

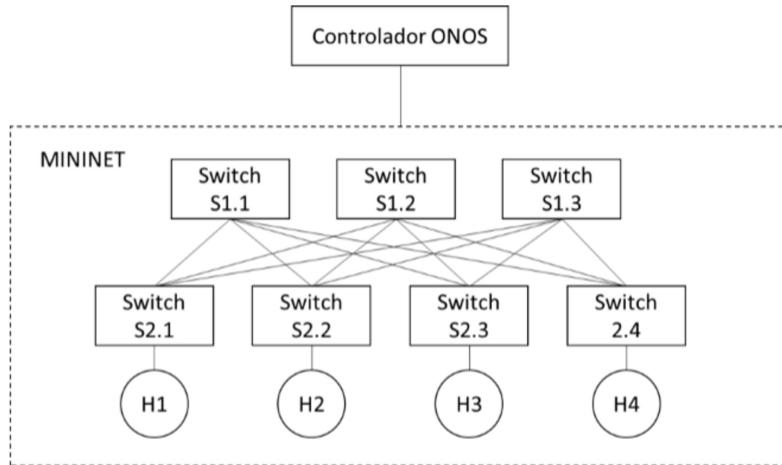
# Ejercicios Práctica 3 SDN Openflow

lunes, 20 de mayo de 2024 19:05

**Junio 2023**

**EJERCICIO 6. Puntuación: 1,5 puntos. Tiempo estimado: 15 minutos**

En el siguiente esquema de red se muestra una topología de switches y hosts ejecutados dentro del entorno Mininet y conectados a un controlador ONOS.



Existen dos niveles de switches: el nivel 1 (que incluye a los switches con nombre S1.X) y tiene funcionalidad similar a los switches Spine de la práctica 3, y el nivel 2 (switches con nombre S2.X) que corresponden a los switches de tipo Leaf en esa misma práctica. Los switches no tienen ningún tipo de inteligencia (entorno SDN puro en las mismas condiciones que en la práctica de SDN de la asignatura) y son compatibles con el protocolo OpenFlow. El controlador también es compatible con el protocolo OpenFlow.

El entorno de despliegue es el mismo que en la práctica 3 de la asignatura. Se han configurado las direcciones IP, máscaras y direcciones MAC según la siguiente tabla:

Equipo	Dirección IP / máscara	Dirección MAC (último octeto)
Controlador	10.10.0.1/30	-
Mininet	10.10.0.2/30	-
H1	10.10.1.1/24	0A
H2	10.10.1.2/24	0B
H3	10.10.1.3/24	0C
H4	10.10.1.4/24	0D

Tras el arranque de Mininet, se ha visto que se han asignado los siguientes puertos TCP a cada uno de los switches (interfaz Mininet-Controlador):

Switch	Puerto TCP
S1.1	10001
S1.2	10002
S1.3	10003
S2.1	20001
S2.2	20002
S2.3	20003
S2.4	20004

Todos los switches tienen cuatro puertos de entrada/salida. Cada puerto se numera del 1 al 4 y está conectado a un equipo concreto que se describe en la siguiente tabla:

Equipo	Puerto	Conectado al equipo
S1.1	$1 \leq X \leq 4$	S2.X
S1.2	$1 \leq X \leq 4$	S2.X
S1.3	$1 \leq X \leq 4$	S2.X
S2.1	$1 \leq X \leq 3$	S1.X
S2.1	4	H1
S2.2	$1 \leq X \leq 3$	S1.X
S2.2	4	H2
S2.3	$1 \leq X \leq 3$	S1.X
S2.3	4	H3
S2.4	$1 \leq X \leq 3$	S1.X
S2.4	4	H4

De la tabla anterior se puede deducir que, por ejemplo, el puerto 2 ( $X=2$ ) del switch S1.1 estará conectado al equipo S2.2 (de nuevo  $X=2$ ). Otro ejemplo es que el puerto 1 ( $X=1$ ) de S2.3 estará conectado al equipo S1.1. Finalmente, el puerto número 4 de todos los equipos de segundo nivel (S2.1, S2.2, S2.3 y S2.4) están conectados a sus respectivos hosts.

Al igual que en la práctica, se pueden monitorizar todas las interfaces, tanto las involucradas en comunicaciones OpenFlow como en las internas de Mininet. Además, están disponibles todas las aplicaciones del controlador ONOS utilizadas en la práctica, con el mismo comportamiento, aunque adaptadas al cambio de topología. Con la información suministrada, indique si las aserciones realizadas en cada uno de los escenarios son verdaderas o falsas (+0,1 por respuesta correcta y -0,1 por respuesta incorrecta).

