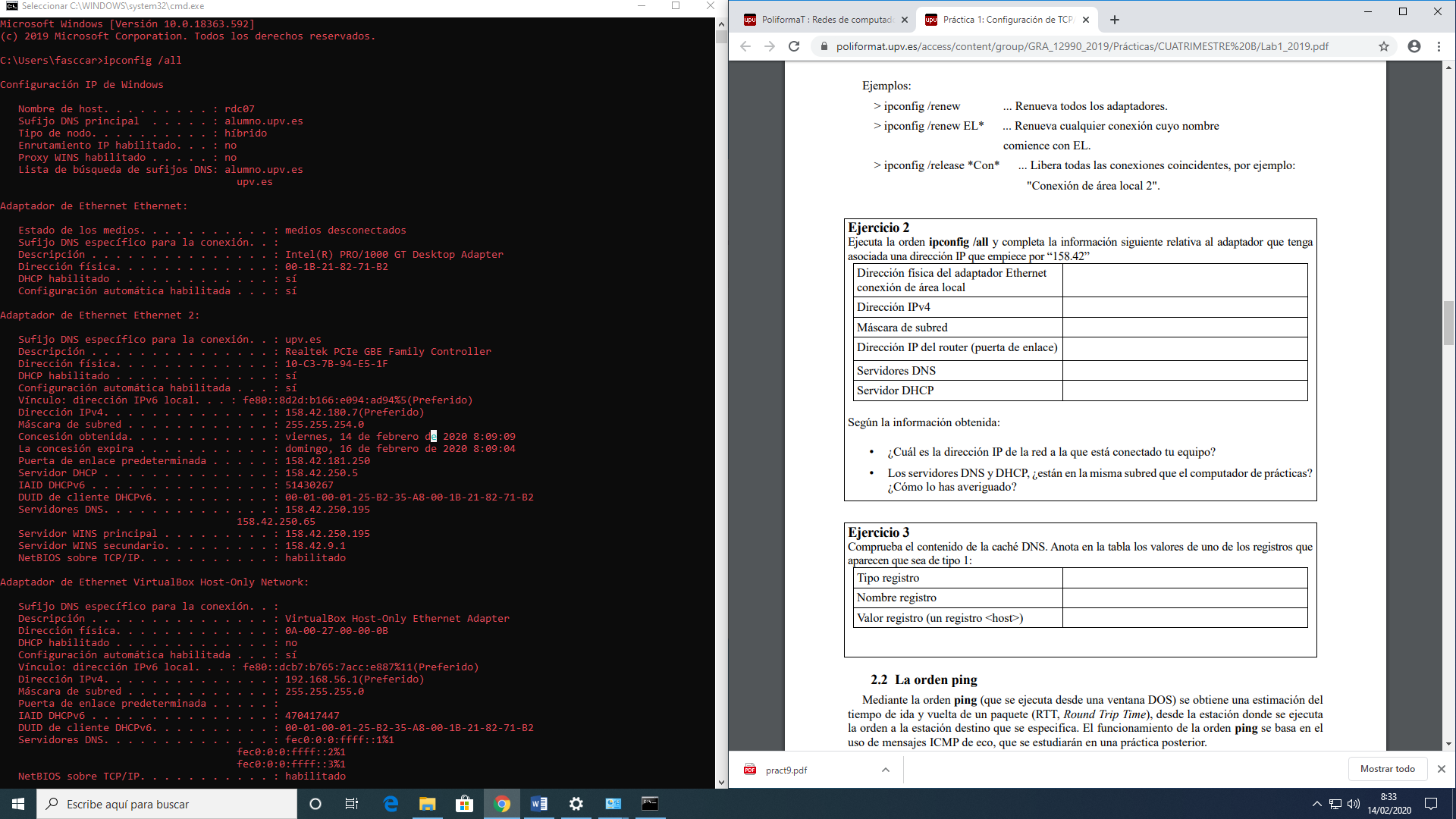
**Ejercicio 1 Identifica cuál de todos los adaptadores que aparecen es el que te conecta a Internet e indica el motivo.**

El adaptador es el Ethernet 2, ya que la red de la UPV tiene asignado el bloque de direcciones IPv4 158.42.0.0 con una máscara de 16b, por ende, si la dirección IPv4 asignada a nuestro equipo por dicho adaptador se realiza una and con una máscara de 16b da como resultado el valor de la red de la UPV.

