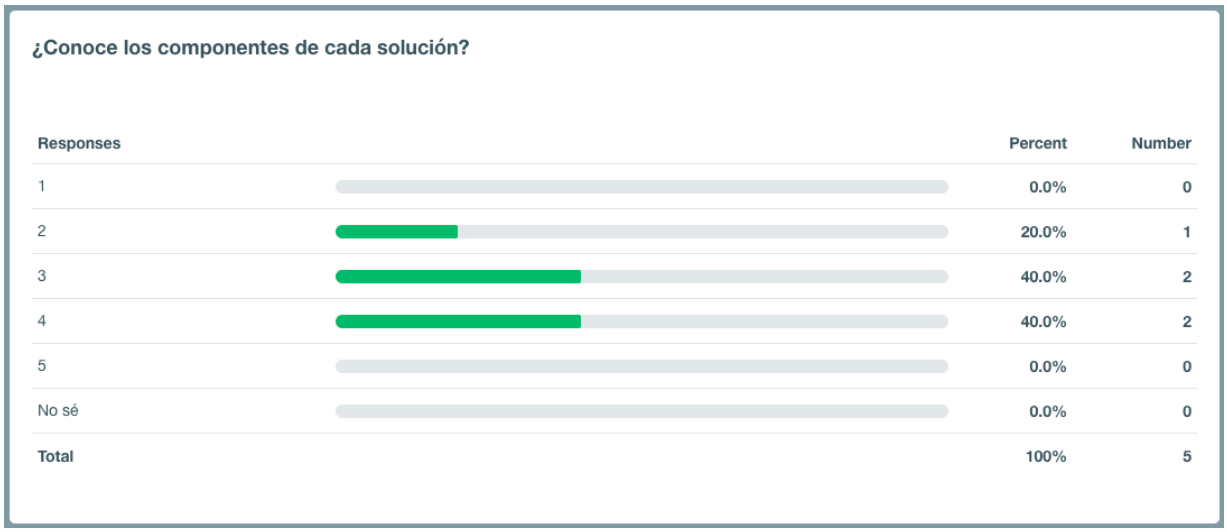
ANEXO A. SECUENCIA DE ENTREVISTAS



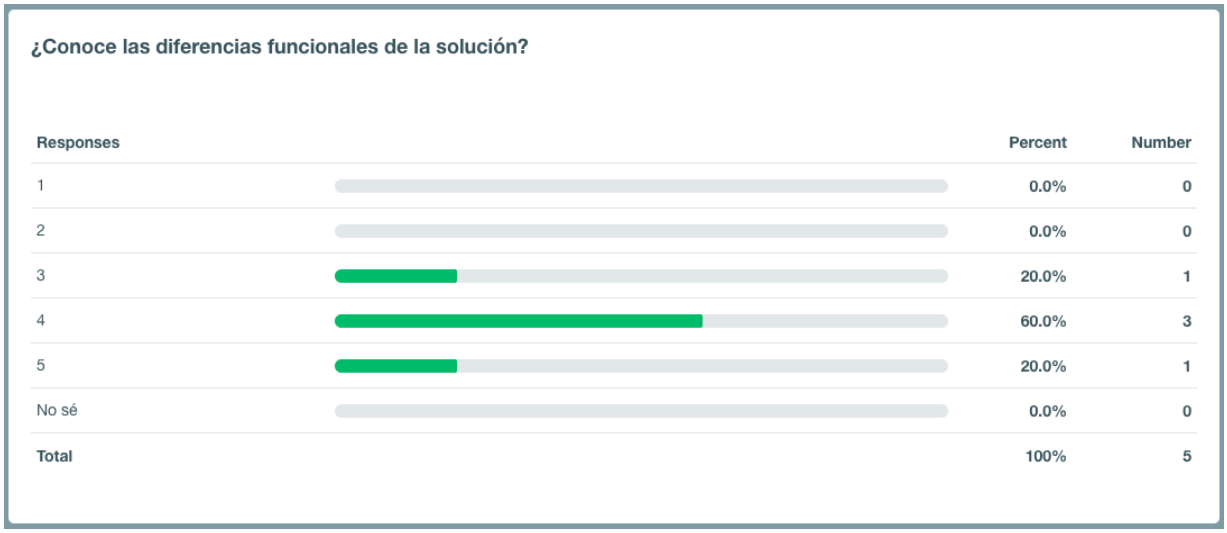
¿Qué tan familiarizado se encuentra con las tecnologías SDN de Cisco?

Responses	Percent	Number
1	0.0%	0
2	20.0%	1
3	0.0%	0
4	20.0%	1
5	60.0%	3
No sé	0.0%	0
Total	100%	5

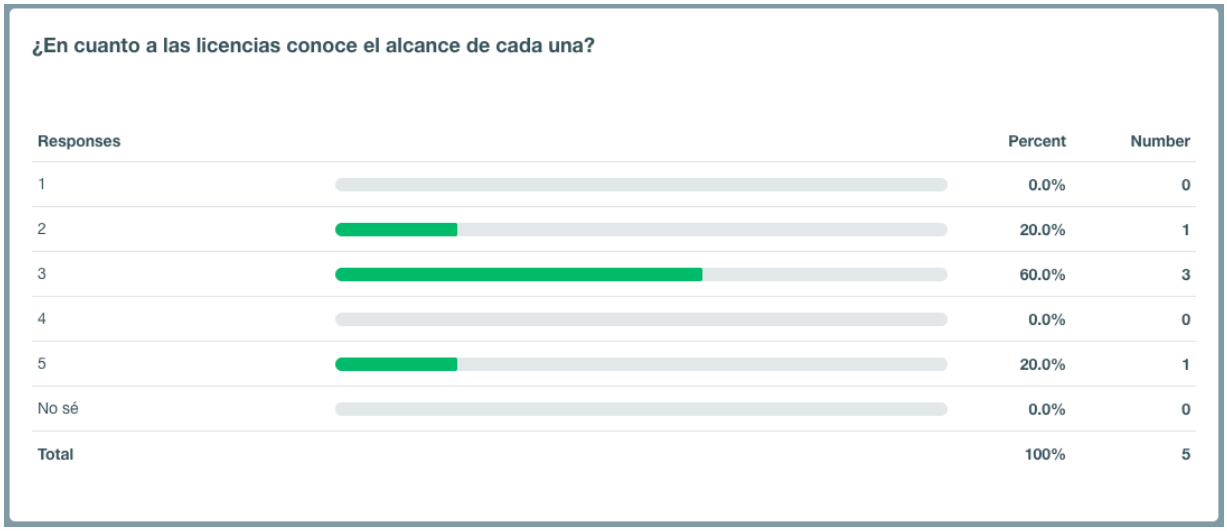
Encuesta Grupos de Preventa Técnico. Resultados Pregunta 1.0
Elaboración propia



