Protocolos de comunicaciones SDN (Software Defined Networking) en un laboratorio portable de redes de ordenadores

Eva M. Castro Barbero (eva.castro@urjc.es)
Pedro de las Heras Quirós (pedro.delasheras@urjc.es)

Tecnologías y Protocolos de Internet de Nueva Generación

Departamento de Teoría de la Señal y Comunicaciones y
Sistemas Telemáticos y Computación

Noviembre de 2017

En esta proyecto práctico vamos a aplicar los conocimientos de SDN estudiados en la práctica anterior dentro del entorno de simulación/emulación mininet a un entorno con hardware físico. Estudiaremos cómo un controlador SDN, en nuestro caso `faucet`[1], envía órdenes a un dispositivo físico, un *switch* SDN que implementa OpenFlow. Vamos a utilizar una raspberry pi para que ejecute el controlador `faucet` y el *switch* hardware Zodiac FX[2]. El programa controlador `faucet`, a partir de un fichero de configuración, enviará los mensajes OpenFlow necesarios para instruir al switch hardware ZodiacFX.

El switch Zodiac FX es un switch pequeño OpenFlow para desarrollar y probar aplicaciones SDN sobre hardware real de bajo coste. Este switch se encuentra en el mercado desde 2015 y ha permitido realizar pruebas SDN con hardware real fuera de un datacenter.

1. Conexión física del escenario de red

Vamos a utilizar el switch Zodiac FX para comunicar la aplicación `ap1` ejecutándose en la máquina `raspberry2` con la aplicación `ap2` ejecutándose en un ordenador. El switch Zodiac FX necesita estar controlado por programa controlador `faucet` que ejecutaremos en la máquina `raspberry`. El plano de datos por tanto se establecerá entre los puertos 1 a 3 del switch y el plano de control se encontrará en la conexión con el puerto 4. Se desea montar el escenario de red de la figura 1.

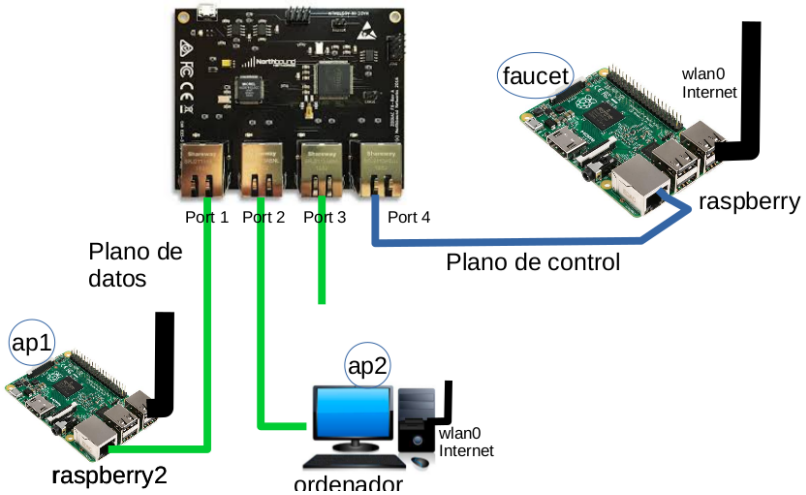


Figura 1: Escenario de red.

2. Instalación de software

Para poder utilizar el escenario de la figura 1 es necesario realizar la instalación del sistema operativo `raspbian`[3] de Linux basada en Debian Jessie para el procesador de la raspberry pi (ARM, Advanced RISC Machine) en la tarjeta microSD que será insertada en cada raspberry.

Puedes usar el programa `dd`[4] para realizar la copia de `raspbian`. Monta el sistema de ficheros que acabas de grabar y observa que en la carpeta donde está montado el sistema de ficheros raíz, se encuentran las carpetas clásicas que se instalan en un sistema operativo Linux: `/etc, /bin, /var, /usr...`

3. Configuración de la raspberry pi

El acceso a la configuración de las máquinas raspberry pi desde otro ordenador se puede hacer de varias formas. En esta práctica te recomendamos que uses el cable USB-TTL serial para establecer una configuración inicial de red.

