

EJERCICIO 2: HSRP – INFORME DE ACTIVIDAD

1. Descripción del caso:

- En este supuesto, basándonos en parte en la red anterior, en la que configuramos el protocolo PVST, queremos configurar el protocolo HSRP. Este protocolo nos evitará que haya un punto de fallo único en el router de nuestra red, añadiendo más routers, y que estos se comuniquen entre si para:
 - Designar cual es el router activo (por el que pasaran los paquetes de la subred/VLAN)
 - Designar cual/cuáles son los routers en espera (que entrarán en acción en caso de que los paquetes no puedan llegar al router primario/activo)
- Este procedimiento se realiza añadiendo los siguientes comandos a los routers:

```
interface GigabitEthernet0/0
ip address 192.168.10.3 255.255.255.0
duplex auto
speed auto
standby 10 ip 192.168.10.1
standby 10 priority 105
standby 10 preempt
standby 10 track GigabitEthernet0/1
!
```

- Standby [nº grupo HSRP] ip [ip]: ip virtual de la red que nos permite enrutar los paquetes salientes de los pcs hacia una “ip común”. Cuando un paquete sale de un PC de la red, este pregunta por la MAC del Gateway, que será la configurada en este comando. Tras esto, respondera el router que este activo.
- Standby [nº grupo HSRP] priority [prioridad numérica]: el router con más prioridad será el activo. Por defecto es 100.
- Standby [nº grupo HSRP] preempt: permite que otro router asuma el rol de activo aunque este router esté funcionando, en caso de que el otro tenga una prioridad mayor
- Standby [nº grupo HSRP] track [interfaz][cantidad a reducir de la prioridad]: reduce la prioridad de el router en el que nos encontramos en caso de que la interfaz indicada deje de funcionar. Se reduce en 10 por defecto.

- Tras este procedimiento, los routers pasan por una serie de estados de comunicación para determinar el activo y el que se encuentre en estado de standby, como vemos aquí:

```
%HSRP-6-STATECHANGE: GigabitEthernet0/1.40 Grp 40 state Speak -> Standby
%HSRP-6-STATECHANGE: GigabitEthernet0/0.10 Grp 10 state Speak -> Standby
%HSRP-6-STATECHANGE: GigabitEthernet0/0.10 Grp 10 state Standby -> Active
```

- Speak: los routers se envían mensajes entre si, para elegir cual será aquel que está activo o en espera
 - Standby: este router tomará el control si el router activo falla
 - Active: este router maneja el tráfico de la red
- Hay que tener en cuenta, que tras este proceso previo de comunicación entre los routers en la configuración del protocolo HSRP, estos siguen comunicandose entre si cada cierto tiempo, mandándose mensajes de tipo “Hello” para confirmar que el otro router sigue activo en la red. Si el router que está en standby no recibe el mensaje “Hello” del router Active, este procederá a ponerse en estado Active .
- Notas:
 - Durante el Informe verá que las capturas contienen señalización de por donde van los paquetes. He considerado hacer esto así, al parecerme que si hacia una captura por cada lugar por donde iba el paquete, quedaría un informe muy cargado de información y por lo tanto, desagradable a la vista.
 - El archivo original de Packet Tracer (.pkt) se adjunta con este informe, así que no dude en hacer cualquier prueba si así lo desea.

