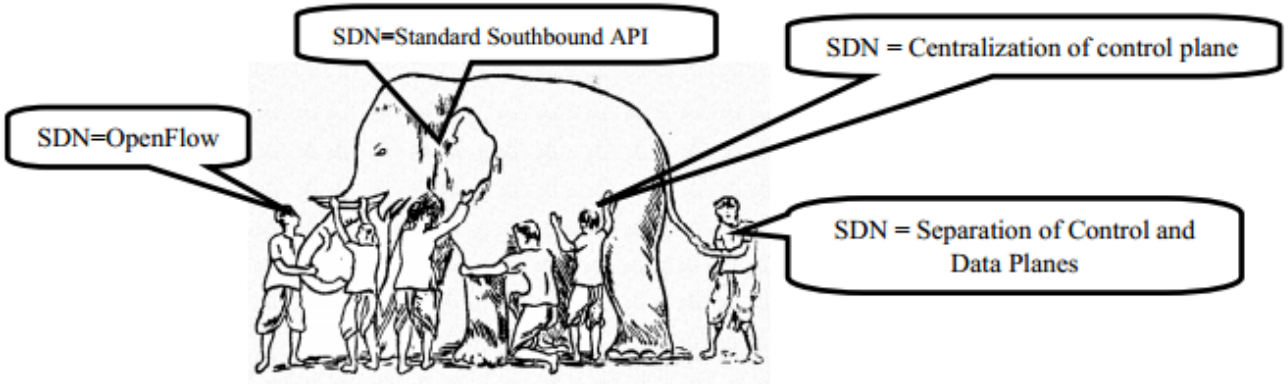
OpenFlow, Software Defined Networking (SDN) and Network Function Virtualization (NFV)



Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130, Jain@cse.wustl.edu

Tutorial at 2014 IEEE 15th International Conference on High Performance Switching and Routing, Vancouver, Canada, July 1, 2014

These slides and audio/video recordings of this tutorial are at:

http://www.cse.wustl.edu/~jain/tutorials/sd_hs14.htm

Índice

1. OpenFlow y sus herramientas
2. Software Defined Networking (SDN)
3. Network Function Virtualization (NFV)

Parte I: OpenFlow y sus herramientas

- Planos de Red
- OpenFlow
- Switches OpenFlow, incluyendo Open vSwitch
- Evolución OpenFlow
- Configuración del Protocolo OpenFlow
- Entorno de Notificaciones OpenFlow
- Controladores OpenFlow

Parte II: Software Defined Networking

- ¿Qué es SDN?
- APIs alternativas: XMPP, PCE, ForCES, ALTO
- Plataforma del Controlador SDN OpenDaylight y herramientas

Parte III Network Function Virtualization

- ¿Qué es NFV?
- Relación entre NFV y SDN
- Especificaciones ETSI, NFV, ISG
- Conceptos, Arquitectura, Requerimientos, Casos de Uso
- Pruebas de Concepto y Cronología

Parte I

OpenFlow y sus Herramientas

Parte I: OpenFlow y sus herramientas

- Planos de Red
- OpenFlow
- Switches OpenFlow, incluyendo Open vSwitch
- Evolución OpenFlow
- Configuración del Protocolo OpenFlow
- Entorno de Notificaciones OpenFlow
- Controladores OpenFlow

Planos de Red

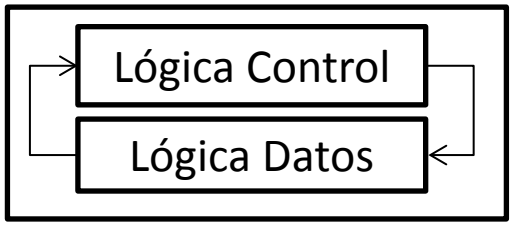
- Plano de Datos: Todas las actividades que involucren o resulten del envío de paquetes por el usuario final, por ejemplo:
  - Envío
  - Fragmentación y reconstrucción
  - Replicación para multicast
- Plano de Control: Todas las actividades que son necesarias para llevar a cabo las acciones del plano de datos pero que no involucran a los paquetes del usuario final. Por ejemplo:
  - Construcción de tablas de ruta
  - Establecimiento de políticas sobre los paquetes (ej. seguridad)
  - Beacons de las estaciones base anunciando disponibilidad de servicios.

Planos de Red (Cont.)

- Plano de Gestión: Todas las actividades relacionadas con el suministro y monitorización de la red.
  - Fallos, Configuración, Contabilidad, Rendimiento y Seguridad (FCAPS)
  - Instanciar nuevos dispositivos y protocolos
  - Es opcional: Puede hacerse de manera manual en redes pequeñas
- Plano de Servicios: Middleboxes que mejoran el rendimiento o la seguridad, etc
  - Balanceadores de Carga, Proxys, Detección de Intrusos...
  - Es opcional: No se requiere en redes pequeñas

Datos vs. Lógica de Control

- El plano de datos se ejecuta a la velocidad de línea de la red; por ejemplo: 100 Gbps para un Ehernet de 100 Gbps → Camino rápido (Fast Path)
  - Típicamente implementado en hardware dedicado; por ejemplo TCAMs (Ternary Content Addressable Memory)
- Algunas actividades de plano de datos son gestionadas por la CPU del switch →Camino Lento (Slow Path)
  - Por ejemplo: Tráfico Broadcast, Desconocido y Multicast
- Todas las actividades de control son manejadas por la CPU



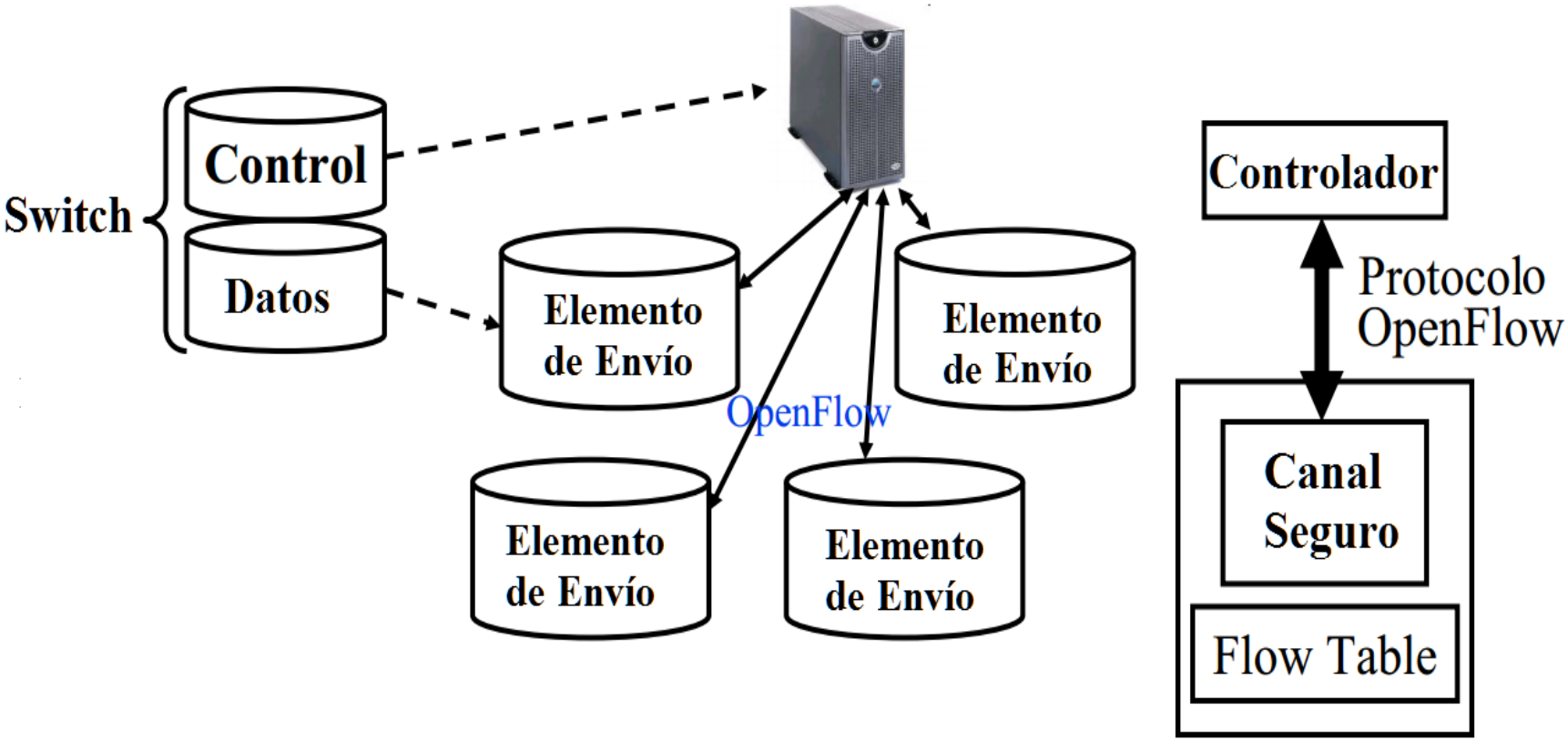
OpenFlow: Ideas Clave

- Separación de los planos de datos y control
- Centralización del control
- Control basado en flujos

Historia de OpenFlow

- 2006: Martin Casado, estudiante de doctorado en Stanford, y su equipo proponen hacer desde cero una arquitectura de seguridad (SANE) que define un control centralizado (en lugar de en los límites como se hacía normalmente).
  Ethane lo generaliza a todas las políticas de acceso
- Abril 2008: Paper OpenFlow en ACM SIGCOMM CCR
- 2009: Stanford publica las especificaciones OpenFlow V1.0.0
- Junio 2009: Martin Casado co-funda Nicira
- Marzo 2010: Guido Appenzeller, director del laboratorio *clean-slate* de Stanford (dedicado a rediseñar Internet desde cero, sin la complejidad acumulada), cofunda Big Switch Networks
- Marzo 2011: Se forma la Open Networking Foundation
- Octubre 2011: Primera Cumbre Open Networking.
- Juniper, Cisco anuncian planes para incorporarse a ONF.
- Julio 2012: VMware compra Nicira por 1.26 mil millones de $
- Noviembre 6, 2013: Cisco compra Insieme por 838 millones de $

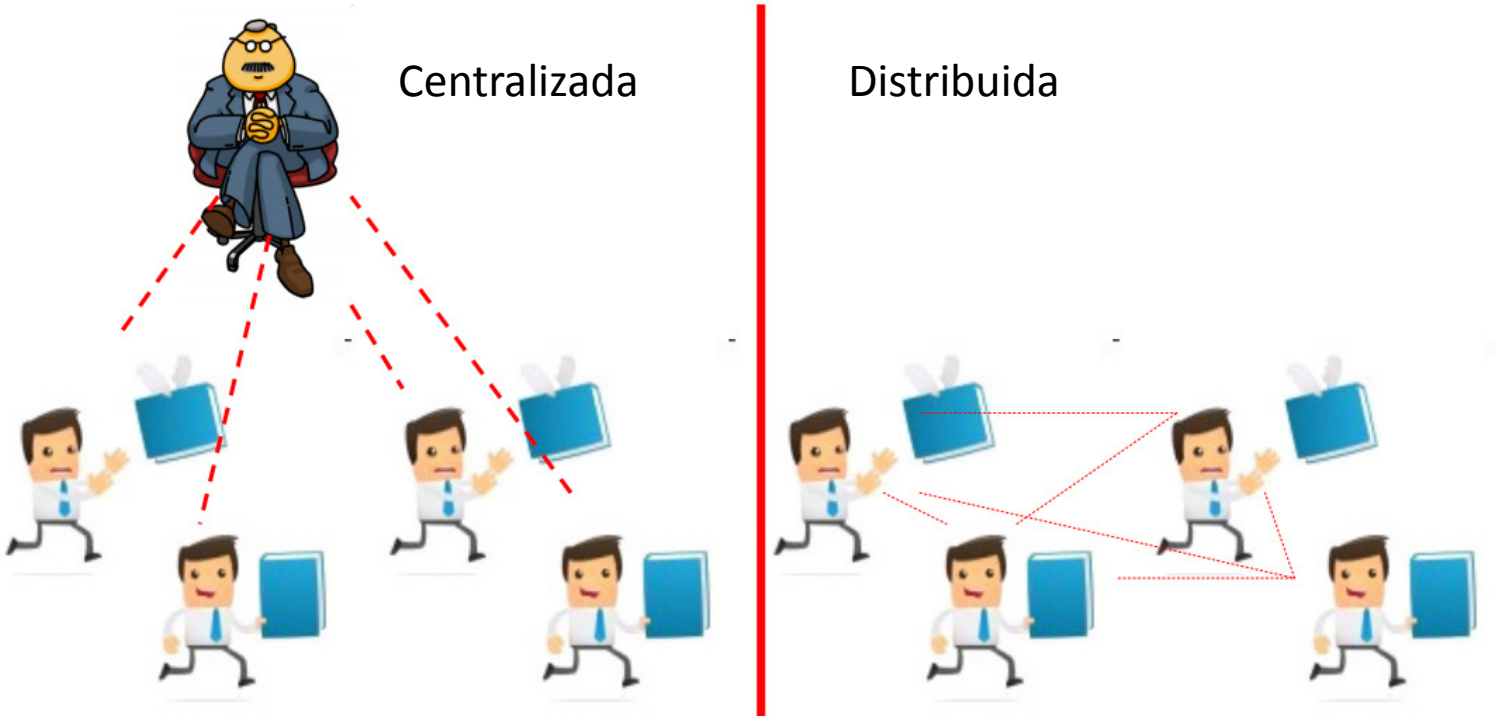
Separación de los Planos de Control y Datos



Separación de los Planos de Control y Datos (Cont.)