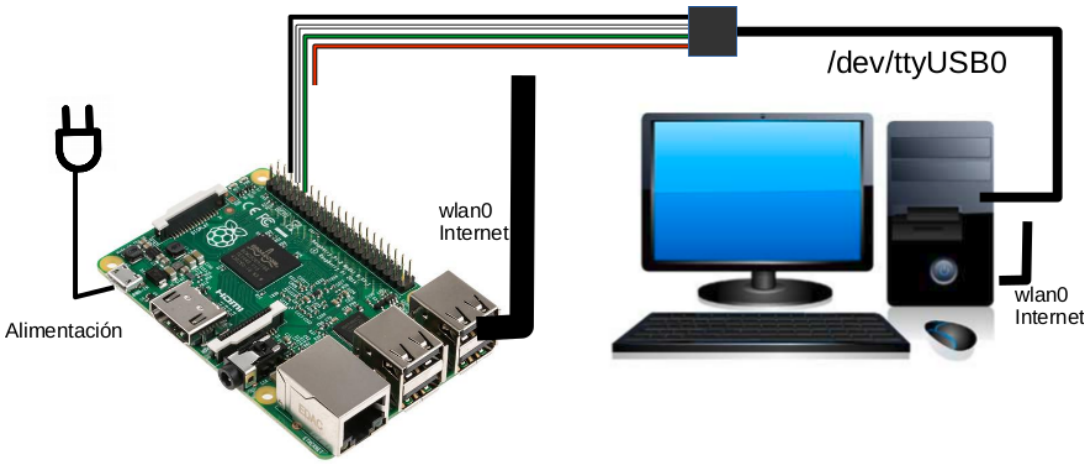


Figura 2: Consola de la Raspberry Pi a través del puerto USB.

3.1. Configuración de interfaz de red Ethernet

Conectamos los hilos del cable a los pines de la raspberry según las especificaciones del cable [5], véase la figura 2. Este cable permite convertir el puerto USB en un puerto serie TTL (Transistor-Transistor Logic) para tener un emulador de terminal.

Siguiendo la configuración de ZodiacFX [2], es necesario que el controlador esté en la dirección IP 10.0.1.8 en la red 10.0.1.0/24, teniendo como gateway la dirección IP 10.0.1.99 que es la que tiene asignada por defecto el switch Zodiac FX. Realiza dicha configuración en la raspberry pi que va a ejecutar el controlador `faucet`.

3.2. Configuración de interfaz de red inalámbrica

Para que la rapsberrry pi se conecte a una red inalámbrica (por ejemplo eduroam o la red inalámbrica de tu casa) se puede hacer a través de `wpa_supplicant`. En particular, la red académica `eduroam` estará asociada a tu cuenta de dominio único y tu contraseña y serán necesarios los certificados de Terena y Digicert [7].

3.3. Instalación de herramientas

Otras herramientas muy útiles para el diagnóstico de problemas son un servidor `ssh` para la comunicación remota con las raspberrys y un programa para análisis de tráfico como `tcpdump`.

4. Plano de control: comunicación entre raspberry pi y ZodiacFX

Observa la figura 3 y realiza las conexiones que permitan establecer el plano de control a través del cuál se comunicarán el controlador de la raspberry y el switch, véase figura 3.

