OpenFlow - Casos de uso

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

- Estas diapositivas tienen contenido significativo distribuidos por:

OpenFlow En La Empresa

Qué puede aportar OpenFlow a la empresa

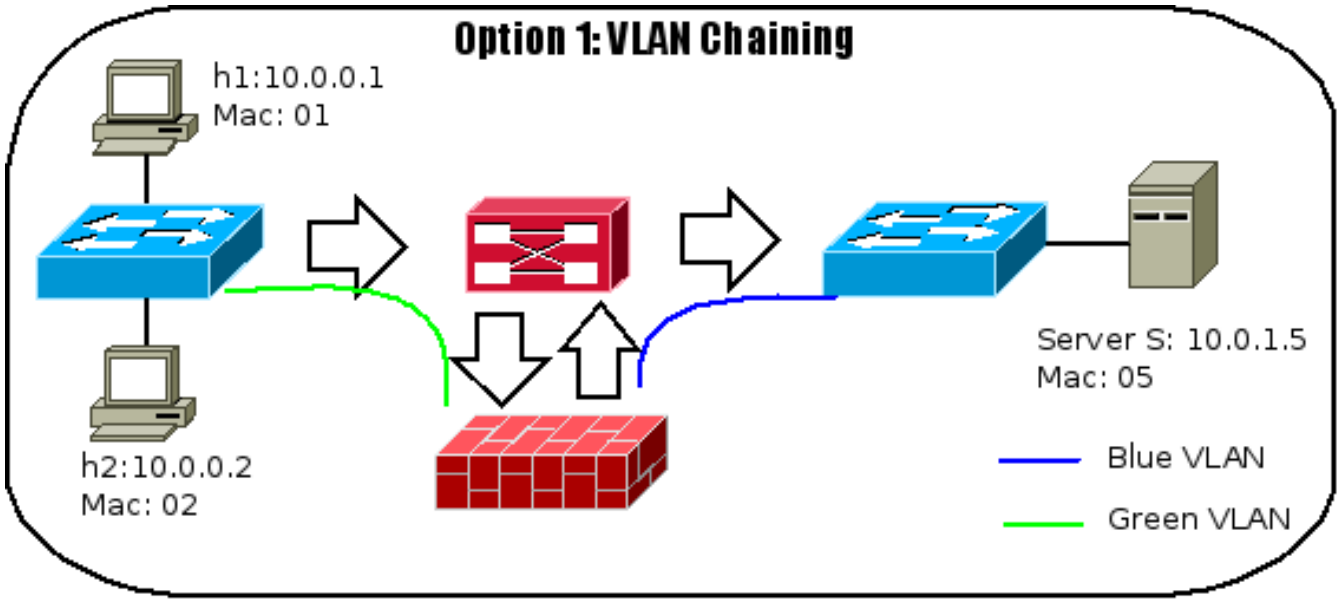
- Configuración Automatizado de nuevos equipos en su red empresarial (piense en un controlador basado en una red inalámbrica)
- Elija entre un mercado de soluciones para los requisitos comunes de red (por ejemplo, el cumplimiento de PCI-DSS, el control de acceso de red NAC, etc.)
- Delegar el control de las rebanadas de la red a su administrador apropiado (por ejemplo, CCTV, cerraduras de puertas, BAS, etc.)
- Encarar los nuevos requisitos (por ejemplo, la impresión bonjour, el acceso para invitados, BYOD) a través de nuevo software, no nuevos equipos

Servicio de inserción o encadenamiento

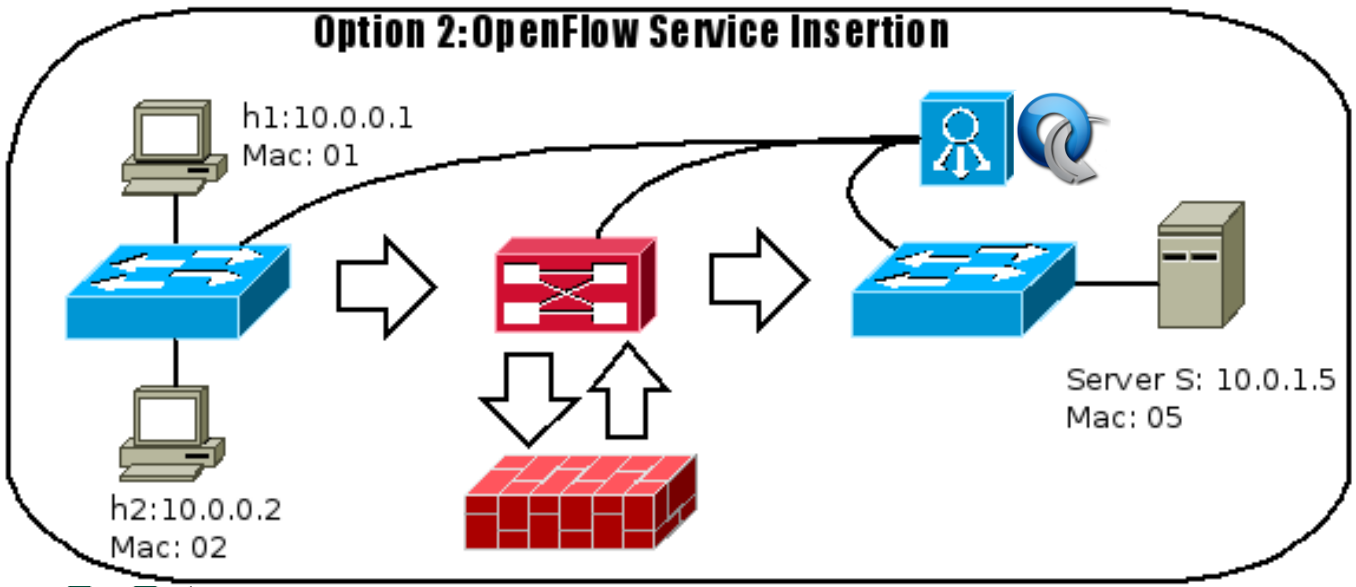
En la ruta de reenvío basado en usuario y/o aplicación

- Nivel de flujo de redireccionamiento del tráfico dinámicamente programable
- Introducir herramientas especializadas o cadenas secuencialmente
  - –Firewall, IPS, filtrado de contenido, almacenamiento en caché, NAT, Balanceo de Carga, Administrador de llamadas ...
  - –Desde/Para cualquier lugar de la red
- Redireccionar paquetes al próximo servicio
  - –Encapsular paquetes
  - –Reescribir direcciones ***dst_mac***

Inserción de servicio - Ejemplo



Potencialmente crea bucle de reenvío



Northbound API
Modo Proactivo

Virtualización de las Funciones de red (NFV)

Marco para

- Aprovisionamiento de máquinas virtuales dentro en la red
- Enhebrar flujos específicos a través de aplicaciones basadas en MV.

aplicaciones incluyen la codificación de vídeo, firewall, balanceador de carga, controladores de frontera de sesión VoIP, etc.

Balanceador de carga

- Balanceo dinámico del tráfico de carga en un dispositivo cluster
  - –IDS / IPS, firewall, servidores Web, filtrado de contenido, almacenamiento en caché …
  - –Integrar Con NFV para girar arribar/abajo servicios como los cambios de la demanda
- (Por ejemplo girar sistemas adicionales de IDS o cortafuegos durante los ataques)
  - –Usar retroalimentación desde servidores/ dispositivos de red
- Rebalancear continuamente basados en la dirección IP, tipo de Ethernet, protocolo IP, puerto TCP / UDP …

Equilibrio de carga en IU con FlowScale

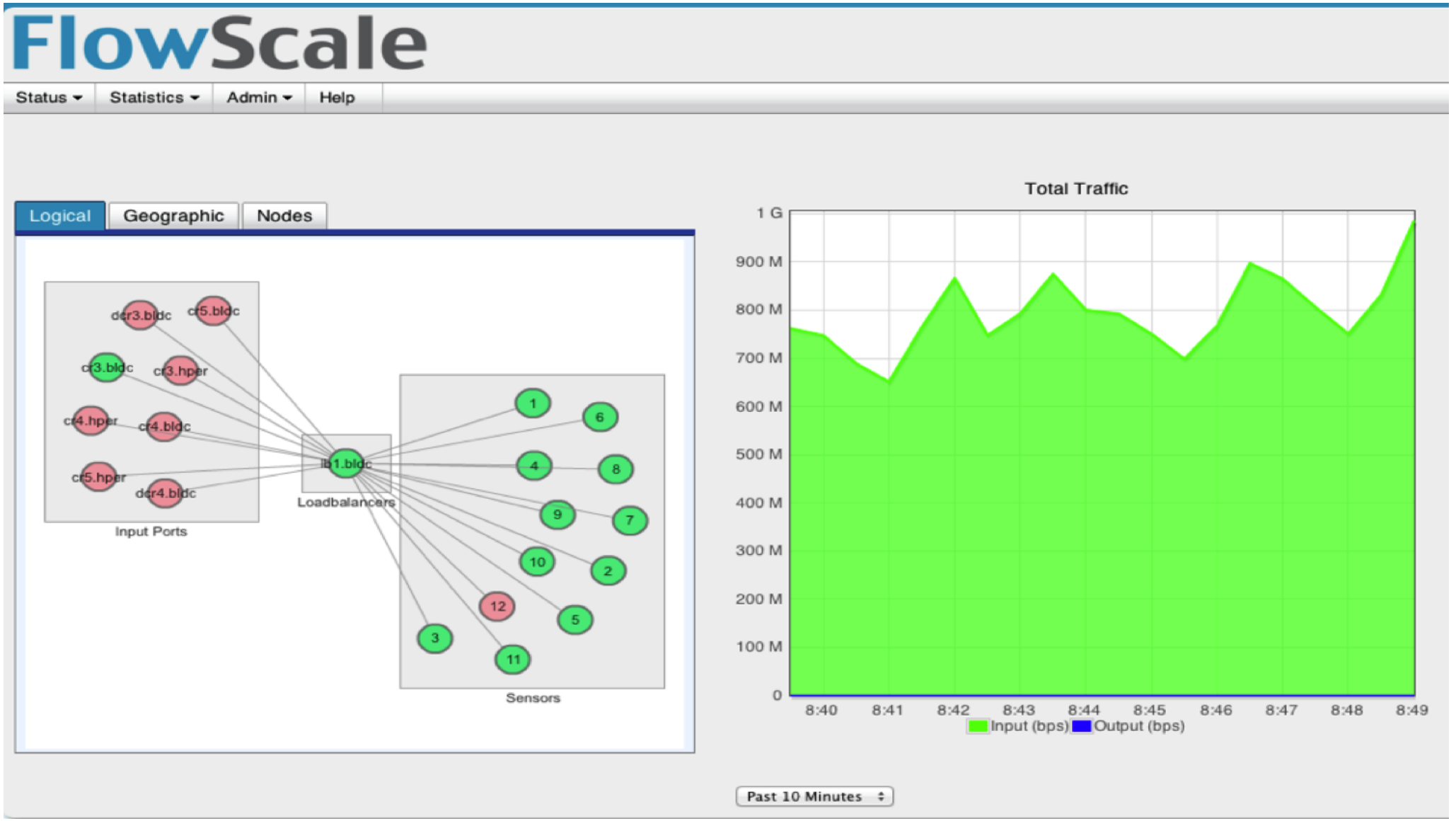
- Balanceador de tráfico de carga como un servicio utilizando OpenFlow
- Utilice el hardware de switches (<$ 20.000) en lugar de un balanceador de carga dedicad0 (~ $ 250.000).
- Ciclo de desarrollo • 6 meses
  - –Principalmente los estudiantes graduadas
- Integración con otras herramientas OpenFlow
  - –Aprovisionamiento L2, migración a MV.

https://www.youtube.com/watch?v=IjqXrML7QgE
https://www.youtube.com/watch?v=3KHI4a6gz5M

