ENXEÑARÍA TELEMÁTICA
UNIVERSIDADE DA CORUÑA

Xestión de Infraestructuras

Diseño e Implantación de un CPD

Clase 6: SDN & NFV

Área de EnxeñaríaTelemática
Facultade de Informática
Universidade de A Coruña

victor.carneiro@udc.es

Virtualización de red

- La necesidad de avanzar más rápido en la creación de nuevos servicios de red, impulsado por el Cloud ha acelerado la migración de funciones de red hardware hacia el software.

- Modelos complementarios:

  - Redes Definidas por Software (SDN)

  - Virtualización de Funciones de Red (NFV)

SDN (Software Defined Network)

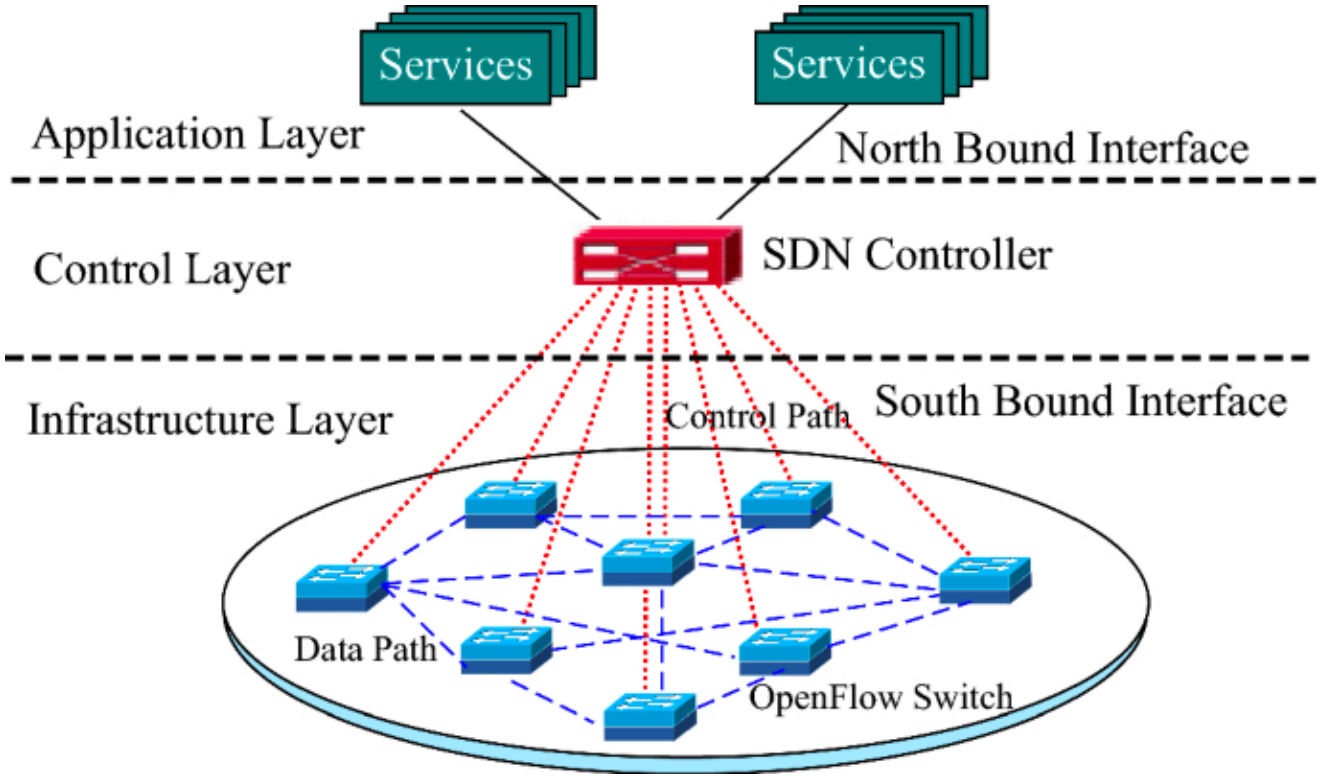
Concepto

- Las redes definidas por software tienen por objetivo simplificar la creación y administración de redes.
- Separan plano de control de plano de datos. Se gestiona el comportamiento de forma centralizada mediante un controlador. La separación de los planos proporciona una abstracción lógica de los recursos de red.
- El protocolo OpenFlow es el elemento central ya que permite la programación remota del plano de control. Dentro de sus módulos y funcionalidad, puede añadir funciones de red virtualizadas (NFV).
- Se están comenzando a utilizar por proveedores de servicio y en Data Centers.