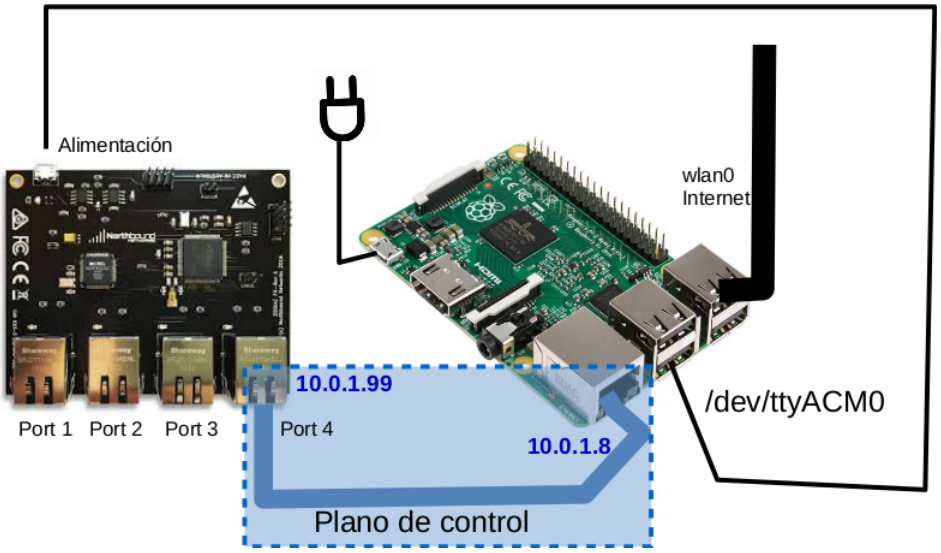


Figura 3: Conexión switch Zodiac FX con raspberry pi.

Utiliza un programa de consola (`screen` o `minicom`) desde la raspberry pi para poder establecer una comunicación remota de consola, lo que te permitirá ejecutar los comandos CLI (consulta el manual de usuario del switch Zodiac FX[6]):

- Accede a la configuración por defecto del switch y observa lso siguientes valores: dirección MAC, dirección IP, máscara, gateway, dirección IP y puerto donde el switch espera conectarse para comunicarse con el controlador.
- Explica el valor de la dirección IP de la raspberry pi y su relación con la dirección IP del controlador.
- Observa la configuración por defecto de las VLAN en el switch y explica su contenido.
- Comprueba el estado actual del switch y justifica el valor obtenido.
- Muestra la información de OpenFlow y explica su contenido.

5. Instalación del controlador faucet-ryu en la raspberry pi

Faucet es un controlador OpenFlow que implementa funciones de reenvío de tramas de nivel de enlace, ACLs, encaminamiento IPv4/IPv6 tanto estático como dinámico vía BGP. Faucet está implementado usando el framework `ryu` para la creación de aplicaciones SDN. Instala el controlador `faucet-1_5_3`[8] en la raspberry pi.

El identificador del Datapath (64 bits) en el switch Zodiac FX se calcula a partir de su dirección MAC (48 bits). Si su dirección MAC es 70:B3:D5:6C:D7:4C su DPID 0x70b3d56cd74c (todos los dígitos juntos borrando ":" y anteponiendo 0x). Calcula el identificador Datapath de tu switch Zodiac FX.

La configuración de `faucet` se realiza a través de archivos en formato YAML (YAML Ain't Markup Language), `faucet.yaml`[9].

Estudia el contenido del fichero `faucet.yaml` para identificar las 2 partes:

- Definición de VLANS.
- Definición de Datapaths.

Crea un fichero `faucet.yaml` con un comportamiento de switch entre los puertos 1 a 3, todos ellos dentro de la VLAN 100. Comprueba su correcto funcionamiento (puede ser útil observar los ficheros de `log`).

Si el arranque de `faucet` no ha ido bien comprueba que el DPID es el de tu switch, revisando la MAC y comprueba el contenido del fichero `faucet.yaml` (es mejor no usar tabuladores y usar una correcta indentación con espacios).

6. Análisis del funcionamiento de faucet

En esta sección se analizará cómo `faucet` instala tablas con flujos en el switch Zodiac FX a través de mensajes OpenFlow para dotarle de dicho comportamiento. En la práctica previa realizaste esta configuración a través de comandos manuales, ahora es el controlador el que automáticamente configurará el switch.

6.1. Análisis de los mensajes OpenFlow en el arranque

Una vez arrancado `faucet` vamos a realizar las siguientes pruebas:

1. Observa ahora cómo ha cambiado el estado de Zodiac FX en el modo `openflow`. Indica qué información te proporciona el switch. ¿Qué crees que ha ocurrido?

2. Interrumpe la ejecución de `faucet` y arranca una captura de tráfico en la raspberry pi, la que permite la comunicación OpenFLow entre `faucet` y el switch, guarda el contenido de la captura en un fichero y lanza `faucet` otra vez. Comprueba que nuevamente se han configurado los mismos flujos que antes e interrumpe la captura de tráfico.

   A partir de la captura de tráfico estudia los mensajes OpenFLow intercambiados por el controlador y el switch:

   a) Indica quién inicia la conexión TCP, `faucet` o el switch.