FlowScale

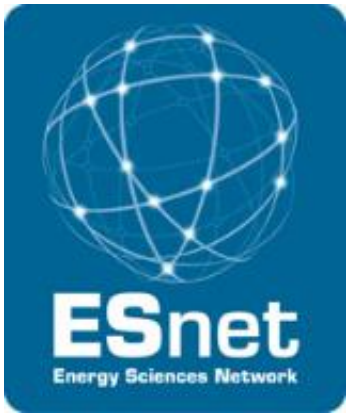
- Hash basados en campos OpenFlow (IP de origen / destino)
  - –Divides espacios de direcciones IU en prefijos IP
  - –Utiliza Round Robin para pre-distribuir los flujos a través de sensores
  - –La utilización de sensores de monitoreo y ajustes dinámicamente
- Redirige tipos específicos de tráfico a sensores especializados (por ejemplo, http o puerto TCP / UDP)
- Monitoreo de la capa de aplicacion y conmutación por error
- Web UI para admin

FlowScale UI

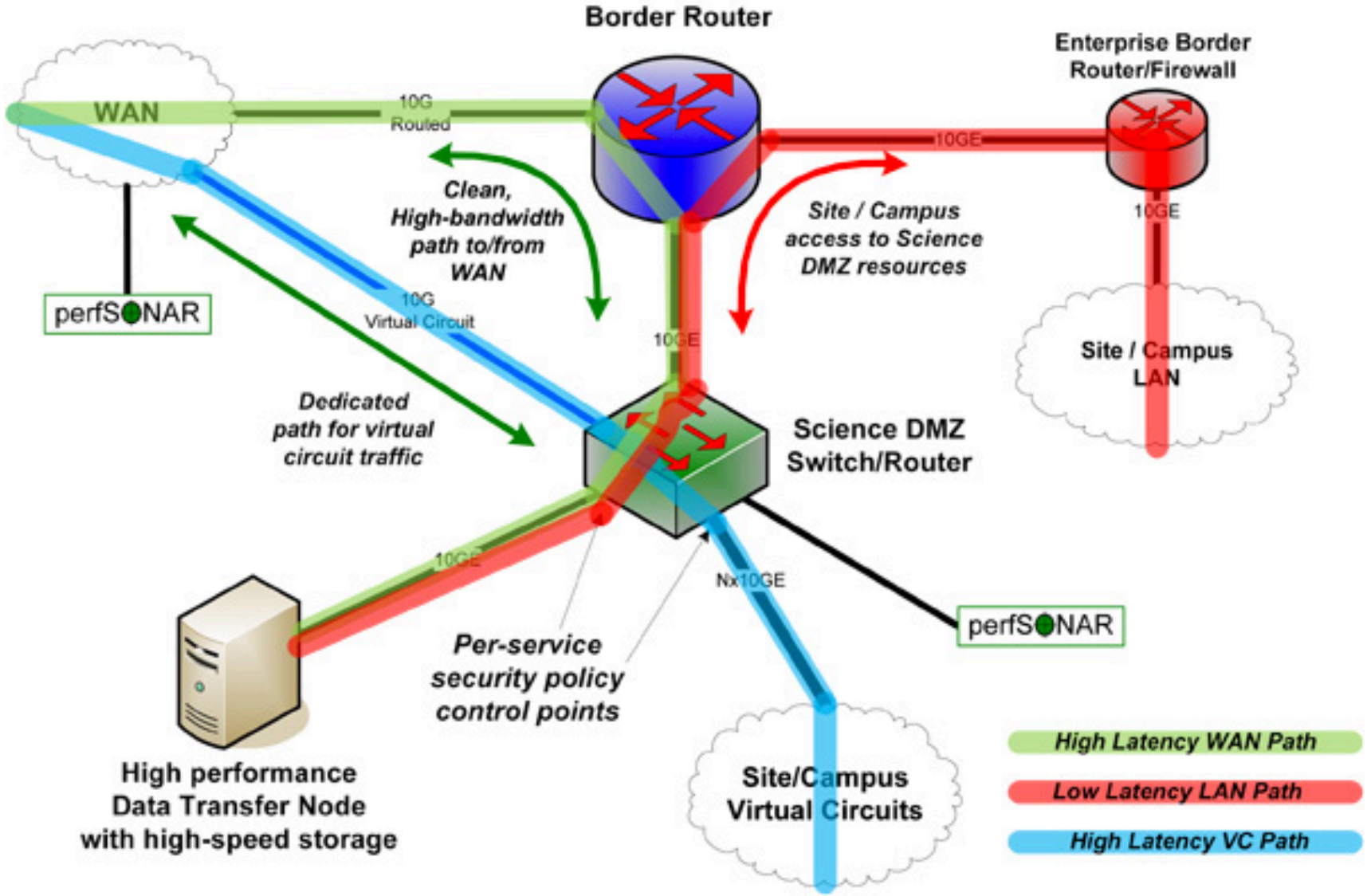


Ciencia DMZ (ESnet)

- Red dedicada para recursos de datos de alta velocidad
- El tráfico de confianza puede eludir los cortafuegos molestos y dispositivos DPI que afectan el desempeño de TCP



Ciencia DMZ Arquitectura



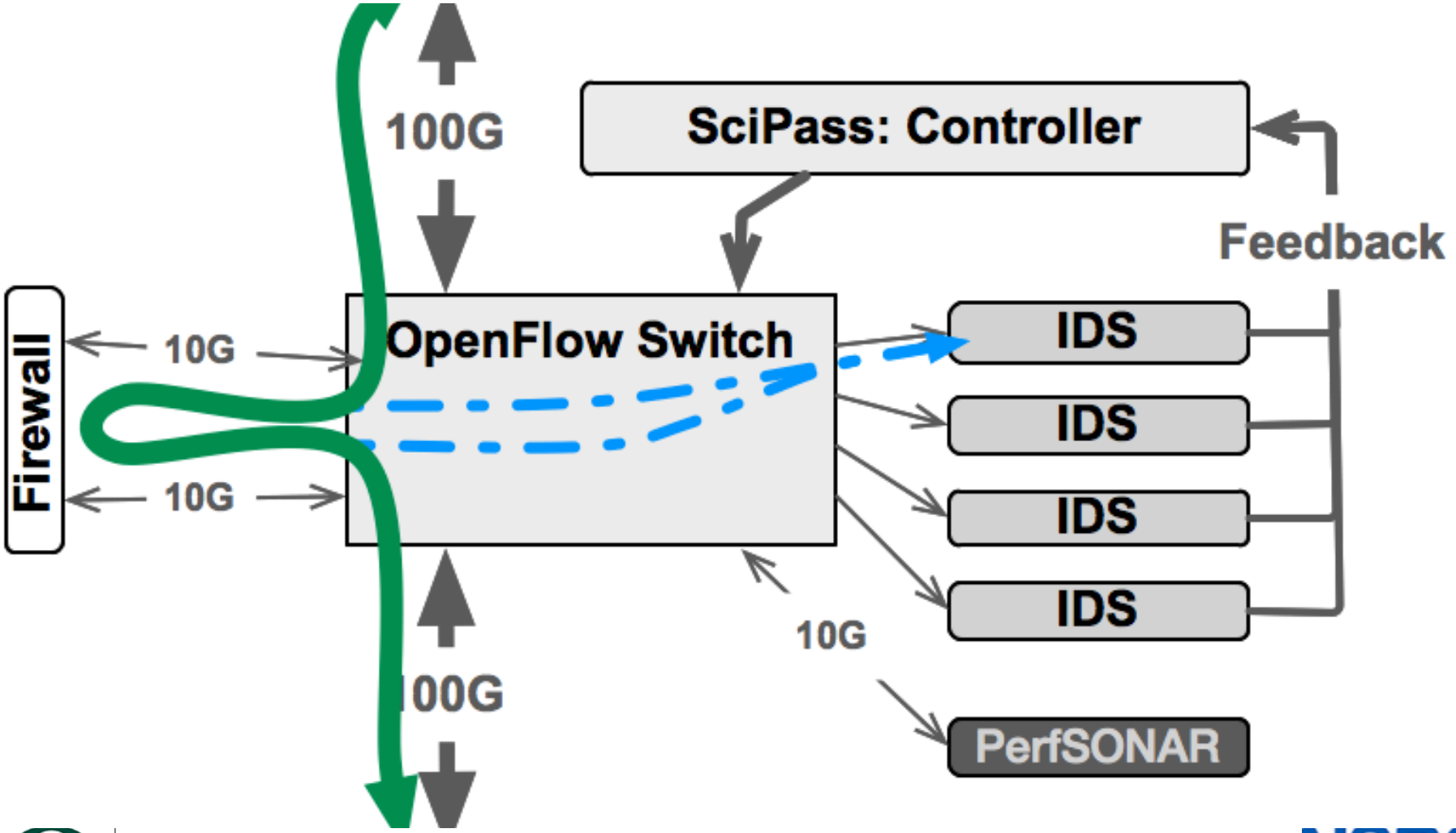
https://fasterdata.es.net/science-dmz/science-dmz-architecture/

sciencedmz@es.net

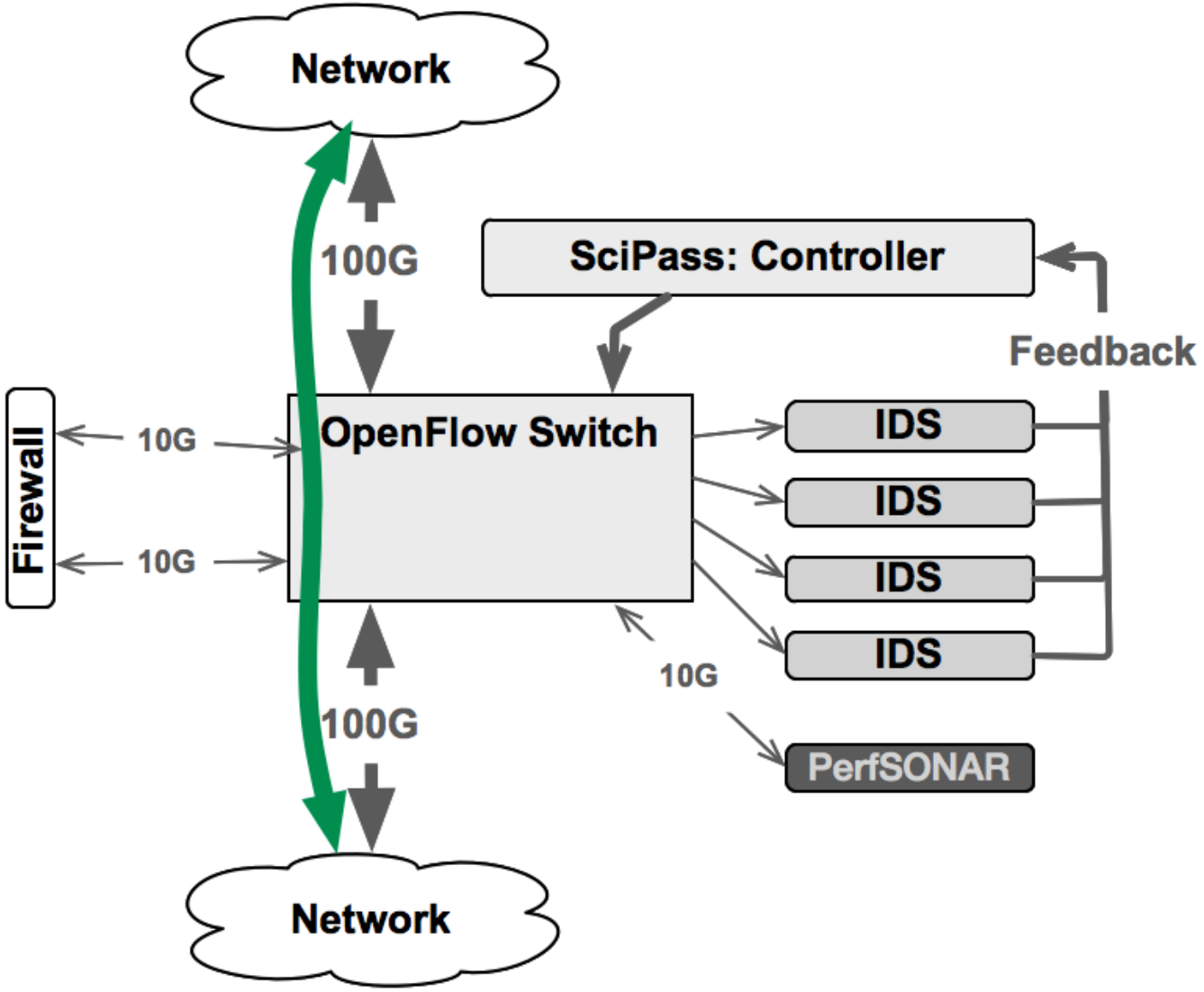
SciPass

- La Universidad de Indiana desarrollo una aplicacion basada en SDN
  - Adaptable clúster IDS de balanceo de carga (Flowscale) (NFV)
    - API de servicios Web para retro-alimentacion de IDS
    - Reactive white and Listas negras.
  - Redirección de cortafuegos (encadenamiento de servicio)
  - Eludir los cortafuegos (Science DMZ)
  - http://globalnoc.iu.edu/sdn/scipass.html