- La lógica de Control se mueve a un controlador
- Los switches tan sólo tienen elementos de envío
- Un controlador caro con muchos switches baratos
- *OpenFlow es el protocolo para enviar/recibir reglas de envío del controlador a los switches*

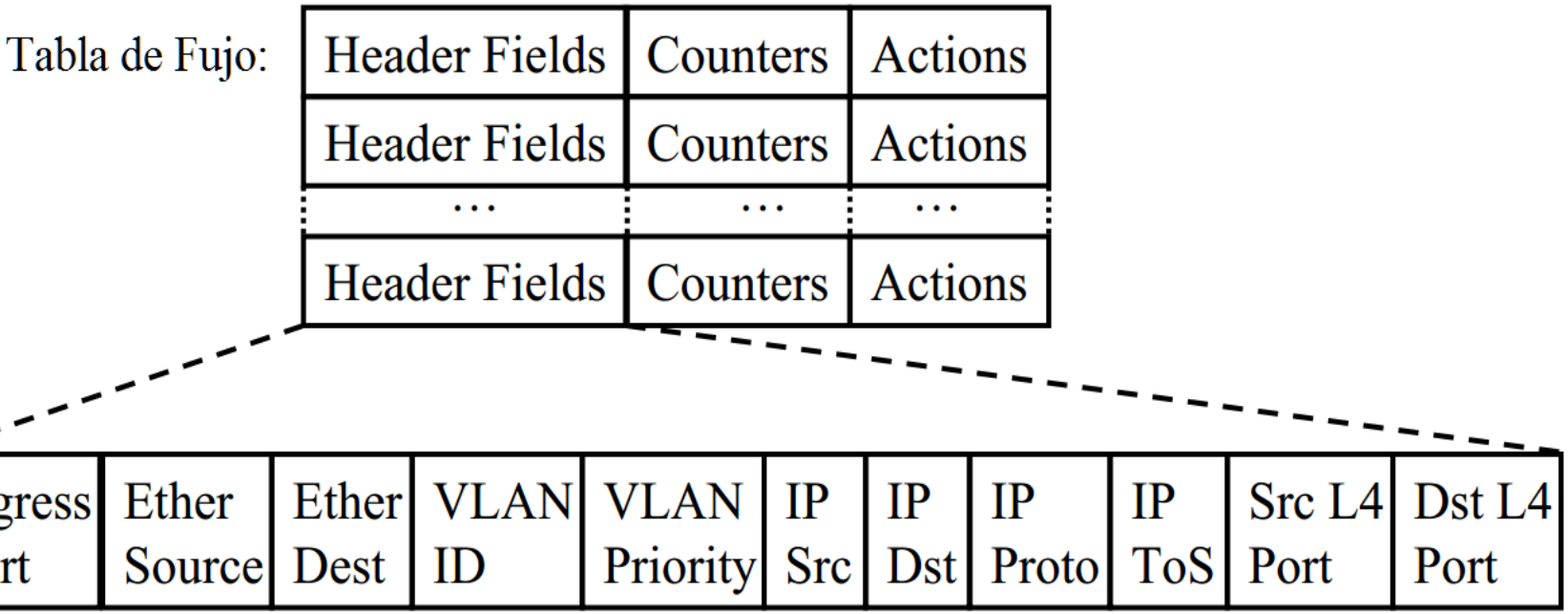
Centralización del Plano de Control



- Consistencia
- Rápida respuesta a cambios
- Fácil gestión de muchos dispositivos

OpenFlow V1.0

- A la llegada del paquete, comparar los campos de cabecera con las entradas de flujo en una tabla, actualizar los contadores indicados en esa entrada y realizar las acciones indicadas

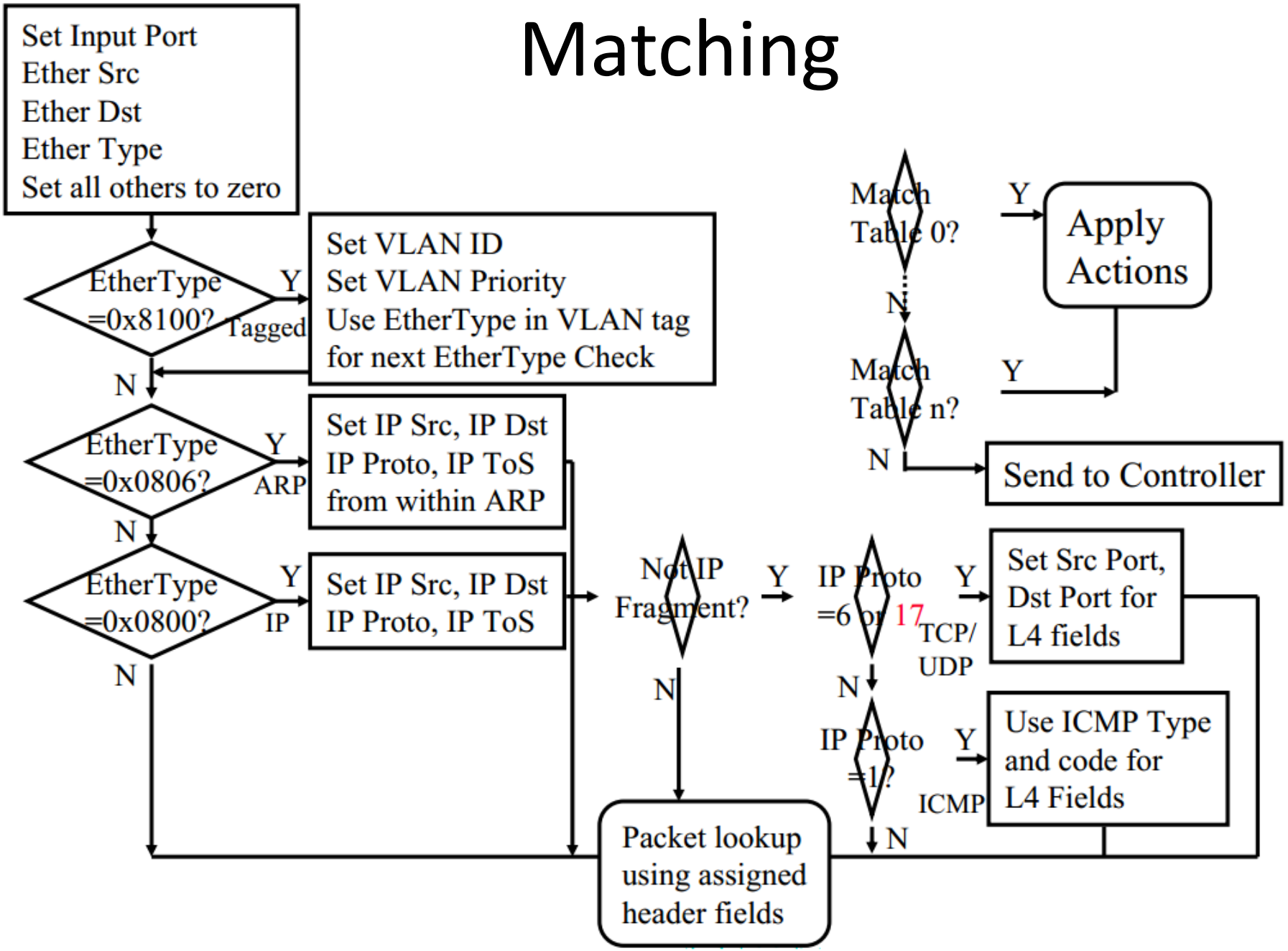


Ejemplo de Tabla de Flujo

Port	Src MAC	Dst MAC	VLAN ID	Priority	EtherType	Src IP	Dst IP	IP Proto	IP ToS	Src L4 Port ICMP Type	Dst L4 Port ICMP Code	Action	Counter
*	*	0A:C8:*	*	*	*	*	*	*	*	*	*	Port 1	102
*	*	*	*	*	*	*	192.168.*.*	*	*	*	*	Port 2	202
*	*	*	*	*	*	*	*	*	*	21	21	Drop	420
*	*	*	*	*	*	*	*	0x806	*	*	*	Local	444
*	*	*	*	*	*	*	*	0x1*	*	*	*	Controller	1

- Idle Timeout: Eliminar la entrada si no se reciben paquetes durante ese tiempo.
- Hard Timeout: Eliminar entrada tras pasar ese tiempo
- Si se establecen las dos, la entrada se elimina si una expira

Matching


Set Input Port
Ether Src
Ether Dst
Ether Type
Set all others to zero
EtherType =0x8100?
Y
Tagged
Set VLAN ID
Set VLAN Priority
Use EtherType in VLAN tag for next EtherType Check
N
EtherType =0x0806?
Y
ARP
Set IP Src, IP Dst
IP Proto, IP ToS
from within ARP
N
EtherType =0x0800?
Y
IP
Set IP Src, IP Dst
IP Proto, IP ToS
N
Not IP Fragment?
Y
N
IP Proto =6 or 17
Y
TCP/ UDP
Set Src Port, Dst Port for L4 fields
N
IP Proto =1?
Y
ICMP
Use ICMP Type and code for L4 Fields
N
Packet lookup using assigned header fields
Match Table 0?
Y
Apply Actions
N
Match Table n?
Y
N
Send to Controller

Contadores

Por Tabla	Por Flujo	Por Puerto	Por Cola
Entradas Activas	Paquetes Recibidos	Paquetes Recibidos	Paquetes Transmitidos
Búsqueda Paquetes	Bytes Recibidos	Paquetes Transmitidos	Bytes Transmitidos
Packet Matches	Duración (s)	Bytes Recibidos	Nº Errores de rebose
	Duración (nano s)	Bytes Transmitidos	
		Nº Pqs desechados TX	
		Nº Pqs desechados RX	
		Errores Recibidos	
		Errores Transmitidos	
		Errores de Alineamiento de Trama Recibidos	
		Errores de rebose Reci.	
		Errores CRC Recibidos	
		Colisiones	

Acciones

- Enviar a Puerto Físico *i* o a uno virtual
  - All: por todos menos por el que entró
  - Controller: Encapsular y enviar al controlador
  - Local: Enviar a la pila de red local
  - Table: Realizar acciones en la tabla de flujo
  - In_port: Reenviarlo por el puerto de entrada
  - Normal: Enviarlo usando Ethernet tradicional
  - Flood: Inundar usando STP, menos por el puerto entrante

Acciones (Cont.)

- Enqueue: Enviar a una cola en el puerto → QoS
- Drop: Desechar
- Modificar Campo: Por ejemplo VLAN tags, bits ToS, cambiar TTL, etc

- Las máscaras permiten comparar sólo campos seleccionados. P. ej: IP dest, MAC dest, etc
- Si la cabecera del paquete recibido coincide con una entrada de tabla, se ejecutan las acciones correspondientes y actualizan los contadores.

Acciones (Cont.)

- Si no coincide con ninguna, el paquete se envía a una cola y la cabecera se envía al controlador, quien envía una nueva regla. Los siguientes paquetes son manejados por esta regla.
- Canal Seguro: Controlador – Switch usando TLS
- Los switches modernos ya implementan tablas de flujo, típicamente usando TCAMS
- El Controlador puede enviar las entradas de flujo de antemano (proactivo) o bajo demanda (reactivo). OpenFlow permite ambos modelos.

Switches OpenFlow, Hardware

- Arista 7050
- Brocade MLXe, Brocade CER, Brocade CES
- Extreme Summit x440, x460, x670
- Plataformas de switches con OpenFlow habilitado Huawei
- HP 3500, 3500yl, 5400zl, 6200yl, 6600, and 8200zl
- HP V2 line cards in the 5400zl and 8200zl IBM 8264
- Juniper (MX, EX)
- NEC IP8800, NEC PF5240, NEC PF5820
- NetGear 7328SO, NetGear 7352SO
- Pronto (3290, 3295, 3780) – ejecuta el software pica8
- Plataforma Switch Light

Switches OpenFlow, Software

- Indigo: Implementación de código abierto que se ejecuta sobre switches físicos y usa las características de las ASICs para ejecutar OpenFlow
- LINC: Implementación de código abierto que se ejecuta en LINUX y Windows, MacOS y FreeBSD
- Pantou: Transforma un router o punto de acceso comercial en un switch con OpenFlow habilitado. OpenFlow se ejecuta sobre OpenWRT. Soporta los Broadcom genéricos y algunos modelos LinkSys y puntos de acceso TP-Link con chipsets Broadcom
- Of13softswitch: Software en espacio de usuario basado en el softswitch Ericsson TrafficLab 1.1
- XORPlus: Software de código abierto para gestionar ASICs de alto rendimiento. Soporta STP/RSTP/MSTP, LCAP, QoS, VLAN, LLDP, ACL,
- OSPF/ECMP, RIP, IGMP, IPv6, PIM-SM
- Open vSwitch

Open vSwitch

- Switch virtual de código abierto
- Concepto creado en Nicira
- Puede ejecutarse como switch aislado o como un switch hypervisor distribuido en varios servidores.
- Es el switch por defecto en XenServer 6.0, Xen Cloud Platform y soporta Proxmox VE, VirtualBox, Xen KVM.
- Integrado en varios sistemas de control de nube incluyendo OpenStack, openQRM, OpenNebula, y oVirt
- Distribuidos con Ubuntu, Debian, Fedora Linux. También FreeBSD
- Intel tiene su versión acelerada de Open vSwitch en su propio Kit de Desarrollo de Planos de Datos (DPDK)

Características del Open vSwitch

- Comunicación entre máquinas virtuales via:
  - NetFlow: Protocolo Cisco para muestrear y recolectar estadísticas de tráfico (RFC 3954)
  - sFlow: Similar a NetFlow, por sflow.org (RFC 3176)
  - Jflow: La versión Juniper de NetFlow
  - NetStream: La versión Huawei de NetFlow
  - IPFIX: IP Flow Information Export Protocol (RFC 7011) – el estándar IETF para NetFlow
  - SPAN, RSPAN: Remote Switch Port Analyzer – mirroring de puertos que envía una copia de todos los paquetes por un puerto de monitorización
  - GRE- mirrors en túnel: El dispositivo de monitorización está conectado de forma remota al swich via túnel GRE

Características del Open vSwitch (Cont.)

- Link Aggregation Control Protocol (LACP)
- IEEE 802.1Q VLAN
- IEEE 802.1ag Connectivity Fault Management (CFM)
- Bidirectional Forwarding Detection (BFD) para detectar fallos en el link (RFC 5880)
- IEEE 802.1D-1998 Spanning Tree Protocol (STP)
- Políticas de tráfico por cada máquina virtual
- OpenFlow
- Tubería de envío multi-tabla (encadenamiento)
- IPv6
- GRE, VXLAN, IPSec tunneling
- Opciones de motor de envío en kernel y espacio de usuario

OVSDB

- Protocolo de Control de la Base de Datos de OvS
- Capacidad de monitorización usando mecanismos publicación-subscripción
- Guarda tanto el estado provisional como el operacional
- Usa JSON para el formato del esquema y JSON-RPC sobre TCP para el protocolo de red (RFC 4627)
- Métodos RPC: List Databases, Get Schema, Update, Lock,…
- El proyecto Open vSwitch incluye implementaciones de clientes y servidores OVSDB

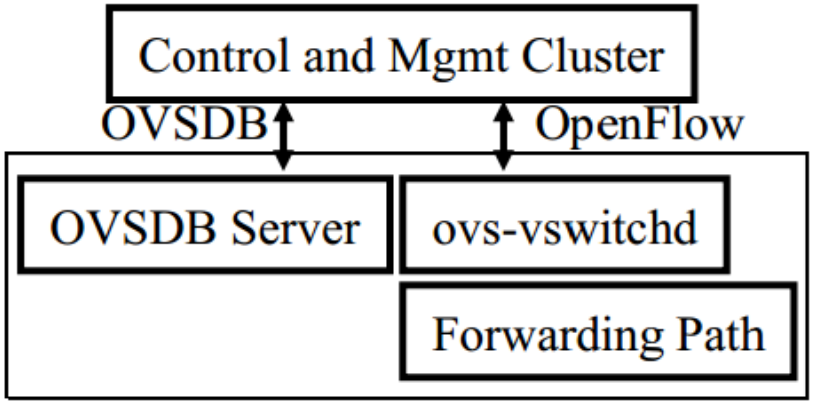
OVSDB (Cont.)