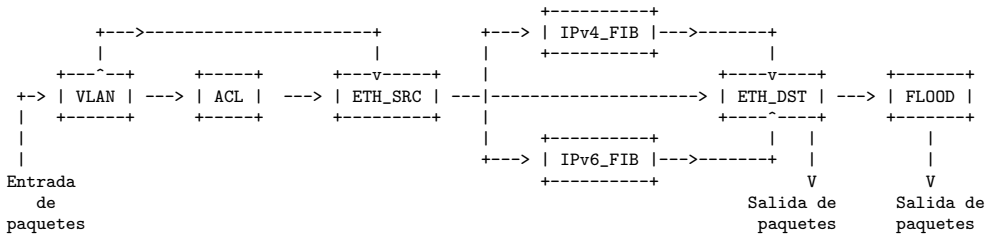
   b) Observa los mensajes `OFPT_HELLO`, se utilizan para darse a conocer el controlador y el switch. Apunta el valor del campo `Transaction ID` que envía el controlador al switch. Explica el valor de `Transaction ID` en los mensajes:
   `OFPT_FEATURES_REQUEST, OFPT_FEATURES_REPLY, OFPT_MULTIPART_REQUEST, OFPT_MULTIPART_REPLY`.

   c) Explica el mensaje `OFPT_FEATURES_REQUEST`. Observa la respuesta e indica: el datapath_id que el switch le envía al controlador y el número de tablas que puede manejar el switch.

   d) Explica el mensaje `OFPT_MULTIPART_REQUEST`. Observa la respuesta e indica cuántos puertos describe el switch, para cada uno de ellos indica: el número de puerto, el nombre, su estado y su dirección hardware.

   e) Observa los mensajes `OFPT_ECHO_REQUEST` y `OFPT_ECHO_REPLY`, pueden ser enviados desde cualquiera de los dos extremos. Observa en tu captura quién manda la solicitud y cuál es el período aproximado entre solicitudes.

   f) `faucet` define las siguientes tablas que configura en el switch a través de mensajes OpenFLow. Estas tablas están encadenadas según el esquema[10]:



   Cuando un paquete se recibe en el switch, se van consultando en orden las tablas anteriores y dentro de una tabla se consultan los flujos que tiene instalados. Si el paquete cumple la condición definida en el flujo, entoces se ejecuta la/s acción/es definidas en dicho flujo. Cada tabla tiene definidos los flujos en función de un objetivo concreto.

   Observa que habrá un total de 8 tablas, indica si concuerda con la configuración que habías observado en el apartado 1 de esta sección.

   g) La configuración de las tablas que realiza `faucet` en el switch se envía a través de los mensajes `OFPT_FLOW_MOD`.
   Los flujos instalados en una tabla se caracterizan porque tienen una prioridad para ser consultados, cuando se recibe un paquete se consulta la primera tabla, el flujo más prioritario y si el paquete cumple las condiciones (véase cuadro 1) de ese (`Match`) se le aplica una determinada acción o acciones (`Instruction`, véase cuadro 2). Si el paquete no cumple las condiciones se pasa a la consulta del siguiente flujo por orden de prioridad en esa tabla. Generalmente existe un último flujo (con la menor prioridad) para saber qué hacer con ese paquete en caso de que no cumpla ninguna de las condiciones de los flujos anteriores en esa tabla.

Condición	Significado
`OFPXMT_OFB_ETH_DST (3)`	Dirección Ethernet destino (al valor puede aplicarse a una máscara para contemplar un rango de direcciones)
`OFPXMT_OFB_ETH_TYPE (5)`	Campo protocolo de Ethernet
`OFPXMT_OFB_IN_PORT (0)`	Puerto de entrada
`OFPXMT_OFB_VLAN_ID (6)`	Identificador VLAN (si está presente y su valor)

Cuadro 1: Condiciones de los flujos

Acción/instrucción	Significado
`OFPAT_PUSH_VLAN(17)`	Añadir etiqueta VLAN
`OFPAT_SET_FIELD(25)`	Almacenar en la etiqueta VLAN_ID el valor dado por `Value`
`OFPAT_POP_VLAN(18)`	Eliminar la etiqueta VLAN
`OFPAT_OUTPUT(0)`	Reenviar por el número de puerto indicado en `Port` (puede ser al puerto del controlador)
`OFPIT_GOTO_TABLE(1)`	Reenviar a la tabla número `Table ID`

Cuadro 2: Acciones de los flujos

Es recomendable usar filtros en wireshark para ver los mensajes de tipo `OFPT_FLOW_MOD`. Por ejemplo para visualizar los mensajes de configuración para la tabla 0, escribiremos la especificación dentro de la caja de filtros de wireshark que se muestra en la figura 4.