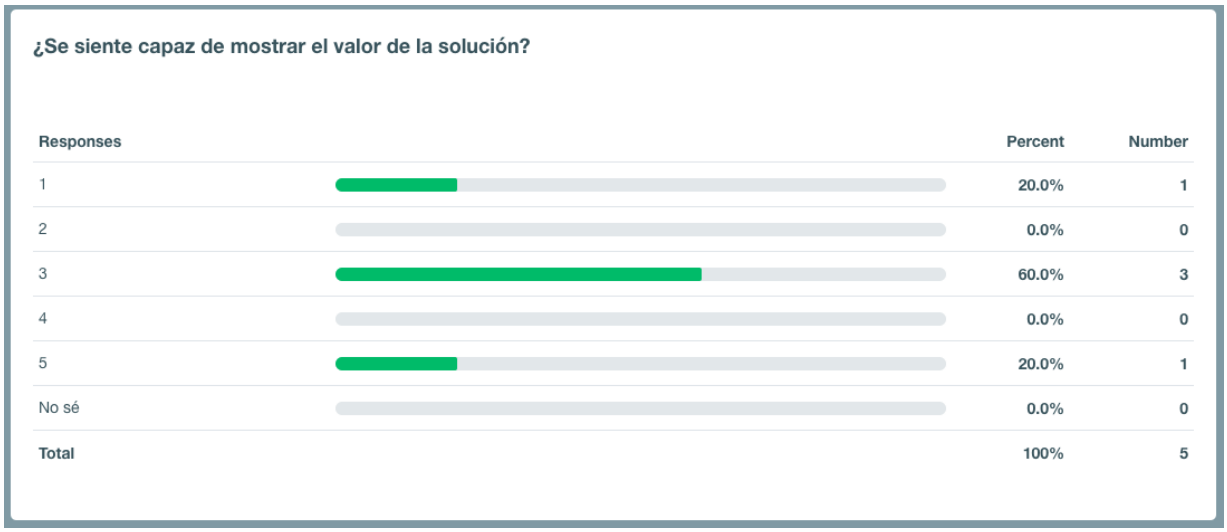
Encuesta Grupos de Preventa Técnico. Resultados Pregunta 2.0
Elaboración propia



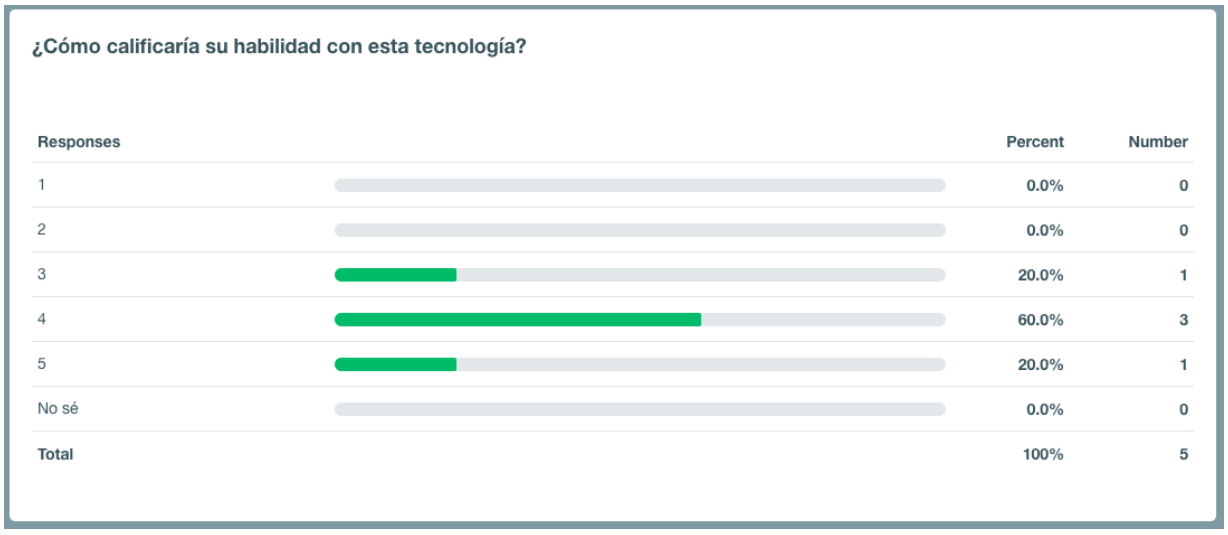
Encuesta Grupos de Preventa Técnico. Resultados Pregunta 3.0
Elaboración propia



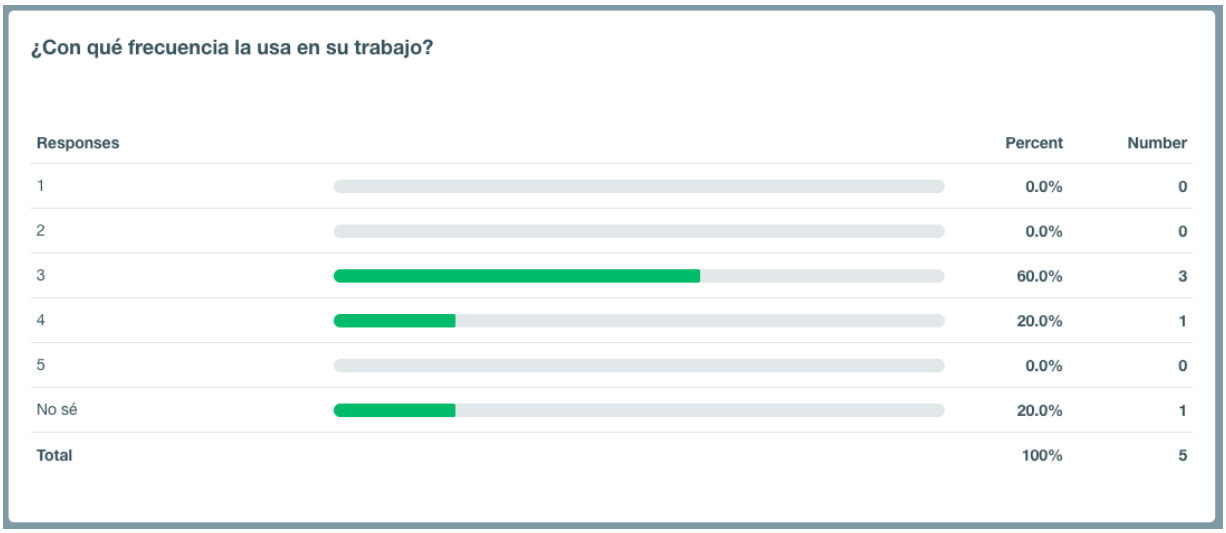
Encuesta Grupos de Preventa Técnico. Resultados Pregunta 4.0
Elaboración propia



Encuesta Grupos de Preventa Técnico. Resultados Pregunta 5.0
Elaboración propia



Encuesta Grupos de Preventa Técnico. Resultados Pregunta 6.0
Elaboración propia



Encuesta Grupos de Preventa Técnico. Resultados Pregunta 7.0
Elaboración propia

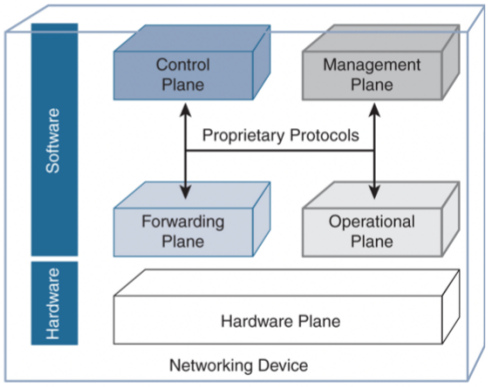
ANEXO B. CAPTURAS DE PANTALLA DE LA CAPACITACIÓN - DIA 1


cisco
Capacitación SDN Día 1
Mas allá de nuestro horizonte
Gustavo Aguilar
Ingeniero en Sistemas
Abril 2020

El paradigma de la red tal como la conocemos

…

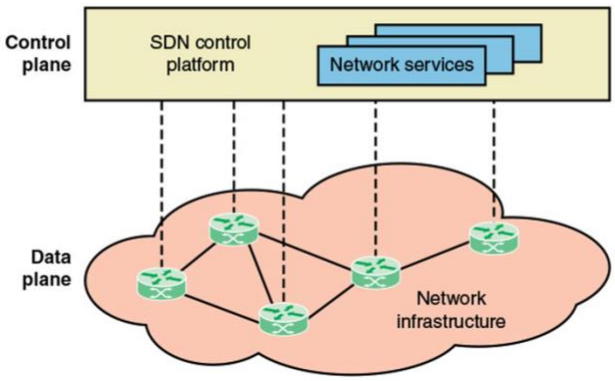
El plano de control y datos reside dentro del dispositivo físico