SciPass - Operación normal



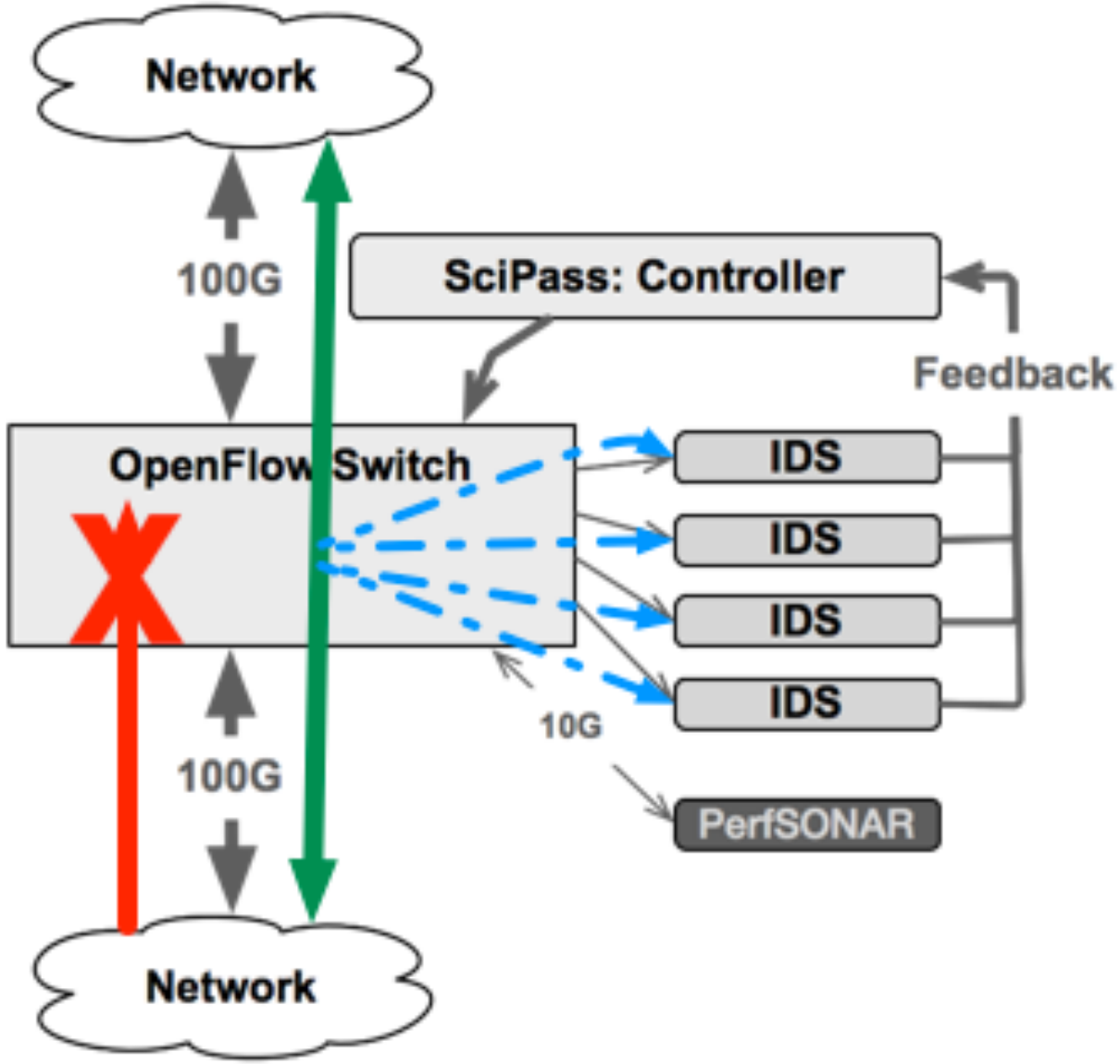
SciPass - Eludir el Firewall



SciPass Característica de la lista negra

- Can match:
  - Source / Destination IP
  - Source / Destination Port
  - Ethernet Type
- SciPass sends OpenFlow rules to switch
  - Flow Based: Block HTTP traffic from Host A to B
  - Prefix Based: Block all traffic to 192.168.0.1/32
  - Prefix Based: Block all traffic to or from 192.168.1.0/24
- IDS signals bad traffic to SciPass via web services

SciPass Blacklist Feature



SciPass Demo

https://www.youtube.com/watch?v=QeTejV3ooQA

OpenFlow en la WAN

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Qué puede aportar OpenFlow a la WAN

- API estándar para el aprovisionamiento de red (por ejemplo, a través de múltiples proveedores y tipos de dispositivos)
- API estándar sobre el cual hacer frente a los nuevos requisitos (por ejemplo, intercepción legal)
- Delegar el control de las rebanadas de la red sobre las cuales las redes virtuales arbitrarias pueden coexistir en una plataforma de red común

Ejemplos de casos de uso WAN

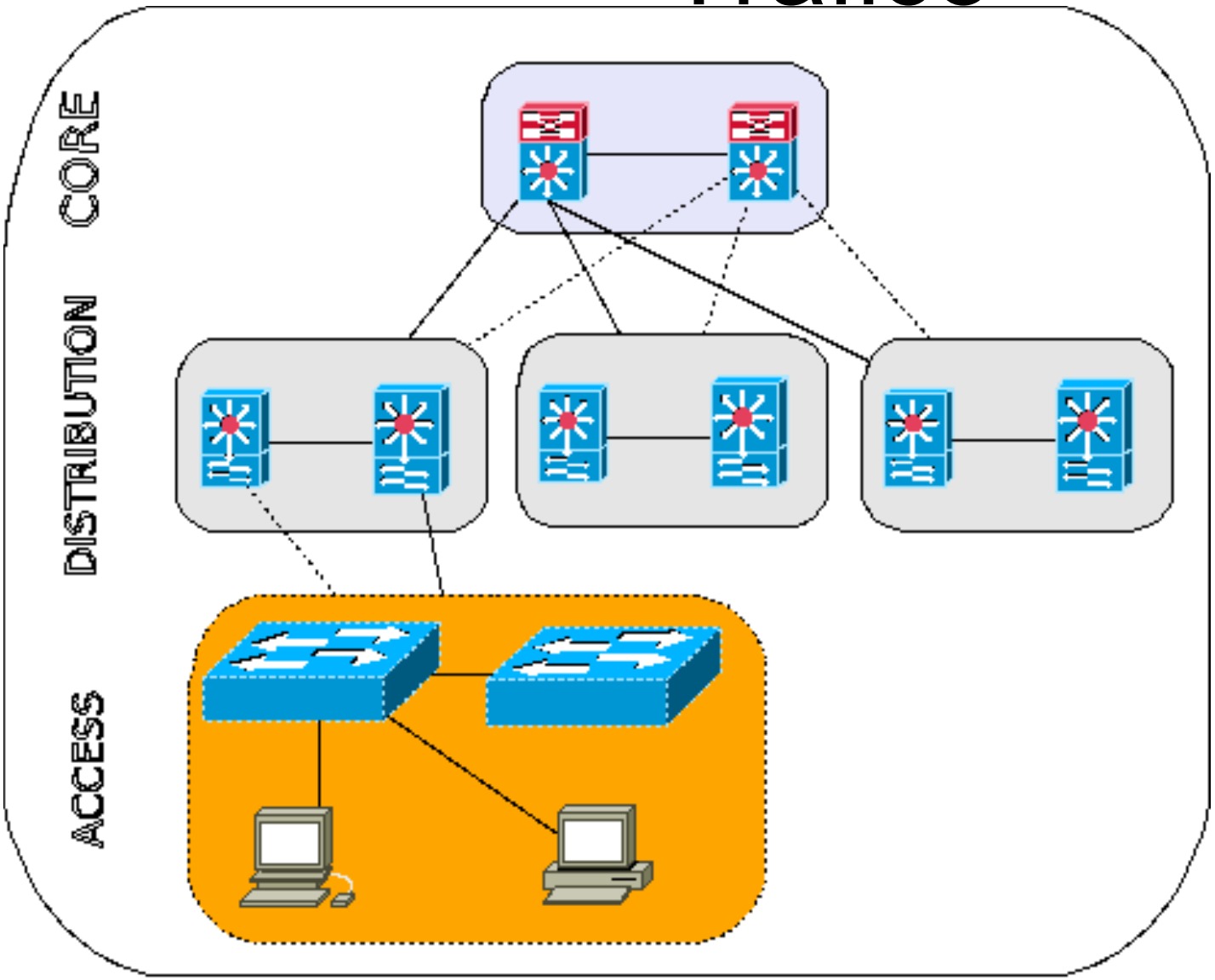
- Ancho de banda bajo demanda
  - –Programación de Solicitud de ancho de banda adicional cuando sea necesario
- Redireccionamiento de WAN dinámico
  - –Redirigir dinámicamente el tráfico de confianza alrededor de los dispositivos de inspección costosos
  - –Re-enrutar flujos sensibles sin latencia sobre rutas alternas durante la congestión
- Distribución de la carga de costos desiguales
  - –Balancear dinámicamente la carga de Tráfico basada en una variedad de definiciones de flujo
  - –Utilizar más los enlaces
- WAN dinámicos Interconectados
  - –Dinámicamente crear interconexiones en puntos de intercambio de Internet

Traffic Mirroring/Tapping

- Replicar y redirigir el tráfico desde cualquier punto de la red a cualquier punto de la red.
- Obtener el tráfico adecuado de la herramienta adecuada
- Reducir el número de dispositivos de derivación
- Centralizar y reducir costosas herramientas