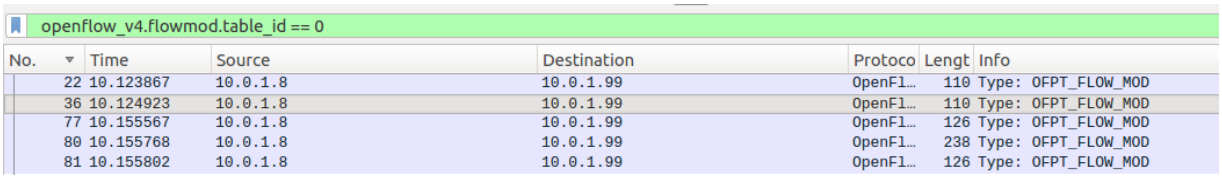


Figura 4: Filtro para visualizar los mensajes OpenFlow que configuran flujos en la tabla 0.

Analiza exhaustivamente para cada una de las 8 tablas, la configuración que se manda desde el controlador. Para ello, crea un resumen del contenido de dichas tablas indicando, la prioridad de cada flujo, la condición para que se aplique dicho flujo y la acción/es a ejecutar si se cumple la condición/es.

h) Observa dentro del modo `openflow` los flujos que se han definido como consecuencia de los mensajes OpenFLow que le ha enviado el controlador al switch. Trata de identificar en esta información uno de los flujos concretos, por ejemplo el flujo en la tabla 7 que tienen definidas las siguientes condiciones: todos los mensajes cuyo puerto de entrada es el número 1, tienen vlan_id=100 y van dirigidos al broadcast Ethernet. Copia la información de dicho flujo explicando su contenido.

i) A la vista de los resultados analizados de las tablas instaladas en el switch, ¿qué crees que ocurrirá cuando se reciba un paquete en el puerto 1 del switch con una determinada dirección Ethernet origen (de una máquina cualquiera) y que vaya dirigido al broadcast Ethernet? Explica qué cadena de flujos se aplicarán sobre ese paquete.

j) A la vista de los resultados analizados de las tablas instaladas en el switch, ¿qué crees que ocurrirá cuando se reciba un paquete en el puerto 1 del switch con una determinada dirección Ethernet origen (de una máquina cualquiera) y que vaya dirigido a una dirección Ethernet destino (de otra máquina cualquiera)? Explica qué cadena de flujos se aplicarán sobre ese paquete.

6.2. Análisis de los mensajes OpenFLow al conectar una máquina al switch

Configura la segunda raspberry pi y asígnale el nombre rapsberry2 para diferenciarla de la que ya tienes instalada. Configura una dirección IP en el rango `X.0.0.0/24` (siendo X el valor que se te asignó en la práctica anterior). Es conveniente que la prepares de una forma equivalente a la raspberry anterior para poder usar con ella herramientas de diagnóstico.

Realiza una captura en raspberry2 para visualizar el tráfico en el plano de datos y guarda su contenido en un fichero `rasp2-1host.cap`). Realiza una captura en la raspberry pi donde se está ejecutando el controlador (fichero `controller-1host.cap`) para visualizar el tráfico del controlador.

Conecta la `raspberry2` que acabas de configurar a uno de los puertos libres del switch, véase la figura 5. Espera 1 minuto e interrumpe las capturas.