SDN en
Latinoamérica
Forbes
Gartner
GALLUP

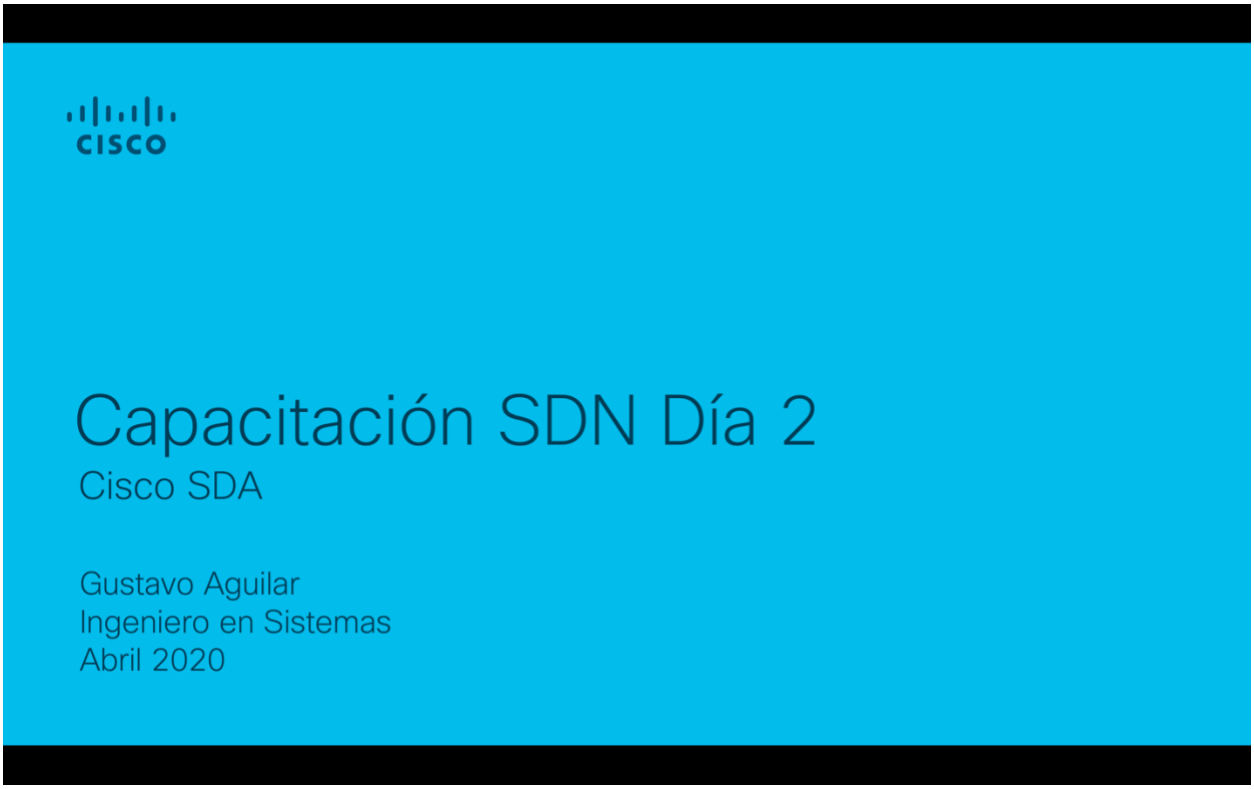
¿Qué es SDN?

SDN, un poco de historia



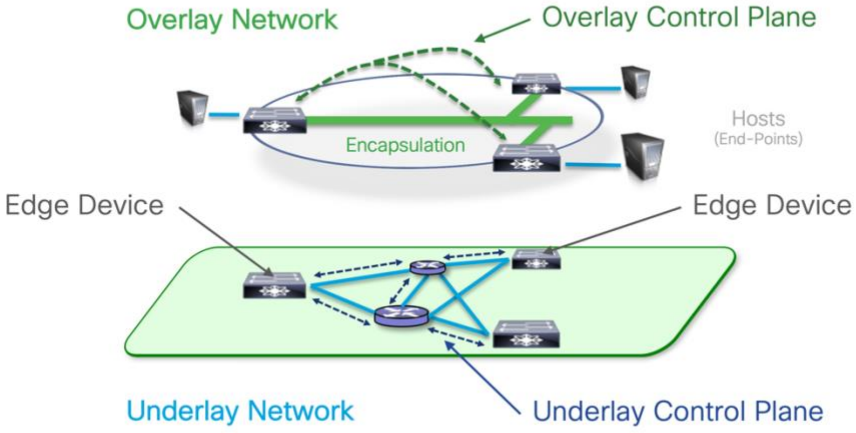
Planos de Control y Datos en redes tradicionales

ANEXO C. CAPTURAS DE PANTALLA DE LA CAPACITACIÓN - DIA 2


cisco
Capacitación SDN Día 2
Cisco SDA
Gustavo Aguilar
Ingeniero en Sistemas
Abril 2020

SD-Access

Fabric Terminology



La Arquitectura SDA

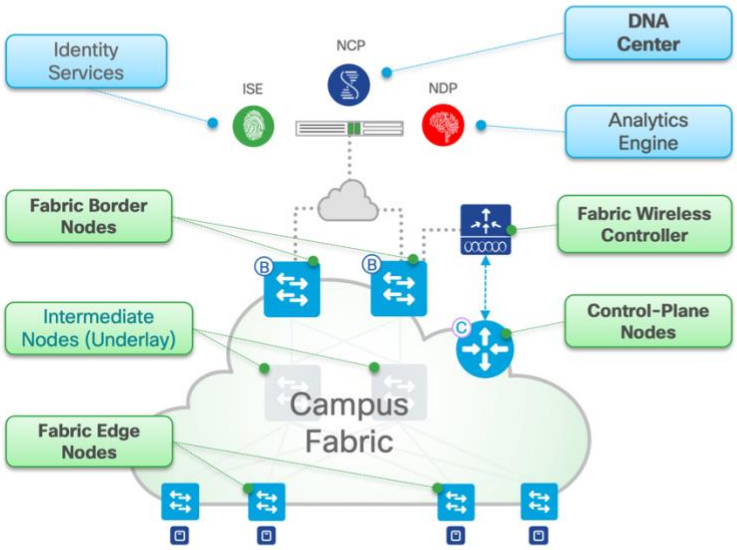
SD-Access Fabric

Fabric Terminology

- "Control-Plane Node" ≈ "LISP Map-Server"
- "Edge Node" ≈ "LISP XTR + Endpoints"
- "Border Node" ≈ "PXTR" + "LISP XTR + Subnets"
- "Intermediate Node" ≈ "Non-LISP IP Forwarder"

