

Ejercicio 4- Seguridad en la capa 3: Protocolos dinámicos de encaminamiento IP. OSPF

Un protocolo de encaminamiento (en inglés, *routing protocol*) tiene el objetivo de rellenar y actualizar la tabla de enrutamiento de los encaminadores (*routers*) de una red con los mejores caminos para el intercambio de datos entre las distintas redes. Fundamentalmente, las tareas que tienen asignadas estos protocolos dinámicos son las siguientes:

- Descubrir redes lejanas con las que intercambiar información
- Mantener la información de encaminamiento actualizada de manera fiable
- Elegir el mejor camino posible en cada momento hacia las redes de destino
- Encontrar nuevas rutas para sustituir a aquellas que dejen de estar disponibles en cualquier momento y en condiciones aceptables

Los protocolos de encaminamiento dinámico se clasifican, según sea su ámbito de aplicación, en protocolos de tipo *Gateway* interior o de exterior, y los primeros se agrupan según consideren como variable el vector distancia o el estado del enlace.

Desde el punto de vista de la seguridad, hay que resaltar el papel fundamental que juegan los protocolos de encaminamiento ip dinámico para garantizar la disponibilidad, confidencialidad e integridad en las comunicaciones. No todos estos protocolos (o versiones de un protocolo de encaminamiento determinado) implementan mecanismos de seguridad, que eviten vulnerabilidades que posibiliten realizar ataques como, por ejemplo, los siguientes:

- Bloquear los mensajes legítimos de actualización de rutas con el objetivo de generar una denegación de servicio de la red (parte de la red podría dejar de ser visible).
- Modificar la tabla de rutas con un objetivo determinado, a través del envío de mensajes de actualización generados artificialmente. La corrupción de esta tabla permitiría a un atacante lograr una denegación de los servicios de la red, bien generando congestión, limitando la visibilidad entre partes de ésta, o creando bucles de encaminamiento. Además, el atacante también podría acceder a información confidencial si logramos encaminar un determinado flujo de tráfico hacia un analizador de red (*sniffer*) instalado en algún equipo de la red no autorizado.

Una manera sencilla de evitar que un encaminador ajeno a una red sea introducido en ésta de manera clandestina y que pueda alterar los mensajes de encaminamiento, es realizar una autenticación por resumen del mensaje. La autenticación por resumen de mensaje es una autenticación criptográfica. En cada encaminador se configura una clave (contraseña) y un ID de clave. El encaminador utiliza un algoritmo basado en el paquete de datos, en la clave y en el ID de clave para generar un "resumen de mensaje" que se agrega al paquete de datos. La clave no se intercambia a través de la red. Cuando el mensaje llega a su destino, se realiza un nuevo cálculo del resumen de dicho mensaje y se compara con el que éste ya incorpora. En caso que no coincidan, entonces se descarta.

En esta práctica se va a trabajar este concepto con el protocolo de encaminamiento OSPF (*Open Shortest Path First*) aplicándolo a la red cuya topología se puede ver en la figura 1. OSPF, cuya versión 2 se define en el documento RFC 2328, es un protocolo de tipo *gateway* interior que se usa para distribuir información de enrutamiento dentro de un mismo sistema autónomo.

Como bibliografía básica de encaminamiento, se recomienda la siguiente:

- Stallings, W.: Data and Computer Communications. Prentice Hall, 2014 (Tenth Edition). ISBN 10: 1-29-201438-5 / ISBN 13: 978-1-29-201438-8. [Chapter 19]
- Manuales de configuración IOS de Cisco: <http://www.cisco.es/> [ver enlace directo a la información en la sección de Recursos de la asignatura en Aula Digital]
- Documento RFC 2328: <https://www.ietf.org/rfc/rfc2328.txt>