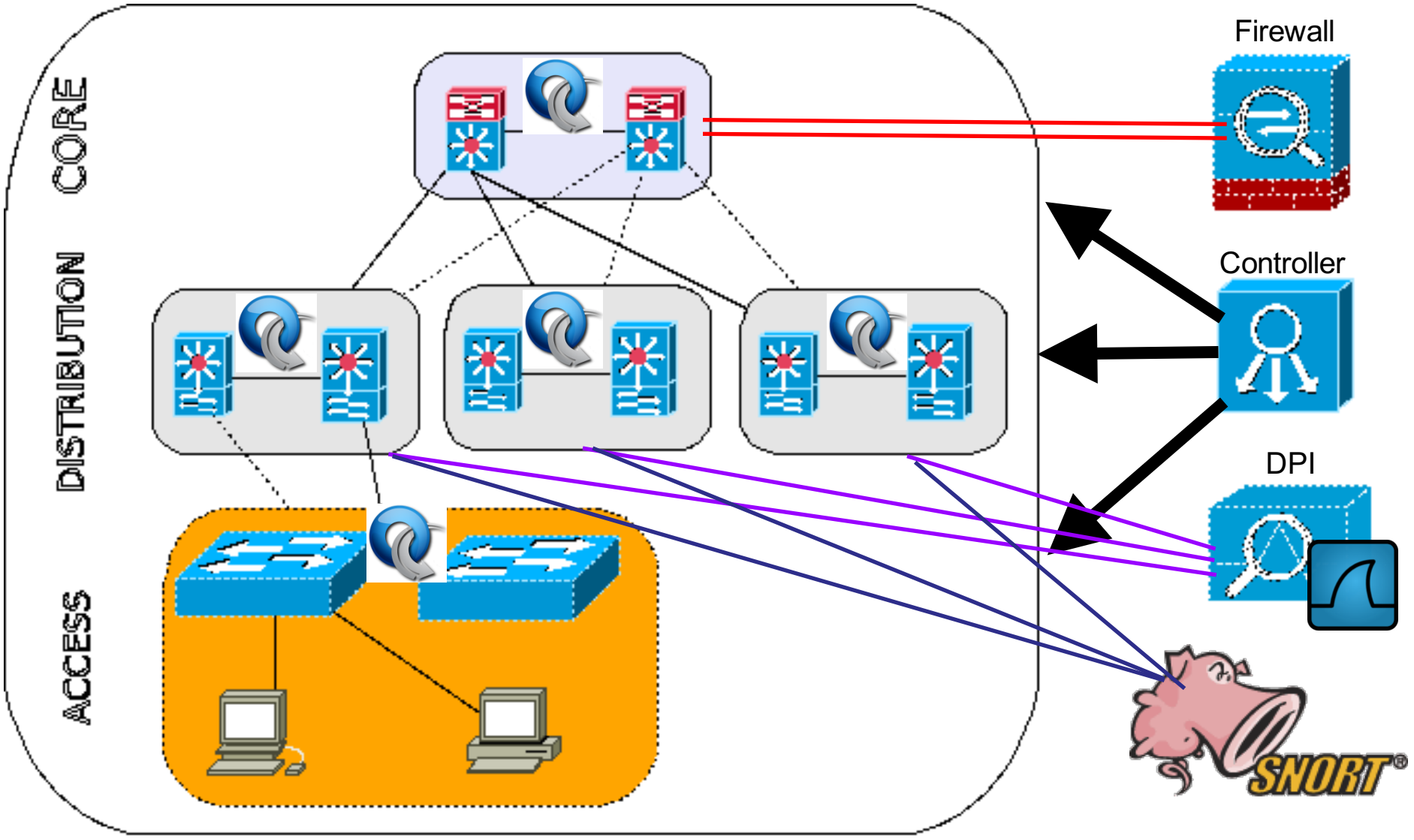
PROBLEMA: todo o nada

Problemas con el Agregador de Tráfico

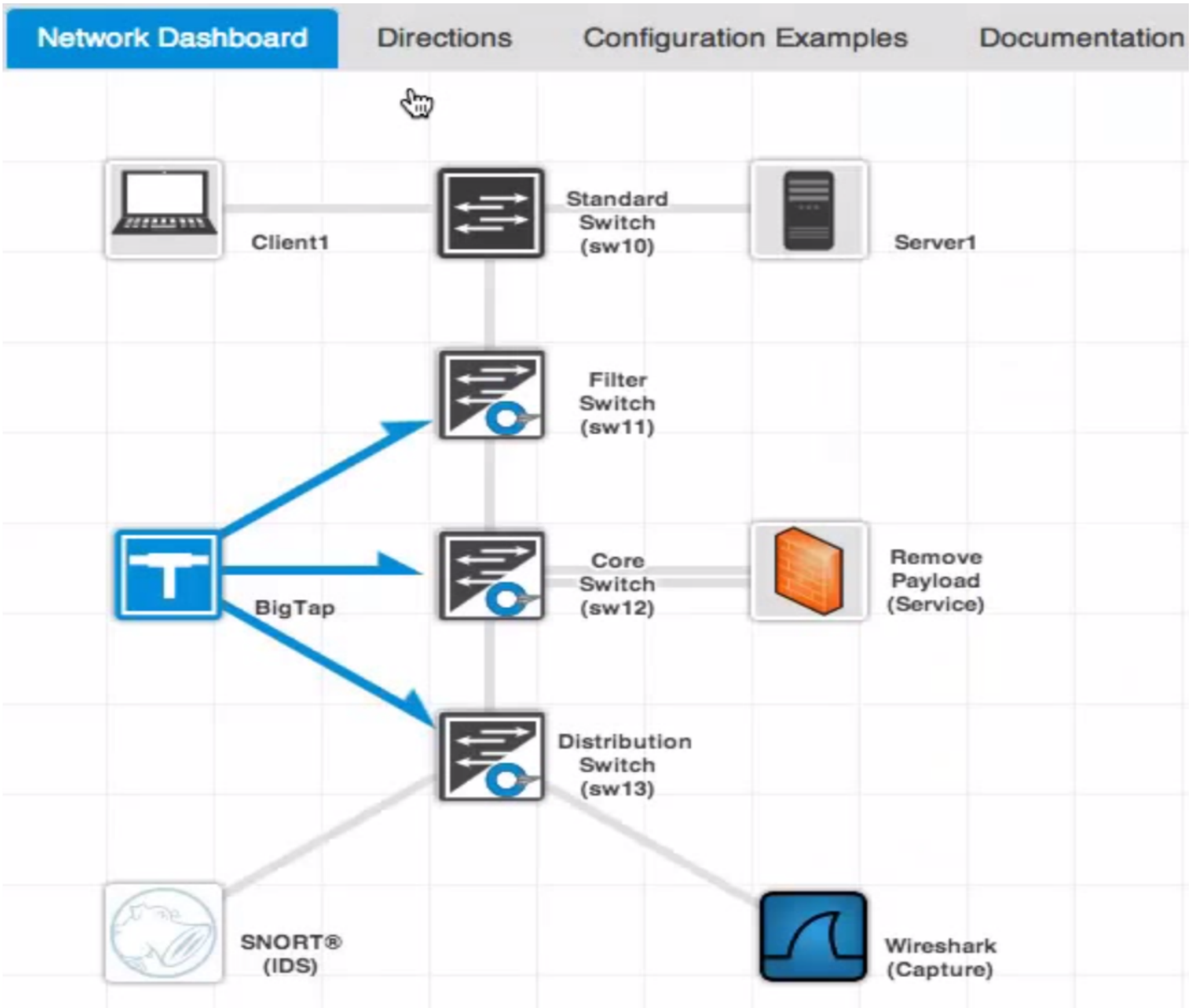


- Costo
- duración de la Limitación del puerto
- Descarte de Paquetes

OpenFlow y SDN



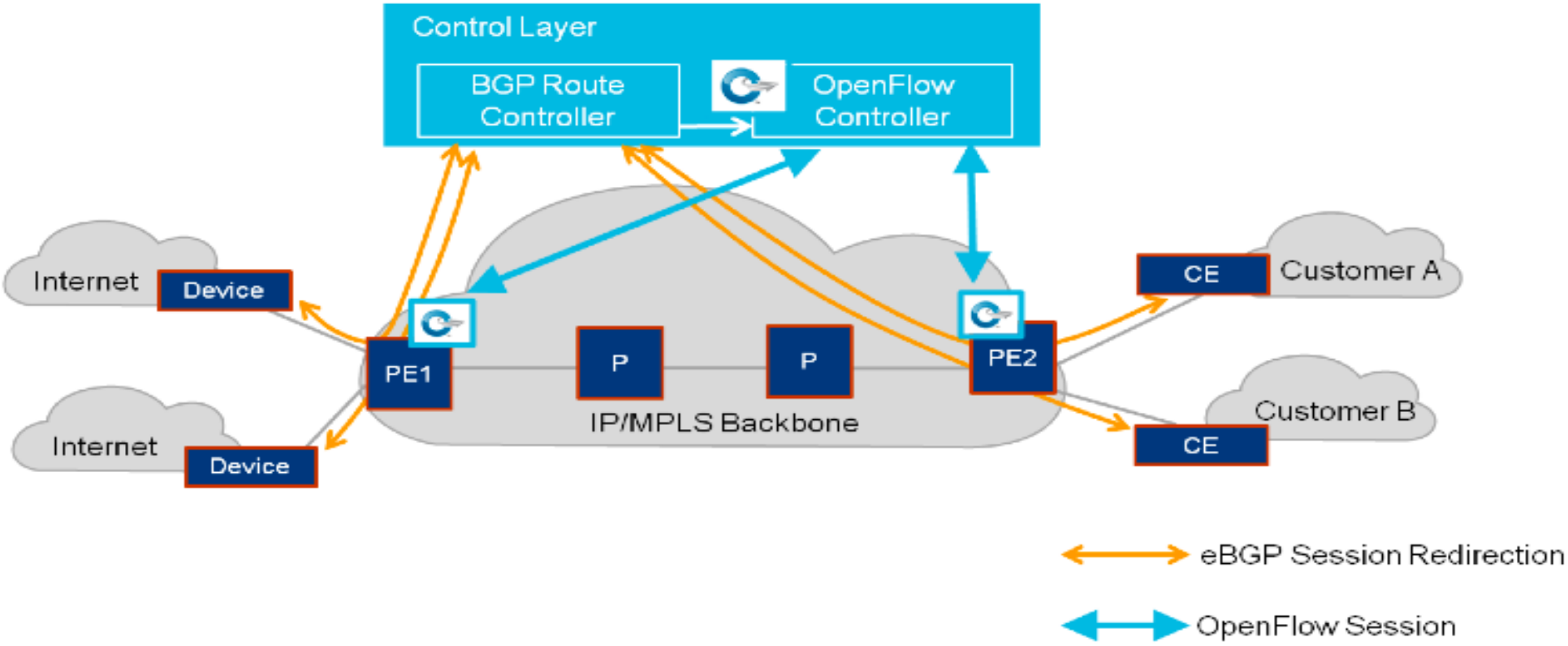
Switch SDN



Big Tap

BGP - Borde Libre

- Simplifica el enrutamiento y reduce la sobrecarga en el PE mediante el almacenamiento y procesamiento de información de enrutamiento BGP en dispositivos de cómputo individuales o en clusters.
- Sesiones BGP remoto en routers CPE “peer” con el controlador de ruta BGP.
- Flujos PE pre-poblado para remitir trafico BGP (TCP 179) al Controlador BGP
- FIB convierte a reglas de reenvío OF e instalado en PE