Comparativa redes convencionales

- En las redes convencionales, el plano de control (protocolos de routing, listas de acceso, políticas…) y el plano de datos (switching, routing) están unidos. Reglas internas del equipo deciden siempre el mismo destino y trayectoria para cada paquete.
- En SDN desde el controlador se aplica la lógica de switching/routing (flow tables) a los equipos de red a través de openFlow. Las operaciones de switching/routing se realizan en base a reglas almacenadas en las flow tables de los switch/routers.
- Se puede modificar el tráfico de forma centralizada sin tocar los equipos individuales.

Arquitectura de una red SDN



© Rohit Kumar Das et al.

Programación

- El controlador está basado en un conjunto de módulos que se pueden activar/desactivar y que se encargan de diversas tareas de red.

  - **Northbound API**: Soportan gran variedad de servicios y aplicaciones para controlar diferentes tipos de aplicaciones a través de un controlador. Permite implementar lógica de negocio sobre la red y las aplicaciones.

  - **Southbound API**: Conexión con equipos de red para cambios en tiempo real del tráfico. Generalmente basada en el protocolo openFlow.

SDN

Ventajas e inconvenientes

- **Flexibilidad**: despliegue de servicios, aplicaciones e infraestructuras de forma rápida.
- **Innovación**: creación de nuevos tipos de aplicaciones, protocolos y modelos de negocio.
- **OPEX**: Sencillez de configuración y gestión de redes, reducción del tiempo de administración y reducción del error humano.
- **CAPEX**: Ampliación de la vida útil de los equipos y reducción de número de equipos. Menor dependencia de fabricantes.
- → **Inconveniente**: dependencia del controlador para escalado y seguridad.

SDN

Funcionamiento

- El controlador implementa reglas y acciones que alimentan las flow tables de los equipos de red.
- Cada regla tiene en cuenta: puerto de entrada, VLAN id, ethernet address, frame type, IP ports, protocol, TCP ports, etc…
- Se realizan acciones como: reenviar paquete, encapsularlo y enviarlo al controlador, eliminar paquete o enviar al procesamiento pipeline del vSwitch.
- El procesamiento pipeline permite evaluar los paquetes en tablas y ejecutar múltiples acciones (cualquier función de red).

Protocolo openFlow

- Protocolo abierto que permite, al controlador, programar las flow tables almacenadas en switches y routers. Esto define el camino de datos de paquetes de un servicio.
- Estandariza la comunicación entre controlador y los switches, así como el conjunto de operaciones que se puede realizar sobre las tablas de flujos.
- Permite trabajar con las características comunes de las tablas de flujos de los switch, incluso de diferentes fabricantes.
- Los flujos se pueden definir por diferentes características: puertos, etiquetas, protocolo, servicio, etc…
- De este modo, la decisión de reenvío de paquetes está centralizada y programada a través del controlador.

Controladores

- **OpenDaylight** – ODL (Linux Foundation, 2013). Licencia Eclipse. Más enfocado a DataCenters. Plataforma Model-View-Controller en Java con facilidad de despliegue de nuevos módulos basada en estándar OSGi. Documentación y curva de aprendizaje mejorable.
- **Onos** (Open Networking Lab, 2014). Licencia Apache 2.0. Más centrado en proveedor de servicios. Mayor número de módulos de NFV que ODL. Desarrollado en Java, buena documentación y despliegue basado en estándar OSGi.
- **Otros**: openContrail, Ryu, Floolight, LOOM, openMUL, …

openVSwitch (OVS)

- Proyecto Open Source (Linux Foundation) bajo licencia Apache 2.0.
- Proporciona un switch de software con funcionalidades avanzadas que puede ser controlado por openFlow para la creación de Datapath.
- Permite funciones como NetFlow, sFlow, SPAN, balanceo, STP, QoS, políticas de tráfico por puerto, etc…
- Soporta múltiples tecnologías de virtualización. Rendimiento de 1.2 Gbps con KVM o >10 Gbps con Intel Data Plane Development Kit (DPDK).

