

Enero, 2022

aruba

a Hewlett Packard
Enterprise company

¡SDN es la respuesta!

¿Cuál era la pregunta?

Diego Dompe, Distinguished Technologist

/usr/bin/whoami

Experto en desarrollo de sistemas empujados.
Especialidad en integración/co-diseño de software
y hardware.

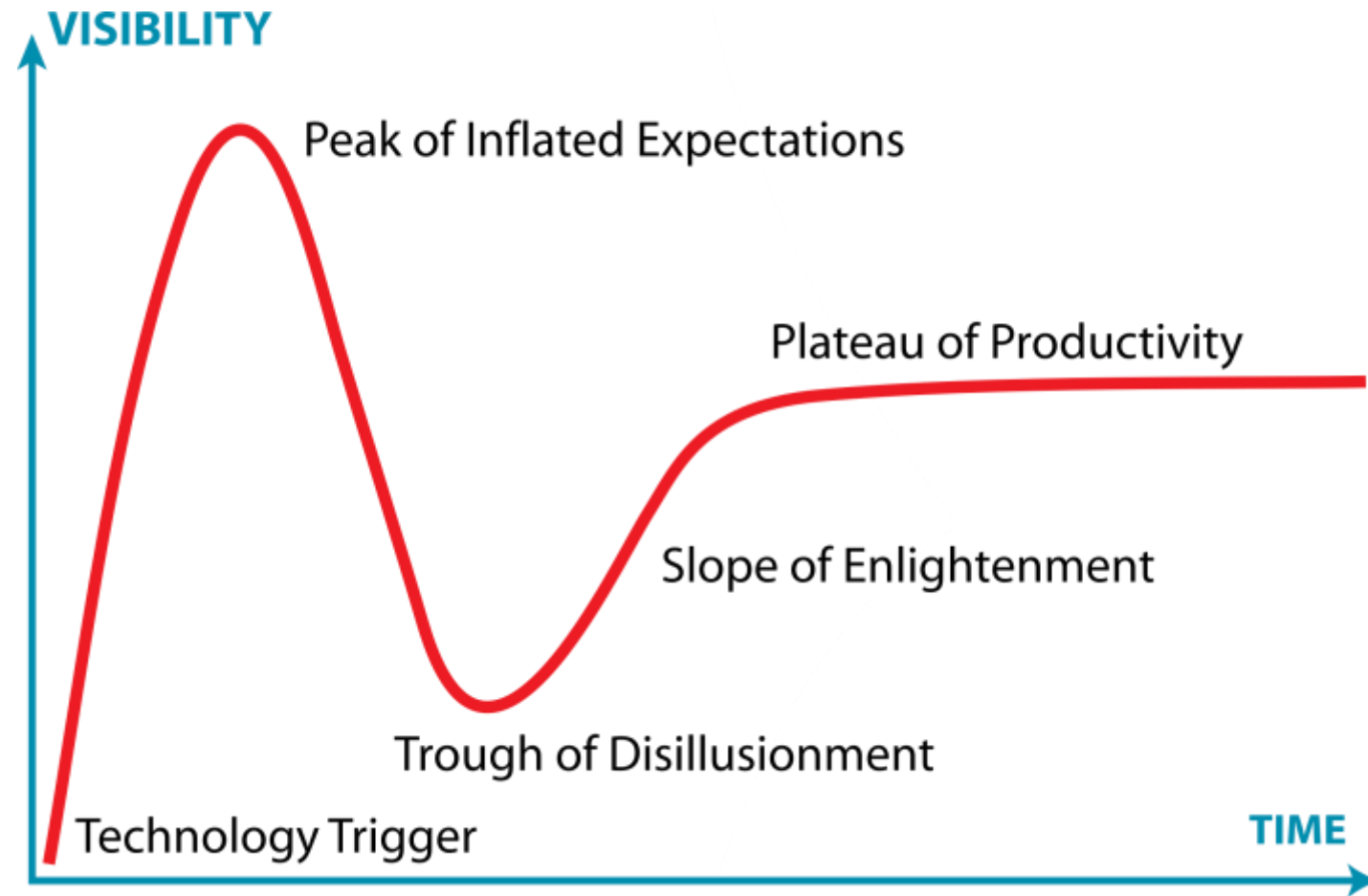
Research and Development at Aruba Networks
Hewlett Packard Enterprise
Costa Rica