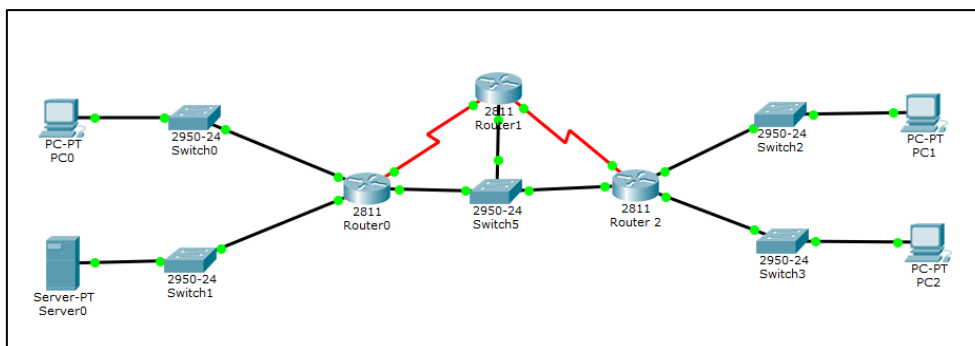


Figura 1. Topología de la red

Guion de la práctica

Tarea 1: Bajar el fichero de trabajo desde *Aula Digital* y abrirlo.

Tarea 2: Una vez que esté operativa toda la red (todas los puntos de luz en color verde), realizar un inventario del direccionamiento de la red (rellenar la tabla 1) y comprobar que hay conectividad entre todos los equipos.

Tabla 1. Direcciones IP asignadas en la red de la figura 1

Equipo	Interfaz	Dirección ip	Máscara de red
Router 0	FastEthernet0/0	192.168.0.1	255.255.255.0
	FastEthernet0/1	192.168.1.1	255.255.255.0
	Ethernet0/0/0	192.168.5.3	255.255.255.0
	Serial0/1/0	192.168.4.1	255.255.255.252
Router 1	Serial0/1/0	192.168.4.2	255.255.255.252
	FastEthernet0/0	192.168.5.4	255.255.255.0
	Serial0/1/1	192.168.4.5	255.255.255.252
Router 2	FastEthernet0/0	192.168.2.1	255.255.255.0
	FastEthernet0/1	192.168.3.1	255.255.255.0
	Ethernet0/0/0	192.168.5.2	255.255.255.0
	Seial0/1/0	192.168.4.6	255.255.255.252
PC0	FastEthernet0	192.168.0.2	255.255.255.0
PC1	FastEthernet0	192.168.2.2	255.255.255.0
PC2	FastEthernet0	192.168.3.2	255.255.255.0
Server0	FastEthernet0	192.168.1.2	255.255.255.0

Tarea 3: Visualizar la información correspondiente a OSPF en los encaminadores (R0, R1 y R2).

- Paso 3.1: Observar el contenido de las tablas de encaminamiento (analice los distintos campos y describa cada una de las entradas de esas tablas). Esto se puede realizar utilizando la herramienta lupa del simulador *Cisco Packet Tracer* y también desde la opción CLI (*Command Line Interface*) de cada encaminador mediante el comando siguiente (ver que se realiza desde la zona con privilegios):

```
Router# show ip route
```

R:

- Type:
- Network: ip address destino.
- Port: puerto de salida para llegar al destino.
- NextHopIP: ip address del primer dispositivo por el que pasará el tráfico cuando se intente alcanzar el destino.
- Metric: valor de la métrica del camino.

- Paso 3.2: Visualizar las adyacencias OSPF y observar la información que aparece. Para ello utilizar el comando siguiente:

```
Router# show ip ospf neighbor
```

R:

```
R0# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.5.4	1	FULL/DR	00:00:38	192.168.5.4	Ethernet0/0/0
192.168.5.2	1	FULL/DROTHER	00:00:38	192.168.5.2	Ethernet0/0/0
192.168.5.4	0	FULL/ -	00:00:38	192.168.4.2	Serial0/1/0

R0#

- Paso 3.3: Realizar una prueba de ruta utilizando el comando *tracert* desde el PC0 a PC1. Para ello acceder a Command Prompt (secuencia: seleccionar PC → Desktop → Command Prompt) y utilizar el comando *tracert* de la forma siguiente:

```
PC0>tracert 192.168.2.2
```

Con la información que va apareciendo en la pantalla, ¿puede determinar el camino que se ha seguido hasta llegar al destino? Indicar qué protocolo y qué mensajes correspondientes utiliza la herramienta *traceroute* (*tracert* en MS Windows).