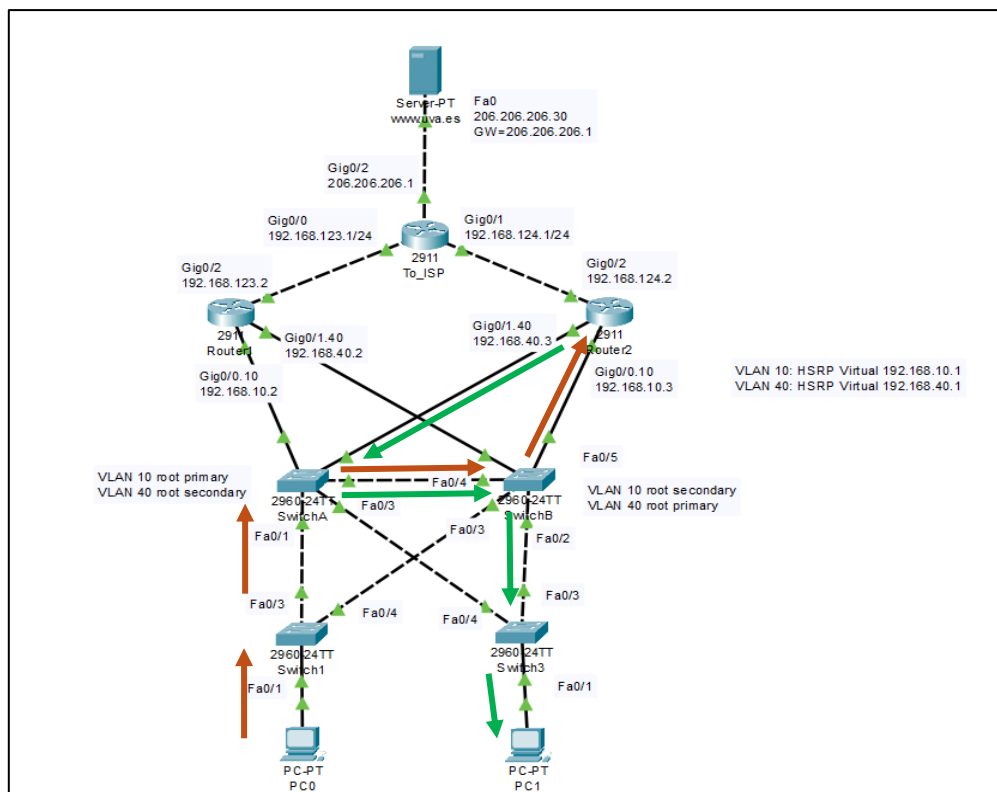
2. Spanning tree y HSRP antes del corte:

Veamos primero la configuración de los routers 1 y 2 con el protocolo HSRP:

ROUTER 1	ROUTER 2
<pre> Router#show standby GigabitEthernet0/0.10 - Group 10 State is Standby 8 state changes, last state change 00:13:46 Virtual IP address is 192.168.10.1 Active virtual MAC address is 0000.0C07.AC0A Local virtual MAC address is 0000.0C07.AC0A (vl default) Hello time 3 sec, hold time 10 sec Next hello sent in 2.406 secs Preemption enabled Active router is 192.168.10.3, priority 105 (expires in 9 sec) Standby router is local Priority 100 (default 100) Group name is hsrp-Gig-10 (default) GigabitEthernet0/1.40 - Group 40 State is Active 5 state changes, last state change 00:00:18 Virtual IP address is 192.168.40.1 Active virtual MAC address is 0000.0C07.AC28 Local virtual MAC address is 0000.0C07.AC28 (vl default) Hello time 3 sec, hold time 10 sec Next hello sent in 0.474 secs Preemption enabled Active router is local Standby router is 192.168.40.3 Priority 105 (configured 105) Track interface GigabitEthernet0/2 state Up decrement 10 Group name is hsrp-Gig-40 (default) </pre>	<pre> Router#show standby GigabitEthernet0/0.10 - Group 10 State is Active 7 state changes, last state change 00:13:36 Virtual IP address is 192.168.10.1 Active virtual MAC address is 0000.0C07.AC0A Local virtual MAC address is 0000.0C07.AC0A (vl default) Hello time 3 sec, hold time 10 sec Next hello sent in 0.009 secs Preemption enabled Active router is local Standby router is 192.168.10.2, priority 100 (expires in 8 sec) Priority 105 (configured 105) Track interface GigabitEthernet0/2 state Up decrement 10 Group name is hsrp-Gig-10 (default) GigabitEthernet0/1.40 - Group 40 State is Standby 5 state changes, last state change 00:00:26 Virtual IP address is 192.168.40.1 Active virtual MAC address is 0000.0C07.AC28 Local virtual MAC address is 0000.0C07.AC28 (vl default) Hello time 3 sec, hold time 10 sec Next hello sent in 1.542 secs Preemption enabled Active router is 192.168.40.2 Standby router is local Priority 100 (default 100) Group name is hsrp-Gig-40 (default) </pre>

Como podemos ver, para la VLAN 10, el router que está en modo activo es el 2 y para la VLAN 40 es el 1

Veamos ahora un ejemplo de comunicación entre las VLANes



- - Camino de ida del paquete ICMP desde el PC0 hasta el router Active
- - Camino de ida del paquete ICMP desde el router hasta el PC1

Explicación de la ruta seguida:

- **Switch 1 > Switch A:** como vimos en la práctica del protocolo PVST, uno de los 2 switches de la capa superior (A y B), se designa como el root primario, mientras que el otro será el root secundario:

VLAN0010									
Spanning tree enabled protocol rstp									
Root ID	Priority	24586							
	Address	000D.BD41.670C							
	Cost	19							
	Port	3(FastEthernet0/3)							
	Hello Time	2 sec	Max Age	20 sec	Forward Delay	15 sec			
Bridge ID	Priority	32778 (priority 32768 sys-id-ext 10)							
	Address	0002.166A.05B5							
	Hello Time	2 sec	Max Age	20 sec	Forward Delay	15 sec			
	Aging Time	20							
Interface	Role	Sts	Cost		Prio.Nbr	Type			

Fa0/3	Root	FWD	19		128.3	F2p			
Fa0/1	Desg	FWD	19		128.1	F2p			
Fa0/4	Altn	BLK	19		128.4	F2p			

- **Switch A > Switch B:** El switch hará un reenvío broadcast por todas sus interfaces (excepto por donde llegó el paquete). Recordemos que esto se hace ya que el switch no contiene la MAC destino en su tabla MAC:

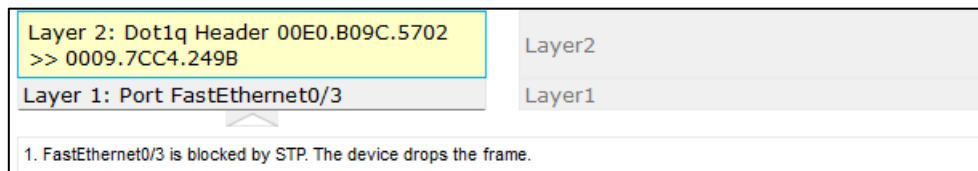
Layer 2: Dot1q Header 0040.0B83.084A >> 0000.0C07.AC0A	Layer 2: Dot1q Header 0040.0B83.084A >> 0000.0C07.AC0A
Layer 1: Port FastEthernet0/1	Layer 1: Port(s): FastEthernet0/2 FastEthernet0/3 FastEthernet0/4 FastEthernet0/5
1. The frame destination MAC address is not in the MAC table. The Switch floods the frame to all ports in the same VLAN except the receiving port.	

El router Activo de la VLAN 10 es el router 2, entonces el paquete deberá ser encaminado hacia este router. El problema es que el Switch A no tiene capacidad para mandarle a este router el paquete ya que el enlace que conecta con este router solo puede encaminar paquetes de la VLAN 40:

Layer 2: Dot1q Header 0040.0B83.084A >> 0000.0C07.AC0A	Layer2
Layer 1: Port GigabitEthernet0/1	Layer1
1. There is no subinterface with this VLAN enabled. The device drops the frame.	

Por esto, el paquete es reenviado al switch B para que este haga el encaminamiento necesario, ya que este será el único que pueda hacer llegar el paquete al router activo por la VLAN 10.

- Switch B > Router 2: Este switch también reenviará por todas sus interfaces menos por la de llegada el paquete. Como se ve en las primeras imágenes de la página anterior, el router activo para la VLAN 10 es el 2 por eso el paquete que se encamina hacia este, es el paquete aceptado.
- Router 2 > Switch A: El router ahora encamina el paquete hacia la VLAN 40 (la forma de comunicar VLANes es mediante un router). Como la interfaz de la VLAN 40 es la Gig0/1.40, y este enlace va a dar al router Switch A, el router se ve obligado a mandarlo por ahí
- Switch A > Switch B: El Switch A manda el paquete en modo broadcast por todas sus interfaces. Los que le llegan a los switches 1 y 3, son descartados ya que STP ha bloqueado el enlace:



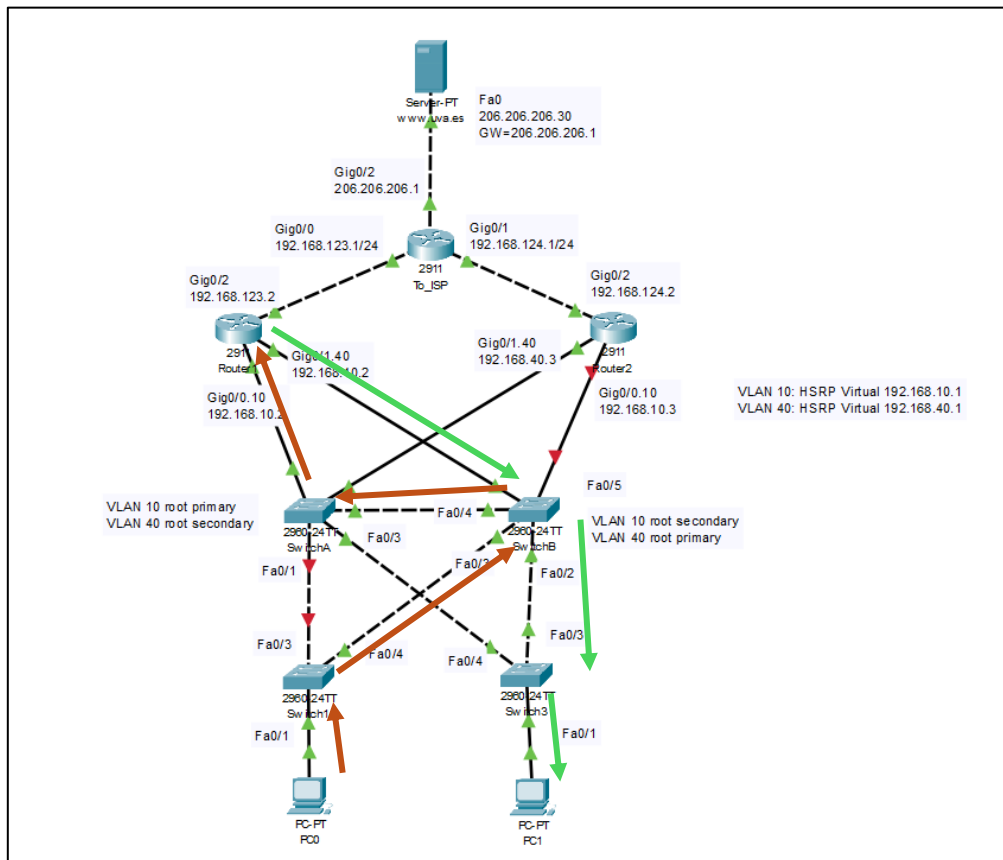
El paquete también le llega al router pero lo descarta al ser de la VLAN incorrecta (manda por el enlace de la VLAN 10 un paquete de la VLAN 40).

Finalmente el paquete también se reenvía por la Fa0/4 que corresponde con el enlace que va a dar al SwitchB, el cual acepta el paquete (el enlace no está bloqueado por STP) y procede a hacer lo mismo que su switch antecesor.

- Switch B > Switch 3: El switch reenvía todos los paquetes por sus interfaces. En este caso, se lo queda el Switch 3 ya que la interfaz por la que sale el paquete a este Switch, es la que no está bloqueada por el protocolo SPT
- Finalmente el paquete llega a su destino (PC1)

3. Cambios relevantes en la red cuando se cae un enlace de nivel 3 y un enlace de nivel 2

- Tomemos ahora el siguiente ejemplo:



- - Camino de ida del paquete ICMP desde el PC0 hasta el router Active
- - Camino de ida del paquete ICMP desde el router hasta el PC1

Cambios relevantes:

- Switch 1 > Switch B: Como el enlace entre el Switch 1 y el Switch A esta caído, el protocolo PVST reasigna al switch B como el primario, enviando los paquetes de la VLAN 10 hacia este:

```

VLAN0010
Spanning tree enabled protocol rstp
Root ID    Priority    24586
           Address    000D.BD41.670C
           Cost       38
           Port       4(FastEthernet0/4)
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID   Priority    32778 (priority 32768 sys-id-ext 10)
           Address    0002.166A.05B5
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time 20
  
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.1	P2p
Fa0/4	Root	FWD	19	128.4	P2p

- Switch B > Switch A: En el caso anterior, el enlace entre el Switch B y el router 2 no estaba caído, por lo que se mandaba el paquete directamente por el enlace que los conectaba. Ahora como no se puede encaminar en esta dirección, una vez que el paquete llega al switch, como la MAC destino no se encuentra en la MAC address-table, el switch se ve obligado a reenviar el paquete de forma broadcast, llegándole al Switch A. En este, el paquete también le llega al router, pero como el enlace que conecta el Switch B con el router 1 corresponde a la VLAN 40 y no la 10, el router lo rechaza

- Switch A > Router 1: Lo mismo que en la explicación anterior, pero en este caso, el paquete que le llega al router si es aceptado al pertenecer el enlace por el que ha sido enviado a la VLAN 10.

PDU Information at Device: Router1

OSI Model Inbound PDU Details Outbound PDU Details

At Device: Router1
Source: PC0
Destination: PC1

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 192.168.10.10, Dest. IP: 192.168.40.10 ICMP Message Type: 8	Layer 3: IP Header Src. IP: 192.168.10.10, Dest. IP: 192.168.40.10 ICMP Message Type: 8
Layer 2: Dot1q Header 0040.0B83.084A >> 0000.0C07.AC0A	Layer 2: Dot1q Header 0002.1683.D002 >> 0009.7CC4.249B
Layer 1: Port GigabitEthernet0/0	Layer 1: Port(s): GigabitEthernet0/1