www.linkedin.com/in/ddompe



Gartner Hype Cycle

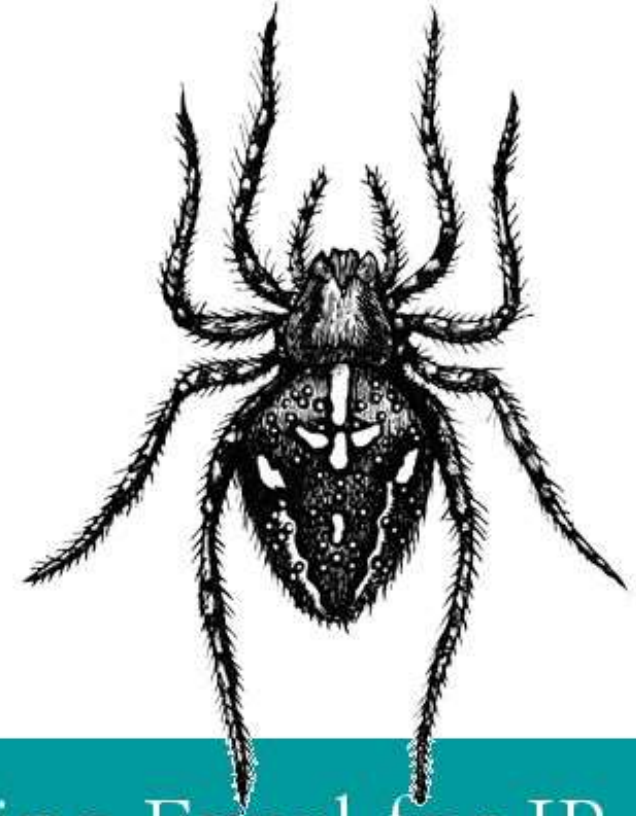


Spreadsheet Defined Networking

¡Parece que todos hemos hecho SDN!



Using Distributed Systems Theory for Enterprise IPAM



Scaling Excel for IP Address Management

The Definitive Guide

O RLY?

@shawski5000

Technology is nothing but an expression of human values. It's not neutral, it's not about efficiency, it's about people's values and their knowledge.

Ramesh Srinivasan

El mundo moderno de las redes

Los diversos y distintos mundos de las redes

- Redes de Hyperscalers
- Redes de DataCenter
- Redes de Telecomunicaciones
- Redes de Campus
 - Redes alámbricas
 - Redes inalámbricas
- Redes SMB
- Redes Cloud
- Redes Edge
 - Telcos
 - Distributed



Los perfiles de los involucrados

- CIOs
- Sysadmins / Operations / Technicians
- Developers
- DevOps



DevOps

- Operations Team
 - También conocidos como sysadmins, administradores, o departamento de TI.
 - Usualmente presta servicios a los equipos de desarrollo.
 - Su principal objetivo es que la red e infraestructura de TI sean estables. ***Por lo tanto son adversos a los cambios.***
 - En lugares maduros van a usar tickets y control de cambios estrictos. Probablemente adoptan prácticas de ITIL.
- Development Team
 - También conocidos como los programadores o desarrolladores.
 - Usualmente requiere los servicios del departamento de TI.
 - Bajo presión para responder a las necesidades del negocio de forma ágil (“el software es barato y fácil de cambiar”). ***Por lo tanto son amigos del cambio.***