**Escenario 1:** Asumiendo que el controlador está previamente arrancado y se despliega satisfactoriamente la red Mininet (se ejecuta el script de creación de dispositivos, enlaces y asignación de direcciones), se captura el intercambio de paquetes en todas las interfaces durante el tiempo suficiente para que todos los equipos hayan completado su inicialización.

- V Se capturan un total de siete mensajes del tipo OFPT\_FEATURES\_REPLY.
- V Se captura un mensaje OFPT\_HELLO con puerto TCP origen 20001.
- F Se captura el doble de mensajes OFPT\_GET\_CONFIG\_REQUEST que OFPT\_FEATURES\_REQUEST.
- F Se puede ver cómo el controlador asigna un "datapath\_id" a cada switch mediante un mensaje OFPT\_FEATURES\_REQUEST.
- F Se capturan un total de siete mensajes del tipo OFPT\_HELLO.

 DEPARTAMENTO DE INGENIERÍA TELEMÁTICA Y ELECTRÓNICA ETSIS TELECOMUNICACIÓN UPM	<b>REDES Y SERVICIOS AVANZADOS</b> Examen de evaluación global EG-EC2. 2 de junio de 2023	
APELLOS: <b>SOLUCIÓN</b>		
NOMBRE:		DNI:

**Escenario 2:** Una vez desplegada la red Mininet y habiéndose realizado el proceso de inicialización de todos los equipos de forma satisfactoria, se realiza un ping entre H1 y H4.

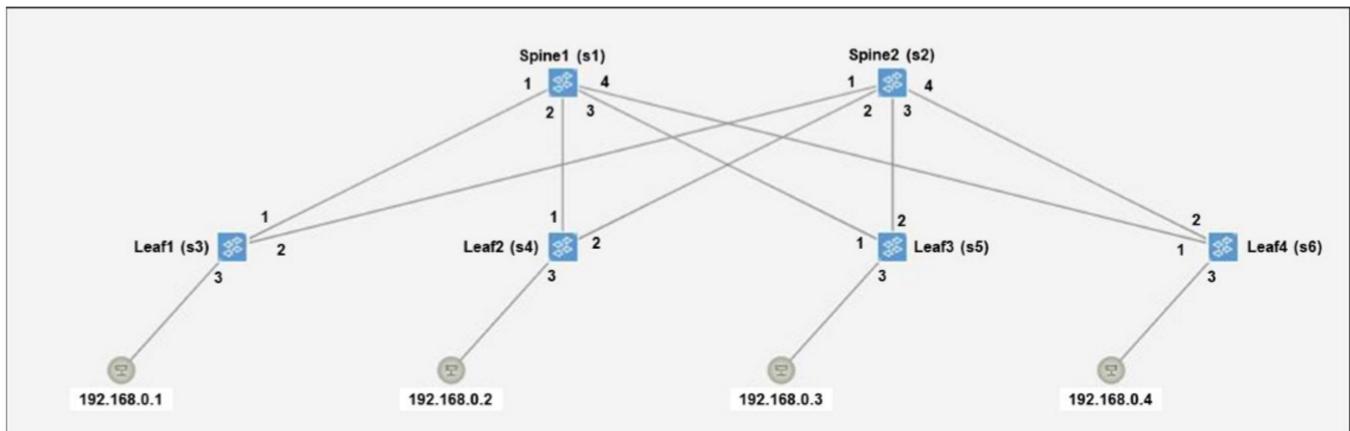
- V** Se captura al menos un paquete “arp request” de forma independiente a que se haya activado la aplicación org.onosproject.proxyarp.
- V** Se captura al menos un paquete “arp request” de forma independiente a que se haya activado la aplicación org.onosproject.fwd.
- F** Se captura un paquete OFPT\_PACKET\_OUT aunque no se haya activado la aplicación org.onosproject.proxyarp.
- F** Se captura un paquete OFPT\_PACKET\_OUT aunque no se haya activado la aplicación org.onosproject.fwd.
- V** Se capturarán tres paquetes OFPT\_PACKET\_OUT con puerto TCP origen 6653 siempre que se haya activado la aplicación org.onosproject.proxyarp.