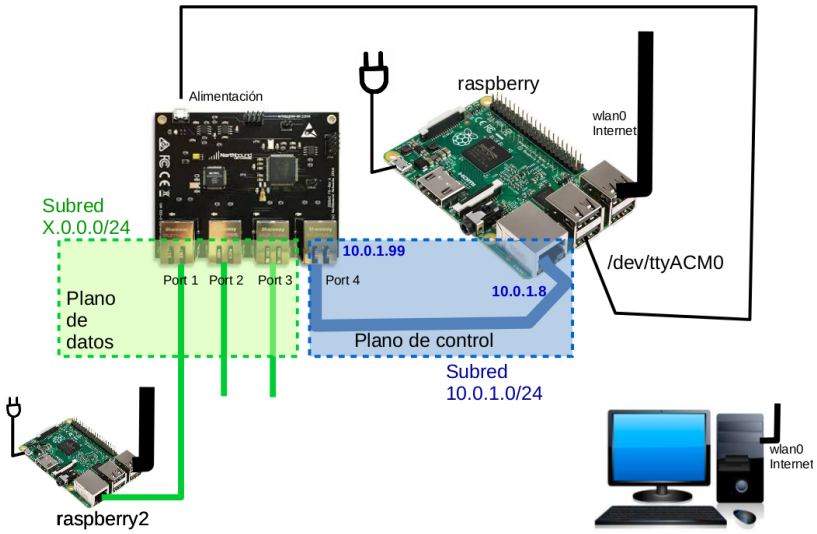


Figura 5: Una máquina conectada al switch Zodiac FX, en el plano de datos.

Interrumpe ambas capturas para analizarlas con wireshark:

1. En el fichero `controller-1host.cap` localiza los paquetes `OFPT_PACKET_IN`. Consulta en estos paquetes el campo `Data` que contiene el paquete original que ha recibido el switch y que ha provocado el envío al controlador. Explica qué son estos paquetes y localízalos en la captura `rasp2-1host.cap`.

2. Busca en la captura `controller-1host.cap` aquellos paquetes que instalan flujos en el switch y en los que interviene la consulta de la dirección Ethernet de la `raspberry2` que acabas de conectar. Explica qué hacen esos flujos y qué provoca que se envíe esa configuración desde el controlador al switch.

6.3. Análisis de los mensajes OpenFLow al comunicar 2 máquinas a través del switch

Configura en tu ordenador la interfaz Ethernet con una dirección IP estática en el rango `X.0.0.0/24` que no hayas utilizado previamente. Conecta tu ordenador a otro puerto del switch que esté libre, veáse la figura 6.

Inicia las capturas de tráfico que consideres necesarias para analizar el comportamiento del switch y las máquinas. Ejecuta un `ping -c 3` desde tu ordenador a la raspberry2.

Interrumpe las capturas y analiza detalladamente el contenido:

- Analiza los paquetes `OFPT_PACKET_IN` provocados por la ejecución del ping.
- Busca en la captura `controller-2host.cap` aquellos paquetes que instalan flujos en el switch y en los que interviene la consulta de las direcciones Ethernet de la raspberry2 y de tu máquina.

7. Configuración de ACLs en faucet

Con el fichero de configuración de `faucet` se pueden configurar escenarios complejos que permitan definir listas de control de acceso (ACL, access control list) para el tráfico que atraviesa el switch.

Estudia la siguiente configuración, donde se configuran reglas en una lista de control de acceso en el switch Zodiac Fx que será aplicada a los puertos 1, 2 y 3 del switch. La lista de control de acceso está definida en el escenario de la figura para:

- Permitir que cualquier máquina pueda enviar mensajes ARP y mensajes ICMP.