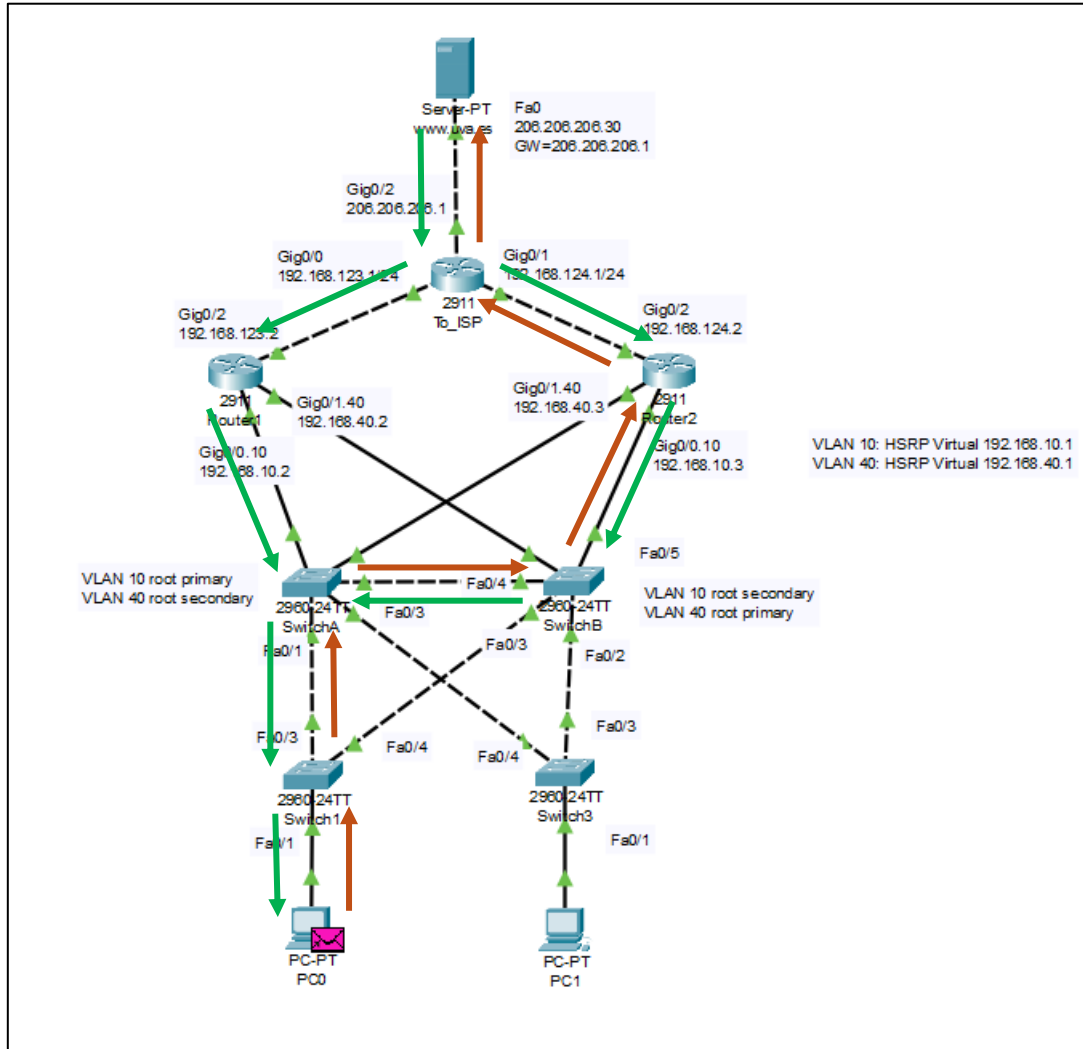
1. GigabitEthernet0/1 sends out the frame.

- Router 1 > Switch B: Como en el ejemplo sin enlaces caídos, el paquete sale por la interfaz configurada para la VLAN 40. Antes era el enlace que daba al Switch A pero ahora es el que llega al B, por eso el paquete sale por esta interfaz.

- Tras esto el paquete sigue su curso hacia el PC1

4. Algunas consideraciones de diseño extras y otros casos en los que el comportamiento de la red varía:

- COMUNICACIÓN CON EL EXTERIOR:

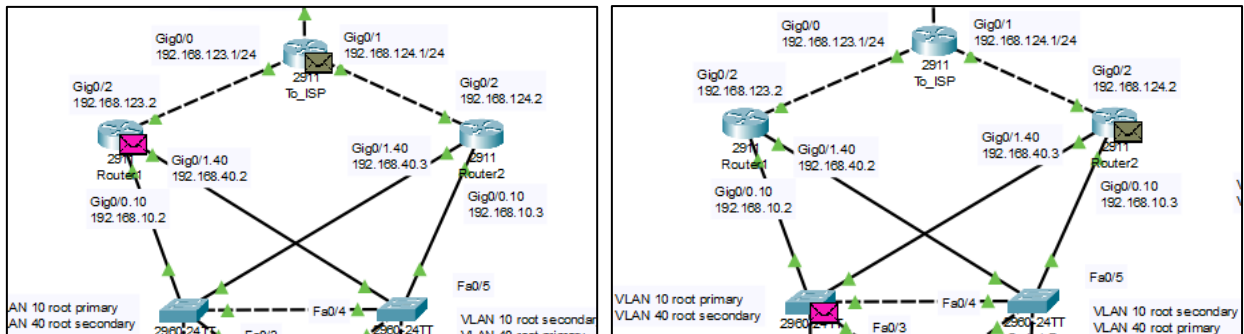


- - Camino de ida del paquete ICMP desde el PC0 hasta el servidor
- - Camino de vuelta del paquete ICMP desde el servidor hasta el PC0

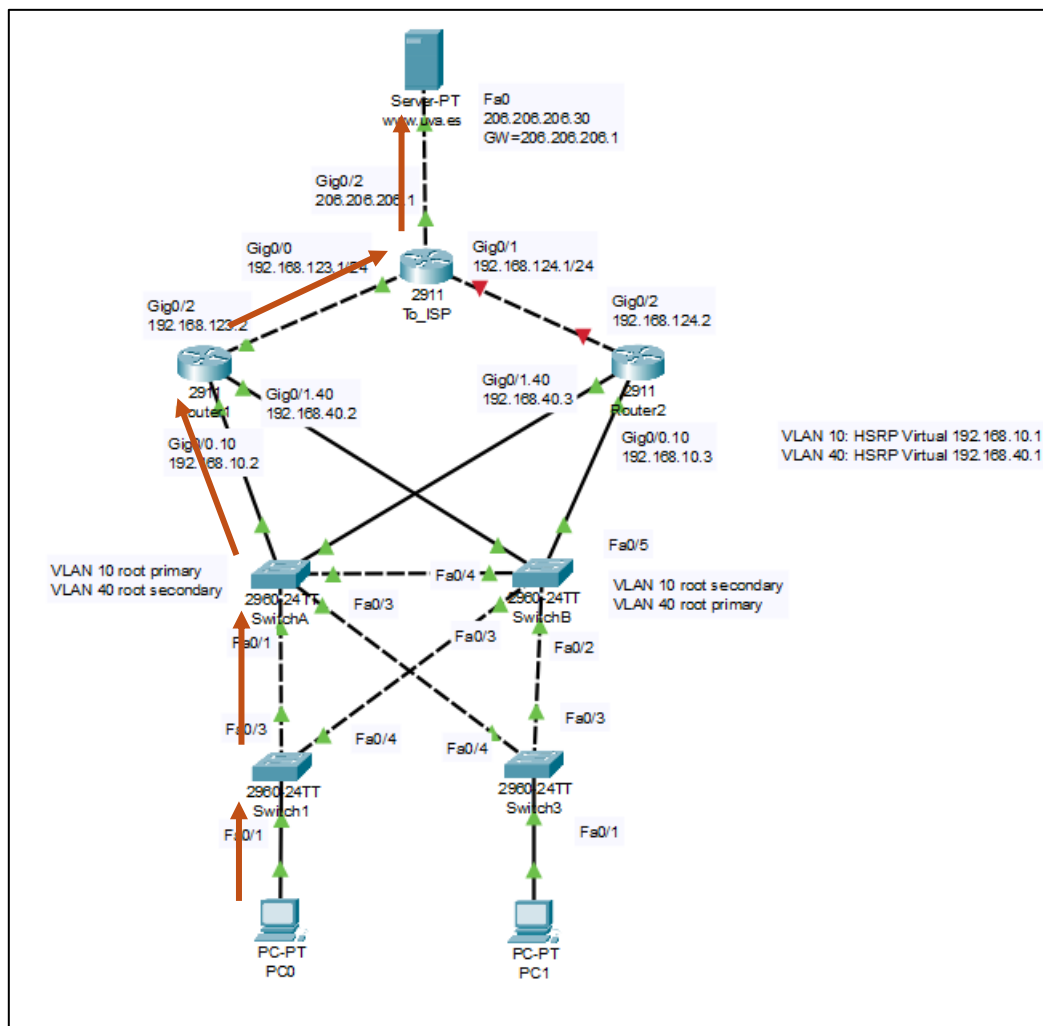
Como podemos ver en este ejemplo, el camino hasta el router es completamente igual que en el primer ejemplo, mandando un ping entre el PC0 y el PC1. Después, simplemente se termina de encaminar el paquete hasta el servidor.

Tras esto llega la peculiaridad. Al volver al router To_ISP, el paquete puede ir tanto al router 1 como al router 2. Esto ocurre ya que, al ser el coste a los dos routers el mismo, el router intermedio decide repartir la carga entre los 2, ya que tanto el

router 1 como el 2 pueden volver al PC0. Se puede ver mejor este caso en la siguiente captura:



- FUNCIONAMIENTO DEL COMANDO TRACK



- - Camino de ida del paquete ICMP desde el PC0 hasta el servidor
- - Camino de vuelta del paquete ICMP desde el servidor hasta el PC0

Como podemos observar, aunque originalmente el router en estado active fuera el 2, gracias al comando track que añadimos a la configuración del router al configurar el protocolo HSRP, la prioridad del router se ve disminuida por estar el enlace entre el router2 y el To_ISP caído. Esto provoca que los routers se comuniquen entre si, cambiando el estado del Router2 a Standby y el estado del router 1 a Active (para la VLAN 10)

ROUTER 2:

```
GigabitEthernet0/0.10 - Group 10
  State is Standby
```

```
%HSRP-6-STATECHANGE: GigabitEthernet0/0.10 Grp 10 state Speak -> Standby
```

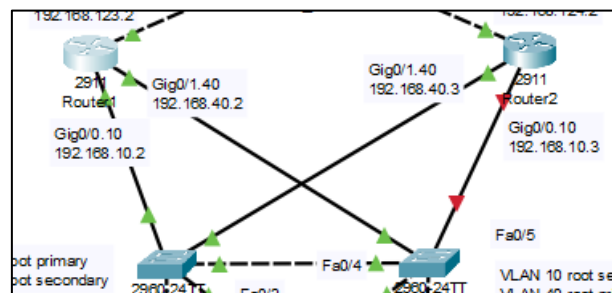
ROUTER 1:

```
GigabitEthernet0/0.10 - Group 10
  State is Active
```

```
%HSRP-6-STATECHANGE: GigabitEthernet0/0.10 Grp 10 state Standby -> Active
```

- ROUTERS INCOMUNICADOS

Para este ejemplo, usaremos la misma configuración que en el ejemplo en el que había un fallo de nivel 3 y un fallo de nivel 2 simultáneamente (aunque solo nos sea relevante la parte de nivel 3 ahora mismo)



```
GigabitEthernet0/0.10 - Group 10
  State is Active
```

```
GigabitEthernet0/0.10 - Group 10
  State is Active
```

Como podemos ver, los 2 routers están en activo para la VLAN 10. Esto ocurre, por culpa del protocolo HSRP. Como el enlace de la VLAN 10 que conecta el router 2 con el Switch B, los 2 routers no se pueden comunicar por la VLAN, entonces aunque el router 1 envía el mensaje de “hello”, este no recibe ninguno, cambiando su estado a Active.