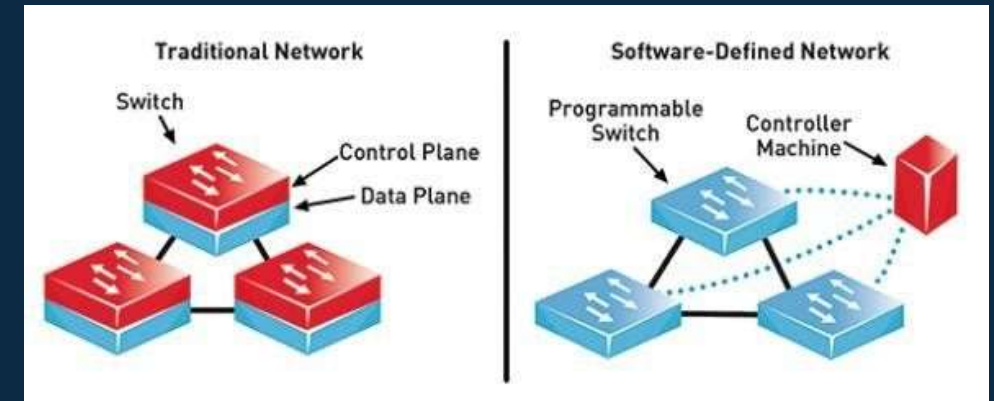


DevOps & Agile

- Los principios de desarrollo Agile están relacionados con el auge de los DevOps.
- Simplemente mezclar equipos con objetivos y motivaciones claramente distintas es una receta para el desastre.
- Para que los DevOps sean posibles es necesario cambiar algunos de los fundamentos tecnológicos detrás de la infraestructura de TI.
 - Para hacer desarrollo ágil se requiere infraestructura ágil.
 - A menos que se tenga capacidad de automatización de *baremetal*, lo anterior obliga al uso de infraestructura basada en software (Software Defined Network/Storage/Compute), mediante virtualización o contenerización.