SD-Access

Fabric Roles & Terminology

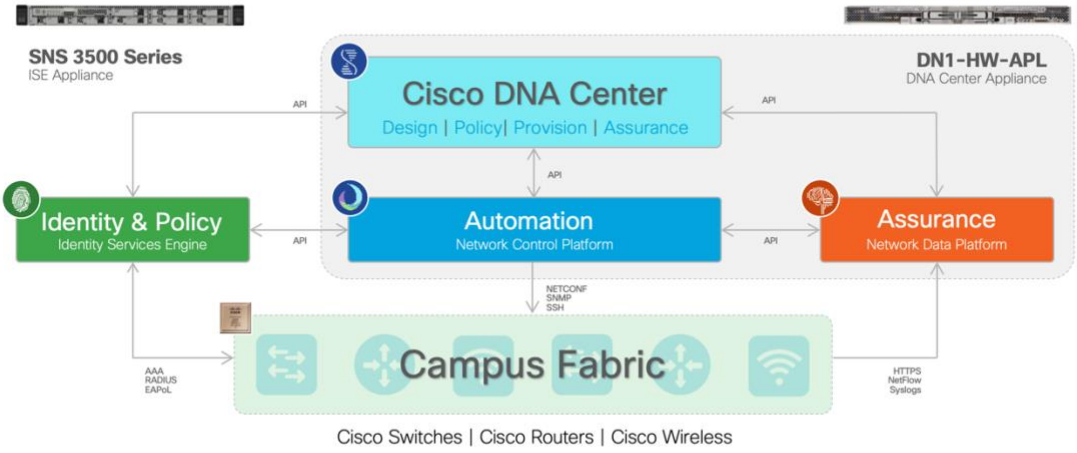


- **DNA Center** – provides simple GUI management and intent based automation (e.g. NCP) and context sharing
- **Identity Services** – NAC & ID Systems (e.g. ISE) for dynamic Endpoint to Group mapping and Policy definition
- **Analytics Engine** – Data Collectors (e.g. NDP) analyze Endpoint to App flows and monitor fabric status
- **Control-Plane Nodes** – Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** – A Fabric device (e.g. Core) that connects External L3 network(s) to the SDA Fabric
- **Fabric Edge Nodes** – A Fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SDA Fabric
- **Fabric Wireless Controller** – A Fabric device (WLC) that connects APs and Wireless Endpoints to the SDA Fabric

Enterprise Networks

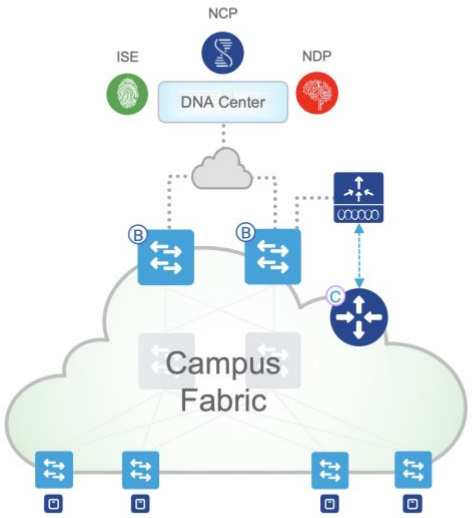
SD-Access

DNA Center – Service Components



What is SD-Access?

Campus Fabric + DNA Center (Automation & Assurance)



- **SD-Access**
  - GUI approach provides automation & assurance of all Fabric configuration, management and group-based policy
  - DNA Center integrates multiple systems, to orchestrate your LAN, Wireless LAN and WAN access
- **Campus Fabric**
  - CLI or API approach to build a LISP + VXLAN + CTS Fabric overlay for your enterprise Campus networks
  - CLI provides backwards compatibility but management is box-by-box. API provides device automation via NETCONF/YANG
  - Separated management systems

Modelos de Sitios Referenciales para Redes SDA

Sitios muy pequeños

Criterios dimensionamiento	Valores
Dispositivos finales, proyecte menos de:	2,000
Nodos Fabric, máximo	1
Nodos de plano de control	1
Nodos de borde	1
Redes virtuales, calcular menos de	8
Grupos de direcciones IP menos de	8
Puntos de Acceso, menos de	100

Sitios pequeños

Criterios dimensionamiento	Valores
Dispositivos finales, proyecte menos de:	10,000
Nodos Fabric, máximo	25
Nodos de plano de control	2
Nodos de borde	2
Redes virtuales, calcular menos de	32
Grupos de direcciones IP menos de	100
Puntos de Acceso, menos de	200

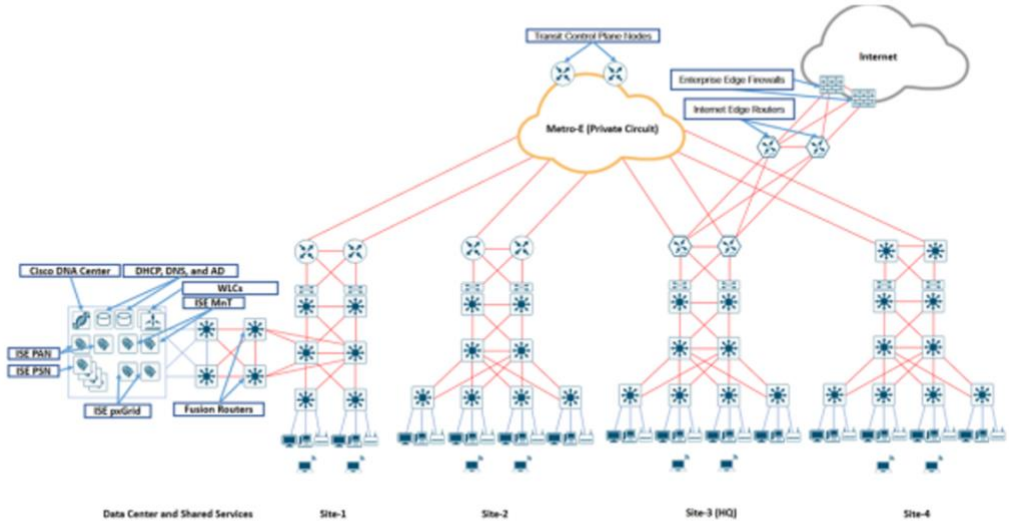
Sitios medianos

Criterios dimensionamiento	Valores
Dispositivos finales, proyecte menos de:	25,000
Nodos Fabric, máximo	250
Nodos de plano de control	2-4
Nodos de borde	2
Redes virtuales, calcular menos de	64
Grupos de direcciones IP menos de	300
Puntos de Acceso, menos de	1000