<database-schema>

"name": <id>

"version": <version>

"tables": {<id>: <table-schema>,…}

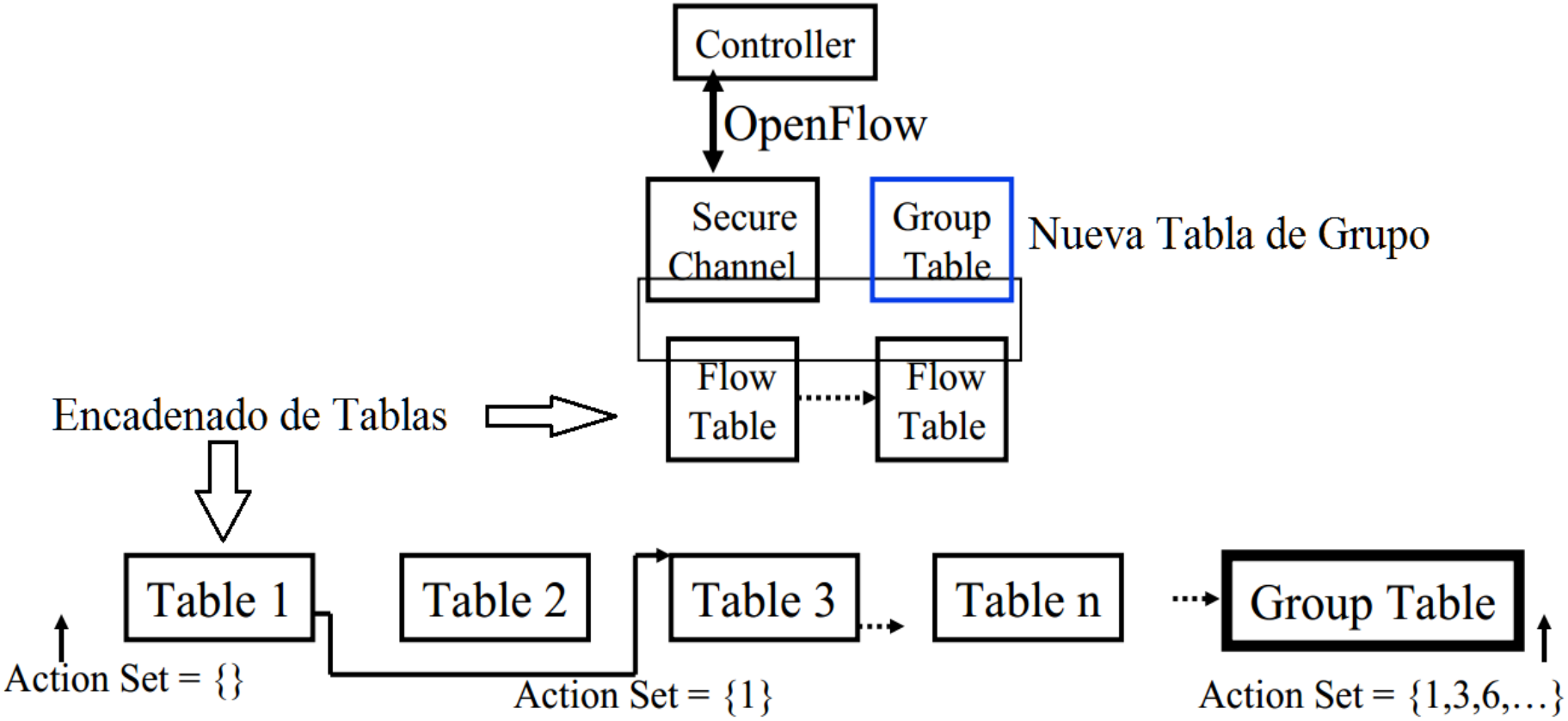


OpenFlow V1.1

- Versión 1: Realiza acciones sobre un match. Sólo Ethernet/IP. Único camino. No cubría MPLS, Q-in-Q, ECMP; ni un Multicast con eficiencia
- Versión 1.1: Introdujo encadenado de Tablas, Tablas de Grupo, y añadió etiquetas MPLS y clase de tráfico MPLS en los campos para hacer match

- Encadenado de tablas: Tras un match, la instrucción puede ser:
  - Acciones inmediatas: modificar paquete, actualizar los campos match y/o
  - Atualizar el Action Set, y/o
  - Enviar los datos match y el Action Set a la Tabla n,
  - Ir a la entrada de la Tabla de Grupo n

OpenFlow V1.1 (Cont.)



OpenFlow V1.1 (Cont.)

- Cuando se produce fallo (no hay match), la instrucción puede ser enviar el paquete al controlador o continuar el procesado por la siguiente tabla en orden secuencial.
- Tablas de Grupo: Cada entrada tiene un número variable de buckets (cubetas)
  - All: Ejecuta cada bucket. Usado para Broadcast, Multicast.
  - Select: Ejecuta un bucket seleccionado. Se usa para mirroring de puertos. La selección se puede mediante el hash de algunos campos
  - Indirect: Ejecuta un bucket predefinido
  - Fast Failover: Ejecuta el primer bucket activo →Puerto activo
- Nuevas características soportadas:
  - Multipath: Un flujo puede ser enviado por varios caminos
  - MPLS: Múltiples etiquetas, clases de tráfico, TTL, push/pop de etiquetas
  - Q-in-Q: Múltiples etiquetas VLAN, push/pop de cabeceras VLAN
  - Túneles: Vía puertos virtuales

OpenFlow V1.2

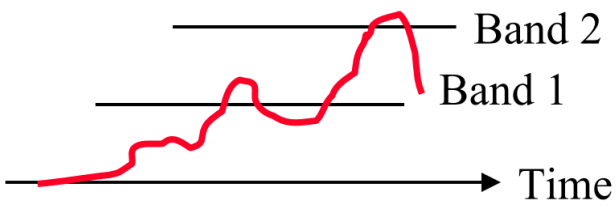
- Soporte para IPv6: Los campos para hacer match incluyen dichas direcciones destino, origen, número de protocolo, clase de tráfico, tipo ICMPv6, código ICMPv6, campos de cabecera de descubrimiento del vecino por ICMPv6, y etiquetas de flujo ICMPv6
- Matches extensibles: Estructura Tipo-Longitud-Valor (TLV). Previamente el orden y la longitud de los campos de match estaban prefijados.
- Extensiones para nueva experimentación a través de campos y código dedicados, asignados por la ONF.

OpenFlow V1.3

- Extensión de las cabeceras IPv6: Puede comprobar si están presentes las cabeceras hop-by-hop, Router, Fragmentación, Opciones de Destino, Autenticación, Carga útil con Seguridad Encriptada (ESP) o cabeceras de extensión desconocida
- Matching con el bit MPLS Bottom-OpenFlow-Stack
- Encapsulación MAC-en-MAC
- Metadatos Tunnel ID: Soporte para túneles (VxLAN,…)
- Filtrado por Evento de Conexión : mejor filtrado de conexiones a múltiples controladores
- Varias conexiones auxiliares al controlador permiten explotar el paralelismo
- Mejor capacidad de negociación: Las peticiones pueden abarcar varios mensajes
- Mejora en las capacidades para la experimentación en general
- Una entrada de flujo separada para las acciones de table miss (si no hay match)

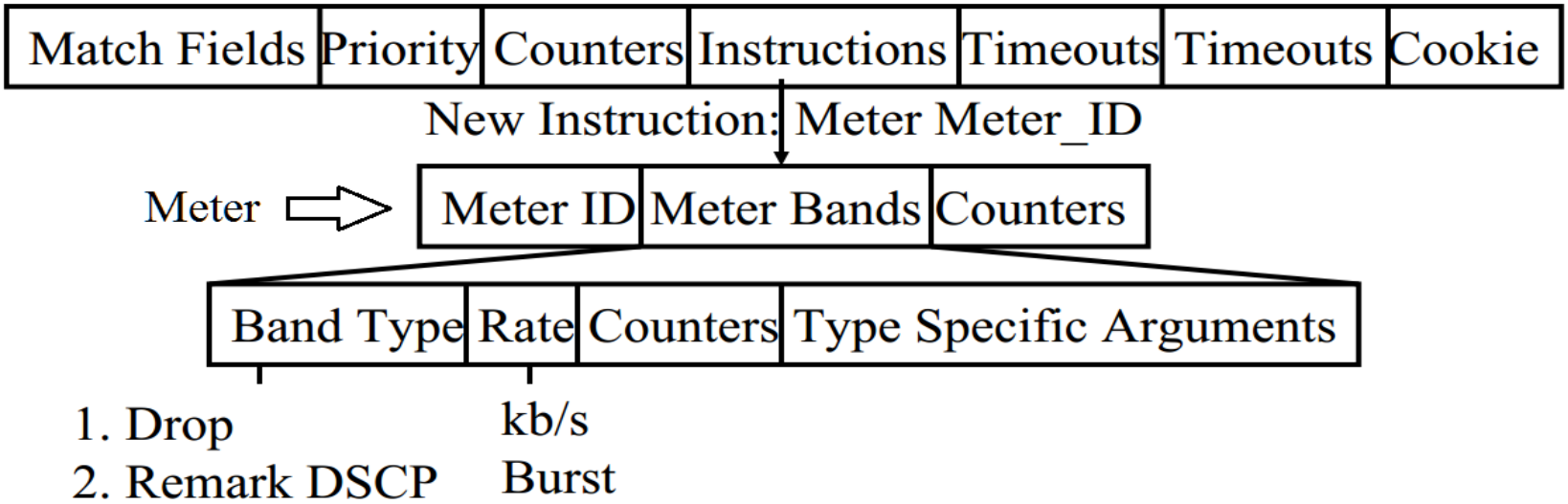
OpenFlow V1.3 (Cont.)

- Cookies: Un campo cookie se añade a los mensajes que contienen nuevos paquetes enviados al controlador. Esto ayuda al controlador a procesar el mensaje más rápido que si tuviera que buscar en toda su base de datos.
- Duración: El campo duración ha sido añadido a la mayor parte de las estadísticas. Ayuda a computar tasas.
- Los contadores por flujo pueden ser deshabilitados para mejorar el rendimiento
- Se han añadido Flow Meters y Meter Bands
- Meter (medidor): Elemento del switch que puede medir y controlar la tasa de paquetes o bytes
  - Si la tasa excede un umbral predefinido → el meter activa la banda
  - Un meter puede tener múltiples bandas



OpenFlow V1.3 (Cont.)

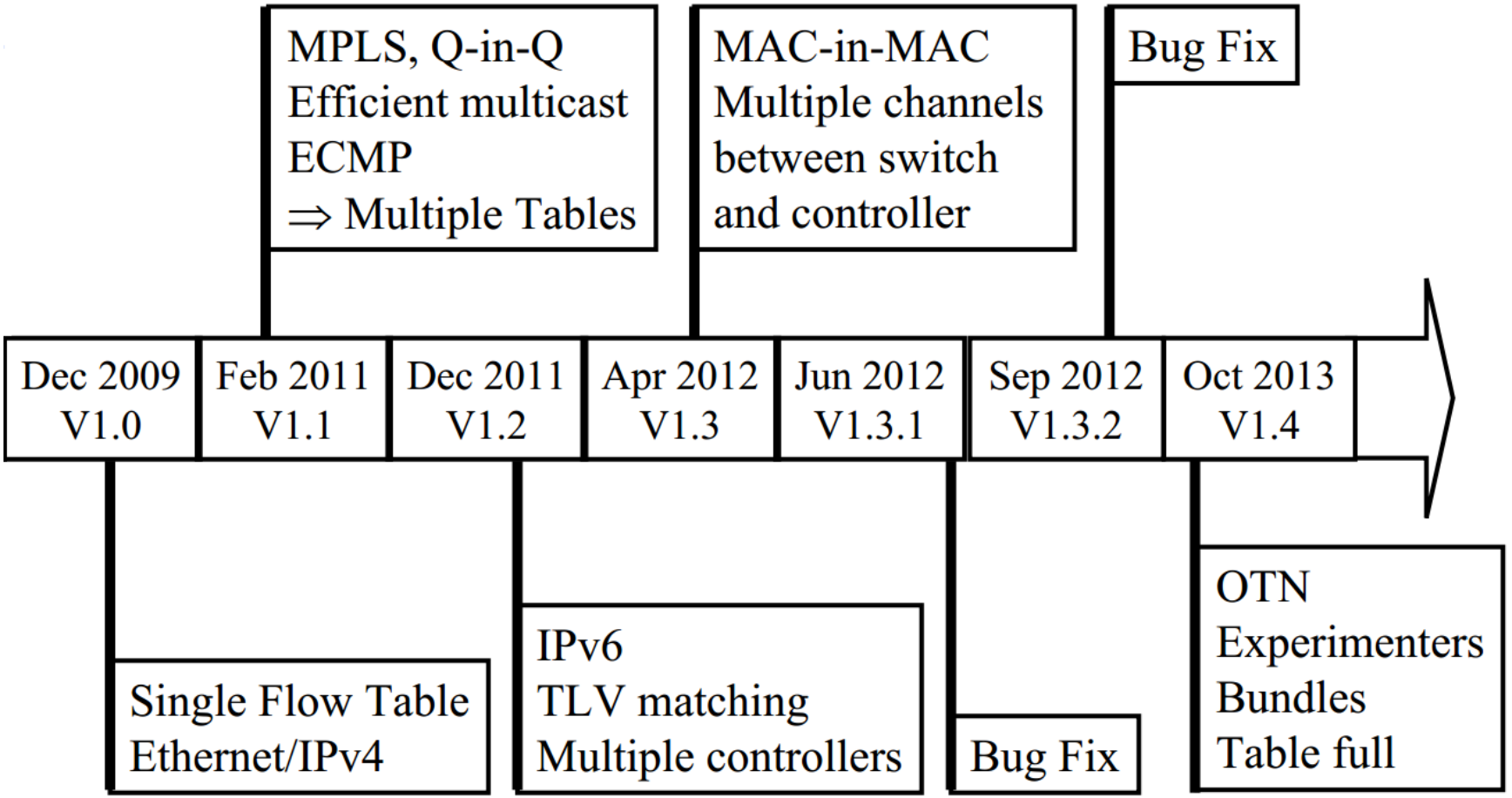
- Si cuando se activa una banda el meter desecha el paquete, se denominará limitador de tasa
- Se pueden diseñar otras políticas de QoS con los meters
- Los metes están adjuntos a una entrada de flujo, no a una cola ni a un puerto. Múltiples entradas pueden apuntar al mismo meter.



OpenFlow V1.4

- Puertos Ópticos: Configura y monitoriza las frecuencias de transmisión y recepción de los lásers y su potencia.
- Extensibildad mejorada: Codificación Tipo-Longitud-Valor en la mayoría de los casos → Facilidad para añadir nuevas características en el futuro
- Extensión de la API Extendida para Experimentador: Puede añadir fácilmente puertos, tablas, colas, instrucciones, acciones, etc
- Más información cuando un paquete es enviado al controlador, p. ej, no hay match, TTL no válido, por un group bucket, una acción…
- Los controladores pueden seleccionar un subconjunto de tablas de flujo para monitorizarlas
- Los switches pueden desalojar entradas de menor importancia si la tabla está llena
- Los switches pueden notificar al controlador si a una tabla se le está acabando el espacio
- Ejecución atómica de un lote de instrucciones

Resumen Evolución OF

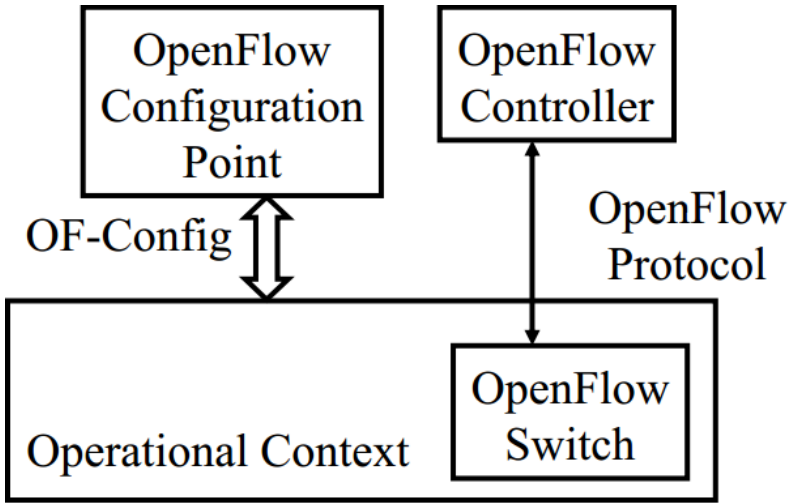


Proceso de Inicio

- Los switches requieren de configuración inicial: dirección IP del switch, Ip del Controlador, puerta de enlace por defecto
- Los switches se conectan al controlador
- El switch provee de información de configuración sobre los puertos
- EL controlador instala una regla para enviar paquetes LLDP al controlador y luego envía, uno por uno, paquetes LLDP para que sean enviados por los puertos i(i=1, 2, …, n) que llegan a sus respectivos vecinos.
- Los vecinos envían los packetes de vuelta al controlador
- El controlador determina la topología a partir de los paquetes LLDP
- LLDP es un protocolo de un solo sentido para anunciar las capacidades a intervalos fijos.

