

Laboratorio Introducción Controlador Floodlight.

Contenido

Laboratorio – Controlador Floodlight.....	2
Objetivo Práctica Laboratorio	2
Requisitos Laboratorio	2
Actividades Laboratorio	2
Instalación Controlador Floodlight.....	2
Acceso Web	4
Simulación con Mininet y Floodlight.....	5
Contraste con otras soluciones.	7
Entregable Proyecto.....	7
Referencias	7

Laboratorio – Controlador Floodlight

Objetivo Práctica Laboratorio

INTEGRAR el controlador SDN Floodlight con una red desplegada en la herramienta mininet.

CONTRASTAR el controlador SDN Floodlight con algunos controladores SDN presentes en el mercado actual.

Requisitos Laboratorio

Para el correcto desarrollo de este laboratorio es necesario contar con lo siguiente:

- Máquina virtual del Laboratorio - Preparación Ambiente.
- Mininet.
- Acceso a Internet.
- Máquina virtual controlador.

Actividades Laboratorio

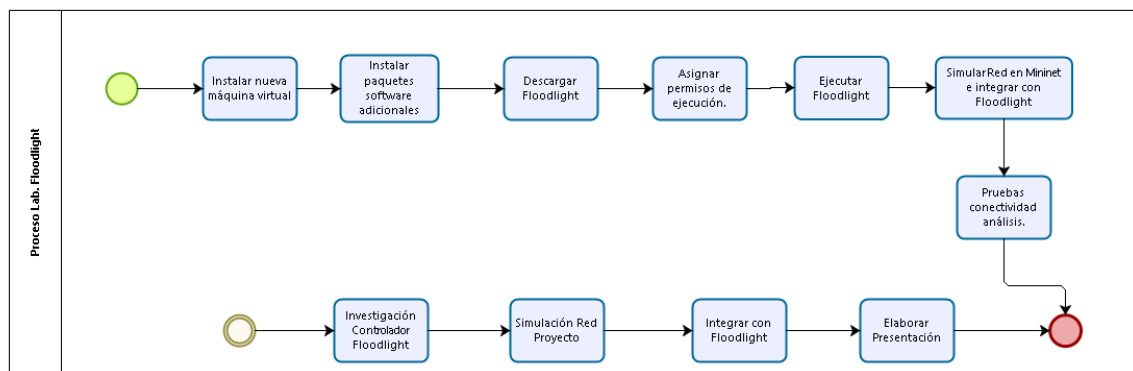


Diagrama 1. Proceso Laboratorio

Instalación Controlador Floodlight

El Floodlight Open SDN Controller, es un Controlador OpenFlow de clase empresarial con licencia de Apache y basado en Java. Es apoyado por una comunidad de desarrolladores que incluye varios ingenieros de Big Switch Networks.

OpenFlow es un estándar abierto administrado por Open Networking Foundation (ONF). Especifica un protocolo mediante el cual, un controlador remoto puede modificar el comportamiento de los dispositivos de red a través de un "conjunto de instrucciones de reenvío" bien definido. Floodlight está diseñado para funcionar con el creciente número de conmutadores, enrutadores, conmutadores virtuales y puntos de acceso compatibles con el estándar OpenFlow (floodlight, 2017).

Es importante tener en cuenta, que este controlador debe instalarse en una máquina virtual diferente, considerando los siguientes recursos:

- **CPU:** 1 Núcleo.
- **Memoria RAM:** 2 GB.
- **Almacenamiento:** 20 GB.
- **Red:** Modo NAT/Conexión Puente.

Para evitar problemas a la hora de ejecutar este controlador SDN, deberemos detener el servicio del ovs-testcontroller instalado en prácticas anteriores:

```
sudo systemctl stop openvswitch-testcontroller
```

Antes de comenzar la instalación y la configuración del controlador Floodlight, tenemos que instalar java, apache maven y ant. Utilizamos el siguiente comando:

```
sudo apt-get install build-essential default-jdk default-jre ant  
python-dev eclipse
```

Ahora bien, debemos descargar el controlador Floodlight desde GitHub de la siguiente manera:

```
git clone git://github.com/floodlight/floodlight.git  
cd floodlight  
git submodule init  
git submodule update  
ant
```

Ahora, debemos crear una carpeta en la siguiente ruta `/var/lib/` y le asignamos el nombre "floodlight" con todos los permisos.

```
mkdir /var/lib/floodlight  
chmod 777 /var/lib/floodlight
```

Para ejecutar el controlador SDN ONOS, ejecutamos el siguiente script:

```
java -jar target/floodlight.jar
```