Software Defined Network

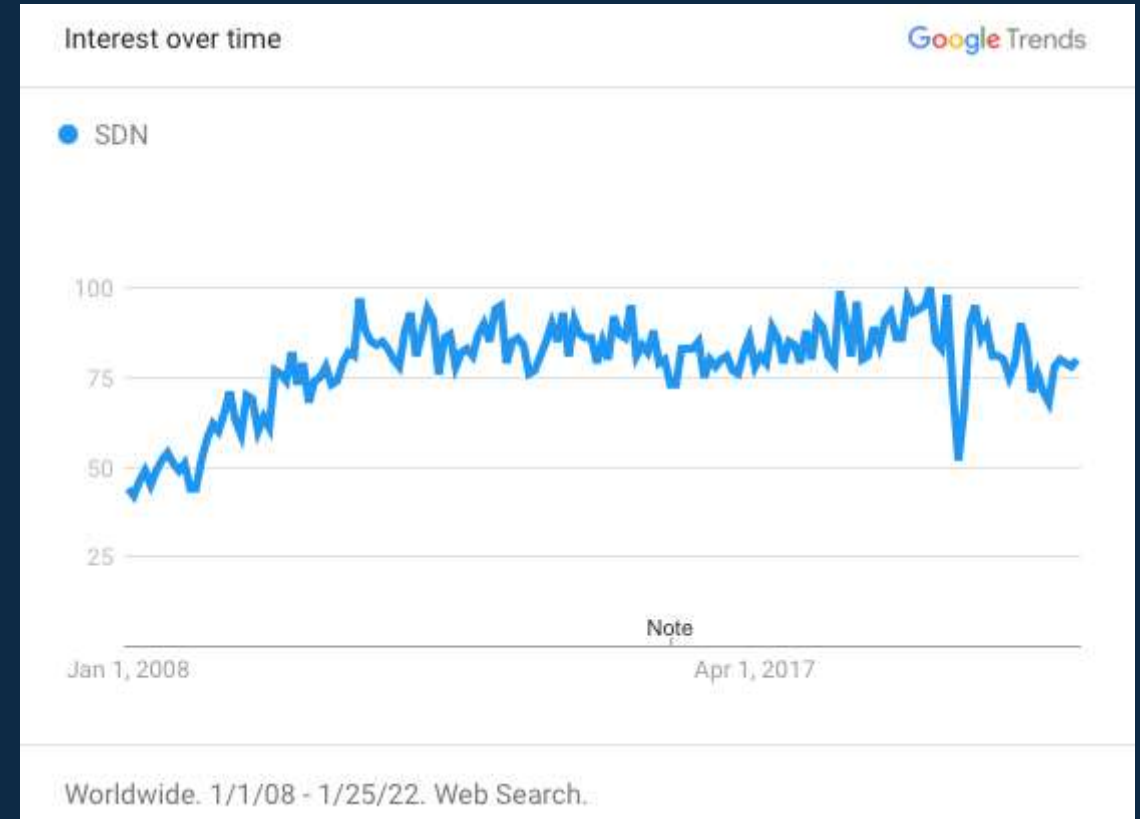
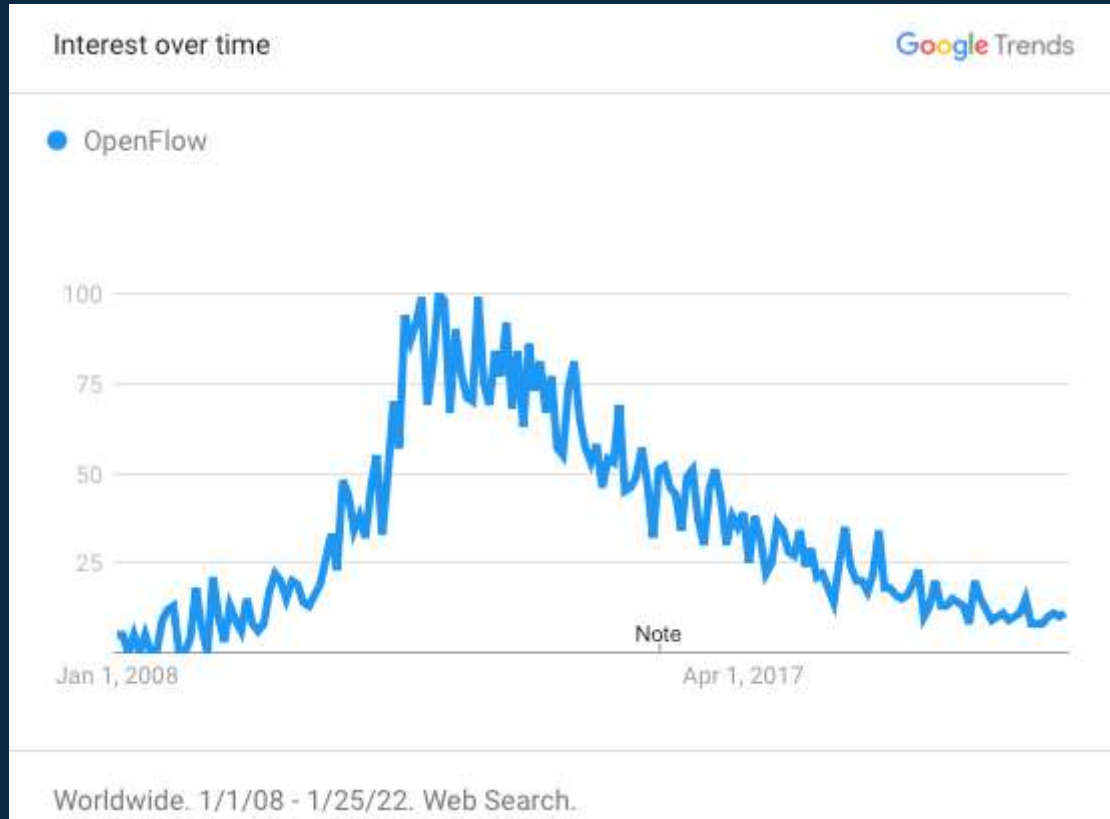
- Separación de los planos de Datos y de Control.
- La separación debe implementarse mediante el uso de una interfaz de programación estandarizada.
- Cuando el plano de datos es una implementación de software, esto es fácil de lograr.
- OpenFlow es la interfaz de programación que popularizó SDN en el hardware de red.
 - Varios vendedores de switches implementaron el protocolo**