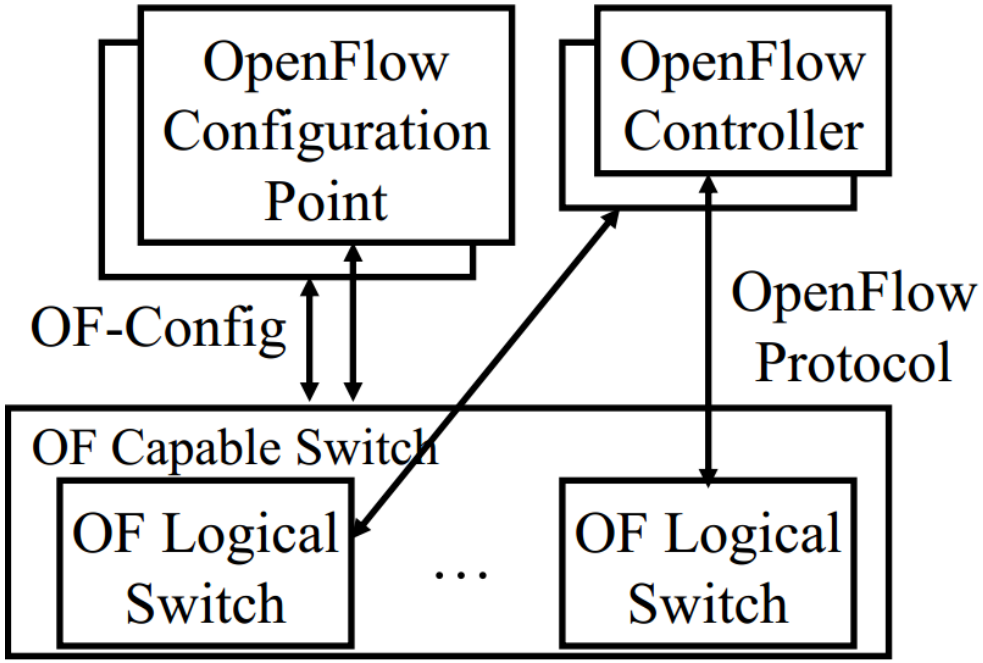
Protocolo de Configuración OF

- Punto de Control OpenFlow : Entidad que configura switches OpenFlow
- OF-Config: Protocolo usado para la configuración y control de los switches
- Asignación de los controles OF para que los switches puedan iniciar la conexión con ellos:
  - Dirección IP del controlador
  - Número de puerto del controlador
  - Protoclo de transporte: TLS o TCP
  - Configuración de colas (tasas min/max) y puertos
  - Habilitar/Deshabilitar velocidad de recepción/envío media en los puertos



OF-Config (Cont.)

- Un switch físico = uno o más switches lógicos cada uno controlado por un controlador OpenFlow
- OF-Config permite la configuración de switches lógicos



Conceptos OF-Config

- OF Capable Switch: Switch OpenFlow físico.
  Puede contener uno o más switches lógicos.
- OpenFlow Configuration Point: servicio de configuración
- OF Controller: Controla el switch lógico vía protocolo OpenFlow
- Operational Context: Switch lógico OF
- OF Queue: Colas de paquetes esperando para ser enviados
- OF Port: Interfaz de envío.Puede ser física o lógica
- OF Resource (recurso): puertos, colas, certificados, tablas de flujo y otros recursos de los switches que soportan OpenFlow asignados a un switch virtual.
- DatapathID: 64 bits de ID del switch. Los 48 bits menos representativos son la MAC del switch, los más son asignados por el operador

Evolución de OF-Config

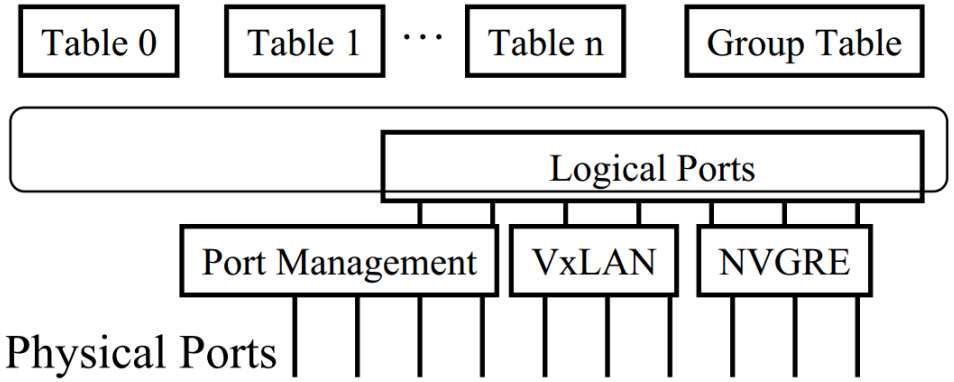
- V1.0 (Enero 2012): Basada en OpenFlow V1.2
  - Asignación de controladores a switchess lógicos
  - Obtención de la configuración de switches lógicos
  - Configuración de puertos y colas
- V1.1 (Mayo 2012): Baseda en OpenFlow V1.3
  - Configuración de certificados
  - Capacidad de descubrimiento: Obtiene capacidades de los switches lógicos
  - Configuración de túneles lógicos (VXLAN, NVGRE ,…)
- V1.1.1 (Enero 2013): Reparación de fallos. Soporte para todas las versiones.
- V1.2: Baseda en OpenFlow V1.4
  - Detección de topolgía simple
  - Asignación de recursos a switches lógicos

Entorno de Notificaciones OpenFlow

- Notificación: Mensajes lanzados por evento, por ejemplo link caído.
- Modelo publicación/subscripción: Switch = publicador. El controlador OpenFlow, los Puntos de Configuración u otros pueden subscribirse a ellos.
  Serán notificados sobre esos eventos.
- Uso de Notificaciones ITU-T M.3702: Cambios del atributo valor, alarma de Comunicación, alarma Abiental, alarma de Equipo, alarma de QoS, alarma de error de Procesado, alarma de Seguridad, cambio de Estado, creació de Objeto y borrado.
- Notifcaciones preexistentes: No están en el entorno pero serán reconocidas.
  - OpenFlow: Packet-in, Flow removed, Port Status, Error,
  - Hello, Echo request, Echo reply, Experimenter
  - OpenFlow Config: Instanciación del switch lógico OpenFlow, capacidad de cambio del switch, establecimiento de la sesión OpenFlow con éxito, establecimiento de la sesión OpenFlow fallido, recuperación o fallo de puerto.

Problemas de Implementación

- Más de 40 campos para comparar en un flujo
- Múltiples tablas, cada una con un gran número de entradas de flujo
- Instrucciones y acciones por cada tabla
- Necesidad de soporte VXLAN, NVGRE, etc.
- Para redes amplias, el nivel de programación de flujos puede llevar un largo tiempo



Trabajo Futuro

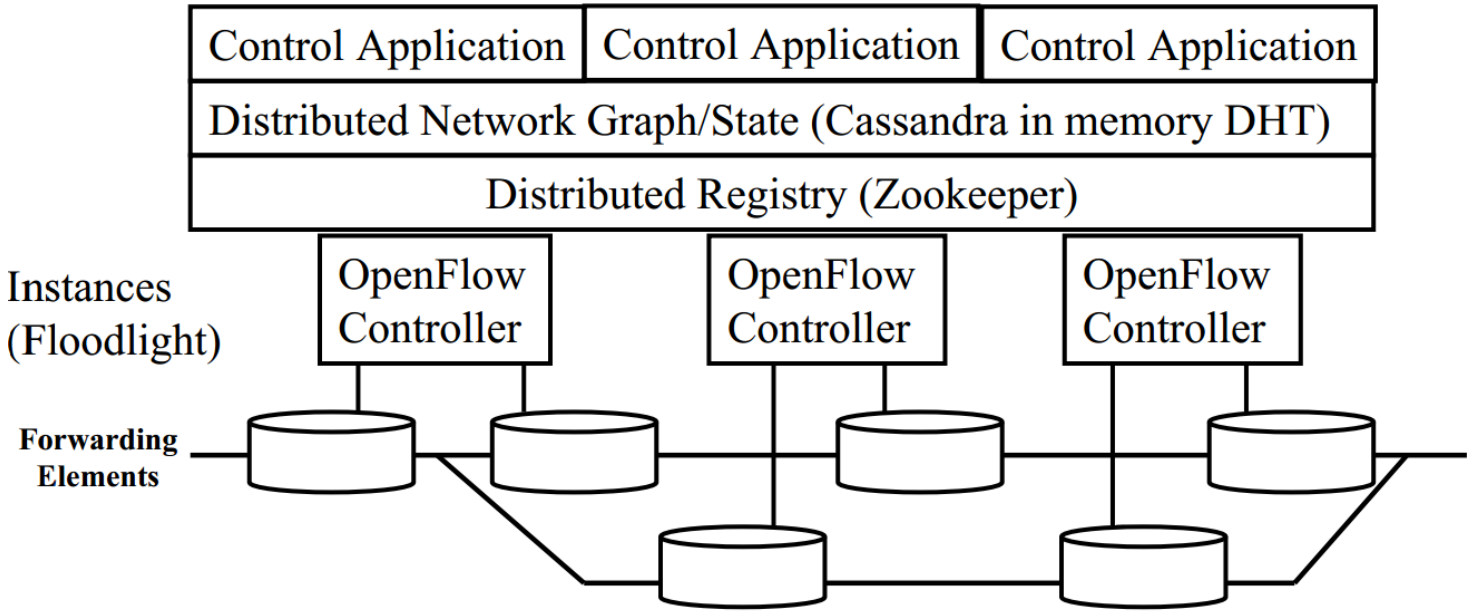
- Cada controlador tiene su propia forma de programar
- Necesidad de un estándar común «Nothbound API» (grupo ONF NBI)
- No hay una API estándar para las comunicaciones entre controladores de dominios superpuestos → Necesidad de una «East-West API»
- Habilidad de seguir operativo si el controlador se cae
- Muchos más formatos de paqutes (no-IP, no-Ethernet, …)
- Flujo →Decidir una vez, usar varias →Rendimiento
  - Pero no ayuda para peticiones de apps no basadas OpenFlow
  - Necesidad de una API para encriptar paquetes en el plano de datos, para inyectar paquetes, o para instanciar un servicio, como un firewall, IDS, en el switch.
- Necesidad de programar una vista abstracta, por ejemplo, origen a destino, desconociendo la red física

Controladores OpenFlow

- NOX
- POX
- SNAC
- Beacon
- Trema
- Maestro
- Floodlight
- ONIX
- ONOS
- Y muchos más; no es una lista completa….

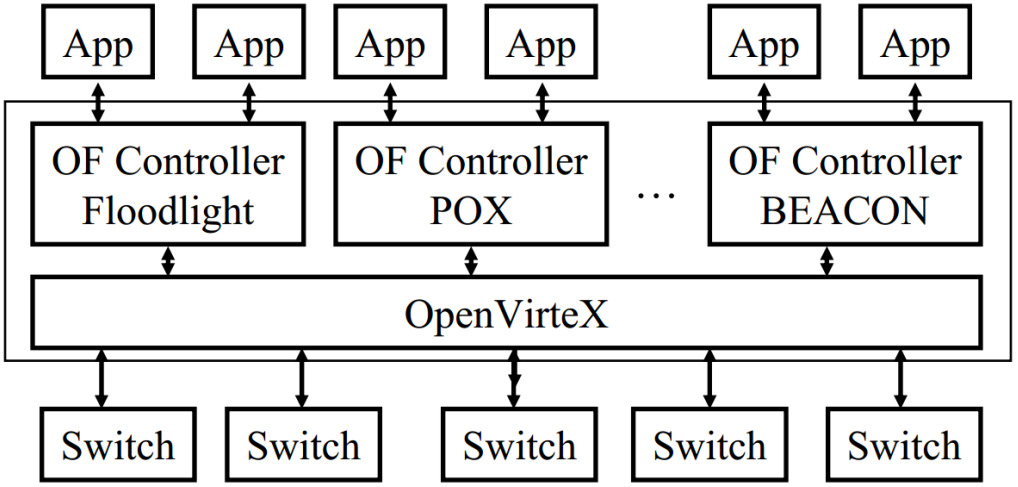
ONOS

- Open Network Operating System: Distributed OpenFlow OS for a large WAN
- 8-10 instancias en un cluster.
- Cada Instancia es responsable de una parte de la red



OpenVirteX(OVX)

- Proxy Tansparente entre switches OpenFlow y múltiples controladores OpenFlow. Las porciones (*slices*) se definen por campos de cabecera.
- Crea porciones de red que pueden ser gestionadas por múltiples controladores
  - Aísla las porciones unas de otras
- Todo el tráfico de control pasa por OVX → Baja Latencia



Mininet

- Entorno de emulación de código abierto ampliamente usado
- Puede emular un número de hosts finales, switches, routers, links en Linux
- Usado para probar prototipos de SDNs
- Incluye Open vSwitch, y un switch software capacitado para OF
- Lanzado por línea de comandos y una API de Python para crear redes de varios tamaños. Por ejemplo: mn –topo tree,depth=2,fanout=3
- Comandos útiles de diagnóstico como iperf, ping, y otros comandos en un host
- Hay disponible código Mininet para varios switches comerciales

Resumen de la Parte I

- Cuatro planos de Red: Datos, Control, Gestión, Servicios
- OpenFlow separa el plano de control y lo mueve a un control centralizado → Simplifica los elementos de envío
- Los switches comparan (match) los campos de cabecera de los paquetes entrantes con las entradas de flujo en una tabla, y lo procesa como está estipulado. El controlador proporciona las entradas y otras instrucciones
- OpenFlow se ha extendido a IPv4, MPLS, IPv6, y redes ópticas, pero todavía hay trabajo por hacer.
- EL controlador ONOS, virtualización OVX y Mininet para emulación.

