

Guía Controlador ONOS.

Contenido

Laboratorio – Controlador ONOS	2
Objetivo Práctica Laboratorio	2
Requisitos Laboratorio	2
Actividades Laboratorio	2
Instalación Controlador ONOS	2
Acceso Web	3
Simulación con Mininet y ONOS	4
Contraste con otras soluciones.	6
Entregable Proyecto.....	6
Referencias	6

Laboratorio – Controlador ONOS

Objetivo Práctica Laboratorio

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

CONTRASTAR el controlador SDN ONOS 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

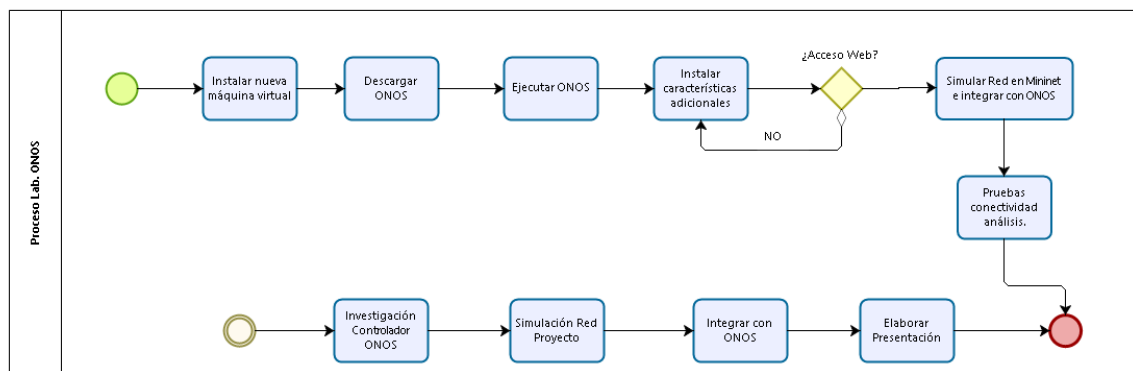


Diagrama 1. Proceso Laboratorio

Instalación Controlador ONOS

ONOS, es un controlador SDN, que admite tanto la configuración como el control en tiempo real de la red, lo que elimina la necesidad de ejecutar enrutamiento y conmutar los protocolos de control, dentro de cada equipo de la red. Al trasladar la inteligencia al controlador ONOS (que puede ser ejecutado en la nube), se habilita la innovación y los usuarios finales pueden crear fácilmente nuevas aplicaciones de red, sin la necesidad de alterar los sistemas actuales (Open Network Foundation, 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
```

Primero, debemos descargar el controlador ONOS de la siguiente manera:

```
wget -nd -c "http://downloads.onosproject.org/release/onos-1.5.1.tar.gz"
tar -xf onos-1.5.1.tar.gz
cd onos-1.5.1
```

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

```
sudo ./bin/onos-service
```

Ahora bien, ya que la arquitectura de ONOS se basa en los microservicios, debemos instalar una serie de características adicionales para lograr tener una operación óptima del controlador:

```
feature:install -v onos-app-fwd onos-host-provider onos-openflow onos-openflow-base
```

Acceso Web

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

```
http://Dir_IP_ONOS:8181/onos/ui
```

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

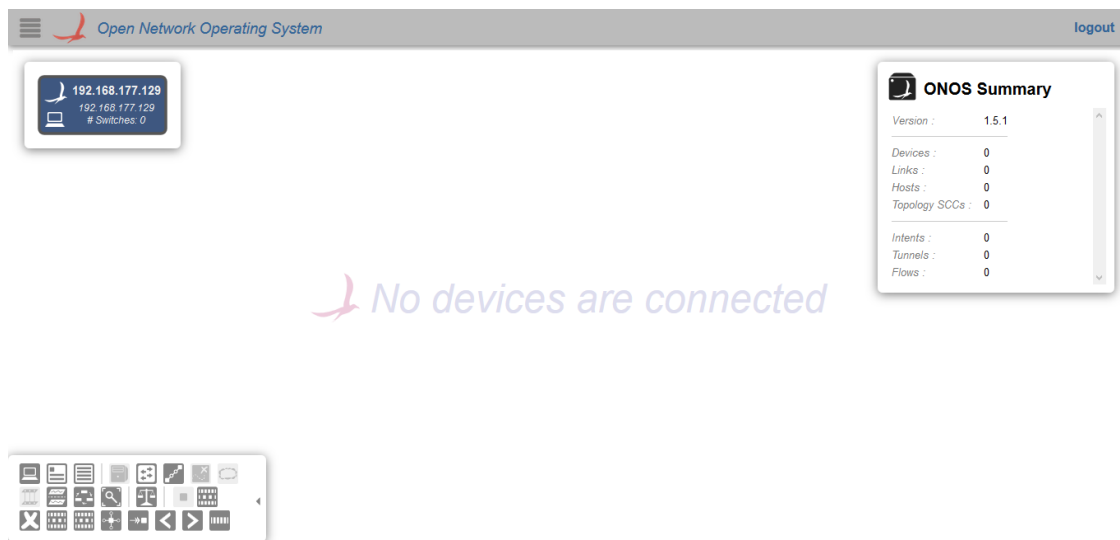


Imagen 1. Vista Web ONOS

Las credenciales para el acceso son:

- Usuario: karaf
- Contraseña: karaf

Simulación con Mininet y ONOS

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

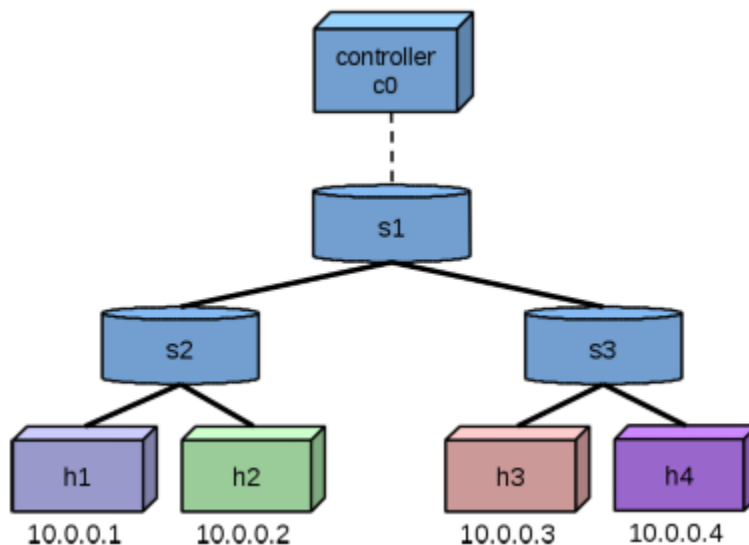





Diagrama 2 Topología de Red

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

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

 ¿Qué cambios se pueden presenciar en el controlador ONOS? 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 ONOS, 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	5.343996773	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 2. Captura Tráfico

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

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 para la siguiente clase, 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 ONOS. Cabe resaltar, que es importante realizar la presentación con capturas de pantalla o videos que sustenten lo mencionado durante la presentación.

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 ONOS**. 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 ONOS. Tener en cuenta los análisis de flujos de tráfico.

Referencias

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

fontes, r. (24 de sep de 2014). *github.com/ramonfontes*. Obtenido de <https://github.com/ramonfontes/vnd-sdn-version>

Open Network Foundation. (2017). *ONOS*. Obtenido de <https://www.opennetworking.org/platforms/onos/>