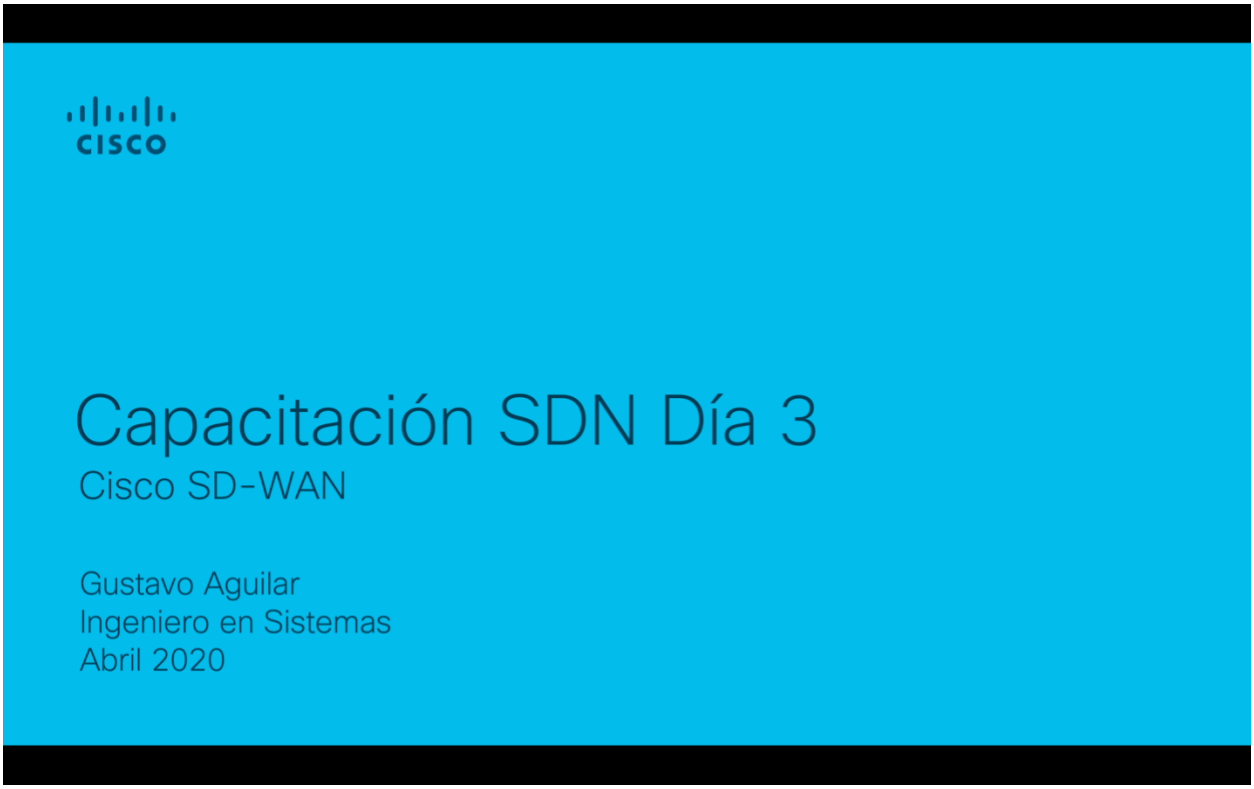
Sitios grandes

Criterios dimensionamiento	Valores
Dispositivos finales, proyecte menos de:	50,000
Nodos Fabric, máximo	1,000
Nodos de plano de control	2-6
Nodos de borde	2-4
Redes virtuales, calcular menos de	64
Grupos de direcciones IP menos de	500
Puntos de Acceso, menos de	2,000

Sitios distruibuidos

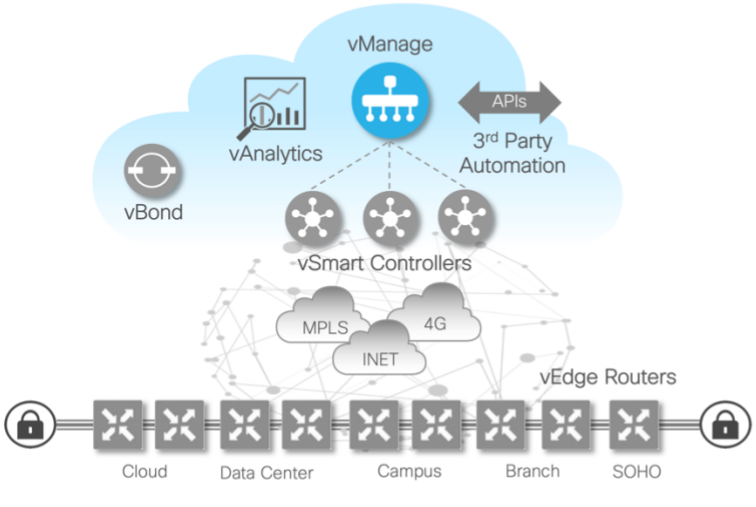


ANEXO D. CAPTURAS DE PANTALLA DE LA CAPACITACIÓN - DIA 3


cisco
Capacitación SDN Día 3
Cisco SD-WAN
Gustavo Aguilar
Ingeniero en Sistemas
Abril 2020

Por qué implementar SD-WAN

Cisco SD-WAN Solution Elements
Management Plane



Management Plane

Cisco vManage

Cisco SD-WAN Cloud OnRamp

SD-WAN Platforms

Branch virtualization

ENCS 5100

- Up to 250Mbps

ENCS 5400

- 250Mbps – 2GB

Public Cloud

Microsoft Azure

amazon web services

SD-WAN

vEdge 100

- 100 Mbps
- 4G LTE & Wireless

vEdge 1000

- Up to 1 Gbps
- Fixed

vEdge 2000

- 10 Gbps
- Modular

Branch Services

ISR 1000

- 200 Mbps
- Next-gen connectivity
- Performance flexibility

ISR 4000

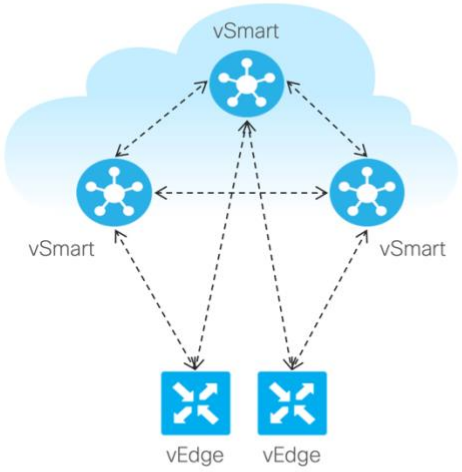
- Up to 2 Gbps
- Modular
- Integrated service containers
- Compute with UCS E

ASR 1000

- 2.5-200Gbps
- High-performance service w/hardware assist
- Hardware & software redundancy

Overlay Management Protocol (OMP)