¿Cuál problema soluciona OpenFlow?

- Flexibilidad de mejorar/personalizar/ajustar el plano de control
 - Depende en habilidades de desarrollo de software
- Centralización
- Independencia de vendedor**
- Inteligencia
- Innovación mediante desagregación
- Agilidad
 - Multi-Tenant

¿Qué sucedió con OpenFlow?



¿Qué sucedió con OpenFlow?

- OpenFlow abrió la puerta para la programabilidad del hardware, pero los usuarios de este tipo de equipo no son mayoritariamente personas con habilidades/entrenamiento en esta área.
- Sin embargo, los principios de SDN han florecido en otras áreas donde la capacidad de tomar ventaja de la programabilidad es posible. Por ejemplo:
 - Cloud
 - DataCenter
 - WAN
 - Edge

SDN en Cloud

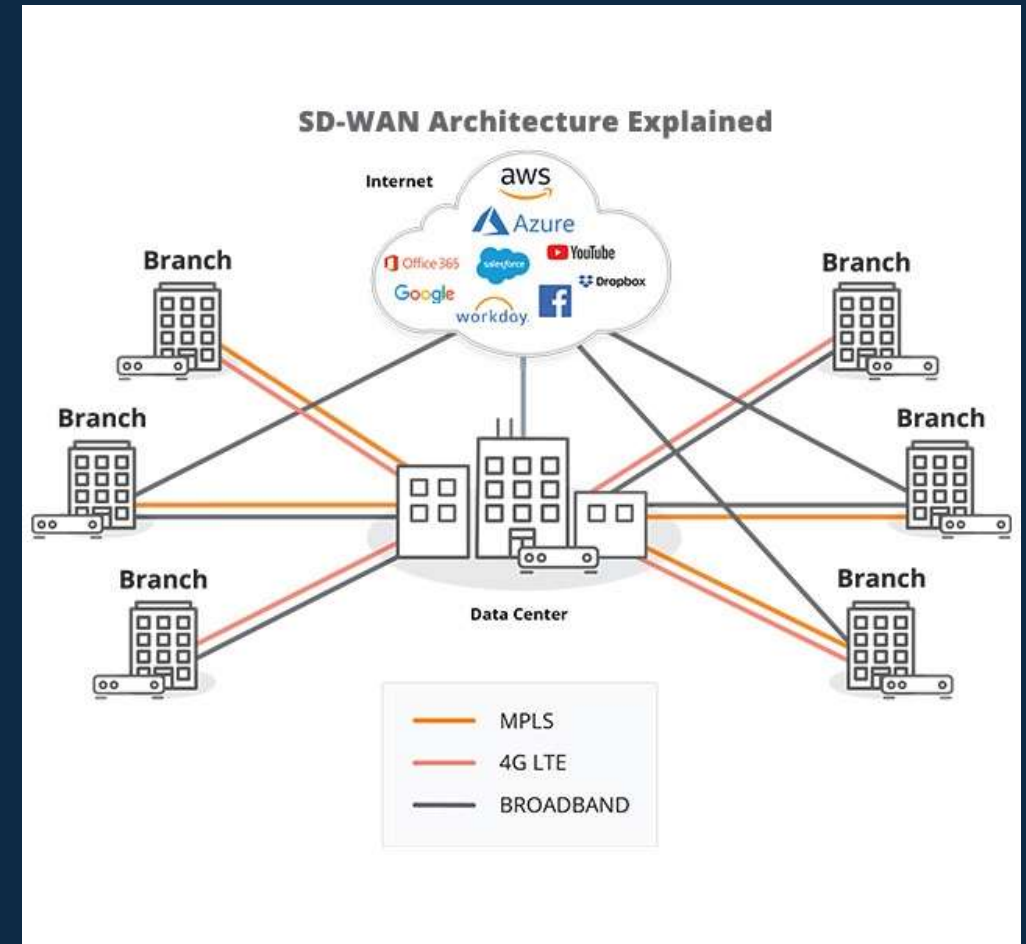
- La infraestructura de Cloud es desde su concepción orquestada por software (no solo a nivel de red).
- Originalmente el plano de datos para VM era implementado mediante software, pero los hyperscalers han ido moviéndolo a implementaciones de hardware para liberar ciclos de cómputo para las cargas de trabajo de los clientes
 - Nitro de Amazon para las VPC
 - Azure Smart NIC
- Para las plataformas de containers (K8S/CNI) el plano de datos es implementado mediante software pero varios proyectos están proponiendo opciones que pueden habilitar aceleración por hardware en el futuro.
- En el caso de los containers las redes de mesh llevan el SDN a un nuevo nivel, ya que permiten la definición ad-hoc de redes con reglas de seguridad definidas por los equipos de DevOps.