```

PC>tracert 192.168.2.2

Tracing route to 192.168.2.2 over a maximum of 30 hops:

  1    3 ms      0 ms      0 ms      192.168.0.1
  2    0 ms      1 ms      0 ms      192.168.5.2
  3    0 ms      0 ms      0 ms      192.168.2.2

Trace complete.

```

Según el output del comando tracert 192.168.2.2, la ruta seguida es:

PC0 -> Router0(192.168.0.1) -> Router2(192.168.5.2) -> PC1(192.168.2.2)

El protocolo y los mensajes correspondientes que usa tracert son:

- Internet Control Message Protocol (ICMP)
- Utiliza concretamente paquetes echo con valores time to live (TTL) variables.

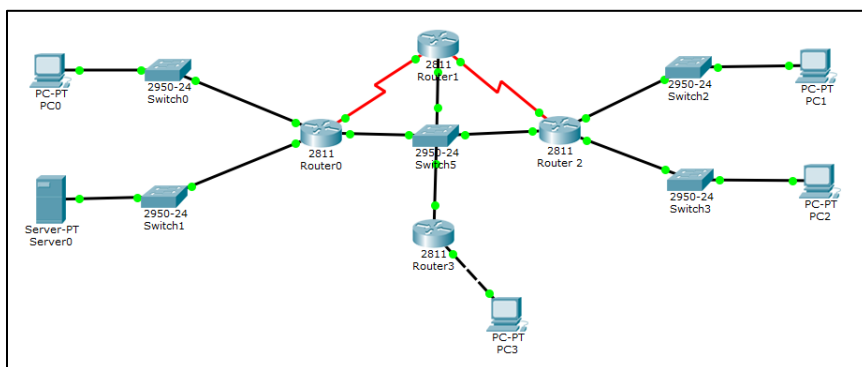


Figura 2. Agregación de nuevos dispositivos de red

Tarea 4: Agregar un nuevo encaminador (Router3) y un nuevo PC (PC3) tal y como se indica en la figura 2 y realizar la configuración siguiente:

– Paso 4.1: Configuración del Router3:

```

Router (config)# hostname R3
R3 (config)# interface FastEthernet0/0          (interfaz donde se conecte PC3)
R3 (config-if)# ip address 192.168.2.1 255.255.255.0
R3 (config-if)# no shutdown
R3 (config-if)# interface FastEthernet0/1      (interfaz conectada a conmutador 5)
R3 (config-if)# ip address 192.168.5.5 255.255.255.0
R3 (config-if)# no shutdown
R3 (config-if)# exit
R3 (config)# router ospf 1                    (se inicia configuración de OSPF en este router)
R3 (config-router)# log-adjacency-changes
R3 (config-router)# network 192.168.2.0 0.0.0.255 area 0
R3 (config-router)# network 192.168.5.0 0.0.0.255 area 0
R3 (config-router)# exit

```

```
R3(config)# exit
```

- Paso 4.2: Configurar los parámetros de red de PC3. Asignarle la dirección ip siguiente: 192.168.2.2
- **Paso 4.3: Volver a realizar los pasos 3.1, 3.2 y 3.3 y observar los cambios.**

```
R0# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
C    192.168.0.0/24 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/1
O    192.168.2.0/24 [110/11] via 192.168.5.2, 00:01:32, Ethernet0/0/0
                        [110/11] via 192.168.5.5, 00:01:32, Ethernet0/0/0
O    192.168.3.0/24 [110/11] via 192.168.5.2, 00:01:32, Ethernet0/0/0
    192.168.4.0/30 is subnetted, 2 subnets
C      192.168.4.0 is directly connected, Serial0/1/0
O      192.168.4.4 [110/74] via 192.168.5.4, 00:01:32, Ethernet0/0/0
                        [110/74] via 192.168.5.2, 00:01:32, Ethernet0/0/0
C    192.168.5.0/24 is directly connected, Ethernet0/0/0
```