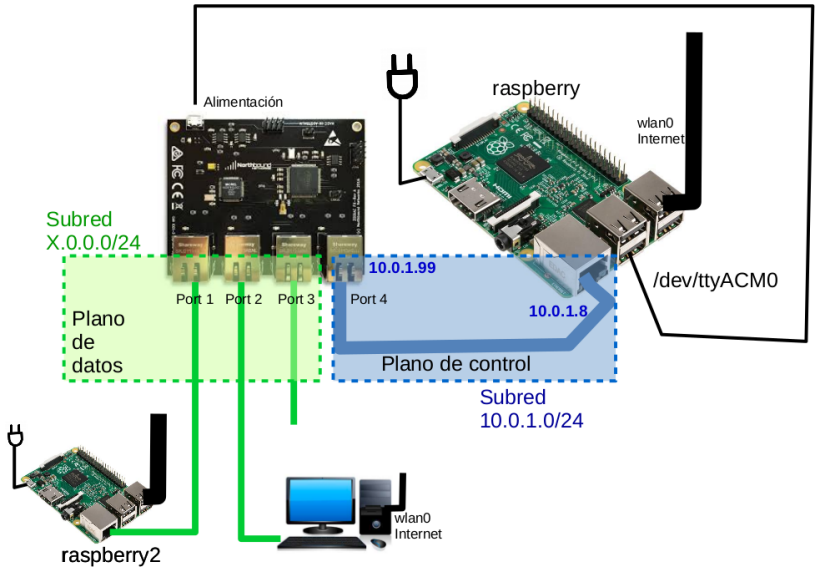
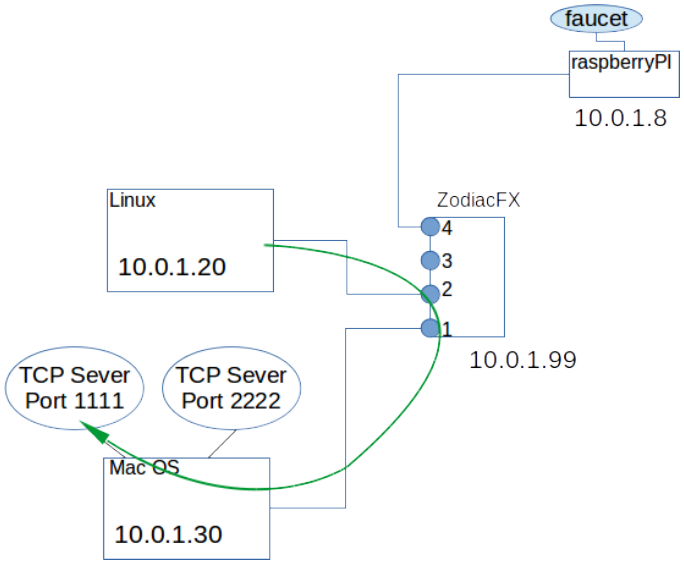


Figura 6: Dos máquinas conectadas al switch Zodiac FX, en el plano de datos.

- Únicamente desde 10.0.1.20 se acceda al servidor 10.0.1.30:1111 y a ningún otro servidor que se pueda estar ejecutando en 10.0.1.30.
- Ninguna otra máquina podrá tener acceso a 10.0.1.30.



El fichero de configuración `faucet.yaml` que establece la configuración descrita previamente es[1]:

```
vlans:
    100:
        name: "test-ACL-faucet-1"
dps:
    zodicac-fx-1:
        dp_id: 0x70B3D56CD74C
        hardware: "ZodiacFX"
        interfaces:
            1:
                native_vlan: 100
                acl_in: 1
            2:
```

[1]Ten en cuenta que la sintaxis de YAML es sensible con los tabuladores y no admite caracteres con tildes en los comentarios.

```
                native_vlan: 100
                acl_in: 1
            3:
                native_vlan: 100
                acl_in: 1

acls:
  1:

    - rule:
        # Permitir trafico ARP
        eth_type: 0x0806 # ARP
        actions:
             allow: 1

    - rule:
        # Permitir trafico ICMPv4
        eth_type: 0x0800 # IPv4
        ip_proto: 0x01 # ICMPv4
        actions:
             allow: 1
    - rule:
        # Permitir trafico  TCP a 10.0.1.30:1111, solo desde 10.0.1.20
        eth_type: 0x0800 # IPv4
        ipv4_dst: 10.0.1.30
        ipv4_src: 10.0.1.20
        ip_proto: 0x06 # TCP
        tcp_dst: 1111
        actions:
             allow: 1

    - rule:
        # Permitir respuesta al trafico  TCP a 10.0.1.30:1111 que fue enviado solo desde 10.0.1.20
        eth_type: 0x0800 # IPv4
        ipv4_src: 10.0.1.30
        ipv4_dst: 10.0.1.20
        ip_proto: 0x06 # TCP
        tcp_src: 1111
        actions:
             allow: 1

    - rule:
        # No permitr cualquier trafico IPv4 a 10.0.1.30
        eth_type: 0x0800 # IPv4
        ipv4_dst: 10.0.1.30
        actions:
             allow: 0

    - rule:
        # Permitir cualquier otro trafico
        eth_type: 0x0800 # IPv4
        ipv4_src: 10.0.1.0/24
        actions:
              allow: 1
```