**Ejercicio 2 Ejecuta la orden ipconfig /all y completa la información siguiente relativa al adaptador que tenga asociada una dirección IP que empiece por “158.42”**



158.42.250.5

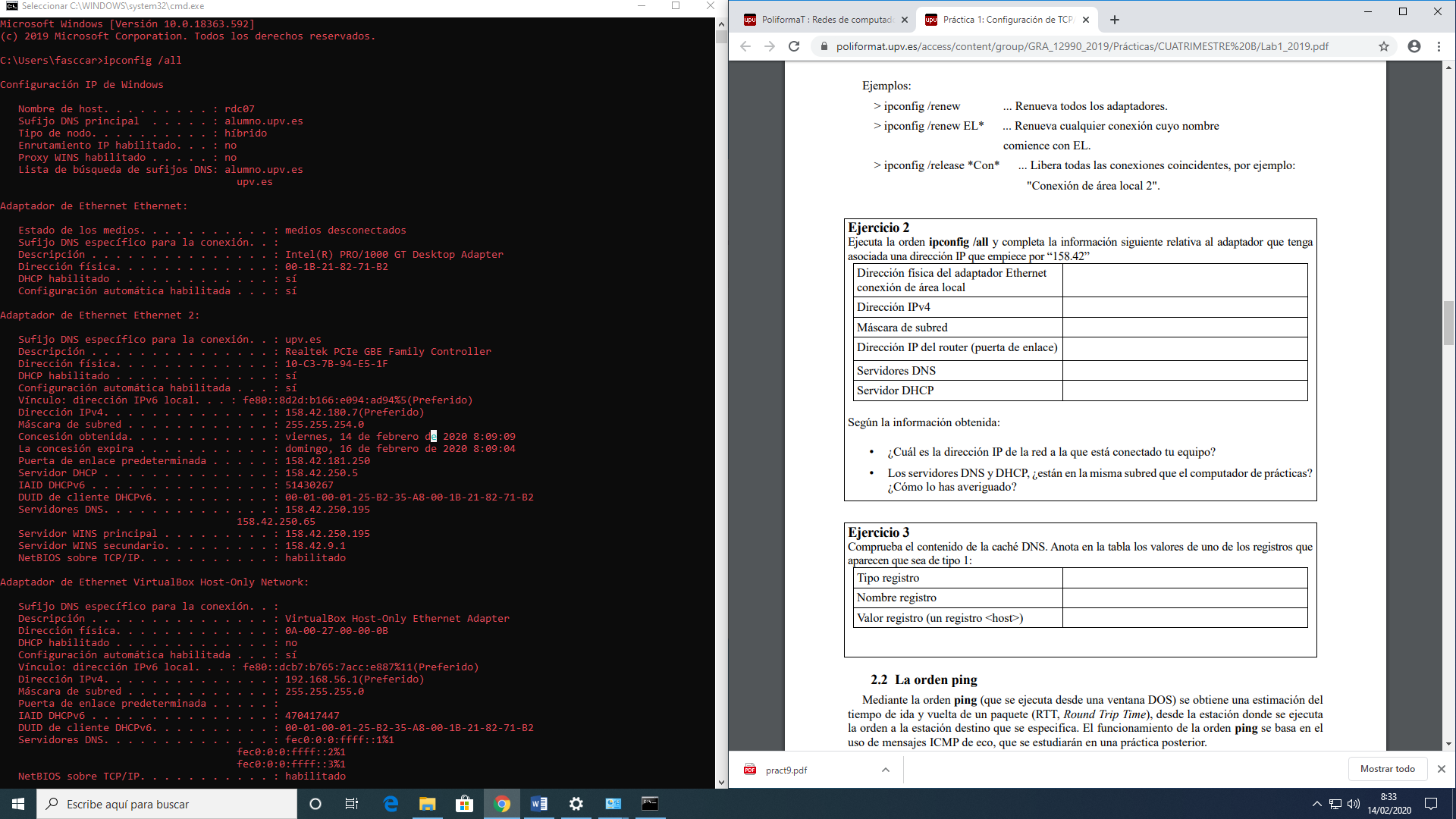
158.42.250.195

158.42.181.250 (puerto de enlace)