**Escenario 3:** Se despliega todo el entorno de forma satisfactoria y se activan en el controlador las aplicaciones org.onosproject.proxyarp y org.onosproject.fwd. A continuación, se ejecuta el siguiente mandato: “h1 ping -c1 h4”.

- F** Los tres switches de la capa más alta (S1.1, S1.2 y S1.3) recibirán un OFPT\_PACKET\_OUT con un “ICMP echo request” encapsulado.
- V** El switch S2.1 recibirá al menos un mensaje OFPT\_FLOW\_MOD donde se añade una entrada de flujo en el que uno de los valores del campo Match es una dirección Ethernet de destino con el valor “0D”.
- F** Tras cada mensaje OFPT\_FLOW\_MOD recibido por un switch aparece otro mensaje OFPT\_BARRIER\_REQUEST enviado desde el controlador.
- V** Dado que la aplicación org.onosproject.fwd está activada, se capturarán tres mensajes OFPT\_PACKET\_IN con puerto TCP de origen 20001.
- V** El switch S2.4 recibirá un mensaje OFPT\_PACKET\_OUT indicando que envíe un paquete ICMP por el puerto 4.

### EJERCICIO 7. Puntuación: 1 punto. Tiempo estimado: 10 minutos

En la figura siguiente se muestra la topología de la red "Spine&Leaf" que se utilizará para la resolución de este ejercicio sobre la práctica 3 "Configuración de una red SDN y análisis de tráfico OpenFlow".



En las figuras siguientes se muestra la información proporcionada por el controlador ONOS sobre los hosts y los flujos instalados en uno de los dispositivos de la red ("Leaf2 (s4)").

Hosts (4 total)						
FRIENDLY NAME	HOST ID	MAC ADDRESS	VLAN ID	CONFIGURED	IP ADDRESSES	LOCATION
192.168.0.4	00:00:00:00:00:D/None	00:00:00:00:00:0D	None	false	192.168.0.4	of:0000000000000006/3
192.168.0.3	00:00:00:00:00:C/None	00:00:00:00:00:0C	None	false	192.168.0.3	of:0000000000000005/3
192.168.0.2	00:00:00:00:00:B/None	00:00:00:00:00:0B	None	false	192.168.0.2	of:0000000000000004/3
192.168.0.1	00:00:00:00:00:A/None	00:00:00:00:00:0A	None	false	192.168.0.1	of:0000000000000003/3

Flows for Device of:0000000000000004 (5 Total)							
STATE	PACKETS	DURATION	FLOW PRIORITY	TABLE NAME	SELECTOR	TREATMENT	APP NAME
Added	2	1,154	55	0	IN_PORT:3, ETH_DST:00:00:00:00:00:D, ETH_SRC:00:00:00:00:00:0B	imm[OUTPUT:2], cleared:false	*net.intent
Added	2	1,154	55	0	IN_PORT:2, ETH_DST:00:00:00:00:00:0B, ETH_SRC:00:00:00:00:00:D	imm[OUTPUT:3], cleared:false	*net.intent
Added	8	2,500	40000	0	ETH_TYPE:arp	imm[OUTPUT:CONTROLLER], cleared:true	*core
Added	1,612	2,500	40000	0	ETH_TYPE:lldp	imm[OUTPUT:CONTROLLER], cleared:true	*core
Added	1,612	2,500	40000	0	ETH_TYPE:bddp	imm[OUTPUT:CONTROLLER], cleared:true	*core

Teniendo en cuenta la información anterior, se pide:

- a) Indique razonadamente si se encuentra activada la aplicación "Reactive Forwarding" en el controlador de ONOS. (0,1 puntos)

No está activada, ya que si lo estuviera aparecería en la tabla de flujos una entrada para el tratamiento del tráfico "ETH\_TYPE:ipv4".

 DEPARTAMENTO DE INGENIERÍA TELEMÁTICA Y ELECTRÓNICA ETSIS TELECOMUNICACIÓN UPM	<b>REDES Y SERVICIOS AVANZADOS</b> Examen de evaluación global EG-EC2. 2 de junio de 2023	
APELLIDOS: <b>SOLUCIÓN</b>		
NOMBRE:	DNI:	

- b) Indique razonadamente las configuraciones que deben realizarse en el controlador de ONOS para obtener el resultado mostrado en la figura siguiente con la ejecución del comando “pingall” en Mininet. (0,2 puntos)

```

mininet> pingall
*** Ping: testing ping reachability
h1 -> X h3 X
h2 -> X X h4
h3 -> h1 X X
h4 -> X h2 X
*** Results: 66% dropped (4/12 received)
mininet>

```

Analizando el resultado del comando “pingall” de Mininet, se ve que hay conectividad entre “h1-h3” y entre “h2-h4”.