Debemos asegurarnos que el servicio que escucha por el puerto 6653 está en ejecución, ya que este es el puerto con el que trabaja el protocolo Openflow, utilizando el comando `netstat -ntl`, como se aprecia en la siguiente captura de pantalla:

```
user@ubuntu:~/floodlight$ netstat -ntl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:5355            0.0.0.0:*               LISTEN
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp6       0      0 :::5355                 :::*                     LISTEN
tcp6       0      0 :::8080                  :::*                     LISTEN
tcp6       0      0 :::4242                  :::*                     LISTEN
tcp6       0      0 :::6642                  :::*                     LISTEN
tcp6       0      0 ::1:631                 :::*                     LISTEN
tcp6       0      0 :::6653                  :::*                     LISTEN
tcp6       0      0 :::6655                  :::*                     LISTEN
user@ubuntu:~/floodlight$
```

Imagen 1. Validación servicios.

Acceso Web

Una de las características que instalamos, nos permite acceder via web al controlador Floodlight, para poder gestionarlo. Para acceder utilizamos la siguiente dirección:

`http://Dir_IP_Floodlight:8080/ui/index.html`

La siguiente es una captura de pantalla del acceso web a ONOS:

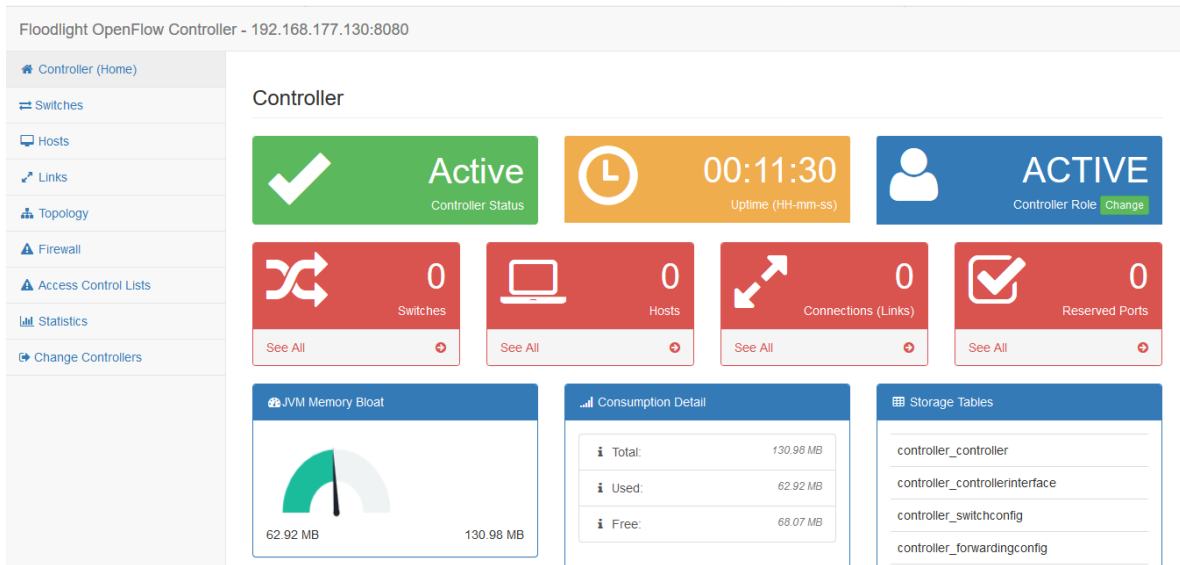


Imagen 2. Vista Web Floodlight

Simulación con Mininet y Floodlight

Iniciamos una nueva instancia de Floodlight, y configuramos la siguiente topología de red en Mininet, esta topología debemos conectarla con el controlador Floodlight:

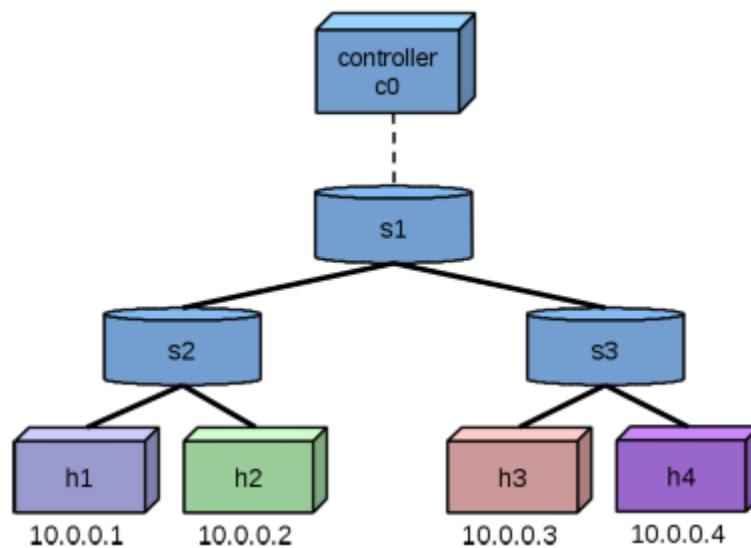



Diagrama 2 Topología de Red

 Recuerden utilizar los comandos aprendidos en la práctica de laboratorio de Mininet.

Una vez tengan simulada la red y conectada con Floodlight, realiza una prueba de conectividad con todos los nodos y revisa:

- ¿Qué cambios se pueden presenciar en el controlador Floodlight? Revise la topología y los nodos, en el menú lateral de la herramienta web.

Una de las ventajas a la hora de utilizar el controlador Floodlight, es que permite analizar los flujos de tráfico generados en nuestra red con mayor facilidad. Así pues, realicé lo siguiente:

- Realicé pruebas de flujos de tráfico con iperf y HTTP. Utilicé los siguientes enlaces como guía: <http://mininet.org/walkthrough/> <http://mininet.org/sampleworkflow/>. Evalué los flujos de tráfico desde la herramienta web de ONOS. ¿Cómo un controlador SDN y esté tipo de soluciones, apoya en la gestión de una red de comunicaciones? Investigué los problemas comunes a los que se enfrentan los administradores de red en su labor, para realizar un mejor análisis.

Ahora bien, iniciamos una captura de tráfico en Wireshark y pasamos a analizar el tráfico del protocolo OpenFlow, las pruebas de iperf y HTTP en nuestra topología de red. Debemos obtener una captura como la siguiente:

203	5.343096773	10.0.2.15	192.168.206.130	OpenFlow	194	Type: OFPT_PACKET_IN	
204	5.343166619	10.0.2.15	192.168.206.130	OpenFlow	194	Type: OFPT_PACKET_IN	
205	5.343241692	192.168.206.130	10.0.2.15	TCP	60	6653 → 36710 [ACK] Seq=1087 Ack=15891 Win=65535 Len=0	
206	5.343249235	192.168.206.130	10.0.2.15	TCP	60	6653 → 36712 [ACK] Seq=1103 Ack=15907 Win=65535 Len=0	
207	5.348032324	10.0.2.15	192.168.206.130	OpenFlow	194	Type: OFPT_PACKET_IN	
208	5.348229245	192.168.206.130	10.0.2.15	TCP	60	6653 → 36710 [ACK] Seq=1087 Ack=16031 Win=65535 Len=0	
209	5.348316710	10.0.2.15	192.168.206.130	OpenFlow	194	Type: OFPT_PACKET_IN	
210	5.348931883	192.168.206.130	10.0.2.15	TCP	60	6653 → 36712 [ACK] Seq=1103 Ack=16047 Win=65535 Len=0	
211	5.499501799	192.168.206.130	10.0.2.15	OpenFlow	62	Type: OFPT_BARRIER_REQUEST	
212	5.499719429	10.0.2.15	192.168.206.130	OpenFlow	62	Type: OFPT_BARRIER_REPLY	
213	5.499851636	192.168.206.130	10.0.2.15	TCP	60	6653 → 36710 [ACK] Seq=1095 Ack=16039 Win=65535 Len=0	
214	6.487919389	192.168.206.130	10.0.2.15	OpenFlow	70	Type: OFPT_MULTIPART_REQUEST, OFPMP_TABLE	
215	6.488198138	10.0.2.15	192.168.206.130	OpenFlow	6166	Type: OFPT_MULTIPART_REPLY, OFPMP_TABLE	
216	6.488959289	192.168.206.130	10.0.2.15	TCP	60	6653 → 36710 [ACK] Seq=1111 Ack=18959 Win=65535 Len=0	
217	6.488971486	192.168.206.130	10.0.2.15	TCP	60	6653 → 36710 [ACK] Seq=1111 Ack=20419 Win=65535 Len=0	
218	6.488972395	192.168.206.130	10.0.2.15	TCP	60	6653 → 36710 [ACK] Seq=1111 Ack=21879 Win=65535 Len=0	
219	6.488973465	192.168.206.130	10.0.2.15	TCP	60	6653 → 36710 [ACK] Seq=1111 Ack=22151 Win=65535 Len=0	
220	6.494064124	192.168.206.130	10.0.2.15	OpenFlow	110	Type: OFPT_MULTIPART_REQUEST, OFPMP_FLOW	
221	6.495158608	10.0.2.15	192.168.206.130	OpenFlow	750	Type: OFPT_MULTIPART_REPLY, OFPMP_FLOW	
222	6.495494431	192.168.206.130	10.0.2.15	TCP	60	6653 → 36710 [ACK] Seq=1107 Ack=22847 Win=65535 Len=0	
223	6.517221354	192.168.206.130	10.0.2.15	OpenFlow	70	Type: OFPT_MULTIPART_REQUEST, OFPMP_GROUP_DESC	
224	6.517366539	10.0.2.15	192.168.206.130	OpenFlow	70	Type: OFPT_MULTIPART_REPLY, OFPMP_GROUP_DESC	
225	6.518582485	192.168.206.130	10.0.2.15	TCP	60	6653 → 36710 [ACK] Seq=1183 Ack=22863 Win=65535 Len=0	
226	6.519329947	192.168.206.130	10.0.2.15	OpenFlow	78	Type: OFPT_MULTIPART_REQUEST, OFPMP_GROUP	
227	6.519481666	10.0.2.15	192.168.206.130	OpenFlow	70	Type: OFPT_MULTIPART_REPLY, OFPMP_GROUP	
228	6.519651186	192.168.206.130	10.0.2.15	TCP	60	6653 → 36710 [ACK] Seq=1207 Ack=22879 Win=65535 Len=0	
229	6.520823288	192.168.206.130	10.0.2.15	OpenFlow	78	Type: OFPT_MULTIPART_REQUEST, OFPMP_PORT_STATS	
230	6.521062597	10.0.2.15	192.168.206.130	OpenFlow	518	Type: OFPT_MULTIPART_REPLY, OFPMP_PORT_STATS	
231	6.521186256	192.168.206.130	10.0.2.15	TCP	60	6653 → 36710 [ACK] Seq=1231 Ack=23343 Win=65535 Len=0	
232	6.523133240	192.168.206.130	10.0.2.15	OpenFlow	78	Type: OFPT_MULTIPART_REQUEST, OFPMP_QUEUE	
233	6.523284944	10.0.2.15	192.168.206.130	OpenFlow	70	Type: OFPT_MULTIPART_REPLY, OFPMP_QUEUE	
234	6.523401804	192.168.206.130	10.0.2.15	TCP	60	6653 → 36710 [ACK] Seq=1255 Ack=23359 Win=65535 Len=0	
235	6.988552654	192.168.206.130	10.0.2.15	OpenFlow	62	Type: OFPT_BARRIER_REQUEST	