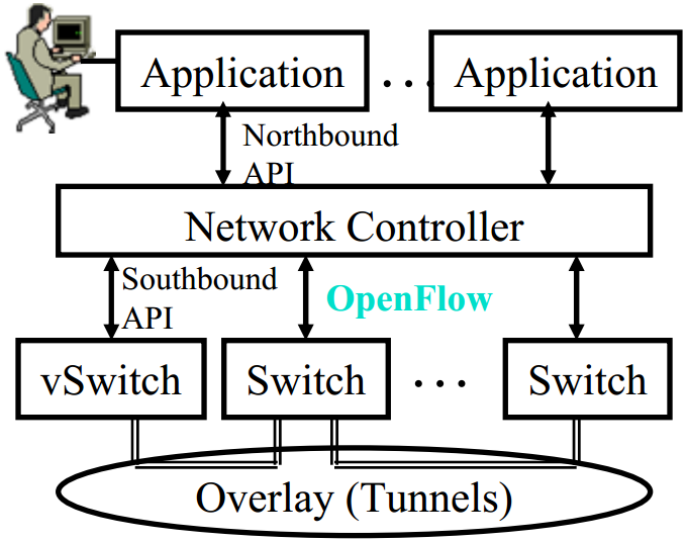
Parte II
Software Defined Networking

Parte II: Software Defined Networking

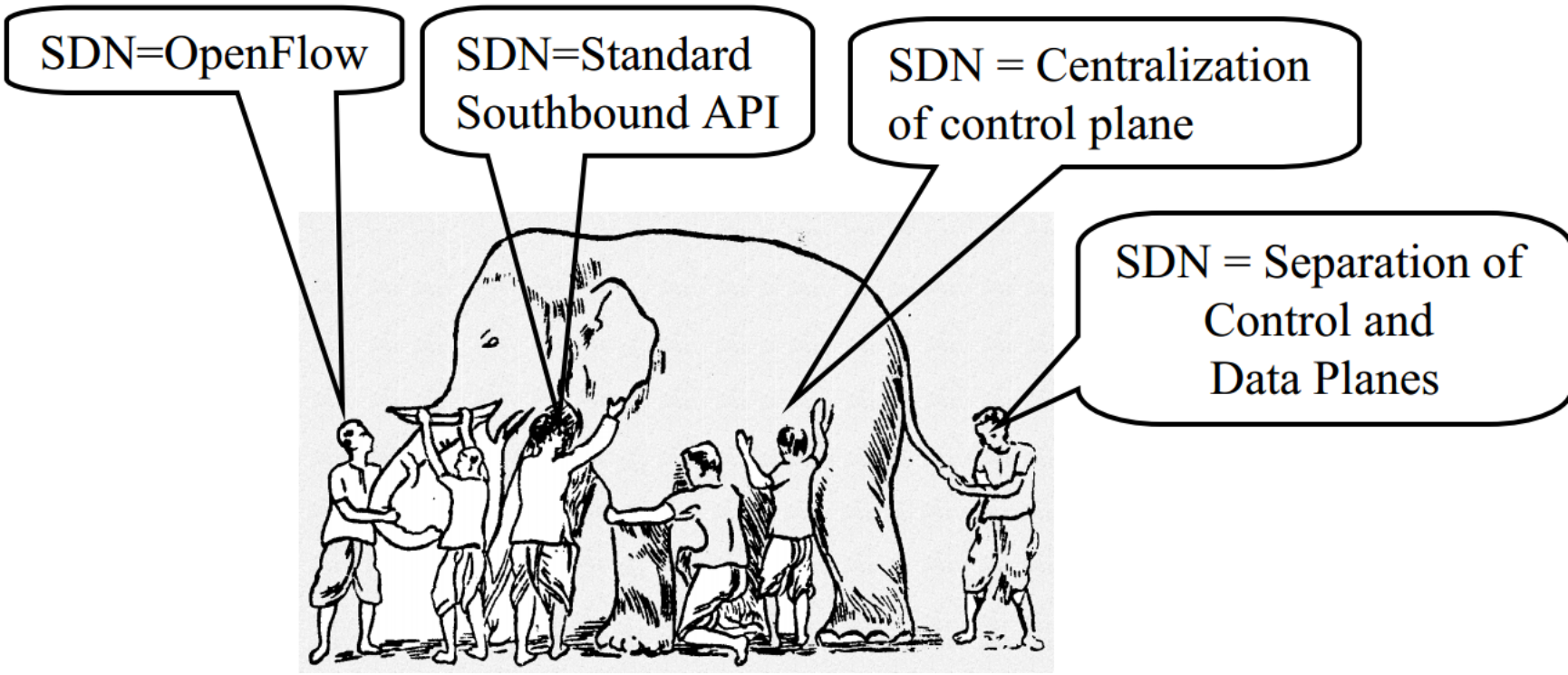
- ¿Qué es SDN?
- APIs alternativas: XMPP, PCE, ForCES, ALTO
- Plataforma del Controlador SDN OpenDaylight y herramientas

SDN 1.0: SDN basado en OpenFlow

- SDn originado por OpenFlow
  - Control centralizado
  - Fácil de programar
  - Cambia las políticas de enrutamiento al vuelo
  - Software Defined Network (SDN)
- Inicialmente: SDN=OpenFlow



¿Qué es SDN?



- Todos esos son mecanismos
- SDN *no* es un mecanismo
- Es un entorno para resolver un conjunto de problemas → Muchas soluciones

Definición de SDN de la ONF

- «¿Qué es SDN?»
  La separación física del plano de control de red del de envío, y en el cual un plano de control controla varios dispositivos.

1. Directamente programable
2. Ágil: Abstrayendo el control del de reenvío
3. Control centralizado
4. Configurado programáticamente
5. Basado en estándares abiertos y neutral en cuanto a fabricante

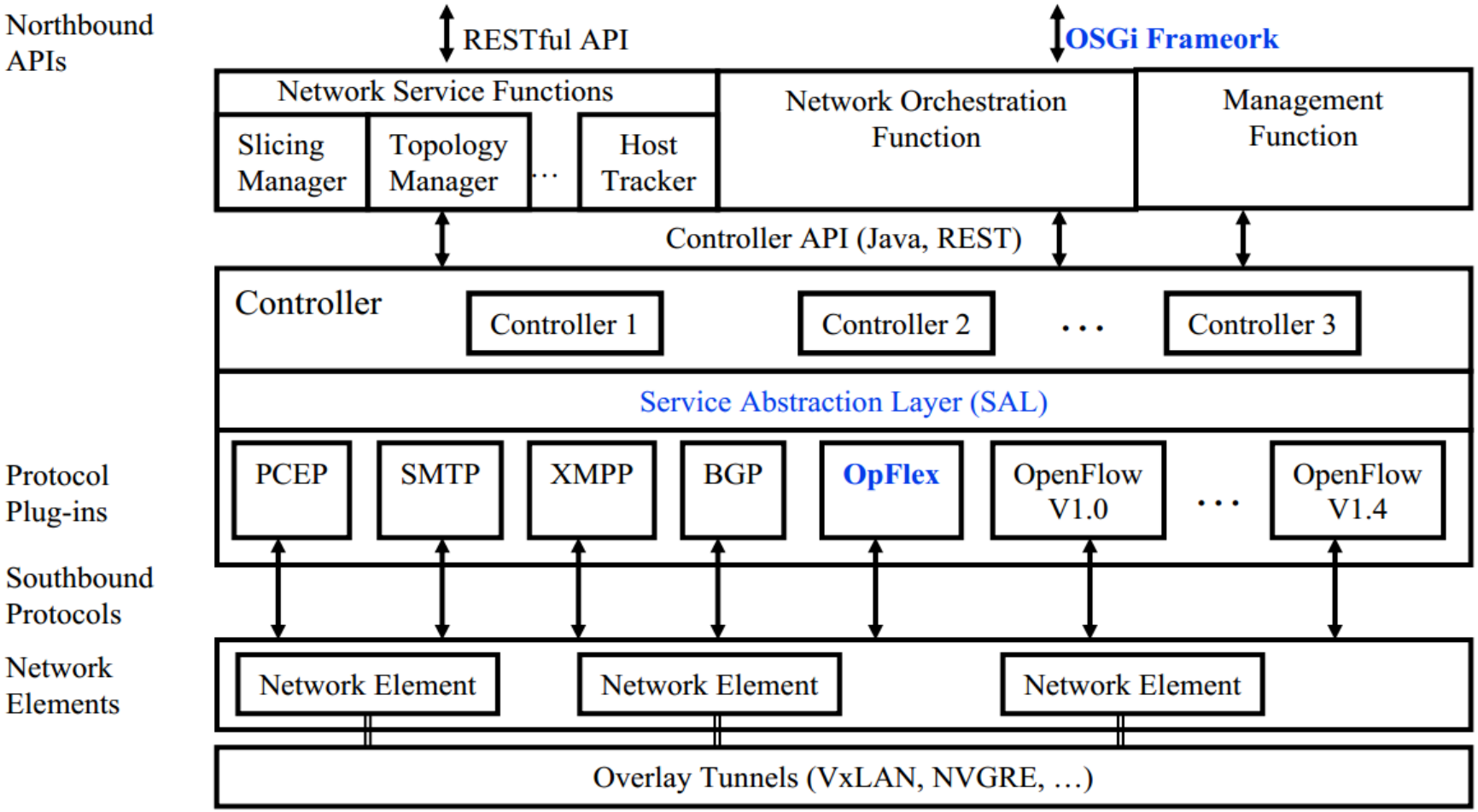
Las definiciones antes citadas incluyen el Cómo

- Ahora existen muchas opiniones diferentes en cuanto a cómo conseguirlo
- SDN se ha convertido en un concepto general. Necesita ser definido por el Qué.

¿Para qué necesitamos SDN?

- Virtualización: Usar los recursos de la red sin necesidad de preocuparse sobre dónde está físicamente localizado, cuánto es, cómo se organiza, etc.
- Orquestación: Gestión de miles de dispositivos
- Programable: DeberIa ser capaz de cambiar el comportamiento al vuelo
- Escalado dinámico: Ser capaz de cambiar de tamaño
- Automatización: Menor OpEx (coste continuado)
- Visibilidad: Monitorización de recursos, conectividad
- Rendimiento: Optimiza la utilización de los dispositivos de red
- Múltiples arrendatarios: Compartiendo una infraestructura costosa
- Integración de Servicios
- Apertura: Elección completa de plug-ins modulares
- Gestión unificada de la computación, red y almacenamiento.

SDN 2.0: SDN estilo OpenDaylight



- NO-OpenFlow(No sólo OpenFlow) Multi-Protocolo
- Nuevo trabajo en IETFXMPP, ALTO, I2RS, PCEP, ….
- Linux Foundation

Open - Todo

- Open Networking Foundation
- OpenFlow
- OpenStack
- OpenDaylight
- Open Access
- Open Source

Debate actual sobre SDN: Qué vs Cómo

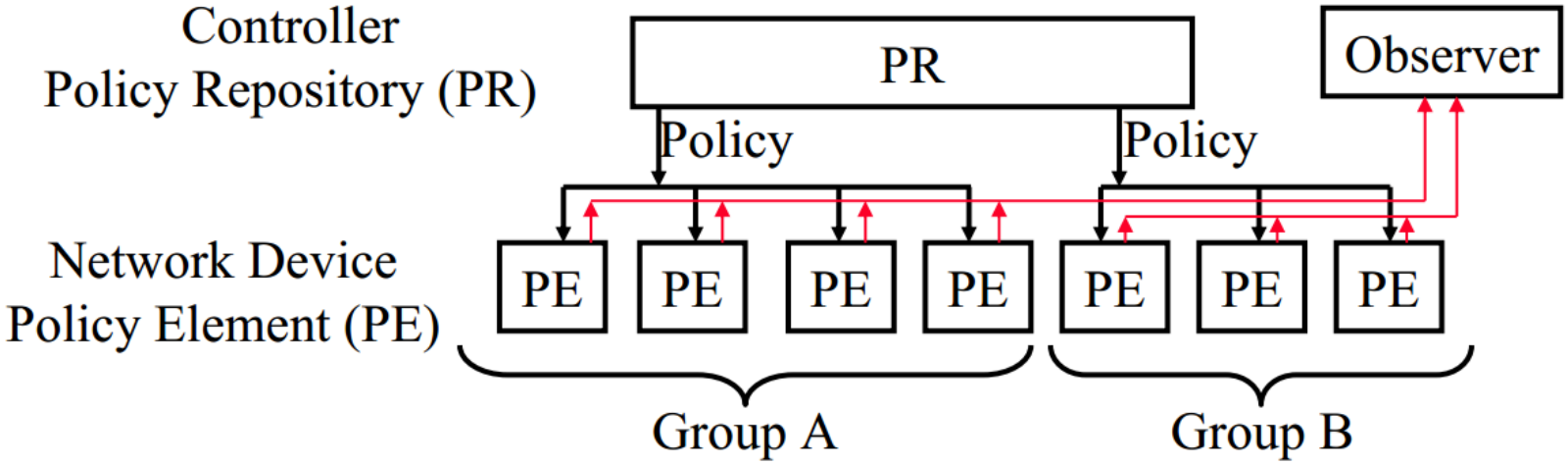
- SDN es sencillo si el control está centralizado, pero no es necesario. Los diseños distribuidos pueden requerirse para equipos desfasados y para operaciones fail-safe
- La eliminación completa del plano de control puede ser dañina. Una división exacta del plano de control entre controlador centralizado y dispositivos distribuidos todavía tiene que llevarse a cabo.
- SDN es sencillo con un protocolo estándar en la parte Southbound, como OpenFlow , pero un solo protocolo puede no escalarse en todos los casos.
  - La diversidad de protocolos es un hecho
  - No hay sistemas operativos distribuidos, procesadores, routers, o switches Ethernet
- Si la industria encuentra un método más sencillo para solventar los mismos problemas, ese método prevalecerá. Por ejemplo ATM vs MPLS.

SDN en todas partes

- Software Defined Switches
- Software Defined Routers
- Software Defined Data Center
- Software Defined Storage
- Software Defined Base Stations
- Software Defined GPS
- Software Defined Radio
- Software Defined Infrastructure
- Software Defined Optical Switches

OpFlex

- Protocolo de Políticas Abiertas
- Control declarativo: El Controlador le dicta las políticas al dispositivo de red, el cual la implementa a su manera.



- Las políticas son comunicadas usando XML, JSON, binario, …
- El observador recolecta info de control, fallos, eventos, …

XMPP

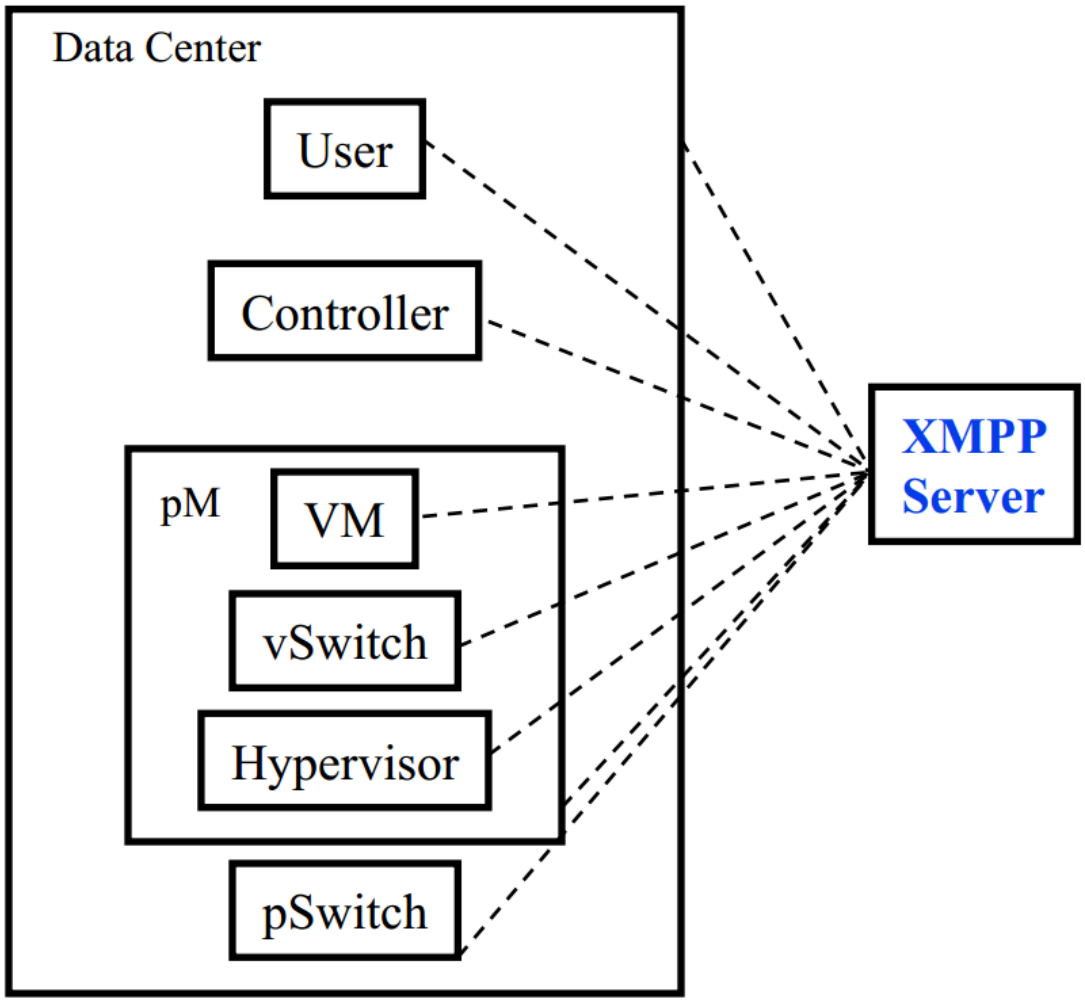
- Extensible Messaging and Presence Protocol
- Extensible → Usando XML
- Similar al protocolo email SMTP pero para comunicaciones cercanas a tiempo real.
- Cada cliente tiene un ID, p.ej: john@wustl.edu/mobile (móvil de John)
- El cliente está en línea
- Presencia: Servidor mantiene las direcciones de contacto y puede dejar a otros contactos saber que su cliente está ahora en línea.
- Mensajería: Cuando un cliente envía un mensaje “chat” a otros clientes, se envía a estos otros clientes
- Los mensajes son «pushed»
- Los mensajes son «pushed»(→tiempo-real) en oposición a «polled» como en emails SMTP/POP