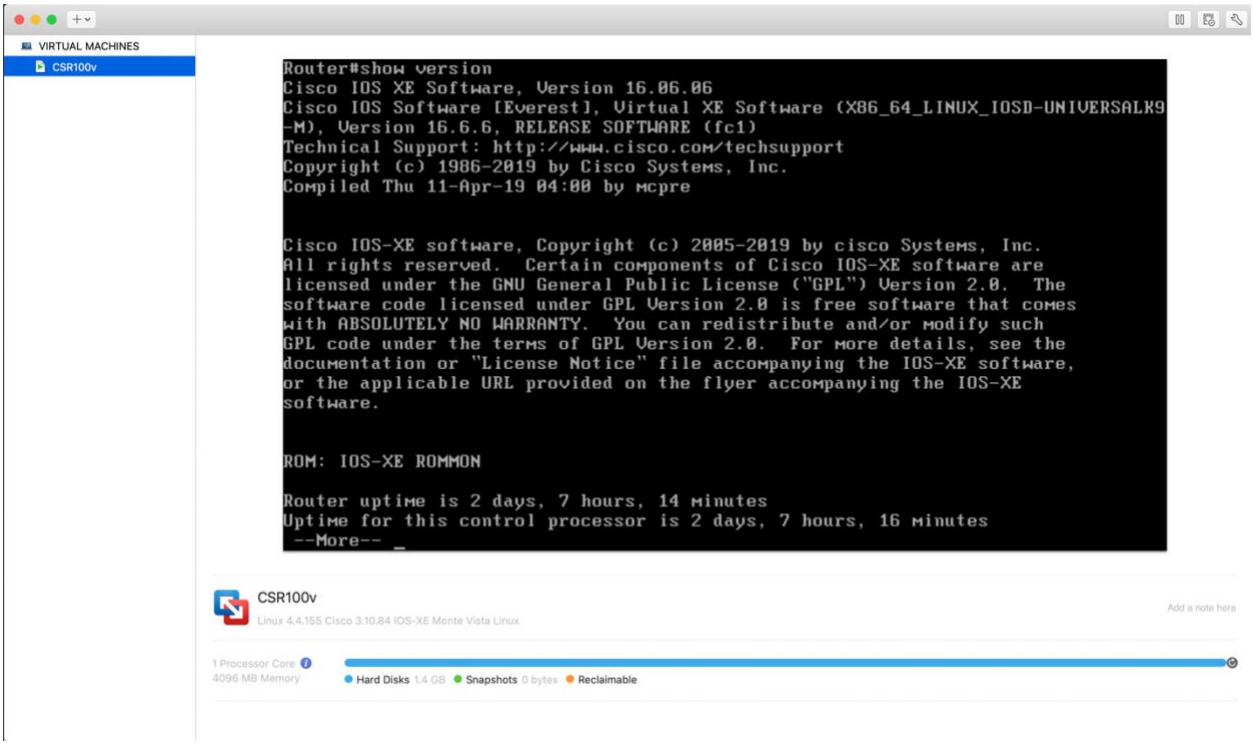
Unified Control Plane

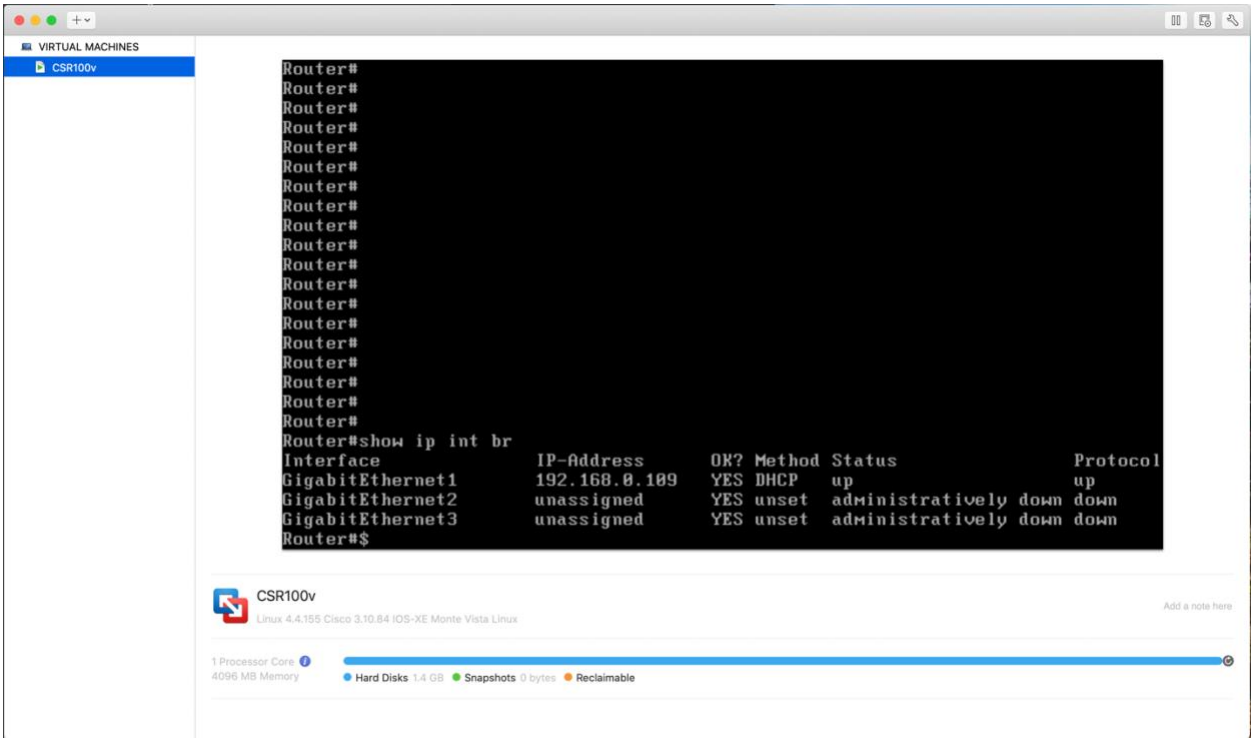


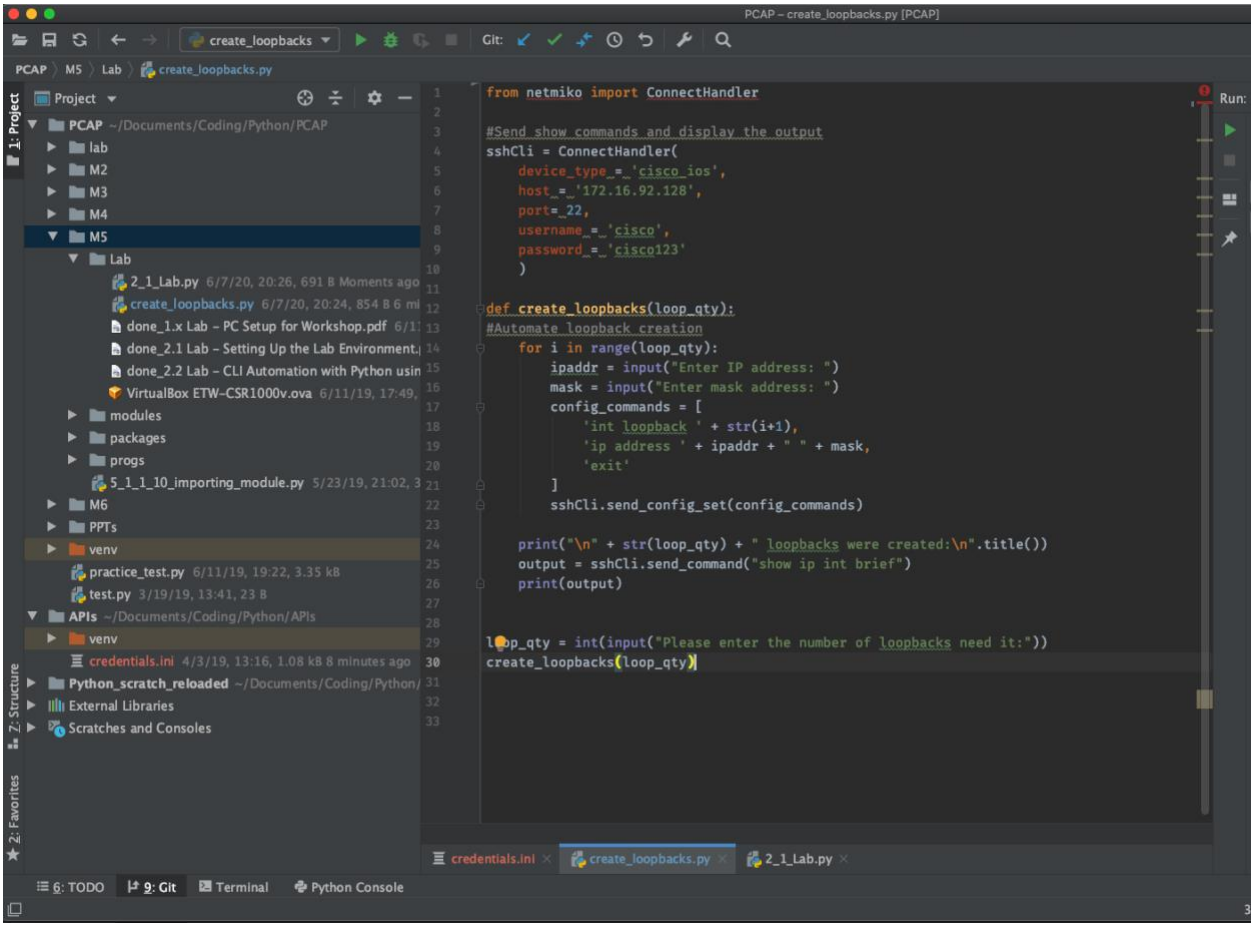
Note: vEdge routers need not connect to all vSmart Controllers