255.255.254.0/23

158.42.180.7

10-C3-7B-94-E5-1F



**¿Cuál es la dirección IP de la red a la que está conectado tu equipo?**

Dir Ip = 158.42.180.7

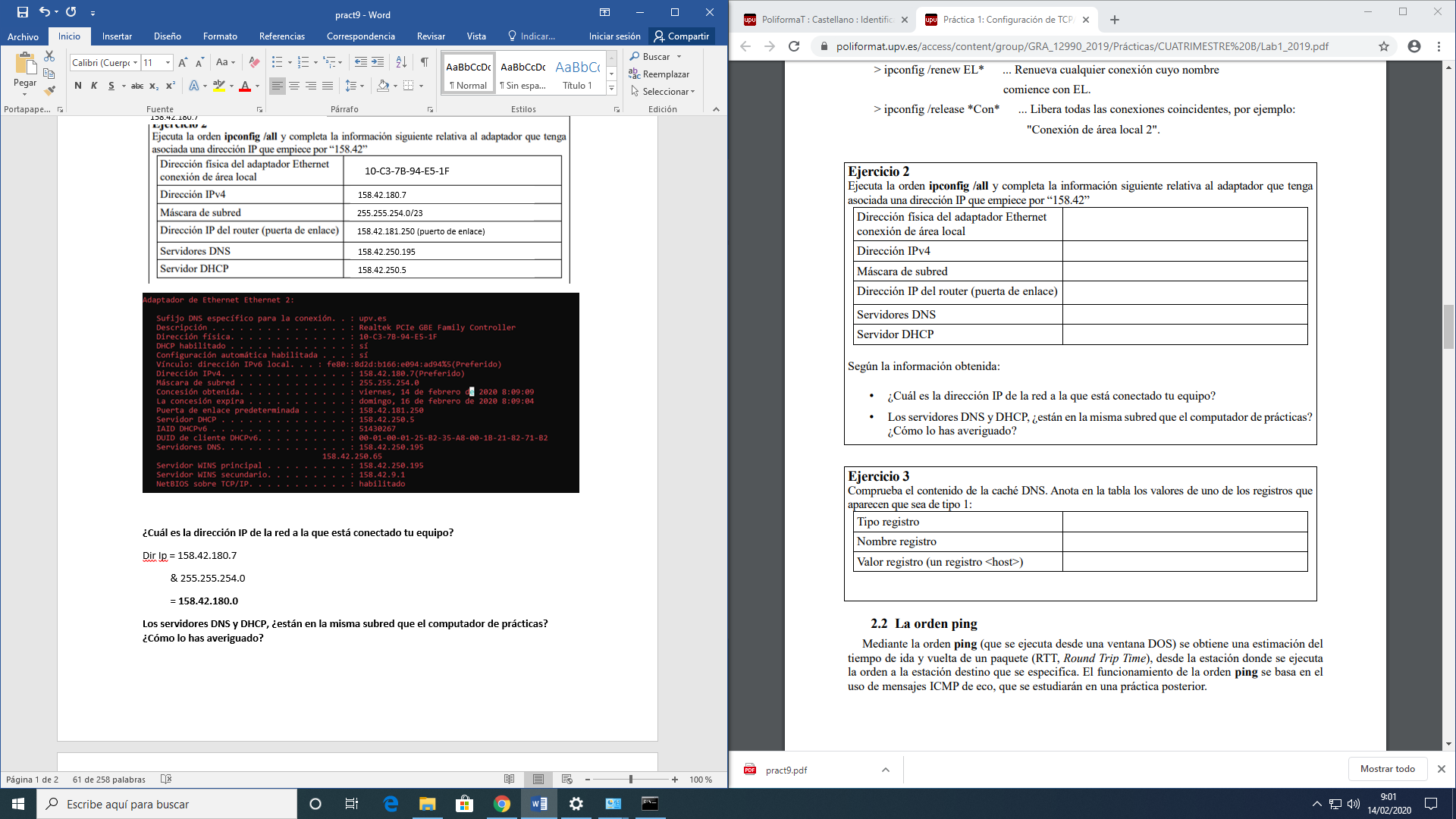
& 255.255.254.0

**= 158.42.180.0**

**Los servidores DNS y DHCP, ¿están en la misma subred que el computador de prácticas? ¿Cómo lo has averiguado?**

No se encuentran en la misma subred, ya que la dir ip de la subred del computador es 158.42.180.0 y la del serv DNS y DHCP tienen una dir Ip diferente al aplicarle una máscara de 23b.