XMPP (Cont)

- XMPP es una estandarización IETF del protocolo Jabber
- La RFC 6121 define XMPP usando conexiones TCP.
  Pero HTTP es a menudo usado como transporte para dirigir firewalls
- Todos los mensajes son codificados en XML
- No es eficiente para transferencia de archivos binarios
- Los canales binarios fuera de banda son a menudo usados con XMPP
- Están disponibles un número de implementaciones de código abierto
- Sus variaciones son ampliamente usadas en la mayoría de programas de mensajería instantánea incluyendo Google, Skype, Facebook, …, muchos juegos
- Usado en Internet de las Cosas (IoT) y centros de datos para gestión. Los dispositivos de red tienen clientes XMPP que responden a mensajes XMPP que contienen peticiones de gestión CLI → Tú puedes manejar la red usando cualquier otro cliente XMPP, por ejemplo, el teléfono móvil
- Los switches de los bordes pueden ser manejados por XMPP; Juniper usa XMPP como protocolo southblound para SDN

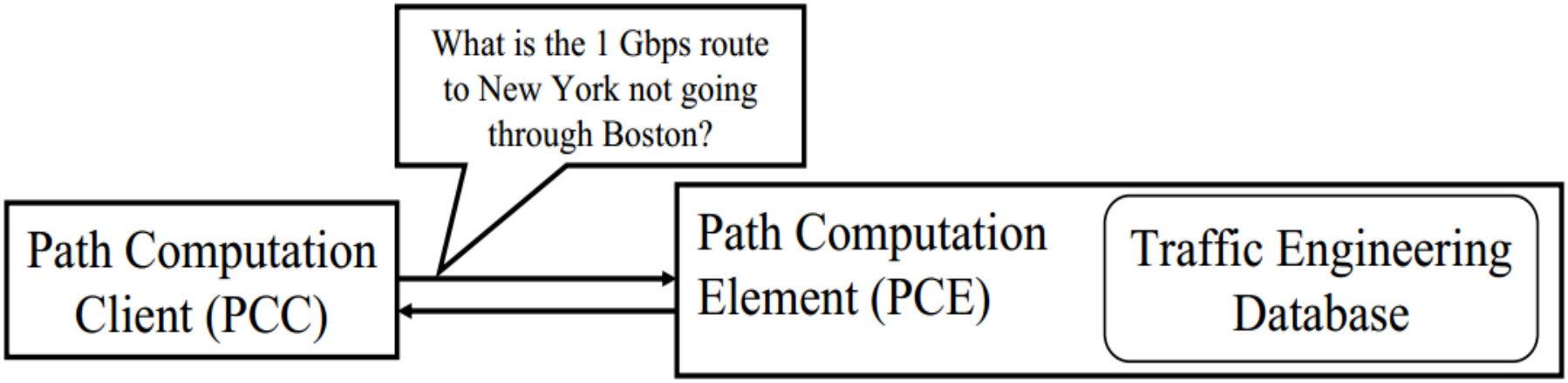
XMPP en Centros de Datos

- Todo es una entidad XMPP
  Tiene su propia lista de contactos y autorizaciones



Path Comutation Element (PCE)

- PLS y GMPLS requieren que los routers originarios encuentren caminos que satisfagan múltiples limitaciones incluyendo no usar ningún router de respaldo, con un ancho de banda dado, etc
- Esto puede requerir más potencia de cómputo o conocimiento de red que un router puede tener.
- El grupo de trabajo IETF PCE ha desarrollado un conjunto de protocolos que permiten un Cómputo de Caminos del Cliente (PCC), es decir, el router obtiene el camino del Path Computation Element (PCE)
- El PCE puede estar centralizado o puede estar distribuido en muchos o todos los routers.

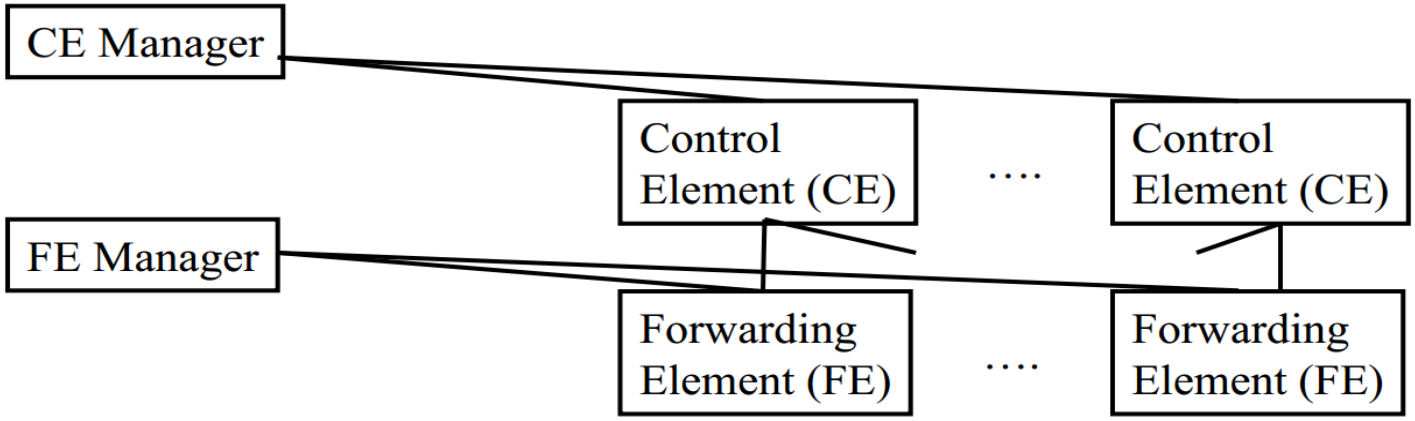


PCE (Cont)

- PCE separa la función de computación de ruta de la función de reenvío
- Ambas funciones pueden residir en la misma caja o en diferentes
- Más de 25 RFCs documentando protocolos para:
  - Comunicación PCE-a-PCC
  - Comunicación PCE-a-PCC (Multiple PCEs)
  - Descubrimiento PCE

Forwarding and Control Element Separation(ForCES)

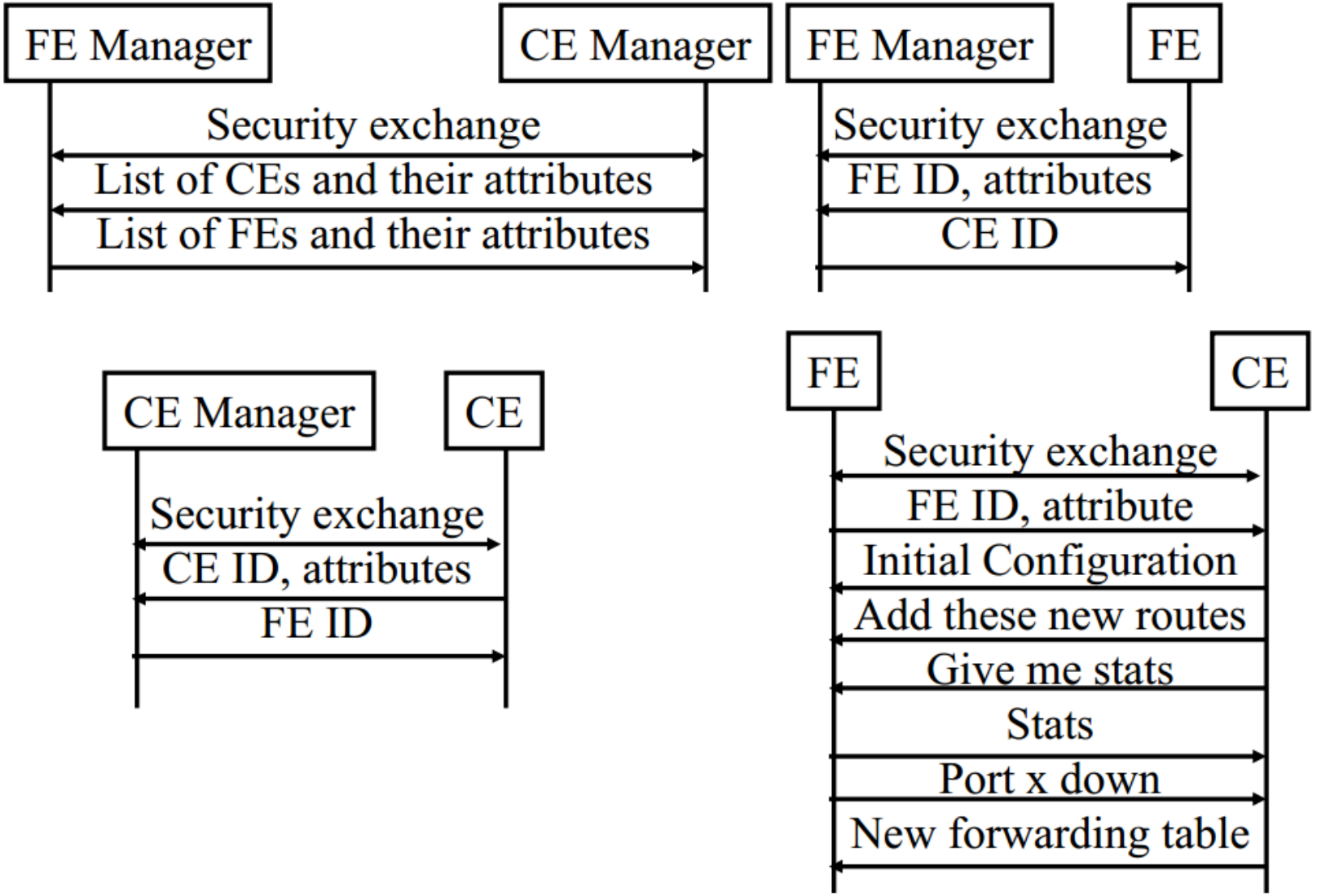
- Grupo de trabajo IETF desde Julio 2001
- Los Elementos de Control (CEs) preparan la tabla de rutas para ser usadas por los elementos de reenvío (Fes)
- Cada CE puede interactuar con uno o más Fes
- Puede haber muchos CEs y FEs gestionados por un CE y un FE directores, respectivamete



ForCES (Cont)

- La idea de los planos de datos y control fue usada en los sockets de enrutado en BSD 4.4, a principios de 1990. Permitía que las tablas de enrutamiento fuesen controladas por línea de comandos o por un demonio.
- El protocolo ForCES soporta el intercambio de:
  - Tipo de puerto, velocidad del link, dirección IP
  - Envío unicast/multicast Ipv4/IPv6
  - QoS incluyendo mediciones, políticas, formado y colas
  - Clasificación de paquetes
  - Funciones personalizadas como NAT o Application –Level-Gateways (ALG)
  - Encriptado de paquetes
  - Medición e informe de información de tráfico por flujo.

Ejemplo de Intercambios ForCES

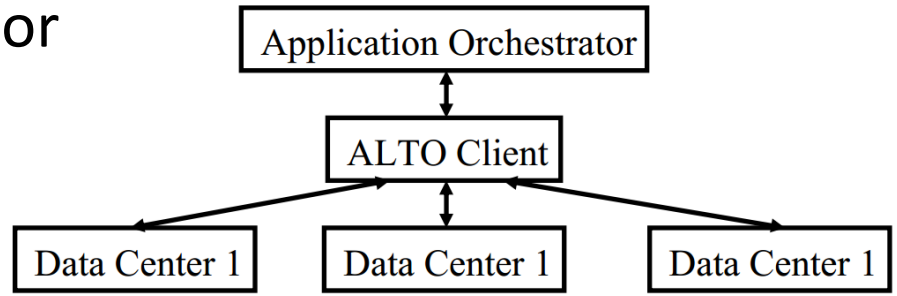


Application Layer Traffic Optimization (ALTO)

- Grupo de trabajo de IETF para optimizar tráfico P2P
- Mejor obtener tráfico de los vecinos cercanos
- Provee una guía para selección de pares
- Servidor ALTO: Tiene conocimiento de los recursos distribuidos
- Cliente ALTIO: Pide información de los servidores sobre los vecinos apropiados
- Ratio Criteria : Criterio a seguir. Por distancia topológica, carga de tráfico, etc
- El Servidor ALTO puede obtener información de los proveedores o de los nodos sobre sus características, por ejemplo, cobro por tarifa plana o por volumen.
- Un cliente puede obtener la lista de pares potenciales y enviarla al servidor, el cual puede devolver una lista ordenada
- También necesita un protocolo para el descubrimiento del servidor ALTO

Extensión ALTO

- Ahora está siendo extendido para localizar recursos en centros de datos
- Necesita ser capaz de expresar:
  - Disponibilidad del recurso (memoria, almacenamiento, CPU, red)
  - Coste de esos recursos
  - Limitaciones en recursos (p.ej. Ancho de banda)
  - Limitaciones en estructura (p.ej. Consumo de potencia)
- El cliente ALTO obtiene la información de varios proveedores
- Problema para la privacidad del recurso y coste de información para el proveedor



Resumen Parte II

- SDN es el entrono de trabajo para gestionar automáticamente y controlar un gran número de dispositivos de red y servicios en un entorno multi-usuario
- OpenFlow originó SDN pero ahora hay disponibles varias APIs Northbound y Southbound, servicios intermedios y herramientas. Como XMPP, ForCES, PCE, ALTO
- El Controlador SDN OpenDaylight encabeza el proyecto SDN de código abierto bajo la Linux Foundation
- Su diseño modular permite varios protocolos Southbound

Parte III

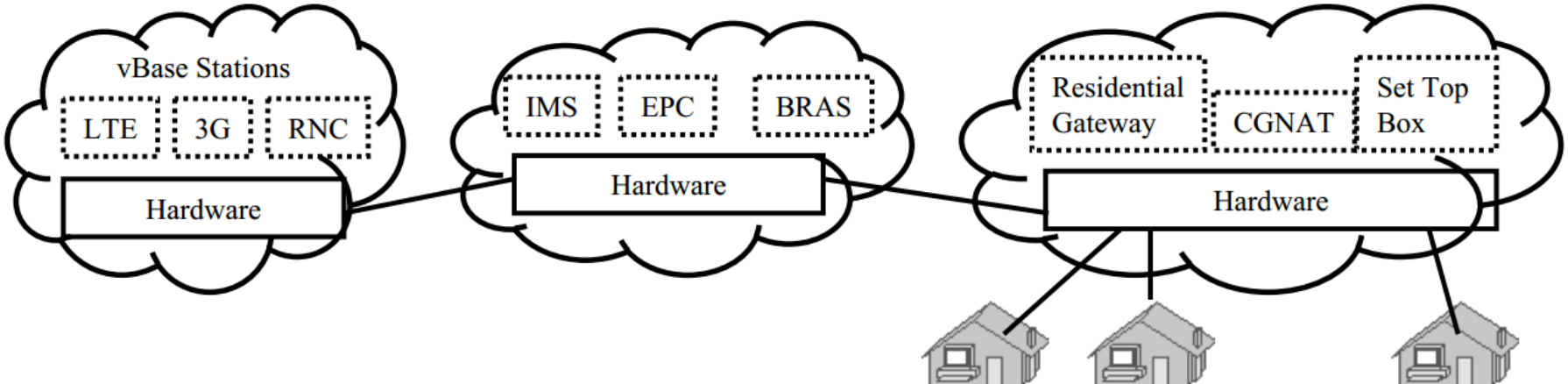
Network Function Virtualization (NFV)

Parte III Network Function Virtualization

- ¿Qué es NFV?
- Relación entre NFV y SDN
- Especificaciones ETSI, NFV, ISG
- Conceptos, Arquitectura, Requerimientos, Casos de Uso
- Pruebas de Concepto y Cronología

Network Function Virtualization (NFV)

- Estándar rápido hardware → Dispositivos basados en Software
- Routers, Firewalls, BRAS → También conocido como implementación caja blanca
- Implementación en máquinas virtuales
  - Aparatos virtuales
  - Todas las ventajas de la virtualización (rápido aprovisionamiento, escalabilidad, movilidad, CapEx reducido)



¿Por qué necesitamos NFV?