Por lo tanto, se tienen configurados dos “host-to-host intent”, uno entre h1 y h3 y otro entre h2 y h4 para permitir el tráfico de datos entre dichos hosts.

- c) Sabiendo que se ha ejecutado la orden “switch s1 stop” en la CLI de Mininet, indique razonadamente cuántos flujos estarían instalados en total en la tabla de flujos del switch “Spine2 (s2)” para que se produzca la salida del apartado anterior con la ejecución del comando “pingall” en la CLI de Mininet. Indique brevemente para qué se utilizaría cada uno de los flujos instalados en “Spine2 (s2)”. (0,2 puntos)

*Nota. No es necesario indicar los valores de los campos de cada uno de los flujos.*

Al estar deshabilitado el dispositivo “Spine1 (s1)” todo el tráfico pasará a través de “Spine2 (s2)”. Por tanto, en el dispositivo “Spine2 (s2)” habrá instalados los siguientes flujos:

- Dos flujos para el “HostToHostIntent” entre “h1” y “h3”, uno para el tráfico de ida y otro para el tráfico de vuelta.
- Dos flujos para el “HostToHostIntent” entre “h2” y “h4” con la misma funcionalidad indicada en el punto anterior.

Los tres flujos instalados por defecto en cada dispositivo para tráfico “ETH\_TYPE:arp”, “ETH\_TYPE:lldp” y “ETH\_TYPE:bddp”.

- d) Rellene los parámetros del cuadro siguiente con los valores adecuados para la configuración de un "Intent" entre "h2" y "h4" utilizando REST API y JSON como formato de intercambio de datos entre la aplicación y el controlador ONOS. (0,2 puntos)

Categoría comando ONOS: **Intent**

Método REST-API: **POST**

Codificación en JSON:

```
{
  "type": "HostToHostIntent",
  "appId": "org.onosproject.ovsdb",
  "priority": 55,
  "one": "00:00:00:00:00:0B/None",
  "two": "00:00:00:00:00:0D/None"
}
```

- e) Como consecuencia de la invocación del método REST API anterior el controlador ONOS envía el siguiente mensaje del protocolo OpenFlow al dispositivo "Leaf2 (s4)". Rellene los cuadros en blanco de dicho mensaje con los valores adecuados para la instalación del primero de los flujos mostrado en la figura con los flujos de dicho dispositivo al comienzo del ejercicio. (0,3 puntos)

OpenFlow 1.4

```

Version: 1.4 (0x05)
Type: OFPT_FLOW_MOD
Length: 104
Transaction ID: 25165939
Cookie: 0x00ac00004279e0ab
Cookie mask: 0x0000000000000000
Table ID: 0
Command: OFPFC_ADD
Idle timeout: 0
Hard timeout: 0
Priority: 55
Buffer ID: OFP_NO_BUFFER (4294967295)
Out port: OFPP_ANY (4294967295)
Out group: OFPG_ANY (4294967295)
Flags: 0x0001
Importance: 0
Match
  Type: OFPMT_OXM (1)
  Length: 32
  OXM field
    Class: OFPXMC_OPENFLOW_BASIC (0x8000)
    0000 000. = Field: OFPXMT_OFB_IN_PORT (0)
    .... ...0 = Has mask: False
    Length: 4
    Value: 3
(Sigue en cuadro derecho)

```

OXM field

```

Class: OFPXMC_OPENFLOW_BASIC (0x8000)
0000 011. = Field: OFPXMT_OFB_ETH_DST (3)
.... ...0 = Has mask: False
Length: 6
Value: 00:00:00:00:00:0D

```

OXM field

```

Class: OFPXMC_OPENFLOW_BASIC (0x8000)
0000 100. = Field: OFPXMT_OFB_ETH_SRC (4)
.... ...0 = Has mask: False
Length: 6
Value: 00:00:00:00:00:0B

```

Instruction

```

Type: OFPIT_APPLY_ACTIONS (4)
Length: 24
Pad: 00000000
Action
  Type: OFPAT_OUTPUT (0)
  Length: 16
  Port: 2
  Max length: 0
  Pad: 000000000000