Imagen 3. Captura Tráfico

- Describe el intercambio de paquetes que ocurre entre el controlador Floodlight y el resto de la red. ¿Puede observar está interacción dentro del controlador Floodlight?

Contraste con otras soluciones.

Parte importante del desarrollo de un Ingeniero profesional, es la capacidad de comparar las diferentes opciones que existen para dar solución a un problema específico. Así, existen una gran cantidad de controladores SDN en el mercado, pero en esta clase se analizarán 4: OpenDayLight, ONOS, Floodlight y SDN CTL (HP). De esta manera, deberán:

- ❓ Realizar una presentación, a través de la cual, poder discutir: la historia, las características principales, la arquitectura, las ventajas, las desventajas, casos de uso éxitos y los desafíos que busca resolver el controlador Floodlight. Cabe resaltar, que es importante realizar la presentación con capturas de pantalla o videos que sustenten las pruebas realizadas en el laboratorio.

Entregable Proyecto.

Tal como se mencionó en clase, la tercera entrega del proyecto será calificada con el desarrollo de estos laboratorios. De esta manera, **simule la red diseñada en la segunda entrega del proyecto del curso a través de Mininet e intégreala con el controlador Floodlight**. Durante la presentación exponga los procedimientos que llevaron a cabo para simular la red y las pruebas que realizaron para validar su funcionamiento. Debe mostrar el procedimiento para realizar la configuración de un flujo adicional, una vez se encuentre en operación el controlador Floodlight. Tener en cuenta los análisis de flujos de tráfico.

Referencias

Linux Foundation. (2014). OpenDayLight, 31(5), 1–58.

floodlight. (2017). *Project Floodlight*. Obtenido de <http://www.projectfloodlight.org/floodlight/>

Jarrin, A. (2014). *Desarrollo Guías de Laboratorio para la Implementación de redes SDN en el Laboratorio de Redes*. Cali.