A partir de la configuración anterior construye tu propia ACL usando `faucet` para configurar el switch Zodiac FX de la siguiente forma:

- Permitir que cualquier máquina pueda enviar mensajes ARP y mensajes ICMP.
- Únicamente desde tu máquina se pueda acceder a un servidor TCP que se está ejecutando en la rapsberry2 en

el puerto 8080, y a un servidor UDP que se está ejecutando también en la raspberry2 en el puerto 5000.

- Ninguna otra máquina podrá tener acceso a los servidores TCP/UDP de la raspberrry2 ni a los que pudiera haber ejecutándose en tu máquina.

Una vez realizada la configuración anterior, responde razonadamente a estas preguntas.

1. Incluye el fichero de configuración de faucet.yaml, explicando las partes más relevantes.
2. Realiza una captura `controller-acl.cap` en la raspberry pi que ejecuta el controlador para capturar los mensajes que se envían entre el controlador y el switch cuando arranques el controlador. Examina los mensajes OpenFLow para localizar aquéllos mensajes que se corresponden con la configuración de la ACL.
3. Observa en el modo `openflow` del switch y observa qué flujos se han creado como consecuencia de las reglas que has configurado.
4. Prueba la configuración lanzando los clientes y servidores que consideres necesarios. Puedes usar la herramienta `nc` en la `raspberry2` para lanzar los servidores. Para lanzar clientes: si tienes windows puedes explorar el uso de `ncat` que viene empaquetado con la herramienta `nmap (https://nmap.org/ncat/)`, si tienes Mac OS podrás usar `netcat` o en Linux `nc`. Incluye en la memoria las pruebas que has realizado.
5. ¿Qué le ocurre a un paquete originado en tu máquina y dirigido a la raspberry2 al puerto 8080 TCP? Explica qué flujos atraviesa en el switch.
6. ¿Qué le ocurre a un paquete originado en tu máquina y dirigido a la raspberry2 al puerto 5000 UDP? Explica qué flujos atraviesa en el switch.
7. ¿Qué le ocurre a un paquete originado en tu máquina y dirigido a la raspberry2 al puerto 9000 TCP? Explica qué flujos atraviesa en el switch.

Entrega de la práctica

Para entregar esta práctica tendrás que subir al aula virtual las capturas de tráfico que se solicitan y la memoria en pdf. Además deberás entregar la memoria en papel en el despacho 112 del edificio Aulario 3.

Referencias

[1] Josh Bailey, Stephen Stuart, "Faucet: Deploying SDN in Enterprise", Magazine Queue - Network Congestion, ACM, 2016.

[2] Nazir, Fahad and Humayun, Qazi and Ahmad, R.Badlishah and Elias, Shamsul Jamel. "Software-Defined Network Testbed Using ZodiacFX a Hardware Switch for OpenFlow", ICST Transactions on Scalable Information Systems, septiembre 2017.

[3] Distribución raspbian. Disponible en: http://www.raspberrypi.org.

[4] dd user command. Disponible en: http://man7.org/linux/man-pages/man1/dd.1.html

[5] Using a console cable. Disponible en: https://learn.adafruit.com/adafruits-raspberry-pi-lesson-5-using-a-console-cable/overview

[6] Zodiac FX User Guide. Disponible en: https://zodiac-fx-germany.de/ZodiacFX_UserGuide_0216.pdf

[7] Certificados Digicert y Terena. Disponible en https://pki.cesnet.cz/en/ch-tcs-ev-ssl-ca-3-crt-crl.html

[8] Código de faucet. Disponible en https://github.com/faucetsdn/faucet/archive/v1_5_3.tar.gz

[9] Documentación de faucet. Disponible en https://media.readthedocs.org/pdf/faucet/1.6.15/faucet.pdf

[10] Dissecting the faucet 1.1 pipeline. Disponible en https://inside-openflow.com/2016/09/16/dissecting-faucet-pipeline.