REDES DE NUEVA GENERACIÓN

TEMA 5

Redes Definidas por Software: SDN

1º Introducción a las LAN Virtuales (VLAN) 3
2º El protocolo SDN 3
3º Open vSwitch 4
    3.1 OpenFlow 4

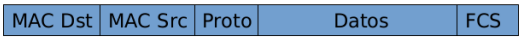
1º Introducción a las LAN Virtuales (VLAN)

- Las redes de área local se organizan en base a la segmentación de su dominio mediante el uso de switches, donde cada uno de dichos segmentos constituye una LAN (grupo de trabajo), las cuales se comunican entre sí de manera jerárquica. Sin embargo, aunque las redes estén segmentadas, estas siguen perteneciendo a un mismo dominio de difusión donde no hay restricciones de tráfico.

- La solución ante esto se encuentra en las Redes de Área Local Virtuales (VLAN), las cuales se basan en la posibilidad de definir redes locales diferentes que en realidad pertenecen a la misma red. Esto se realiza mediante la configuración software de los switches que se encuentran en dicha área, los cuales realizarán las operaciones de filtrado de los mensajes.

- Las máquinas solo pueden comunicarse directamente con aquellas que pertenecen a su misma VLAN, de modo que el switch es el encargado de separar el tráfico que pertenece a cada una de dichas redes virtuales. Un mismo equipo puede pertenecer a varias VLAN al mismo tiempo y estas pueden configurarse de forma dinámica sin la necesidad de modificar las conexiones.

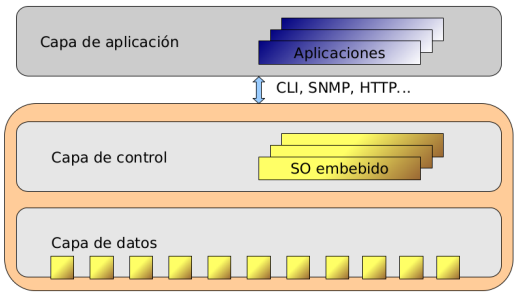
- Podemos diferenciar dos maneras diferentes de definir las VLAN:
  - **VLAN basadas en puertos:** El administrador decide que puerto de cada switch pertenece a cada red virtual. Esto dificulta la tearea de comunicar varios conmutadores.
  - **VLAN basadas en etiquetas:** A cada trama se le añade una etiqueta que indica a que red virtual pertenece (protocolo 802.1Q), las cuales serán eliminadas cuando el datagrama llegue al router de salida. Estas etiquetas se insertan en la cabecera de nivel 2 después de las direcciones MAC de origen y destino, abarcan un total de 32 bits y están conformadas por los siguientes campos:
    - **Tipo (16 bits).**
    - **Prioridad (4 bits).**
    - **VLAN Identified – VID (12 bits).**



- El primero de los conmutadores añade la etiqueta a los masajes y el último la elimina, las cuales no cambian durante todo el recorrido. Los conmutadores son gestionables, de modo que pueden aplicarte actualizaciones de firmware para modificar las redes VLAN que se quieran implementar.

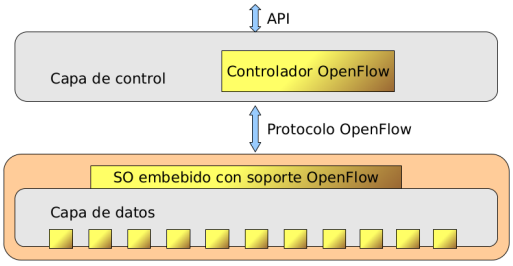
2º El protocolo SDN

- En los switches gestionables (Switch Ethernet Gestionable) se utilizan diversas APIS como herramienta para poder configurar el funcionamiento del mismo. En estos se pueden definir tres capas bien diferenciadas: La capa de datos, la capa de control y la capa de aplicación.



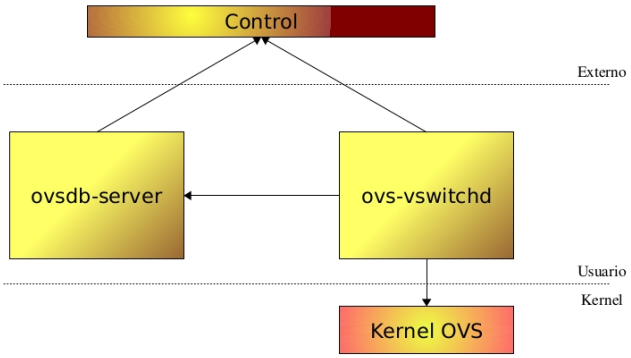
- La capa de control se encarga de determinar por donde debe transmitirse cada una de las tramas que recibe el switch, la cual avisa a la capa de datos para indicarle como realizar dicho encaminamiento.

- El funcionamiento de los switches SDN (Software Defined Network) consiste en separar la capa de control de la capa de datos con el objetivo de poder hacer gestionable esta última de manera versátil. La API utilizada pasa a ser un estándar, de modo que un mismo controlador puede gestionar diferentes switches.



3º Open vSwitch

– Vswitch es un software abierto utilizado para la implementación de un switch virtual en entornos de servidores virtualizados. Esta switch se encarga de reenviar el tráfico entre las distintas Máquinas Virtuales que se ejecutan en la misma máquina física y de controlar su acceso a la red física.



– Esta herramienta también permite el manejo de switches físicos que utilicen la misma arquitectura, la cual esta constituida por:

- **Módulo de control**
- **Ovsdb-server:** Demonio encargado de gestionar la bases de datos del switch virtual, la cual almacena información a cerca de: Puentes, interfaces túneles etc. La información de configuración se almacena en memoria no volátil.
- **Ovsdb-vswitchd:** Demonio encargado de la gestión de Open vSwitch, realizando labores como: mantener actualizada la base de datos, configurar el módulo OVS del kernel y gestionar las interfaces virtuales. Además de esto:
  - Da soporte al uso de múltiples puentes independientes (datapaths).
  - Permite la clasificación de paquetes para la definición de las VLAN.
  - Soporta las definiciones de QoS.
  - **Mirroring:** Redirección del tráfico que pasa por un puerto concreto para llevar a cabo acciones de auditoría y seguridad.
  - **Trunking:** Trabajo conjunto de varias puertas del switch para simular un mayor ancho de banda en el enlace.
  - **Pratching:** Permite unir dos switches físicamente para que se comporten como uno solo.
- **Kernel OVS**

– Cuando utilizamos Open vSwitch, el primer paquete del flujo de datos que cumpla unas características determinadas será tratado en la parte de la arquitectura que conforma el espacio de usuario (es decir, el ovsdb-server y el ovsdb-vswitchd). El motivo de esto es instruir al Kernel para realzar de forma correcta y eficiente la gestión de los siguientes paquetes del flujo.

– Cuando implementamos topologías complejas puede producirse la aparición de bucles que causan saturación de mensajes. Para evitar esto se utiliza el protocolo STP, el cual poda algunas ramas para convertir el grafo de conexiones en un árbol de recubrimiento mínimo.

3.1 OpenFlow

– El verdadero potencial de Open vSwitch es la capacidad de controlar de manera dinámica los flujos de datos que atraviesan el switch. Un flujo de datos es un conjunto de paquetes que cumplen un determinado criterio, los cuales se establecen mediante reglas implementadas por *ovs-ofctl*.

– Los distintos flujos se agrupan en tablas numeradas (desde 0 hasta 253) y ordenadas por prioridad. Cada una de las reglas cuenta con una sección match y una sección action.