BGP Borde Libre -Ventajas

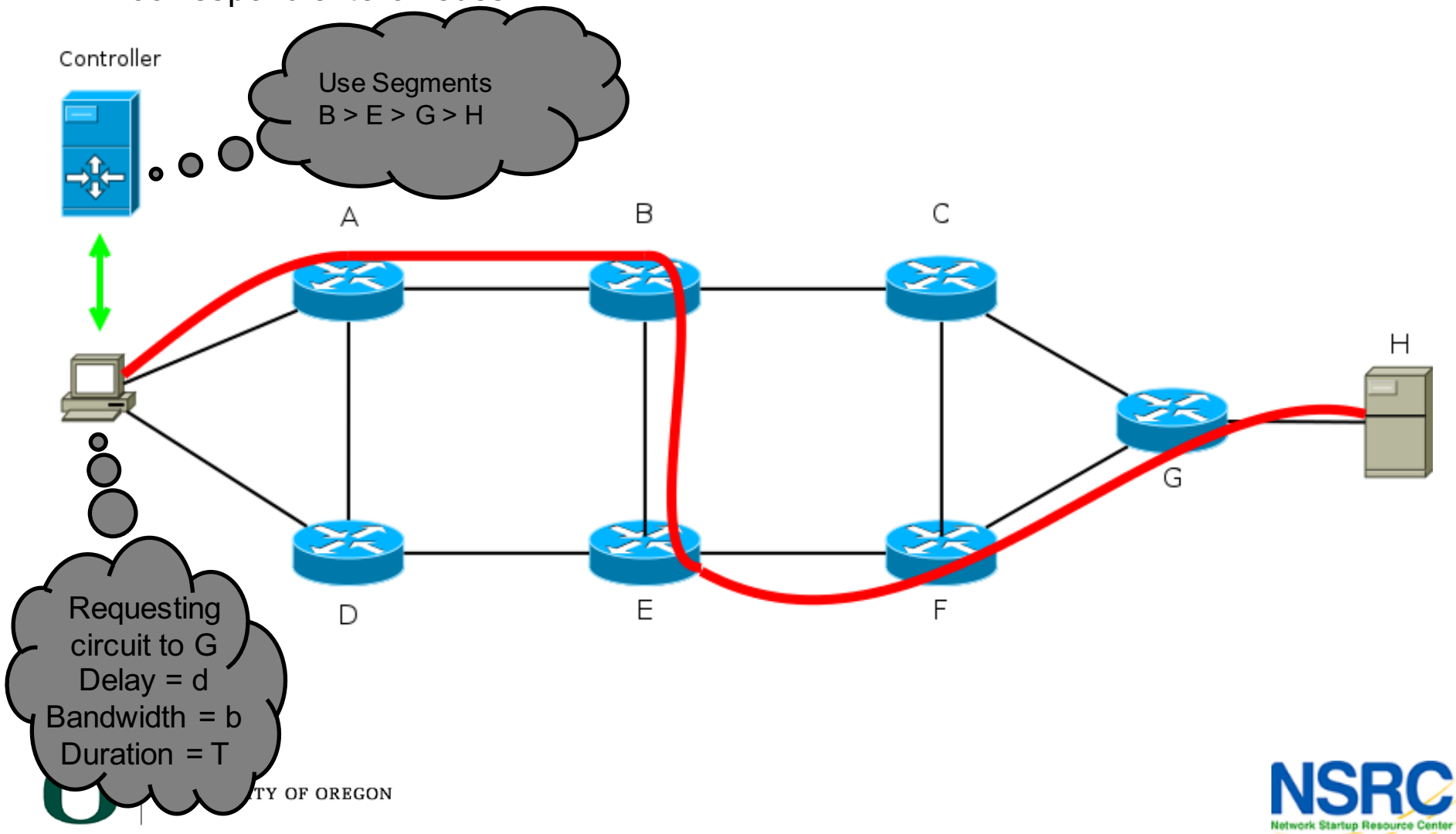
- Enrutamiento de bajo costo simplificado con la política BGP centralizada
- Despliegue acelerado de nuevos servicios de última generación
- Mejor control de los patrones de tráfico en el core.
- Personalizar mejores rutas por cliente
- Puede ayudar a reducir la inestabilidad de BGP en Internet
- Más fácil monitoreo y notificación de BGP debido al controlador de ruta BGP consolidado.
- ESnet “TREEHOUSE” network using BGP-Free-Edge-like for WAN routing
- La red ESnet "ARBOL" utilizando BGP-borde-libre para el enrutamiento WAN

Segmento de enrutamiento

- Ruta expresada como una lista de segmentos (incluidos los servicios !! de entrada (el enrutamiento de origen)
- Soporte de plano de datos para MPLS para IPv6
- Use hardware MPLS existente y plano de datos MPLS o la cabecera del estándar IPv6 existente (es decir, no rompe cosas)
- No LDP, RSVP, T-LDP (señalización salto por salto)
- Menos estados en la red (menos etiquetas y túneles)
- Disponibilidad automática de FRR en cualquier topología
- No hay que esperar para la señalización de nuevss rutas

Aplicación - Enrutamiento Habilitado a través de SR

- La aplicación solicita una ruta específica con atributos.
- El controlador OpenFlow provisiona rutas a través solicitud de aplicación correspondiente a redes.



Circuito de aprovisionamiento

- L2, L3, MPLS, VLAN o su combinación
- CWDM, DWDM (a través de extensiones de protocolo ópticos)
- Dinámico, Programado o Permanente
- Rutas de respaldo predeterminadas o permite la selección dinámica
- La aplicación puede estar vinculado a otros sistemas y conocimiento de
  - Inventario
  - Estados del puerto, circuito y la utilización del punto final
  - Las tasas de error, Jitter y latencia
  - Los tiempos de mantenimiento Programado
- Reducir los tiempos de aprovisionamiento
- Permitir el aprovisionamiento de autoservicios

Circuito de aprovisionamiento en Internet 2 usando OESS

- OESS - Servicio
  - – intercambio de Capa-2 distribuido a nivel nacional
  - –Persistente, bajo demanda y programada L2 VLAN
  - –SPF o selección de ruta manual (primario y de respaldo)
  - –QoS y Selección de ancho de banda
- OESS - Casos de uso
  - –Rutas de alta ancho de banda para la transferencia de archivos grandes
  - –Conectividad de capa 2 entre bancos de prueba
  - –Intercambio Distribuido para peering IP

Circuito de aprovisionamiento en Internet 2 usando OESS

- http://www.internet2.edu/products-services/advanced-networking/oess/
- https://globalnoc.iu.edu/sdn/oess.html

Circuito de aprovisionamiento OESS (Cont)

OpenFlow Ventajas

- Los comandos de la CLI no se requieren para el aprovisionamiento
  - –Diferente a través de las plataformas
  - –cambios con nuevas revisiones
  - –No espera Scripts
  - –Reduce los tiempos de aprovisionamiento a <1 seg
- Igual través múltiples plataformas de conmutación
- No Spanning Tree Requerido

OESS Características principales

- Desarrollada una vez he implementada en muchos tipos diferentes de switches
- Utiliza D-Bus para comunicarse con el controlador OpenFlow permitiendo una fácil migración a otros controladores OpenFlow en el futuro.
- Tiempo del circuito de aprovisionamiento: <1 segundo típicamente
- Failover automatizado para ruta de respaldo
- Redundancia del Controlador

OESS Demo

Provisioning a VLAN: http://youtu.be/LncYCJ2QCIw

Qué puede aportar OpenFlow para el centro de datos

- API estándar para el aprovisionamiento de la red (ejemplo orquestación)
- Integración con conmutadores basados en VM (por ejemplo Open vSwitch)
- New network behaviors that permit scaling to million-VM data centers
- Nuevos comportamientos de red que permiten la ampliación de millones de centros de datos Virtuales.
- Potencial para ODMs para proporcionar soluciones más rentables

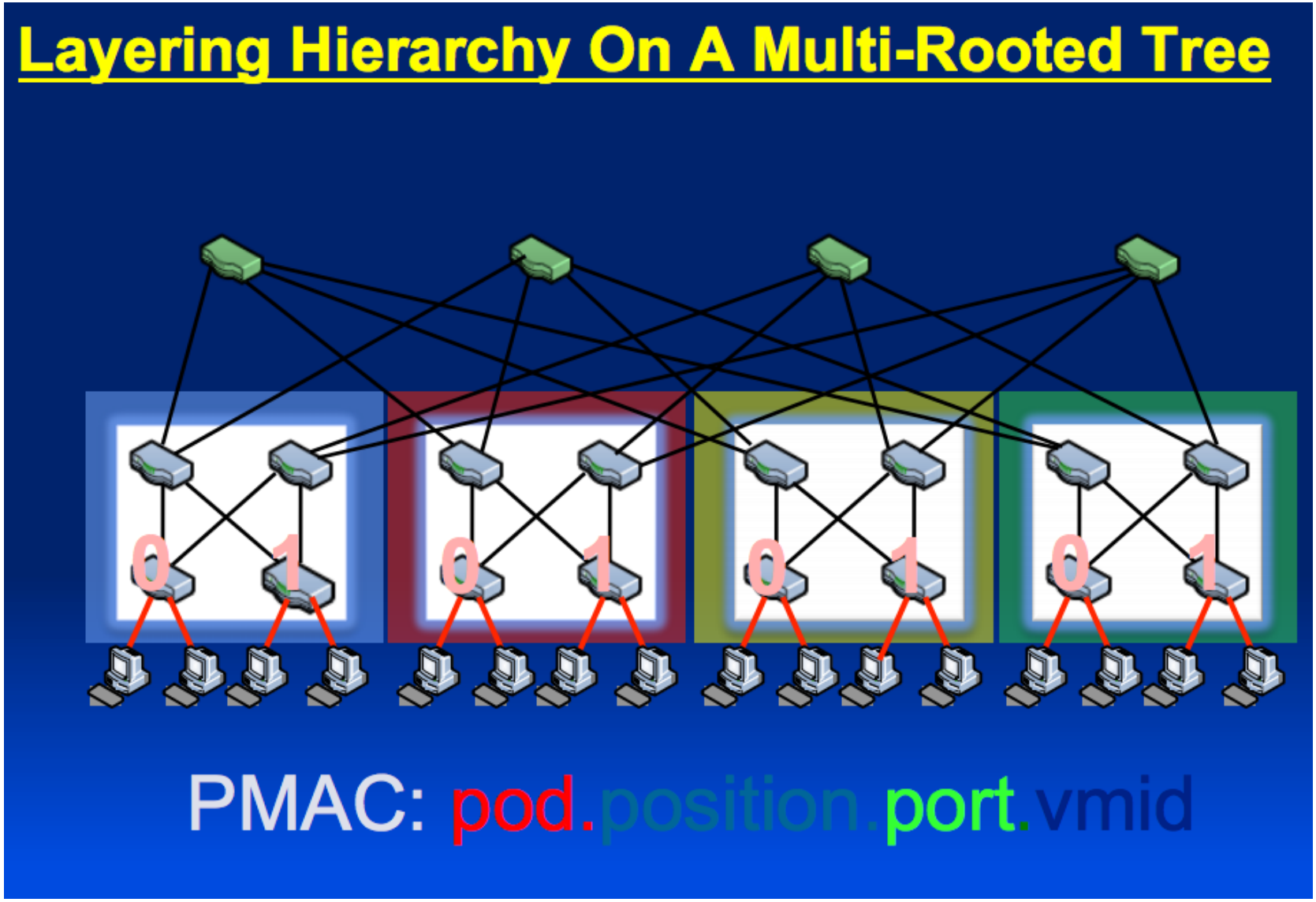
Resolviendo Desafíos en los centros de datos

Los grandes operadores de centros de datos andan por su propia cuenta. Ellos hacen sus propios servidores, sus propios diseños de centros de datos, y su propio software para resolver problemas específicos. Ofrecerles un protocolo estándar que proporciona un control detallado de hardware de red barato, y ellos lo compraran son dudarlo.
Ejemplos incluyen:

Si “El Plano Entropía" había tenido un ancho de banda de bisección bajo, construir redes de árboles de grasa a base de switches de bajo costo mediante la programación de la red para el centro de datos a través de OpenFlow (por ejemplo, de Portland)

si el aprovisionamiento de red es lenta y manual, aprovechar una API de red abierta para crear una mejor orquestación

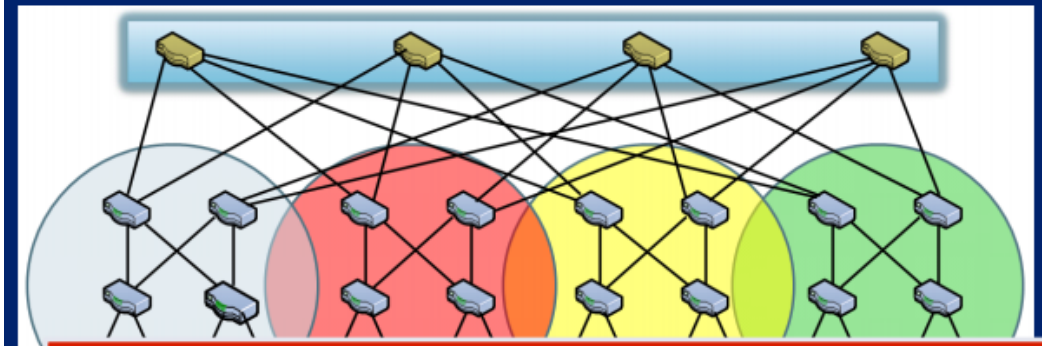
Portland direccionamiento jerárquico



from: http://web.stanford.edu/class/ee380/Abstracts/091118-DataCenterSwitch.pdf

Portland direccionamiento jerárquico

PortLand: Plug and Play + Small Switch State



\+ Pair-wise communication

1. PortLand switches learn location in topology using pair-wise communication
2. They assign topologically meaningful addresses to hosts using their location