```
R0# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.5.4	1	FULL/DROTHER	00:00:39	192.168.5.4	Ethernet0/0/0
192.168.5.2	1	FULL/DROTHER	00:00:39	192.168.5.2	Ethernet0/0/0
192.168.5.5	1	FULL/DR	00:00:39	192.168.5.5	Ethernet0/0/0
192.168.5.4	0	FULL/ -	00:00:39	192.168.4.2	Serial0/1/0

Por otro lado, realizar una prueba de conectividad con el comando “*ping -t*” desde PC0 hacia PC3 y mediante el modo de simulación observar lo que sucede (Nota: editar los filtros y realizar la configuración para que sólo muestre los mensajes de OSPF e ICMP). **Después de observar el intercambio de mensajes por la red, describir y explicar lo que está sucediendo.**

```
PC> ping -t 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

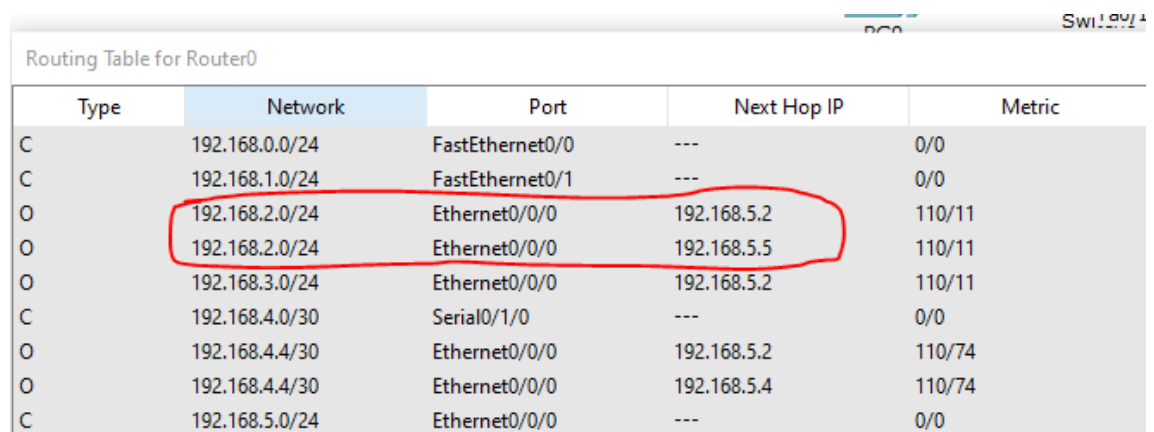
Reply from 192.168.2.2: bytes=32 time=12ms TTL=126
Request timed out.
Reply from 192.168.2.2: bytes=32 time=12ms TTL=126
Request timed out.
Reply from 192.168.2.2: bytes=32 time=12ms TTL=126
Request timed out.
Reply from 192.168.2.2: bytes=32 time=12ms TTL=126
Request timed out.
```

Se ha conectado un nuevo router y se ha activado OSP en él. A este router se ha conectado un PC con una IP que ya corresponde a otro PC. Como no se ha configurado autenticación de los mensajes en los routers, este nuevo router interfiere en el funcionamiento correcto de la red:

Al hacer un ping -t desde PC0 hasta PC1, si lo capturamos con el modo de simulación vemos que OSPF se comporta de manera que el ping se envía alternadamente a un PC y al otro, por tanto hay pérdida de información.

- Paso 4.4: Cambiar la dirección ip de PC3 (por ejemplo: 192.168.2.3) y repetir la prueba de conectividad con “ping – t” desde PC0 hacia la dirección ip 192.168.2.2. Observar el resultado que aparece, desde el modo “Realtime”, en la interfaz de comandos del PC. ¿Qué sucede ahora? Razonarlo.

Al utilizar el PC3 cuando tenía la misma IP que PC1, 192.168.2.2, se ha creado una entrada adicional en la tabla de encaminamiento. Entonces ahora cuando intentamos hacer ping a 192.168.2.2, aunque esta IP solo pertenezca al PC1, la mitad de los pings se desvían hacia la interfaz de entrada del router malicioso, 192.168.5.5.