```

 DEPARTAMENTO DE INGENIERÍA TELEMÁTICA Y ELECTRÓNICA ETSIS TELECOMUNICACIÓN UPM	<b>REDES Y SERVICIOS AVANZADOS</b> Examen de evaluación continua EC2. 27 de mayo de 2022	
APELLOS: <b>SOLUCIÓN</b>		
NOMBRE:		DNI:

**EJERCICIO 8. Puntuación: 1,2 puntos. Tiempo estimado: 10 minutos**

Las siguientes preguntas de test están referidas a la práctica de laboratorio “Configuración de una red SDN y análisis de tráfico OpenFlow”. Rodee con un círculo la respuesta correcta para cada pregunta:

- Respuesta acertada: 0,15 puntos.
  - Respuesta errónea: -0,05 puntos.
  - En blanco: 0 puntos.
1. ¿De qué mensaje aprende el controlador el “Datapath Id” (el identificador a efectos de Openflow) de cada switch?
    - a. OFPT\_HELLO
    - b. OFPT\_MULTIPART\_REPLY
    - c. **OFPT\_FEATURES\_REPLY**
    - d. OFPT\_PACKET\_IN
  2. El controlador consigue aprender los puertos que tiene cada dispositivo mediante una pareja REQUEST/REPLY de mensajes Openflow que contienen un campo de tipo específico para esta información. ¿Qué pareja de mensajes son?
    - a. **OFPT\_MULTIPART\_REQUEST/REPLY**.
    - b. OFPT\_BARRIER\_REQUEST/REPLY.
    - c. OFPT\_FEATURES\_REQUEST/REPLY.
    - d. OFPT\_GET\_CONFIG\_REQUEST/REPLY.
  3. En la práctica de laboratorio, al inicio de cada sesión Openflow se observan varios mensajes OFPT\_HELLO. ¿Quién envía el primero de esos mensajes para cada sesión Openflow?
    - a. Siempre el controlador.
    - b. **Siempre el switch.**
    - c. Siempre el host conectado al switch.
    - d. Depende de la sesión Openflow concreta.
  4. ¿Qué función principal tienen los mensajes OFPT\_BARRIER\_REQUEST/REPLY?
    - a. Permiten al controlador impedir la comunicación directa entre dos switches.
    - b. Permiten al controlador bloquear la validez de un flujo en una tabla de un switch.
    - c. **Permiten al controlador controlar la ordenación de la ejecución de órdenes por parte de un switch.**
    - d. Permiten al controlador activar o desactivar tablas de flujos completas en un switch.
  5. Un mensaje OFPT\_PACKET\_OUT:
    - a. Siempre se envía en respuesta a un mensaje OFPT\_PACKET\_IN.
    - b. **Siempre se envía en el sentido de controlador a switch.**
    - c. Siempre está precedido por un mensaje OFPT\_FLOW\_MOD.
    - d. Siempre contiene una trama que lleva encapsulado un paquete IP.
  6. El campo de prioridad en un flujo de una tabla de flujos de un switch permite:
    - a. Saber qué flujo eliminar de la tabla si dos flujos tienen selectores idénticos.
    - b. Establecer el orden en el que se aplican los flujos de una tabla a un paquete que encaja con los selectores de varios flujos.
    - c. Determinar el tiempo máximo durante el que se mantiene el flujo activo si ningún paquete encaja con su selector.
    - d. **Saber qué flujo aplicar cuando un paquete encaja con los selectores de varios flujos.**

7. La interfaz REST API se utiliza para comunicar:
  - a. El controlador con los dispositivos (switches).
  - b. El controlador con los hosts.
  - c. Los dispositivos (switches) con los hosts.
  - d. Las aplicaciones de red con el controlador.
  
8. Como consecuencia directa del establecimiento de un host-to-host Intent:
  - a. Se desactiva la aplicación “Reactive Forwarding” en caso de estar previamente activa.
  - b. El controlador envía varios mensajes PACKET\_OUT.
  - c. El controlador envía varios mensajes OFPT\_FLOW\_MOD.
  - d. Se activa la aplicación “Proxy ARP” en caso de estar previamente inactiva.

**EJERCICIO 9. Puntuación: 1,3 puntos. Tiempo estimado: 20 minutos**

Las siguientes preguntas están referidas a la práctica de laboratorio “Configuración de una red SDN y análisis de tráfico OpenFlow”.