NFV (Network Functions Virtualization)

Concepto

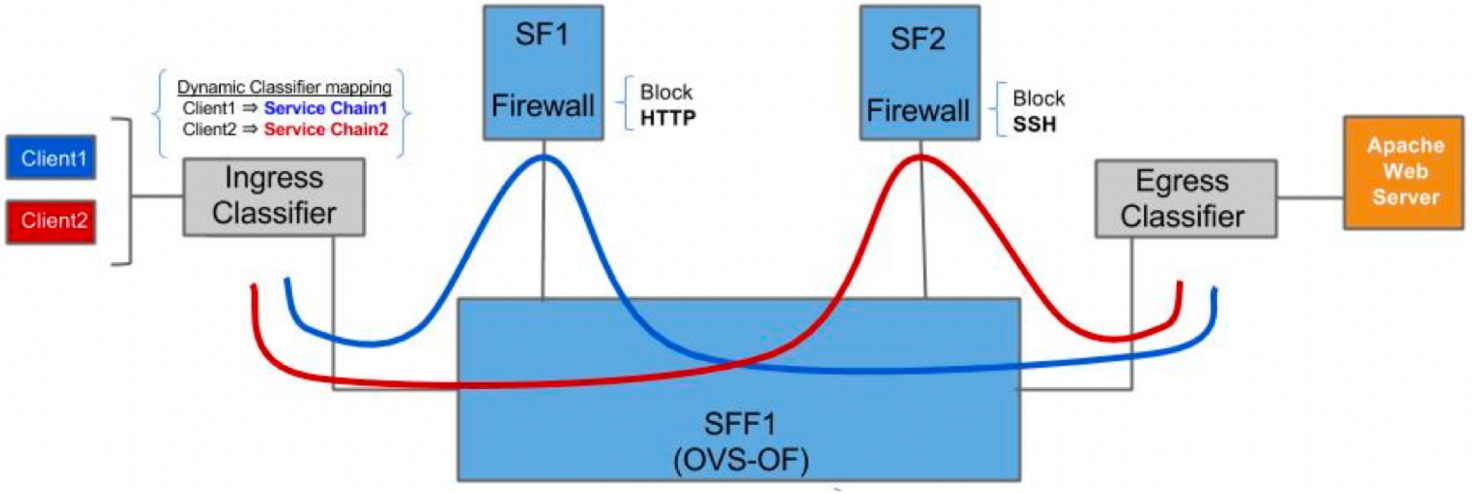
- Promovido por ETSI desde 2012.
- La virtualización de funciones de red permite implementar las funciones de red mediante software, en lugar de hardware, lo que evita dispositivos dedicados como routers, switches y firewalls.
- Permite optimizar recursos, su mantenimiento y su infrautilización.
- La combinación con SDN permite desarrollar nuevos servicios de red basados en aplicaciones sin la restricciones del software propietario de los actuales dispositivos de red. Aunque no es necesario una red SDN para su implantación.