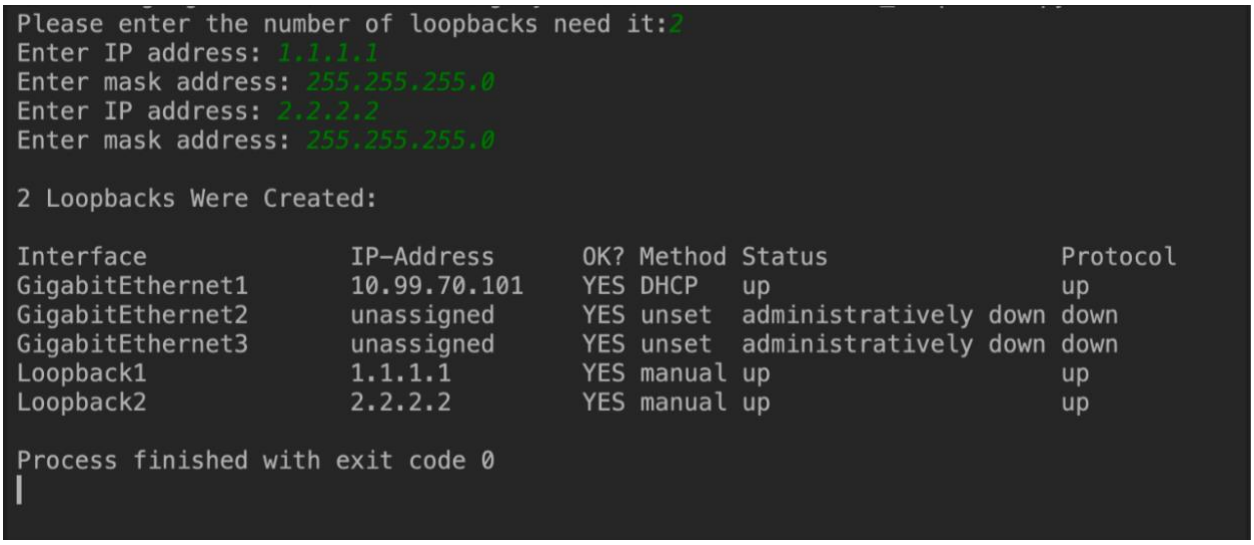
- TCP based extensible control plane protocol
- Runs between vEdge routers and vSmart controllers and between the vSmart controllers
  - Inside TLS/DTLS connections
- Advertises control plane context
- Dramatically lowers control plane complexity and raises overall solution scale

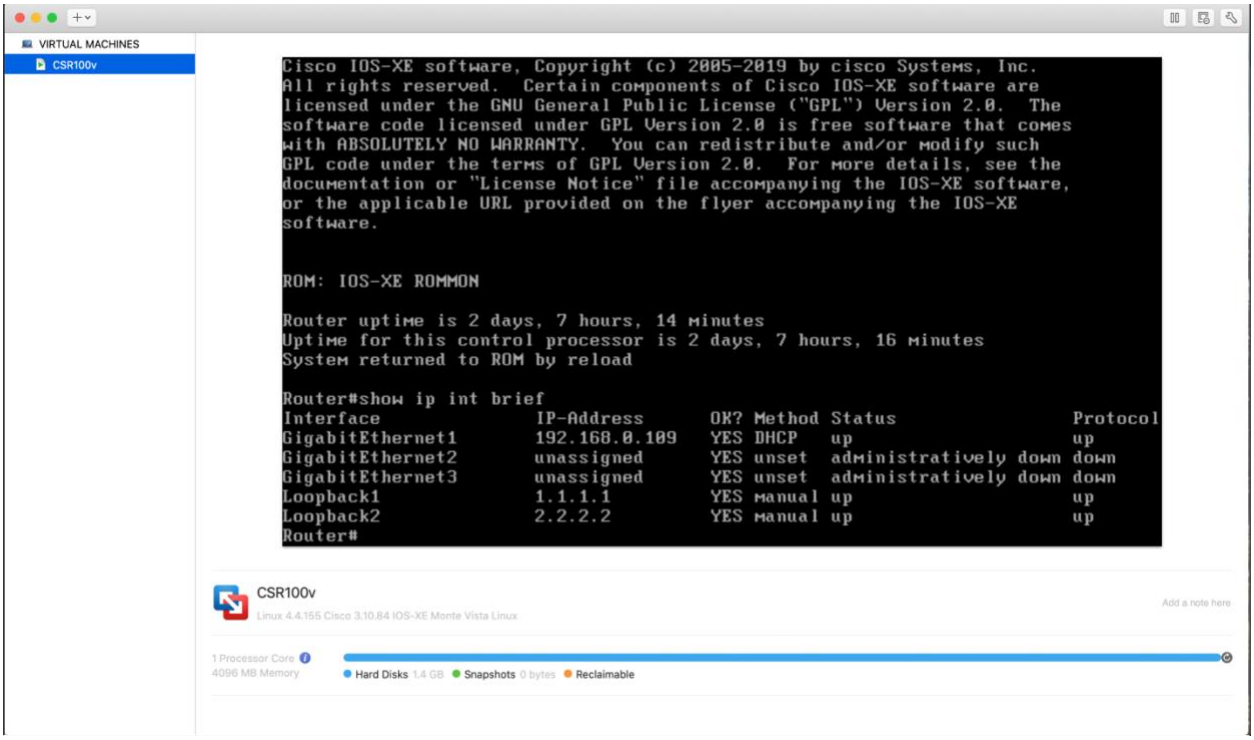
ANEXO E. CAPTURAS DE PANTALLA DEL LABORATORIO DE PROGRAMABILIDAD ORIENTADO A LA AUTOMATIZACIÓN DE UNA RED SDN


VIRTUAL MACHINES
CSR100v
Router#show version
Cisco IOS XE Software, Version 16.06.06
Cisco IOS Software [Everest], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9
-M), Version 16.6.6, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 11-Apr-19 04:00 by mcpre
Cisco IOS-XE software, Copyright (c) 2005-2019 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
ROM: IOS-XE ROMMON
Router uptime is 2 days, 7 hours, 14 minutes
Uptime for this control processor is 2 days, 7 hours, 16 minutes
--More--
CSR100v
Linux 4.4.155 Cisco 3.10.84 IOS-XE Monte Vista Linux
Add a note here
1 Processor Core
4096 MB Memory
Hard Disks 1.4 GB
Snapshots 0 bytes
Reclaimable


VIRTUAL MACHINES
CSR100v
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#show ip int br
Interface IP-Address OK? Method Status Protocol
GigabitEthernet1 192.168.0.109 YES DHCP up up
GigabitEthernet2 unassigned YES unset administratively down down
GigabitEthernet3 unassigned YES unset administratively down down
Router#$
CSR100v
Linux 4.4.155 Cisco 3.10.84 IOS-XE Monte Vista Linux
Add a note here
1 Processor Core
4096 MB Memory
Hard Disks 1.4 GB
Snapshots 0 bytes
Reclaimable


PCAP – create_loopbacks.py [PCAP]
create_loopbacks
Git:
PCAP 〉 M5 〉 Lab 〉 create_loopbacks.py
Project
PCAP ~/Documents/Coding/Python/PCAP
lab
M2
M3
M4
M5
Lab
2_1_Lab.py 6/7/20, 20:26, 691 B Moments ago
create_loopbacks.py 6/7/20, 20:24, 854 B 6 mi
done_1.x Lab – PC Setup for Workshop.pdf 6/1
done_2.1 Lab – Setting Up the Lab Environment.
done_2.2 Lab – CLI Automation with Python usin
VirtualBox ETW-CSR1000v.ova 6/11/19, 17:49,
modules
packages
progs
5_1_1_10_importing_module.py 5/23/19, 21:02, 3
M6
PPTs
venv
practice_test.py 6/11/19, 19:22, 3.35 kB
test.py 3/19/19, 13:41, 23 B
APIs ~/Documents/Coding/Python/APIs
venv
credentials.ini 4/3/19, 13:16, 1.08 kB 8 minutes ago
Python_scratch_reloaded ~/Documents/Coding/Python/
External Libraries
Scratches and Consoles
from netmiko import ConnectHandler
#Send show commands and display the output
sshCli = ConnectHandler(
device_type = 'cisco_ios',
host = '172.16.92.128',
port = 22,
username = 'cisco',
password = 'cisco123'
)
def create_loopbacks(loop_qty):
#Automate loopback creation
for i in range(loop_qty):
ipaddr = input("Enter IP address: ")
mask = input("Enter mask address: ")
config_commands = [
'int loopback ' + str(i+1),
'ip address ' + ipaddr + " " + mask,
'exit'
]
sshCli.send_config_set(config_commands)
print("\n" + str(loop_qty) + " loopbacks were created:\n".title())
output = sshCli.send_command("show ip int brief")
print(output)
loop_qty = int(input("Please enter the number of loopbacks need it:"))
create_loopbacks(loop_qty)
Run:
credentials.ini
create_loopbacks.py
2_1_Lab.py
6: TODO
9: Git
Terminal
Python Console
1: Project
7: Structure
2: Favorites