PMAC Address	Out Port
0:2:x:x:x:x	0
0:4:x:x:x:x	1
0:6:x:x:x:x	2
0:8:x:x:x:x	3

- 10 million virtual endpoints in 500,000 servers in data center

- 100 – 1000 address mappings → ~10 KB of memory → easily accommodated in switches today

from: http://web.stanford.edu/class/ee380/Abstracts/091118-DataCenterSwitch.pdf

Otros ejemplos de SDN

SDN vs NFV

	Software-Defined Networking	**Network Function Virtualization**
Basic Concept	Separate control & data plane, centralized control & programmable network	Move network functions from dedicated appliances to generic servers
Target Location	Campus, Data Center, Cloud	Service Providers
Target Devices	Commodity servers and switches	Commodity servers and switches
Initial Applications	Cloud orchestration & networking	Routers, firewalls, gateways, CDN, WAN accelerators, SLA assurance
New Protocols	OpenFlow	None
Formalization	Open Networking Foundation	ETSI NFV Working Group

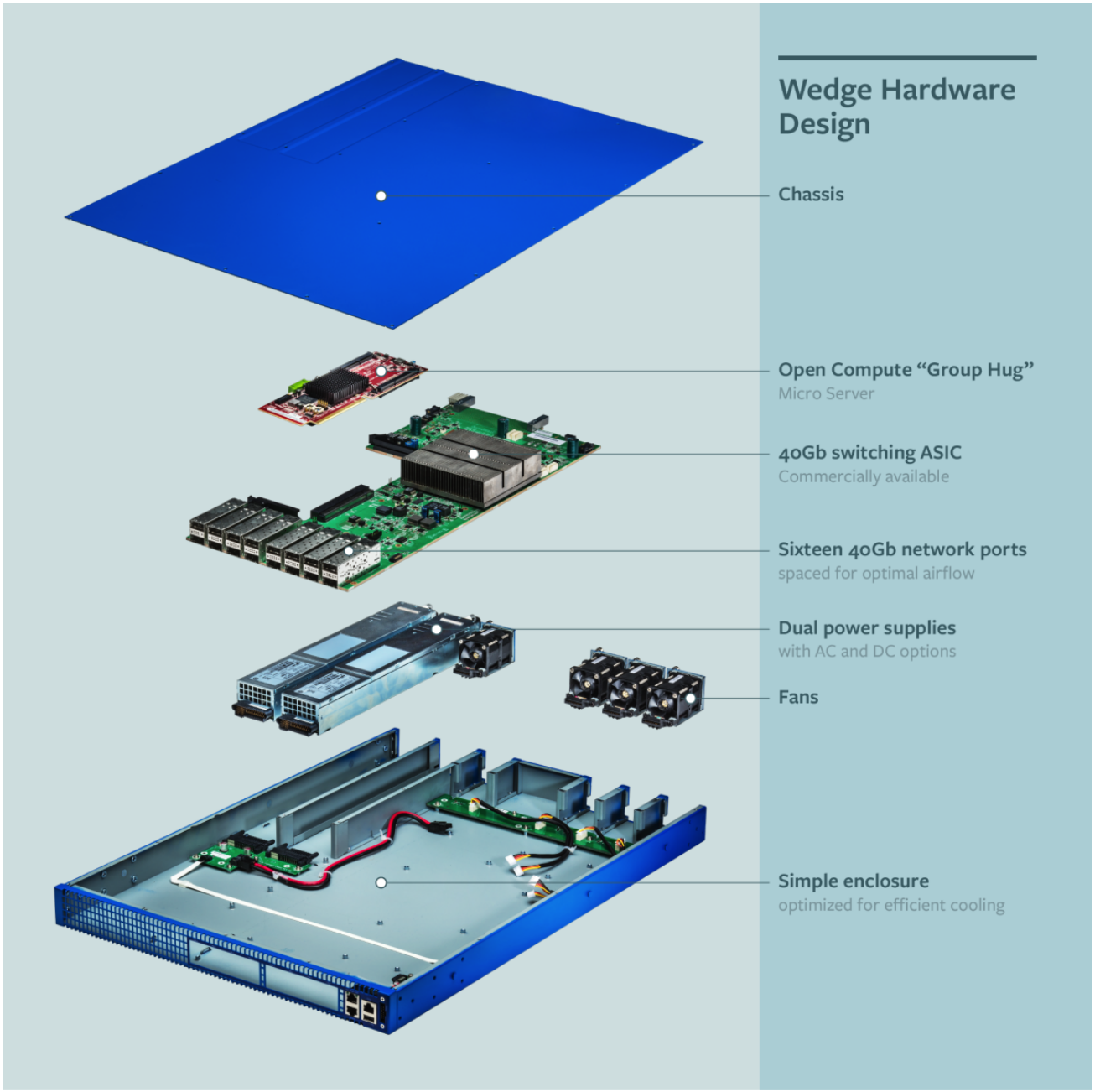
Red Virtualizada

Proyecto Open Compute

- Diseños de hardware de código abierto
- Inicialmente servidores y rack, pero ahora incluye switches en la parte superior de los rack (ToR)
- Otro facilitador para switches de caja blanca (Basados en Linux)
- Rackspace servidores de la nube de solo metal

http://www.opencompute.org/

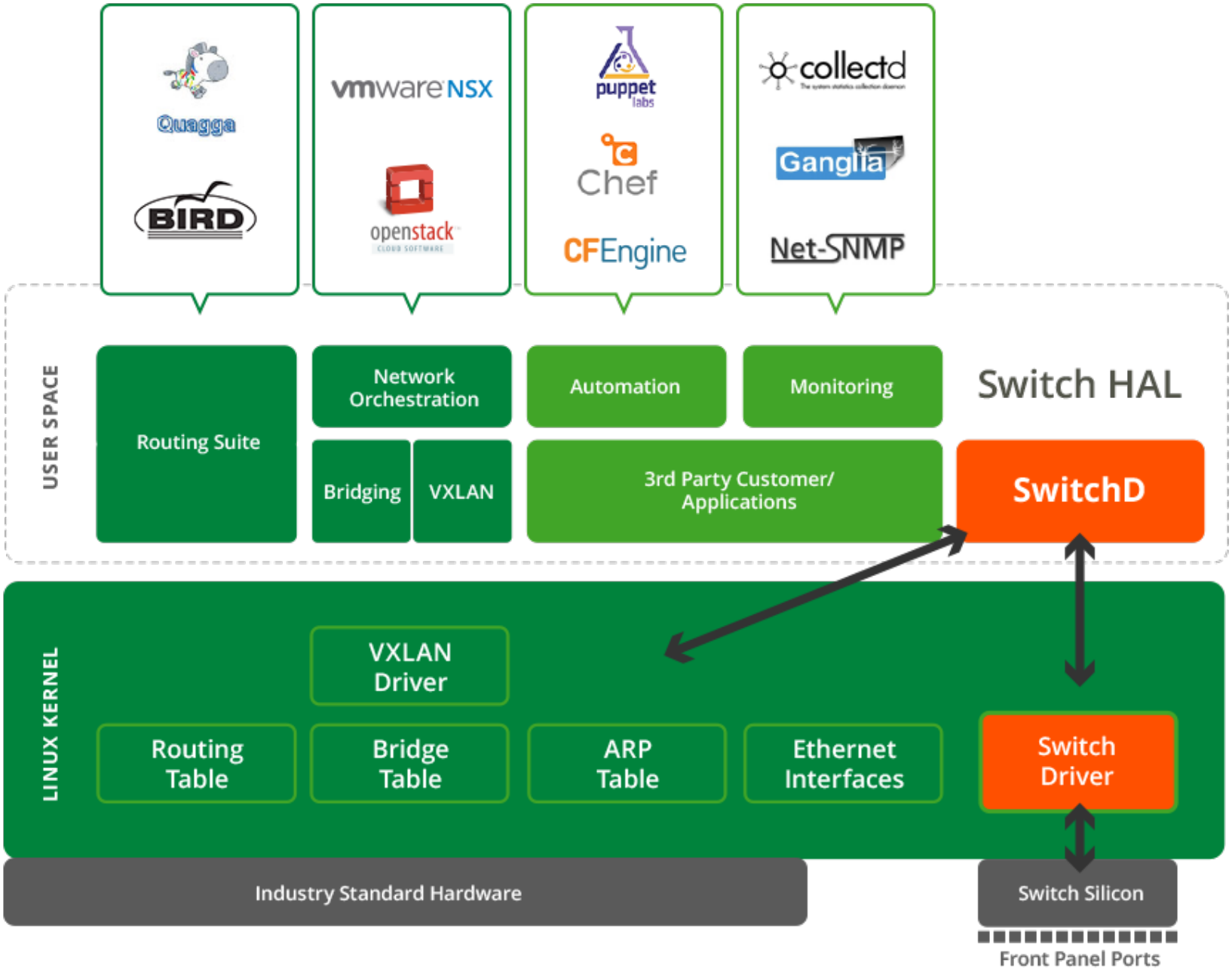
Facebook “Wedge”



NSRC
Network Startup Resource Center

Switches de caja blanca (Basados en Linux)

- Construido sobre silicona (x86 equivalente)
- Network OS Boot Loaders
- Sistemas operativos basados en Linux
- Puede provisionar con herramientas de orquestación
- Muchos Proyectos
  - Cumulus Linux & ONIE
  - Facebook "Wedge"
  - ARISTA (API abierta)
  - PICA8 (OpenFlow + OVS)
  - Big Switch networks (Switch Light)



Source: http://cumulusnetworks.com/product/architecture/

Switch de caja blanca (Linux)
Cumulus Networks - Switch OS

40G Portfolio	Model number	Description	Switch Silicon	CPU Type	Minimum Cumulus Linux Release
DELL	S6000-ON (S6000 with ONIE)	32 x 40G-QSFP+	Broadcom Trident II	x86	Cumulus Linux 2.1
Edge-corE	AS6701-32X (AS6700-32X with ONIE)	32 x 40G-QSFP+	Broadcom Trident II	PowerPC	Cumulus Linux 2.0.1
PENGUIN COMPUTING	Arctica 3200XL (with ONIE)	32 x 40G-QSFP+	Broadcom Trident II	PowerPC	Cumulus Linux 2.0
Quanta	QuantaMesh T5032-LY6 (with ONIE)	32 x 40G-QSFP+	Broadcom Trident II	PowerPC	Cumulus Linux 2.1

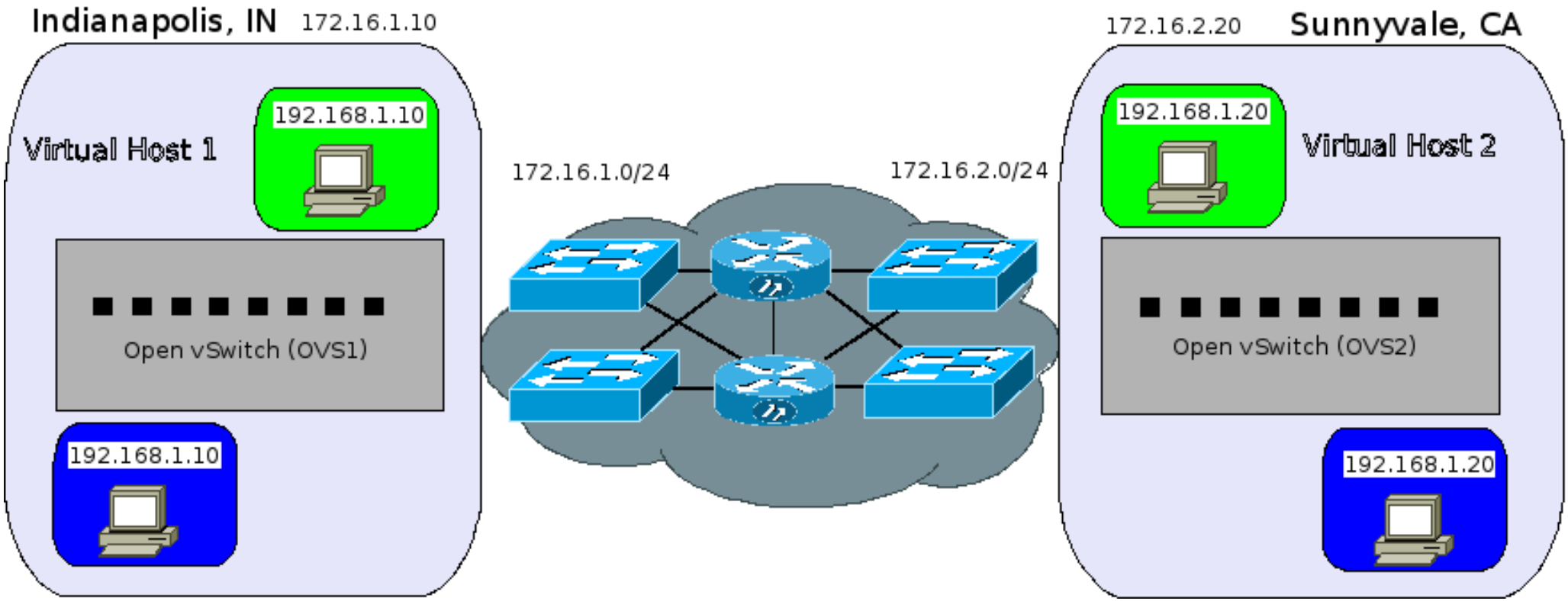
Superposiciones (e.g., VXLAN)

- La construcción de una red de capa 2 (por ejemplo, VLAN) en la parte superior de una red IP a través de un túnel
- El factor clave es el vSwitch
- Superposiciones de capa 2 expuestas como VLAN para máquinas virtuales
- onramp/offramp para hacer un túnel a través de VXLAN túnel de punto final (VTEP.)