NFV

Origen

- La industria de networking siempre ha seguido estándares muy estrictos de calidad, estabilidad y estandarización, pero eso provoca ritmos de desarrollo de producto muy largos y dependencia de hardware especializado.
- Máquinas virtuales se despliegan sobre servidores estándar, equipos de red o infraestructuras cloud para proporcionar los mismos servicios que sobre dispositivos de red especializados.
- Se pueden crear servicios complejos mediante “cadenas de funciones de servicios” SFC. De este modo se puede añadir funciones de red, de forma dinámica, en el recorrido de una conexión de datos.
- Ahora mismo se encuentra en fase de transición, conviviendo con redes tradicionales

Cadenas de servicios (SFC)



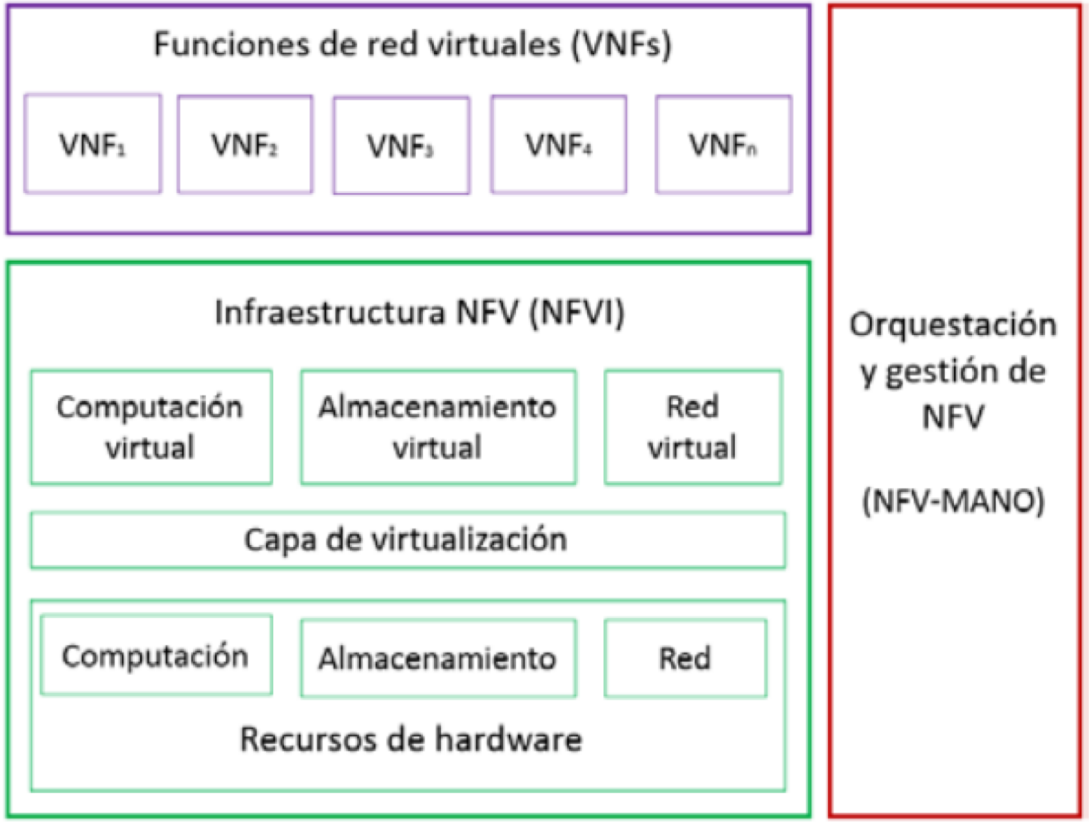
© OPNFV

Arquitectura

- Tres bloques principales:
  - Infraestructura de virtualización (NFVI): Hardware que aloja las máquinas virtuales que implementan las funciones de red.
  - Las Funciones de red virtualizadas (VNFs), mediante el despliegue de instancias.
  - Gestión y orquestación (MANO): Capa de orquestación capaz de gestionar, escalar, monitorizar, etc.. tanto las NFV como la NFVI.

- Permite provisión de servicios bajo demanda, escalables y de alta disponibilidad.

Marco de referencia



NFV

Ventajas

- Simplificación del despliegue y gestión de nodos de red.
- Mejora la escalabilidad de la red con independencia de fabricantes.
- Time to market de nuevas funcionalidades se reduce enormemente.
- Adapta las capacidades y recursos a las demandas del cliente. Alta disponibilidad del servicio.
- Reduce CAPEX y OPEX para operadores.
- RoI (Retorno de la Inversión) mucho más rápido.