Please enter the number of loopbacks need it:2
Enter IP address: 1.1.1.1
Enter mask address: 255.255.255.0
Enter IP address: 2.2.2.2
Enter mask address: 255.255.255.0
2 Loopbacks Were Created:
Interface IP-Address OK? Method Status Protocol
GigabitEthernet1 10.99.70.101 YES DHCP up up
GigabitEthernet2 unassigned YES unset administratively down down
GigabitEthernet3 unassigned YES unset administratively down down
Loopback1 1.1.1.1 YES manual up up
Loopback2 2.2.2.2 YES manual up up
Process finished with exit code 0



ÍNDICE DE FIGURAS Y GRÁFICOS

ÍNDICE DE TABLAS

BIBLIOGRAFÍA

Bibliography

Anderson, J., & Morreale, P. (2014). *Software Defined Networking* (Vols. https://learning.oreilly.com/library/view/software-defined-networking/9781482238631/). CRC Press.

Bent, K. (21 de 08 de 2014). *IDC: Next Two Years To Be 'Significant Launch Point' For SDN In The Enterprise*. Obtenido de https://www.crn.com/news/networking/300073778/idc-next-two-years-to-be-significant-launch-point-for-sdn-in-the-enterprise.htm

Cisco. (2016). *The Digitization of Work.* Obtenido de https://cdn2.hubspot.net/hubfs/1885982/The%20Digitization%20of%20Work.pdf

Cisco. (10 de 2019). *Software-Defined Access.* Obtenido de https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/sda-sdg-2019oct.pdf

Cisco. (s.f.). *Cisco Costa Rica #2 IT, #3 Overall Y #7 En GPTW 2018*. Obtenido de gblogs.cisco: https://gblogs.cisco.com/cansac/cisco-costa-rica-2-it-3-overall-y-7-en-gptw-2018/

Cisco DNA Software for SD-WAN and Routing. (2020). Obtenido de Cisco: https://www.cisco.com/c/dam/en/us/products/collateral/software/one-wan-subscription/guide-c07-740642.pdf

Cisco SD-WAN Design Guide. (10 de 2018). Obtenido de Cisco: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/CVD-SD-WAN-Design-2018OCT.pdf

Cisco SD-WAN Getting Started Guide . (2020). Obtenido de Cisco: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/cisco-sd-wan-overlay-network-bringup.html#c_Bringup_Sequence_of_Events_7833.xml

Configuring Localized Data Policy for IPv4. (2016). Obtenido de Cisco: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_17.2/06Policy_Basics/05Localized_Data_Policy/Configuring_Localized_Data_Policy_for_IPv4

Edelman, J., Oswalt, M., & Lowe, S. (2018). *Network Programmability and Automation* (Vols. https://learning.oreilly.com/library/view/network-programmability-and/9781491931240/). O'Reilly Media, Inc.

Forbes. (8 de 1 de 2018). *3 Ways Automation And AI Amplify The Role Of Firstline Workers*. Obtenido de https://www.forbes.com/sites/insights-microsoft/2018/01/08/3-ways-automation-and-ai-amplify-the-role-of-firstline-workers/#7ac29efc3b5c

Gartner. (18 de 05 de 2016). *Automation: The Next Frontier For IT*. Obtenido de https://www.gartner.com/smarterwithgartner/automation-the-next-frontier-for-it-2/

Gartner. (12 de 1 de 2018). *Report Highlight for Survey Analysis: NFV/SDN Adoption in CSPs Calls for Strategic Changes in Transformation Programs.* Obtenido de Gartner: https://www.gartner.com/en/documents/3843397/report-highlight-for-survey-analysis-nfv-sdn-adoption-in0

Graziani, R. (2017). *IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6, 2nd Edition* (Vols. https://learning.oreilly.com/library/view/ipv6-fundamentals-a/9780134670584/). Cisco Press.

Hucaby, D., Garza, R., & Edgeworth, B. (2019). *CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide* (Vols. https://learning.oreilly.com/library/view/ccnp-and-ccie/9780135262047/). Cisco Press.

Kumaran, M., & Maddison, T. (2016). *Distributed Learning* (Vols. https://learning.oreilly.com/library/view/distributed-learning/9780081006092/). Chandos Publishing.

Lerner, A. (14 de 10 de 2014). *Beyond The Hype: SDN Delivers Real-World Benefits In Mainstream Enterprises*. Obtenido de Gartner: https://www.gartner.com/en/documents/2874018/beyond-the-hype-sdn-delivers-real-world-benefits-in-main

Liu, D. (2015). *Systems Engineering* (Vols. https://learning.oreilly.com/library/view/systems-engineering/9781482282467/). CRC Press . Obtenido de https://learning.oreilly.com/library/view/systems-engineering/9781482282467/

Lutz, M. (2013). *Learning Python, 5th Edition* (Vols. https://learning.oreilly.com/library/view/learning-python-5th/9781449355722/). O'Reilly Media, Inc.

Paresh, S., Syed, H., & Chayapathi, R. (2016). *Network Functions Virtualization (NFV) with a Touch of SDN* (Vols. https://learning.oreilly.com/library/view/network-functions-virtualization/9780134464312/). Addison-Wesley Professional.

Ravindran, A., Hillar, G., & Romano, F. (2018). *Learn Web Development with Python: Get hands-on with Python Programming and Django web development* (Vols. https://learning.oreilly.com/library/view/learn-web-development/9781789953299/). Packt Publishing.

Revista Summa. (Setiembre de 2017). *Cisco Celebra Hoy 20 Años De Su Presencia En Costa Rica* . Obtenido de https://revistasumma.com/cisco-celebra-hoy-20-anos-presencia-costa-rica/

Riemer, F., Quartaroli, M., & Lapan, S. (2011). *Qualitative Research: An Introduction to Methods and Designs* (Vols. https://learning.oreilly.com/library/view/qualitative-research-an/9781118118832/).

Silicon Valley Historical Association. (2008). *Cisco Systems*. Obtenido de Silicon Valley Historical Association: https://www.siliconvalleyhistorical.org/cisco-systems

Stallings, W. (2015). *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud* (Vols. https://learning.oreilly.com/library/view/foundations-of-modern/9780134175478/). Addison-Wesley Professional.

Tegarden, D., Wixom, B., & Dennis, A. (s.f.). *Systems analysis design, UML version 2.0* (Vols. https://learning.oreilly.com/library/view/systems-analysis-and/9781118037423/). Wiley.

The 5 Steps Sales Process | A Flowchart For Success | Act!365. (s.f.). Obtenido de https://www.act365.com/5-step-sales-process/

Unicast Overlay Routing Overview . (2016). Obtenido de Cisco: https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.2/03Routing/01Unicast_Overlay_Routing_Overview