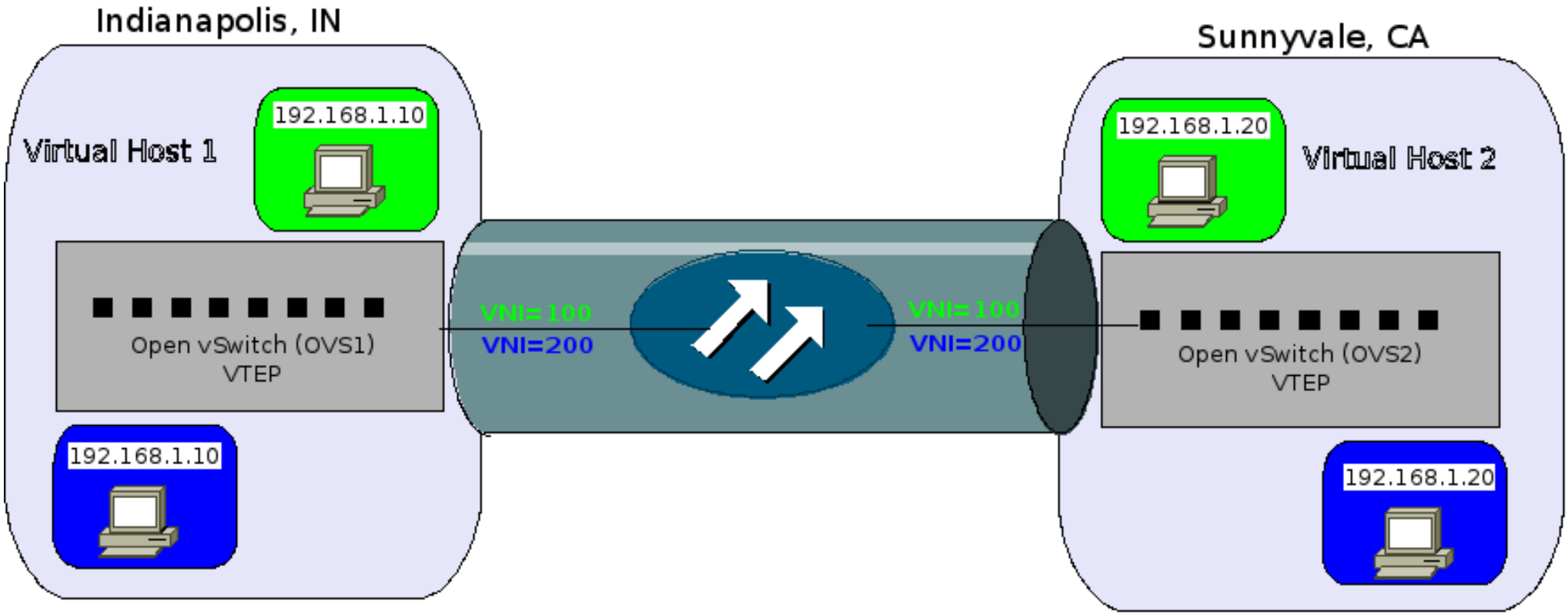
Objetivo - redes dinámicas para nubes multi-tenant construidas en la parte superior de la red IP estática

- Aplicación bajo demanda

4096 VLAN Limitacion



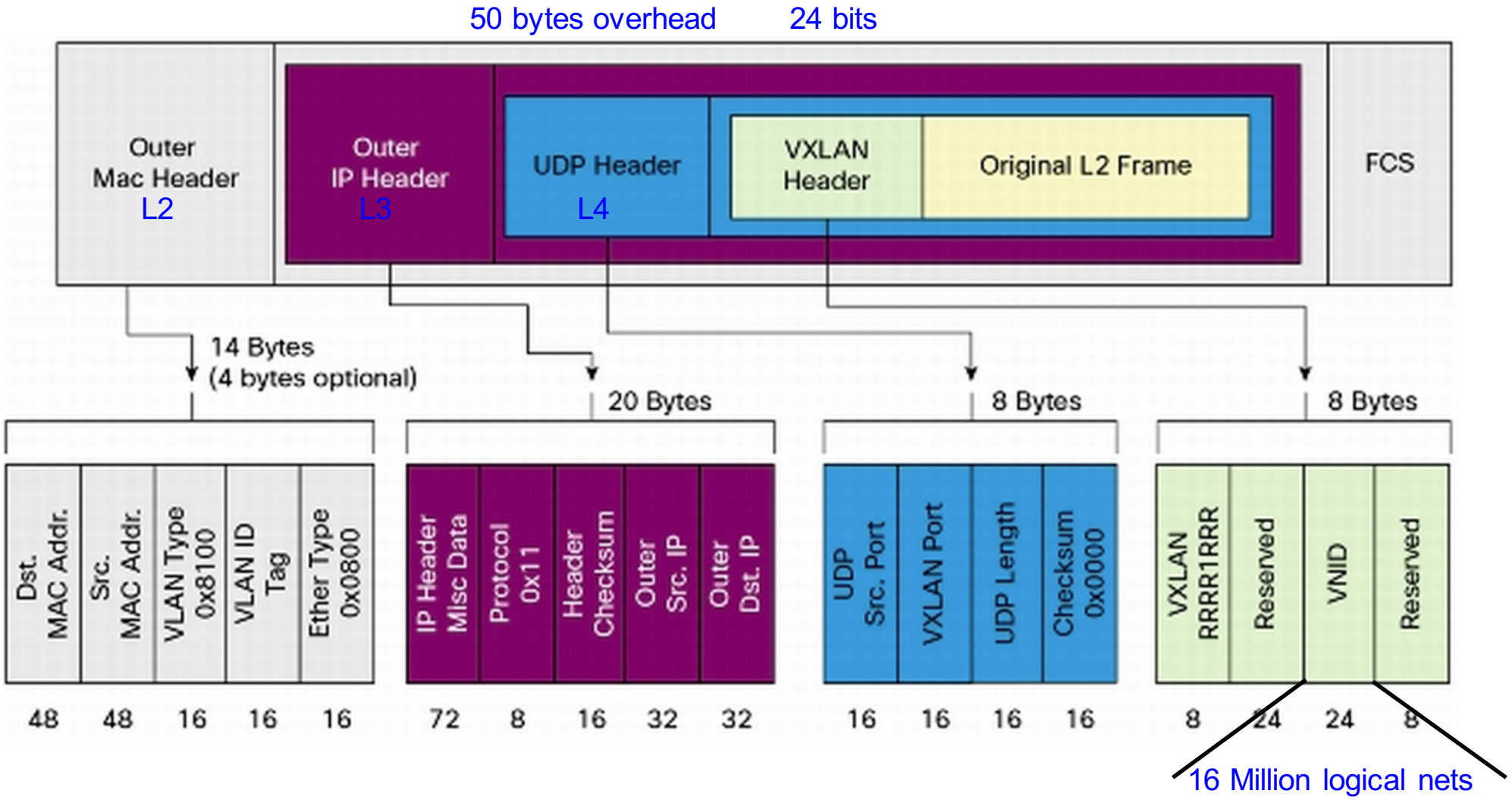
Identificador de Virtual de red



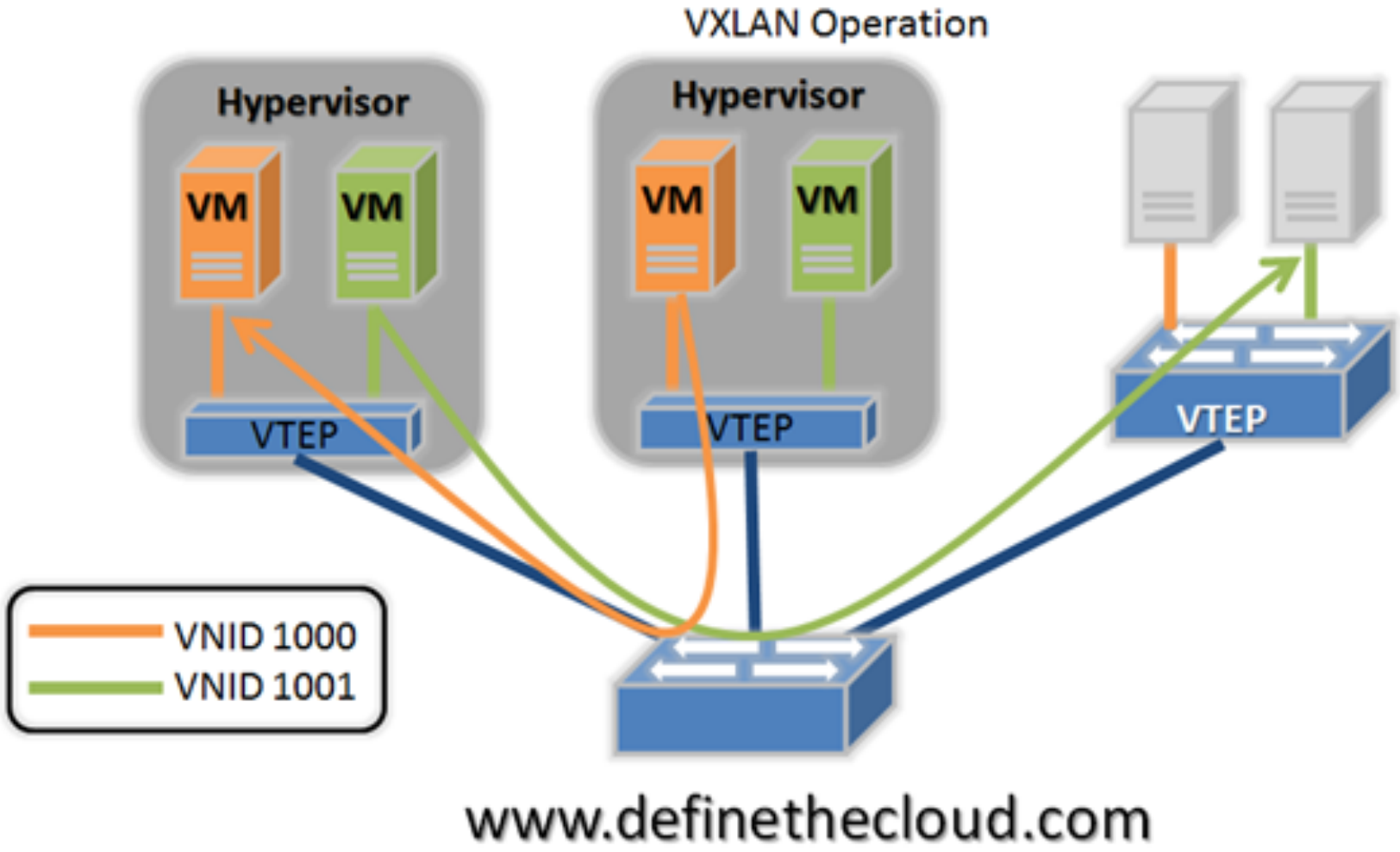
sudo ovs-vsctl add-port ovs1 vtep --
set interface vtep type=vxlan
option:remote_ip=192.168.1.20
option:key=flow ofport_request=5

sudo ovs-vsctl add-port ovs2 vtep --
set interface vtep type=vxlan
option:remote_ip=192.168.1.10
option:key=flow ofport_request=5