SDN en DataCenter

- Para la infraestructura virtualizada si bien la mayoría de los orquestadores ofrecen características de SDN, es raro encontrar sistemas que tomen ventaja de forma programática.
- Para la infraestructura en containers se tienen las mismas características que las cargas de K8S/CNI en el cloud.
- Para la infraestructura de baremetal existe un auge en el uso de DPU/IPU/SmartNIC para proveer seguridad y/o funciones de red virtualizadas (NFV) de manera distribuida.

SDN en WAN

- Software Defined WAN (SD-WAN) es un tema que ha tenido mucho auge en los últimos años con gran éxito en la práctica.
- Consiste en centralizar el plano de control (usualmente en el Cloud) y usar pequeños CPEs que agregan múltiples proveedores de WAN con tecnología comodotizada (Cable, Fibra, DSL, Celular) en lugar de enlaces dedicados de MPLS.
- El plano de datos es implementado mediante software en el CPE, y se puede aumentar con características de desempeño, seguridad y observabilidad de manera dinámica desde el plano de control.
- Provee un alto retorno de inversión y ha visto un auge durante la pandemia.



SDN en Edge

- Las redes 5G proveen una oportunidad para innovación que capitaliza en sus altas velocidades y baja latencia de red.
- Para usar el potencial de estos ambientes, al igual que en los casos de WAN, se requiere de capacidades de SDN para optimizar/administrar de manera remota.
- Virtualización de funciones de red (NFV) es un caso muy común en el mundo de las telecomunicaciones que hace uso de paradigmas de SDN.
- Aunque todavía no se ha identificado un “killer-app” en el 5G, cuando surja, será construido en las tecnologías de agile que estamos viendo en el cloud y probablemente utilizará muchos de sus paradigmas.
 - El tema de la seguridad con cero confianza va a ser crítico en el Edge.

SDN para Seguridad

- Redes con confianza cero (Zero Trust Security) y la micro-segmentación son imposibles de implementar sin SDN.
- El panorama de la seguridad es cambiante y dinámico, por lo que requiere la capacidad de corregir rápida y fácilmente la infraestructura (tanto de software como de hardware).
 - Gran cantidad de CVEs recientes contra stacks de IP usados en switches, access points, etc.
- Todo lo anterior está siendo implementado mediante técnicas de SDN por los diferentes vendedores.

Q&A

Gracias