Type	Network	Port	Next Hop IP	Metric
C	192.168.0.0/24	FastEthernet0/0	---	0/0
C	192.168.1.0/24	FastEthernet0/1	---	0/0
O	192.168.2.0/24	Ethernet0/0/0	192.168.5.2	110/11
O	192.168.2.0/24	Ethernet0/0/0	192.168.5.5	110/11
O	192.168.3.0/24	Ethernet0/0/0	192.168.5.2	110/11
C	192.168.4.0/30	Serial0/1/0	---	0/0
O	192.168.4.4/30	Ethernet0/0/0	192.168.5.2	110/74
O	192.168.4.4/30	Ethernet0/0/0	192.168.5.4	110/74
C	192.168.5.0/24	Ethernet0/0/0	---	0/0

- Paso 4.5: Indicar qué tipo o tipos de ataque se han llevado a cabo en el paso 4.3 y en el paso 4.4.

Ataque de denegación de servicio (Ataque contra la disponibilidad), MITM, por explotación de vulnerabilidades OSPF. (Ataques contra integridad y confidencialidad).

Tarea 5: Configuración de la autenticación del resumen de mensaje OSPF. En esta tarea se reconfigurará OSPF en cada uno de los encaminadores de la figura 2 que formaban parte de la red de la figura 1 para iniciar el proceso de autenticación entre vecinos.

- Paso 5.1: En cada uno de los encaminadores (excepto en Router3) realizar la siguiente configuración para cada una de las interfaces activas con otros encaminadores:

```
Router# configure terminal
Router(config)# interface <interfaz>
Router(config-if)# ip ospf message-digest-key 1 md5 7 PASSWORD
Router(config-if)# router ospf 1
Router(config-router)# area 0 authentication message-digest
Router(config-router)# exit
```

- Paso 5.2: Esperar varios segundos para que se produzca la convergencia de la red y volver a realizar los pasos 3.1, 3.2 y 3.3 y observar el resultado.
- Paso 5.3: ¿Qué conclusiones puede sacar de los resultados obtenidos? Razonarlo.

```
R0# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

Gateway of last resort is not set

```
C    192.168.0.0/24 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/1
O    192.168.2.0/24 [110/11] via 192.168.5.2, 00:02:37, Ethernet0/0/0
O    192.168.3.0/24 [110/11] via 192.168.5.2, 00:02:37, Ethernet0/0/0
     192.168.4.0/30 is subnetted, 2 subnets
C      192.168.4.0 is directly connected, Serial0/1/0
O      192.168.4.4 [110/74] via 192.168.5.2, 00:02:37, Ethernet0/0/0
C    192.168.5.0/24 is directly connected, Ethernet0/0/0
```

```
R0# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.5.2	1	FULL/BDR	00:00:30	192.168.5.2	Ethernet0/0/0
192.168.5.4	0	FULL/ -	00:00:36	192.168.4.2	Serial0/1/0

```
PC> tracert 192.168.2.2

Tracing route to 192.168.2.2 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.0.1
  2    0 ms      0 ms      0 ms      192.168.5.2
  3    0 ms      1 ms      0 ms      192.168.2.2

Trace complete.

PC>
```

Tarea 6: Realizar un resumen del ejercicio (describir la situación inicial, la intermedia producida por la realización de la tarea 4 e indicar el objetivo que se ha conseguido al finalizar la tarea 5).

R:

En la situación inicial, se ha realizado un inventario de direccionamiento IP y se ha probado la conectividad entre los equipos. Se hacia uso del protocolo OSPF, pero no se habían aplicado aún las medidas de seguridad que CPT permite implementar en este contexto.

En la situación intermedia (tarea 4), mediante el uso de pruebas de conectividad y el análisis de estas con el modo de simulación, se ha analizado los problemas que pueden existir si no se implementan las medidas de seguridad recomendadas en este contexto.

En la situación final, se ha configurado la autenticación del resumen de mensaje OSPF para que se inicie la autenticación entre vecinos. Al final la tarea se ha conseguido que el router malicioso conectado a la red no interfiera en el correcto funcionamiento de la red legítima, a través del uso de autenticación de los mensajes que envían los routers.

(Se acabó la práctica)