En el escenario de la práctica de laboratorio se ejecuta la siguiente orden en la consola de Mininet:

```
mininet> h2 ping -c 4 h3
PING 10.0.0.3 (10.0.0.3) 56(84) bytes of data.
From 10.0.0.2 icmp_seq=1 Destination Host Unreachable
From 10.0.0.2 icmp_seq=2 Destination Host Unreachable
From 10.0.0.2 icmp_seq=3 Destination Host Unreachable
From 10.0.0.2 icmp_seq=4 Destination Host Unreachable

--- 10.0.0.3 ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3103ms
pipe 4
mininet>
```

Como consecuencia de dicha orden, se capturan las siguientes tramas:

No.	Time	Leng	Source	Destination	Protocol	TCP src	TCP dst	Info
308	3.781089745	42	00:00:00_00:00:00:02	Broadcast	ARP			Who has 10.0.0.3? Tell 10.0.0.2
309	3.781555230	150	172.17.0.1	172.17.0.2	OpenFlow	38412	6653	Type: OFPT_PACKET_IN
392	4.811983804	42	00:00:00_00:00:02	Broadcast	ARP			Who has 10.0.0.3? Tell 10.0.0.2
393	4.813051817	150	172.17.0.1	172.17.0.2	OpenFlow	38412	6653	Type: OFPT_PACKET_IN
466	5.824698142	42	00:00:00_00:00:02	Broadcast	ARP			Who has 10.0.0.3? Tell 10.0.0.2
467	5.825161026	150	172.17.0.1	172.17.0.2	OpenFlow	38412	6653	Type: OFPT_PACKET_IN
543	6.852573312	42	00:00:00_00:00:02	Broadcast	ARP			Who has 10.0.0.3? Tell 10.0.0.2
544	6.853528704	150	172.17.0.1	172.17.0.2	OpenFlow	38412	6653	Type: OFPT_PACKET_IN
605	7.873005427	42	00:00:00_00:00:02	Broadcast	ARP			Who has 10.0.0.3? Tell 10.0.0.2
606	7.873992681	150	172.17.0.1	172.17.0.2	OpenFlow	38412	6653	Type: OFPT_PACKET_IN
697	8.896727631	42	00:00:00_00:00:02	Broadcast	ARP			Who has 10.0.0.3? Tell 10.0.0.2
698	8.896997433	150	172.17.0.1	172.17.0.2	OpenFlow	38412	6653	Type: OFPT_PACKET_IN

En esta captura el filtro de visualización utilizado es “arp || icmp” (es decir, muestra cualquier paquete que contenga alguno de estos dos protocolos), y la captura ha sido realizada en todas las interfaces del escenario de la práctica.

Utilizando la información anterior, conteste a las siguientes preguntas. La justificación de las respuestas es imprescindible.

- a) ¿Es posible saber la dirección IP de h2? En caso afirmativo, diga cuál es esa dirección IP y explique a partir de qué información de la anteriormente mostrada se puede saber y por qué. En caso negativo, explique por qué no es posible. (0,1 puntos)

**Sí, es 10.0.0.2. Al ser en h2 en el que se ejecuta el ping, será el equipo que necesite al inicio lanzar la pregunta acerca de la dirección MAC de h3, por lo que su dirección IP debe ser la del equipo que hace la consulta en la trama 308 (y 392, 466, ..) (“Tell 10.0.0.2”)**

 DEPARTAMENTO DE INGENIERÍA TELEMÁTICA Y ELECTRÓNICA ETSIS TELECOMUNICACIÓN UPM	<b>REDES Y SERVICIOS AVANZADOS</b> Examen de evaluación continua EC2. 27 de mayo de 2022	
APELLOS: <b>SOLUCIÓN</b>		
NOMBRE:	DNI:	

- b) ¿Es posible saber la dirección IP de h3? En caso afirmativo, diga cuál es esa dirección IP y explique a partir de qué información de la anteriormente mostrada se puede saber y por qué. En caso negativo, explique por qué no es posible. (0,1 puntos)

**Sí, es 10.0.0.3. Al ser en h2 en el que se ejecuta el ping, será el equipo que necesite al inicio lanzar la pregunta acerca de la dirección MAC de h3, por lo que la dirección IP de h3 debe ser la del equipo por el que se hace la consulta en la trama 308 (y 392, 466, ..) ("Who has 10.0.0.3?")**