- Virtualización: Usar los recursos de la red sin necesidad de preocuparse sobre dónde está físicamente localizado, cuánto es, cómo se organiza, etc.
- Orquestación: Gestión de miles de dispositivos
- Programable: DeberIa ser capaz de cambiar el comportamiento al vuelo
- Escalado dinámico: Ser capaz de cambiar de tamaño
- Automatización: Menor OpEx (coste continuado)
- Visibilidad: Monitorización de recursos, conectividad
- Rendimiento: Optimiza la utilización de los dispositivos de red
- Múltiples arrendatarios: Compartiendo una infraestructura costosa
- Integración de Servicios
- Apertura: Elección completa de plug-ins modulares
- Gestión unificada de la computación, red y almacenamiento.
- Nota: Son las mismas que para SDN

Relación NFV y SDN

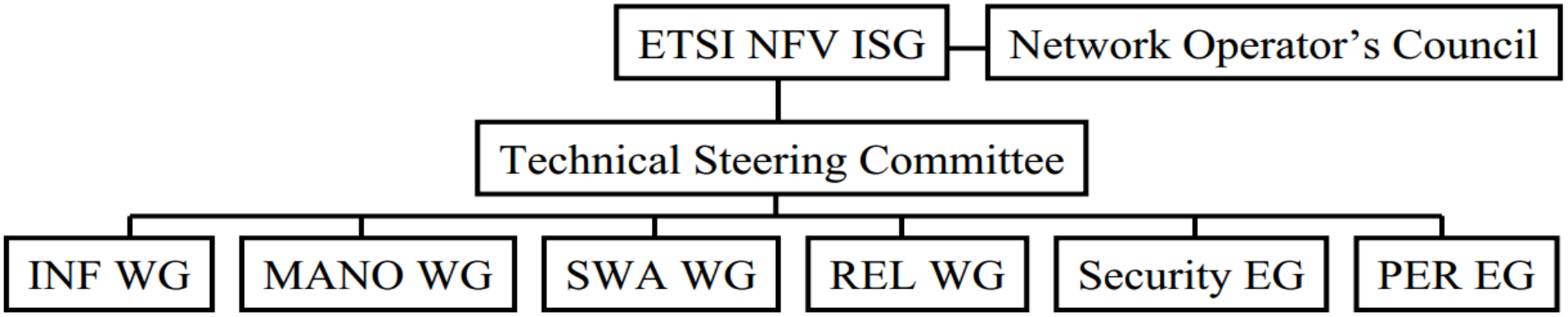
- El concepto de NFV se originó a partir de SDN
- Primero un white paper de ETSI mostró un diagrama solapado Venn
- Fue eliminado en la segunda versión
- NFV y SDN son complementarios. El uno no depende del otro
- Ambos tienen objetivos similares, pero aproximaciones muy diferentes
- SDN necesita nuevas interfaces, módulos de control, aplicaciones
- NFV requiere mover las aplicaciones de red de un hardware dedicado a contenedores virtuales sobre hardware genérico
- NFV es el presente. SDN es el futuro
- La virtualización por sí sola provee muchas de las características requeridas
- No hay mucho debate sobre NFV

Funciones de Red Movil

- Switches, por ejemplo Open vSwitch
- Routers, por ejemplo , Click
- Home Location Register (HLR),
- Serving GPRS Support Node (SGSN),
- Gateway GPRS Support Node (GGSN),
- Combined GPRS Support Node (CGSN),
- Radio Network Controller (RNC),
- Serving Gateway (SGW),
- Packet Data Network Gateway (PGW),
- Residential Gateway (RGW),
- Broadband Remote Access Server (BRAS),
- Carrier Grade Network Address Translator (CGNAT),
- Deep Packet Inspection (DPI),
- Provider Edge (PE) Router,
- Mobility Management Entity (MME),
- Element Management System (EMS)

ETSI NFV ISG

- El objetivo del Grupo de Especificación de Industria (ISG) es definir los requisitos.
- Cuatro grupos de trabajo:
  - INF: Arquitectura para la Infraestructura de virtualización
  - MANO: Gestión y Orquestación
  - SWA: Arquitectura del Software
  - REL: Fiabilidad y Disponibilidad, adaptación y tolerancia a fallos



ETSI NFV ISG (Cont)

- Dos grupos de expertos:
  - Security
  - Rendimiento y Portablidad: Escalabilidad, eficiencia, y rendimiento de las NFVs relativo al hardware dedicado

Especificaciones NFV

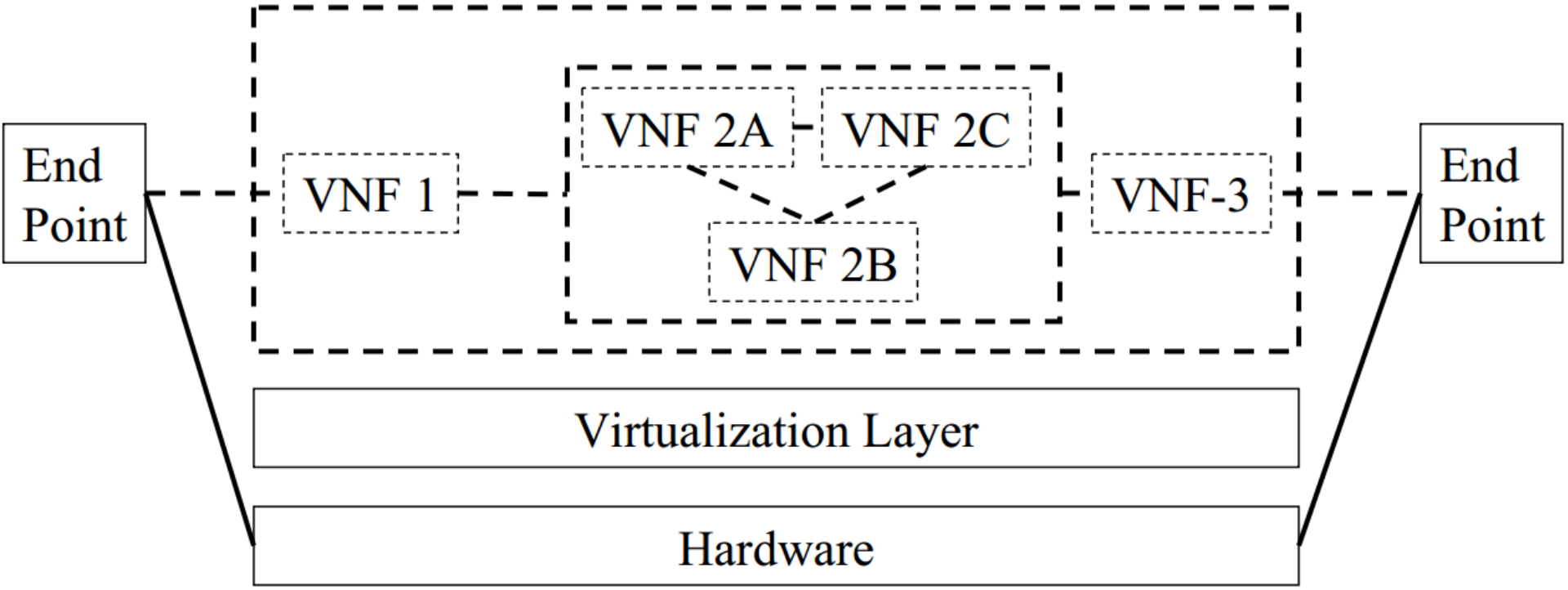
1. NFV Casos de Uso (GS NFV 001)
2. NFV Entorno de la Arquitectura (GS NFV 002)
3. Terminología para los principales conceptos en NFV (GS NFV 003)
4. NFV Requerimientos de Virtualización (GS NFV 004)
5. NFV Entorno de Pruebas de Concepto (GS NFV-PER 002)

Conceptos NFV

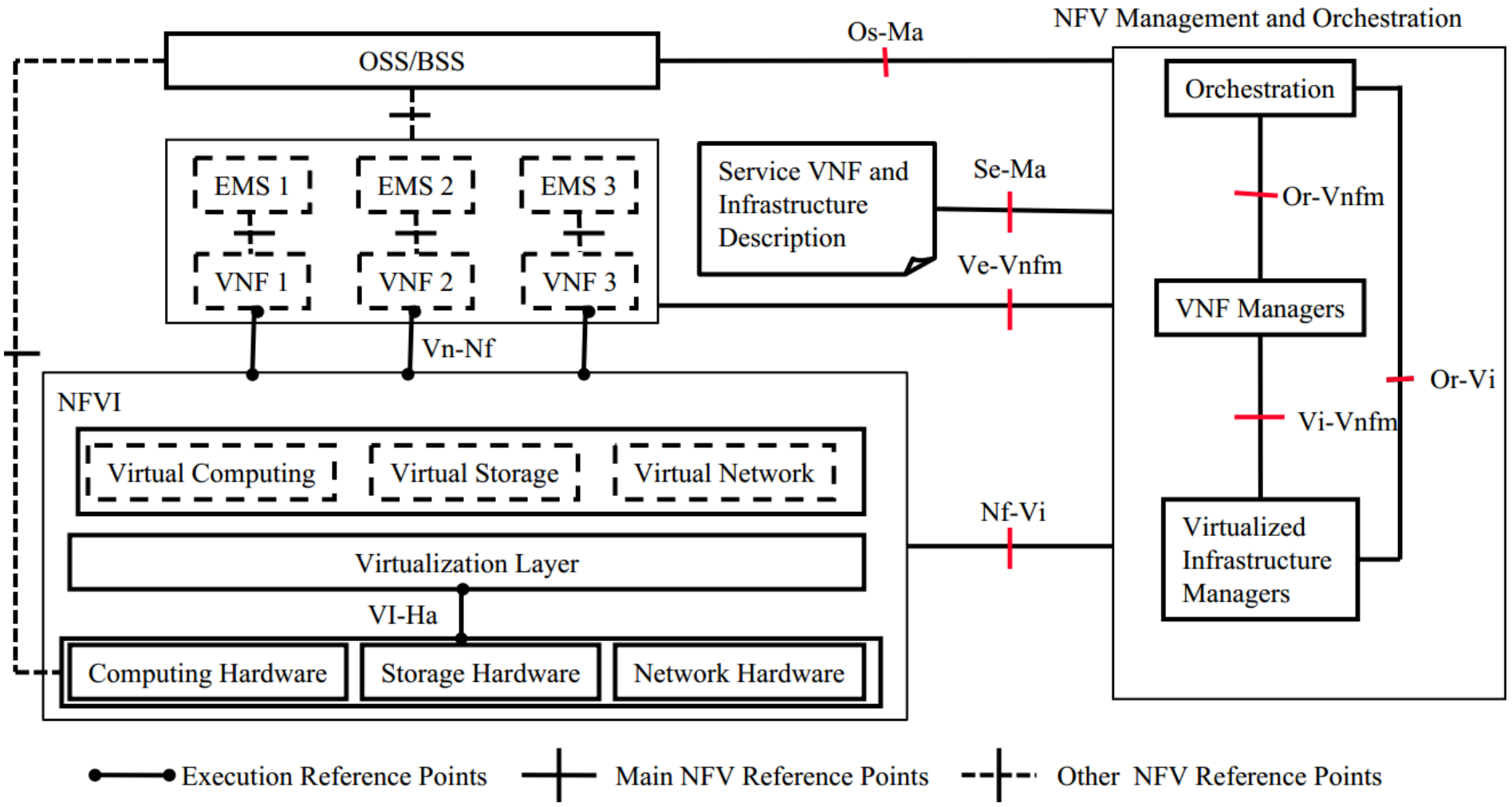
- Network Function (NF): Bloque de construcción funcional con interfaces bien definidas así como un comportamiento funcional bien definido
- Virtualized Network Function (VNF): Implementación Software de NF que puede ser implementada en una infraestructura virtualizada
- VNF Set: La conectividad entre VNFs no se especifica, por ejemplo, gateways residenciales
- VNF Forwarding Graph: Servicio en cadena cuando el orden en la conectividad de la red es importante, por ejempo, firewall, NAT, balanceador de carga
- NFV Infrastructure (NFVI): Hardware y software requeridos para implementar, gestionar y ejecutar VNFs incluyendo el la potencia de cómputo, red y almacenamiento

Grafo de Reenvío en la Red

- Un servicio extremo a extremo que puede incluir gráficos de envío anidados



Arquitectura NFV



Espec. De Requisitos de un Framework NFV

- General: Virtualización parcial o total, rendimiento predecible
- Portabilidad: Separada de la infraestructura subyacente
- Rendimiento: Como se describe y facilita la monitorización
- Tolerancia a fallos: Escalable para llegar a los SLAs (Acuerdos de nivel de Servicio). Movible a otros servidores
- Adaptación: Ser capaz de recrearse tras un fallo
- Especificación de la tasa de pérdida de paquetes, caídas, tiempo de recuperación, etc
- Seguridad: autorización basada en roles, autenticación
- Continuidad de servicio: Continuidad interrumpida o no interrumpida después de fallos o de migración

NFV Framework Requirements (Cont)

- Servicio Asegurado: Sello de tiempo y copias de envío de los paquetes para detección de fallo
- Requisitos de Eficiencia energética: Debería ser posible poner un subconjunto de VNF en un estado de ahorro energético
- Transición: Coexistencia con implementaciones desfasadas y de varios fabricantes
- Modelos de Servicios: Los operadores pueden usar la infraestructura NFV operada por otros operadores

Casos de Uso de NFV

- Nube:
  - La Infraestructura NFV como Servicio (NFVIaaS) como IaaS
  - Virtual Network Functions (VNFs) como Servicio (VNFaaS) como SaaS
  - VNF gráficos de envío (Service Chains)
  - Virtual Network Platform como Servicio (VNPaaS) como PaaS
- Móvil:
  - Virtualización del Mobile Core Network y IMS
  - Virtualización de una Mobile Base Station
- Centros de Datos:
  - Virtualización de CDNs
- Acceso/Residencial:
  - Virtualización del entorno del Hogar
  - Acceso Fijado a NFV