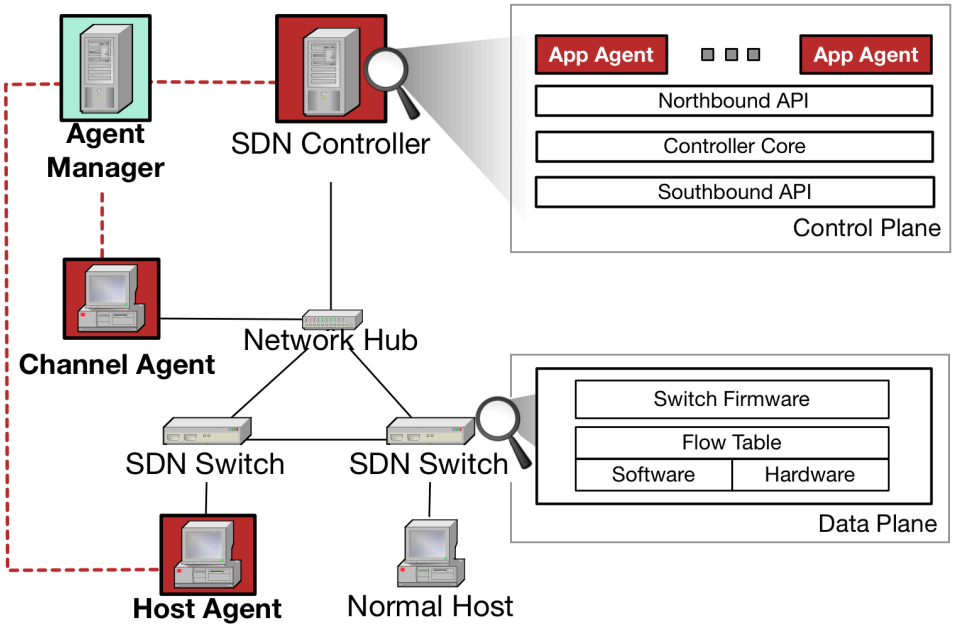
Soluciones comerciales

- **Cisco One**: Software para CPD y WAN, basada en SDN. API, controladores y tecnología de red. Orientada a dispositivos Cisco.
- **HP**: Switchs compatible con OpenFlow y una SDN App Store. P.e. F5 Big DDoS Umbrella o HP Network Protector o HP Network Optimizer.
- **Microsoft**: Desarrollo de SDN para Azure, cerrado a la comunidad.
- **IBM**: Promotor de OpenDaylight y acelerador de OpenStack. Ofrece controlador y Switch openFlow, así como la arquitectura SDN VE Platform.
- **Google**: La arquitectura de red de los centros de datos están basados en una red SDN desarrollada por ellos.
- **Dell**: Solución Active Fabric diseñada para SDN, basada en openStack.
- **VMWare**: controlador NSX para gestión de todos los switch virtuales. Definición de VXLANs y API northbound.
- **Otras soluciones**: NEC, Alcatel-Lucent, Huawei, etc…

Ejemplos: Frameworks SDN

Delta Framework

- Delta Framework orientado a seguridad SDN:
  - Permite simular más de 40 casos de ataque sobre redes SDN
  - Ayuda a descubrir problemas de seguridad en una red SDN
- Utiliza diversas herramientas de pen-testing orientada a entornos SDN.



victor.carneiro@udc.es

Uso: Plataformas IaaS

- **OpenNebula** (UPM – 2008): Plataforma para la creación de Clouds híbridas. Virtualización de computación, almacenamiento y red. API Rest para programación remota e interfaces abiertas con otras plataformas como AWS o Azure.
- **OpenStack** (NASA – 2010): Fundación con más de 200 empresas, arquitectura modular. Última distribución con cerca de 40 módulos: computación, red, almacenamiento, balanceadores, DNS, authentication, orquestación, BdD, Containers, BigData processing framework, backup, etc…