- c) ¿Es posible saber la dirección MAC de h2? En caso afirmativo, diga cuál es esa dirección MAC y explique a partir de qué información de la anteriormente mostrada se puede saber y por qué. En caso negativo, explique por qué no es posible. (0,1 puntos)

**Sí, es 00:00:00\_00:00:02. Al ser en h2 en el que se ejecuta el ping, será el equipo que necesite al inicio lanzar la pregunta acerca de la dirección MAC de h3, por lo que su dirección MAC debe ser la de origen de las tramas en las que se hace dicha consulta (308, 392, 466, ..).**

- d) ¿Es posible saber la dirección MAC de h3? En caso afirmativo, diga cuál es esa dirección MAC y explique a partir de qué información de la anteriormente mostrada se puede saber y por qué. En caso negativo, explique por qué no es posible. (0,1 puntos)

**No es posible saberlo ya que no se recibe respuesta a las consultas ARP que realiza h2, y es en dichas respuestas en las que se podría observar la dirección MAC del equipo h3, por el que se pregunta.**

- e) ¿Por qué se generan las tramas cuya columna Info es "OFPT\_PACKET\_IN"? ¿Qué contenido tendrán esos mensajes Openflow y quién los envía a quién? (0,1 puntos)

**Al llegar la pregunta ARP al switch al que está conectado h2, este switch incluirá esa pregunta ARP en un mensaje OFPT\_PACKET\_IN y se lo enviará al controlador (aplicando el tratamiento indicado en la correspondiente entrada de flujo), de manera que el controlador decida en su caso qué acciones tomar al respecto.**

- f) ¿Por qué no hay ningún paquete ICMP en la captura, a pesar de provenir de la ejecución de un “ping” entre dos hosts? (0,1 puntos)

Porque h2 nunca recibe respuesta a su petición ARP, con lo que no sabe qué dirección MAC tiene h3 y por tanto no puede encapsular la petición de eco en una trama Ethernet que vaya destinada a h3.

- g) ¿Estaba activada la aplicación “proxy ARP” en el controlador ONOS cuando se realizó este experimento? Razona su respuesta. (0,1 puntos)

No, ya que, de haberlo estado, la consulta ARP realizada por h2 habría recibido la correspondiente respuesta con la dirección MAC de h3, y se habría observado más tráfico en la captura.

A continuación se muestran los flujos de uno de los dispositivos del escenario tal y como se visualiza con ONOS:

TATE	PACKETS	DURATION	FLOW PRIORITY	TABLE NAME	SELECTOR	TREATMENT	APP NAME
Added	7	417	5	0	ETH_TYPE:ipv4	imm[OUTPUT:CONTROLLER], cleared:true	*core
Added	87	2,970	40000	0	ETH_TYPE:arp	imm[OUTPUT:CONTROLLER], cleared:true	*core
Added	259	265	10	0	IN_PORT:2, ETH_DST:00:00:00:00:00:02, ETH_SRC:00:00:00:00:00:03	imm[OUTPUT:3], cleared:false	*fwd
Added	259	265	10	0	IN_PORT:3, ETH_DST:00:00:00:00:00:03, ETH_SRC:00:00:00:00:00:02	imm[OUTPUT:1], cleared:false	*fwd
Added	1,917	2,970	40000	0	ETH_TYPE:lldp	imm[OUTPUT:CONTROLLER], cleared:true	*core
Added	1,917	2,970	40000	0	ETH_TYPE:bddp	imm[OUTPUT:CONTROLLER], cleared:true	*core

- h) Si este dispositivo recibe un paquete IP por su puerto 2, encapsulado en una trama Ethernet con direcciones de destino = 00:00:00:00:00:02, y de origen = 00:00:00:00:00:03, ¿qué entrada o entradas de la tabla anterior utilizará el dispositivo para dar el tratamiento correspondiente a ese paquete? ¿Por qué? ¿Qué tratamiento le dará a dicho paquete? (0,2 puntos)

Utilizará la tercera entrada, siendo el tratamiento (TREATMENT) enviar el paquete por el puerto 3 (imm[OUTUPUT:3]). Por qué: el paquete “encaja” con los selectores del flujo de la primera (por ser IP) y la tercera (por el puerto de entrada y las direcciones Ethernet de origen y destino) entradas. La tercera tiene prioridad mayor, por lo que es la que se aplicará.