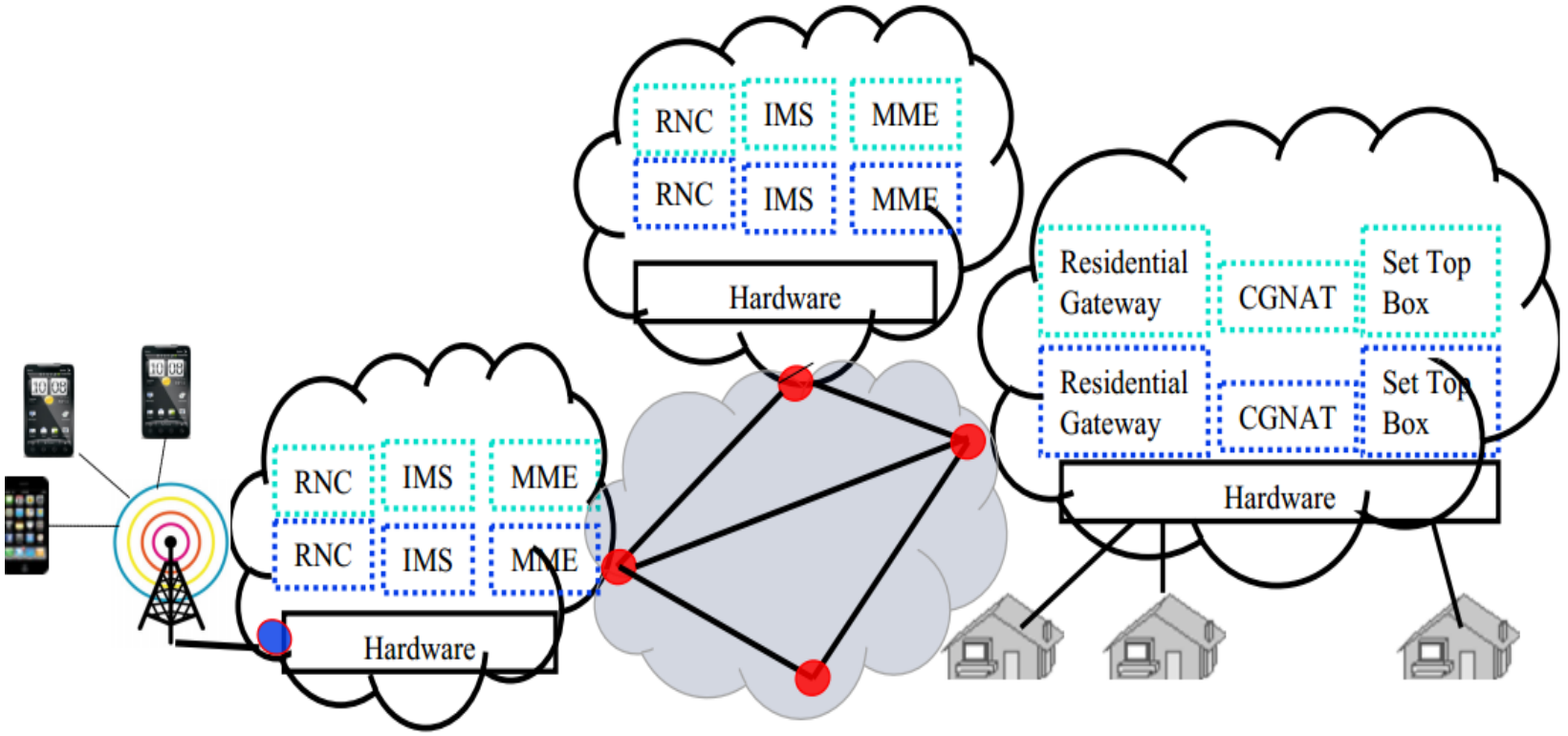
Pruebas de Concepto (PoCs) NFV

- ETSI ha formado un Foro de PoC NFV ISG
- Los siguientes módulos han sido demostrados:
  - Virtual Broadband Remote Access Server (BRAS) por British Telecom
  - Virtual IP Multimedia System (IMS) por Deutsche Telekom
  - Virtual Evolved Packet Core (vEPC) por Orange Silicon Valley
  - Carrier-Grade Network Address Translator (CGNAT) y Deep Packet Inspection (DPI), Home Gateway por Telefónica
  - PerimetaSession Border Controller (SBC) por Metaswitch
  - Deep packet inspection por Procera
- La mayoría de estos están basados en tecnologías Cloud, como OpenStack

Encadenado de Servicios en un entorno Multi-Cloud y Multi-Tenant

- VNFs (Virtual network fns) pertenecen a varios clientes. Cada Cloud pertenece a un proveedor de Servicios de Nube (CSP) distinto
- La infraestructura de internet pertenece a un proveedor de servicios de red (NSP)
- Enacadenamiento de Servicios = Flujo de Trabajo
- Grupo de trabajo IETF SFC

Encadenado de Servicios (Cont.)



Cualquier Function Virtualization (FV)

- NFV es de interés para los proveedores de servicios de red
- Pero el mismo concepto puede aplicarse a cualquier otra industria; por ejemplo la financiera, banca, bolsa, etc
- Todo el mundo se puede beneficiar de:
  - Descomposición en funciones de su industria
  - Virtualización de esas funciones
  - Encadenado de servicios de esas funciones virtuales (FVs) → Un servicio que lo traerá la siguiente generación de ISPs

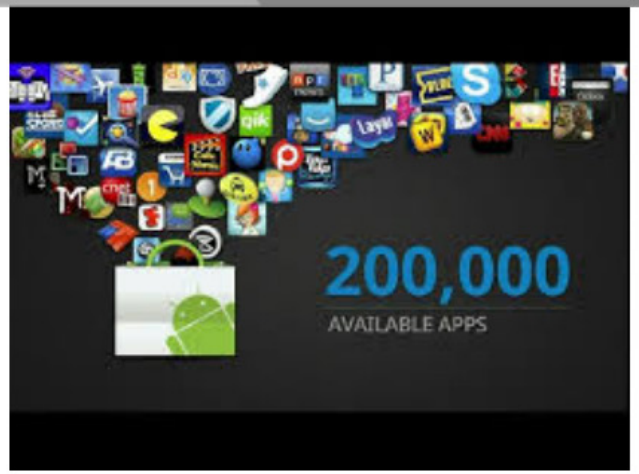
Empresas en el Mercado APP: Menor CapEx

Virtual IP Multimedia System

Available on the App Store

amazon.com and you're done.™ App Store

android



Resumen de la Parte III

- NFV pretende reducir los costes OpEx mediante la automatización y la escalabilidad que se alcanza al implementar las funciones de red como dispositivos virtuales
- NFV permite todos los beneficios de la virtualización y la computación en red incluyendo orquestación, escalado, automatización, independencia de hardware, pagar-por-usar, tolerancia a fallos…
- NFV y SDN son independientes y complementarios. Pueder usar ambos o ninguno.
- NFV requiere la estandarización de los puntos de referencia las interfaces para ser capaz de mezclar y unir VNFs de distintos orígenes
- NFV puede se implementada ahora. Varias funciones virtuales ya han sido demostradas por operadoras

Resumen General

- Cuatro planos de Red: Datos, Control, Gestión, Servicio
- OpenFlow separa el plano de control y lo mueve a un control centralizado → Simplifica los elementos de envío
- SDN es el entrono de trabajo para gestionar automáticamente y controlar un gran número de dispositivos de red y servicios en un entorno multi-usuario
- OpenFlow originó SDN pero ahora hay disponibles varias APIs Northbound y Southbound, servicios intermedios y herramientas.
- El Controlador SDN OpenDaylight encabeza el proyecto SDN de código abierto bajo la Linux Foundation
- NFV reduce los costes OpEx mediante la automatización y la escalabilidad que se alcanza al implementar las funciones de red como dispositivos virtuales

Acrónimos

- ACI Application Policy Infrastructure
- ACL Access Control List
- AEX Application Information Exposure
- ALG Application Level Gateway
- ALTO Application Layer Traffic Optimization
- ANDSF Access Network Discovery and Selection Function
- API Application Programming Interface
- APIC Application Policy Infrastructure Controller
- ARP Address Resolution Protocol
- ASICs Application Specific Integrated Circuit
- ATIS Association for Telecom Industry Solutions
- ATM Asynchronous Transfer Mode
- AVNP Active Virtual Network Management Protocol
- BFD Bidirectional Forwarding Detection
- BGP Border Gateway Protocol

Acrónimos (Cont.)

- BIRD BirdInternet Routing Daemon
- BNC Big Switch Network Controller
- BRAS Broadband Remote Access Server
- BSD Berkeley Software Distribution
- BSS Business Support Systems
- BUM Broadcast, Unknown, and Multicast
- CapEx Capital Expenditure
- CDN Content Distribution Network
- CDN Content Distribution Network
- CDNI Content Distribution Network Interconnection
- CE Control Element
- CFM Connectivity Fault Management
- CGNAT Carrier-Grade Network Address Translator
- CGSN Combined GPRS Support Node
- CLI Command Line Interface
- CMS Content Management System

Acrónimos (Cont.)

- COTS Commercial-off-the-shelf
- CPU Central Processing Unit
- CRUD Create, Read, Update, Delete
- CSP Cloud Service Provider
- DDIO Data Direct I/O Technology
- DFCA Dynamic Frequency Channel Allocation
- DHCP Dynamic Host control Protocol
- DNS Domain Name System
- DOVE Distributed Overlay Virtual Ethernet
- DPI Deep Packet Inspection
- DSCP Differentiated Service Control Point
- DVS Distributed Virtual Switch
- ECMP Equal Cost Multipath
- EID Endpoint Identifier
- EMS Element Management System
- ESP EncrytecSecurity Payload

Acrónimos (Cont.)

- ETSI European Telecom Standards Institute
- FCAPS Faults, configuration, accounting, performance, and security
- FE Forwarding Element
- FIB Forwarding information base
- ForCES Forwarding and Control Element Separation
- GGSN Gateway GPRS Support Node
- GMPLS Generalized Multi-Protocol Label Switching
- GRE Generic Routing Encapsulation
- GUI Graphical User Interface
- HLR Home Location Register
- HTML Hypertext Markup Language
- HTTP Hypertext Transfer Protocol
- I2AEX Infrastructure to Application Information Exposure
- IaaS Infrastructure as a Service
- ICMP Internet Control Message Protocol
- ICSI International Computer Science Institute

Acrónimos (Cont.)

- ID Identifier
- IDS Intrusion Detection System
- IEEE Institution of Electricaland Electronic Engineers
- IETF Internet Engineering Task Force
- IGMP Internet Group Management Protocol
- IGP Interior Gateway Protocol
- IMS IP Multimedia System
- INF Architecture for the virtualization Infrastructure
- IoT Internet of Things
- IP Internet Protocol
- IPFIX IP Flow Information Export Protocol
- IPSec IP Security
- IPv4 Internet Protcolversion 4
- IPv6 Internet Protocol version 6
- IRTF Internet Research Taskforce
- IS-IS Intermediate System to Intermediate System

Acrónimos (Cont.)

- ISG Industry Specification Group
- ISO International Standards Organization
- JSON Java Script Object Notation
- JVM Java Virtual Machine
- KVM Kernel-based Virtual Machine
- LACP Link Aggregation Control Protocol
- LAN Local Area Network
- LISP Locator-ID Separation Protocol
- LLDP Link Layer Discovery Protocol
- LS Link State
- LSP Label Switched Path
- MAC Media Access Control
- MAN Metropolitan Area Network
- MANO Management and orchestration
- MME Mobility Management Entity
- MPLS Multi-protocol Label Switching

Acrónimos (Cont.)

- NAT Network Address Translation
- NF Network Function
- NFV Network Function Virtualization
- NFVI Network Function Virtualization Infrastructure
- NFVIaaS NFVI as a Service
- NIB Network Information Base
- NIC Network Interface Card
- NSF National Science Foundation
- NTP Network Time Protocol
- NTT Nippon Telegraph and Telephone
- NVGRE Network Virtualization using Generic Routing Encapsulation
- NVO3 Network Virtualization over L3
- NVP Network Virtualization Platform
- OF OpenFlow
- OFlops OpenFlow Operations Per Second
- OLSR Optimized Link State Routing

Acrónimos (Cont.)

- ON.LAB Open Networking Lab at Stanford
- OnePK Open Network Environment Platform Kit
- ONF Open Networking Foundation
- ONV OpenDaylight Network Virtualization
- openQRM Open Clusters Resource Manager
- OpenWRT Open WRT54G (Linksys product name) software
- OpEx Operational Expenses
- OS Operating System
- OSCP OpenDaylight SDN Controller Platform
- OSGi Open Services Gateway Initiative
- OSPF Open Shortest Path First
- OSS Operation Support System
- OTN Optical Transport Network
- OVS Open Virtual Switch
- OVSDB Open Virtual Switch Database
- PaaS Platform as a Service

Acrónimos (Cont.)

- PCC Path Computation Client
- PCE Path Computation Element
- PCEP Path Computation Element Protocol
- PE Provider Edge
- PGW Packet Data Network Gateway
- PIM-SM Protocol Independent Multicast -Sparse Mode
- PIM Protocol Independent Multicast
- PoC Proof-of-Concept
- PoP Point of Presence
- POP Post Office Protocol
- PSTN Public Switched Telephone Network
- PWE3 Pseudo wire Emulation Edge to Edge
- QoS Quality of Service
- RAN Radio area networks
- REL Reliability, Availability, resilience and fault tolerance group

Acrónimos (Cont.)

- REST Representational State Transfer
- RFC Request for Comments
- RGW Residential Gateway
- RIB Routing Information Base
- RIP Routing Information Protocol
- RLOC Routing Locator
- RNC Radio Network Controller
- RPC Remote Procedure Call
- RS Routing System
- RSPAN Remote Switch Port Analyzer
- SaaS Software as a Service
- SAL Service Abstraction Layer
- SBC Session Border Controller
- SDN Software Defined Networking
- SGSN Serving GPRS Support Node
- SGW Serving Gateway

Acrónimos (Cont.)

- SIP Session Initiation Protocol
- SLA Service Level Aggrement
- SMTP Simple Mail Transfer Protocol
- SNAC Name of an OpenFlow controller
- SNMP Simple Network Management Protocol
- SPAN Switch Port Analyzer
- SSH Secure Socket Host
- SSL Secure Socket Layer
- STP Spanning Tree Protocol
- STT Stateless TCP-like Transport
- SWA Software architecture
- TAS Telephony Application Server
- TCAM Ternary Content Addressable Memory
- TCL Tool Command Language
- TCP Transmission Control Protocol
- TE Traffic Engineering

Acrónimos (Cont.)

- TIA Telecom Industry Association
- TLS Transport Level Security
- TLV Type-Length-Value
- TMF TM Forum
- ToS Type of Service
- TRILL Transparent Interconnection of Lots of Links
- TTL Time to Live
- TTP Table Typing Patterns
- UC University of California
- UDP User Datagram Protocol
- URI Uniform Resource Identifier
- vBridge Virtual Bridge
- vEPC Virtual Evolved Packet Core
- VIRL Virtual Internet Routing Lab
- VLAN Virtual Local Area Network
- VM Virtual Machine

Acrónimos (Cont.)

- VNF Virtual Network Function
- VNFaaS VNF as a Service
- VNS Virtual Network Segement
- VPN Virtual Private Network
- vSwitch Virtual Switch
- VT-d Virtualization Technology for Direct IO
- VT-x Virtualization Technology
- VTEP Virtual Tunnel End Point
- VTN Virtual Tenant Network
- VxLAN Virtual Extensible Local Area Network
- WAN Wide Area Network
- WG Working Group
- XML Extensible Markup Language
- XMPP Extensible Messaging and Presence Protocol
- XORP eXensibleOpen Router Platform