Encapsulación VXLAN

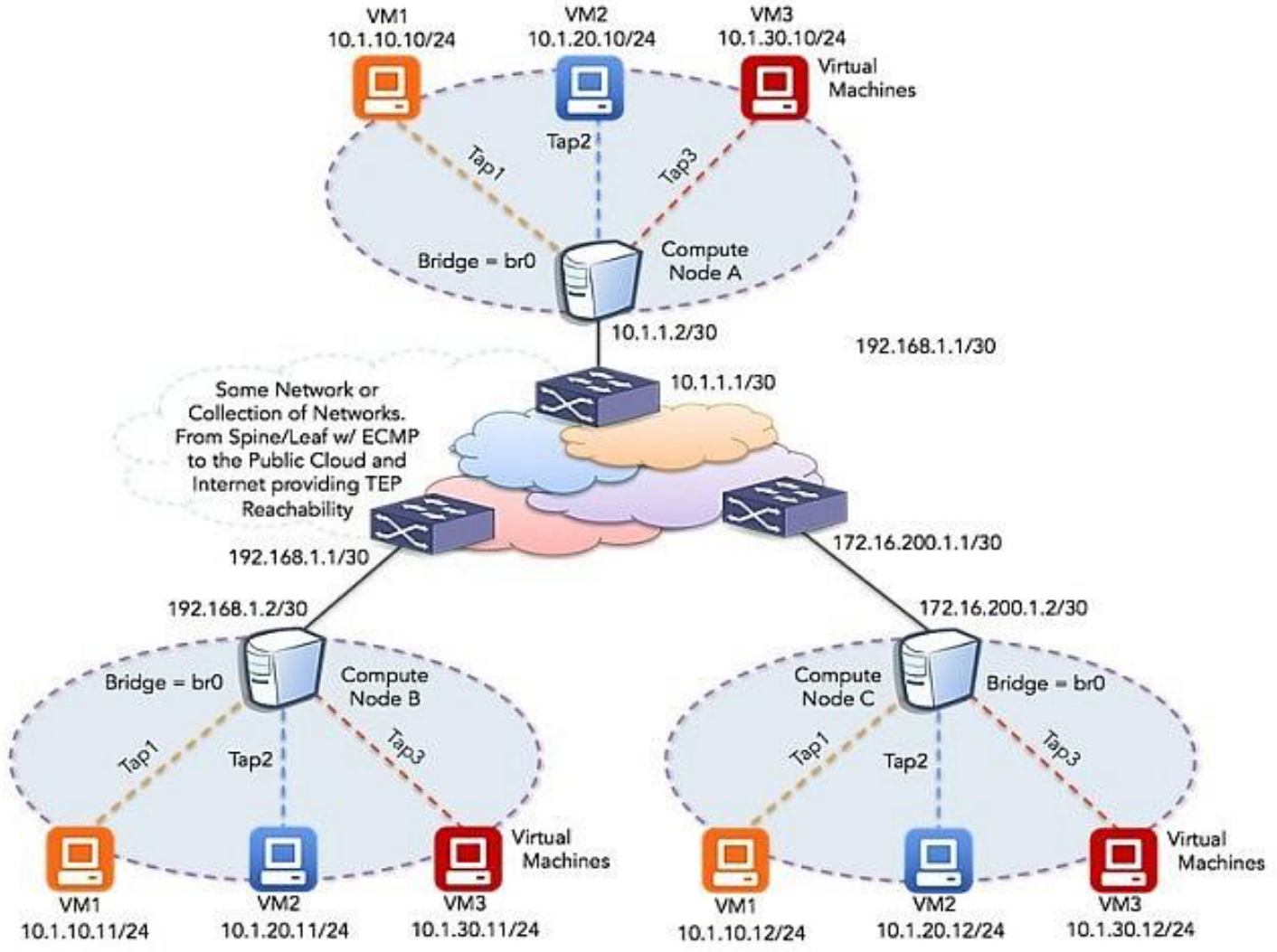


VXLAN Reenvío de paquetes



from: http://ipengineer.net/2014/06/vxlan-mtu-vs-ip-mtu-consideration/

Configuración de superposiciones en Open vSwitch



Source: http://networkstatic.net/setting-overlays-open-vswitch/

OpenStack

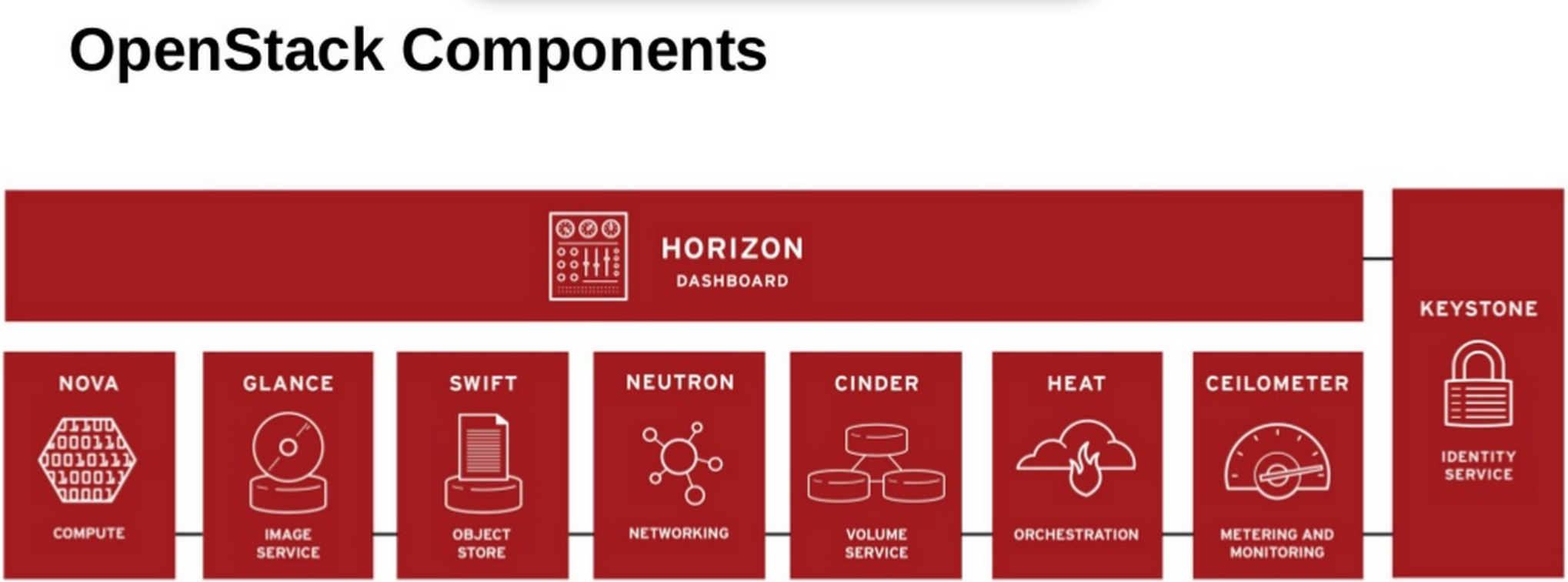
La Pila de nube de código abierto

Soporta SDN (servicios de red se aprovisionan, junto con otras infraestructura en la nube)

Todas las Controladoras de SDN se integrarán con OpenStack

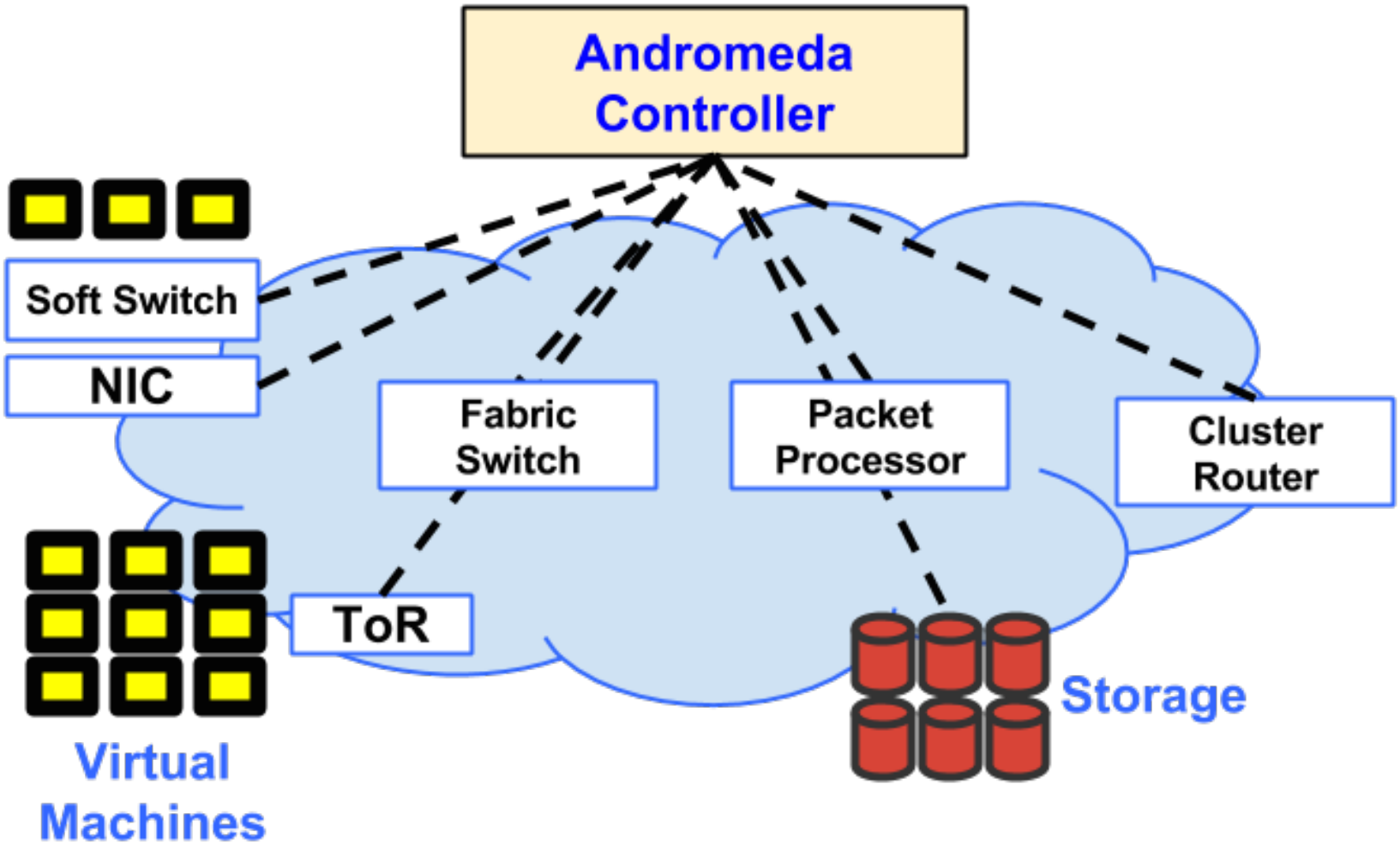
RackSpace está usando GRE como protocolo de túnel para el aprovisionamiento de red dinámico

OpenStack



from: http://www.slideshare.net/ProxyServices/open-stack-latest-pure-tech-proxyservices?related=1#

Andromeda de Google



Souce: Gigaom

Preguntas / Discusión?

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center