**Ejercicio 3 Comprueba el contenido de la caché DNS. Anota en la tabla los valores de uno de los registros que aparecen que sea de tipo 1:**

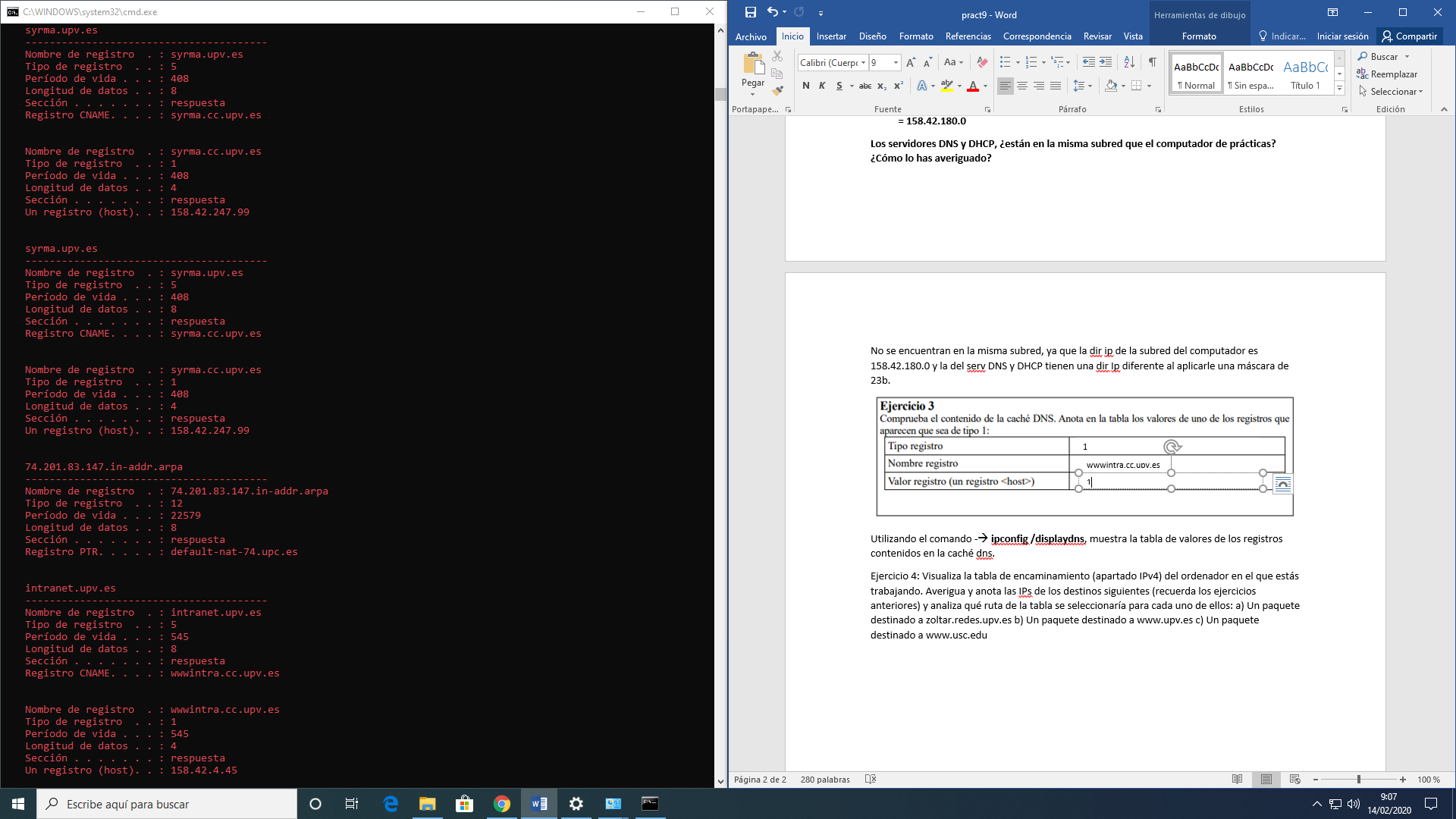


158.42.4.45

wwwintra.cc.upv.es

1

Utilizando el comando -🡪 **ipconfig /displaydns**, muestra la tabla de valores de los registros contenidos en la caché dns.



Esta lista de registros es más extensa uwu

**Ejercicio 4 Visualiza la tabla de encaminamiento (apartado IPv4) del ordenador en el que estás trabajando. Averigua y anota las IPs de los destinos siguientes (recuerda los ejercicios anteriores) y analiza qué ruta de la tabla se seleccionaría para cada uno de ellos:**

**(para conocer la tabla de encaminamiento se escribe el comando: netstat -r)**

**a) Un paquete destinado a zoltar.redes.upv.es**

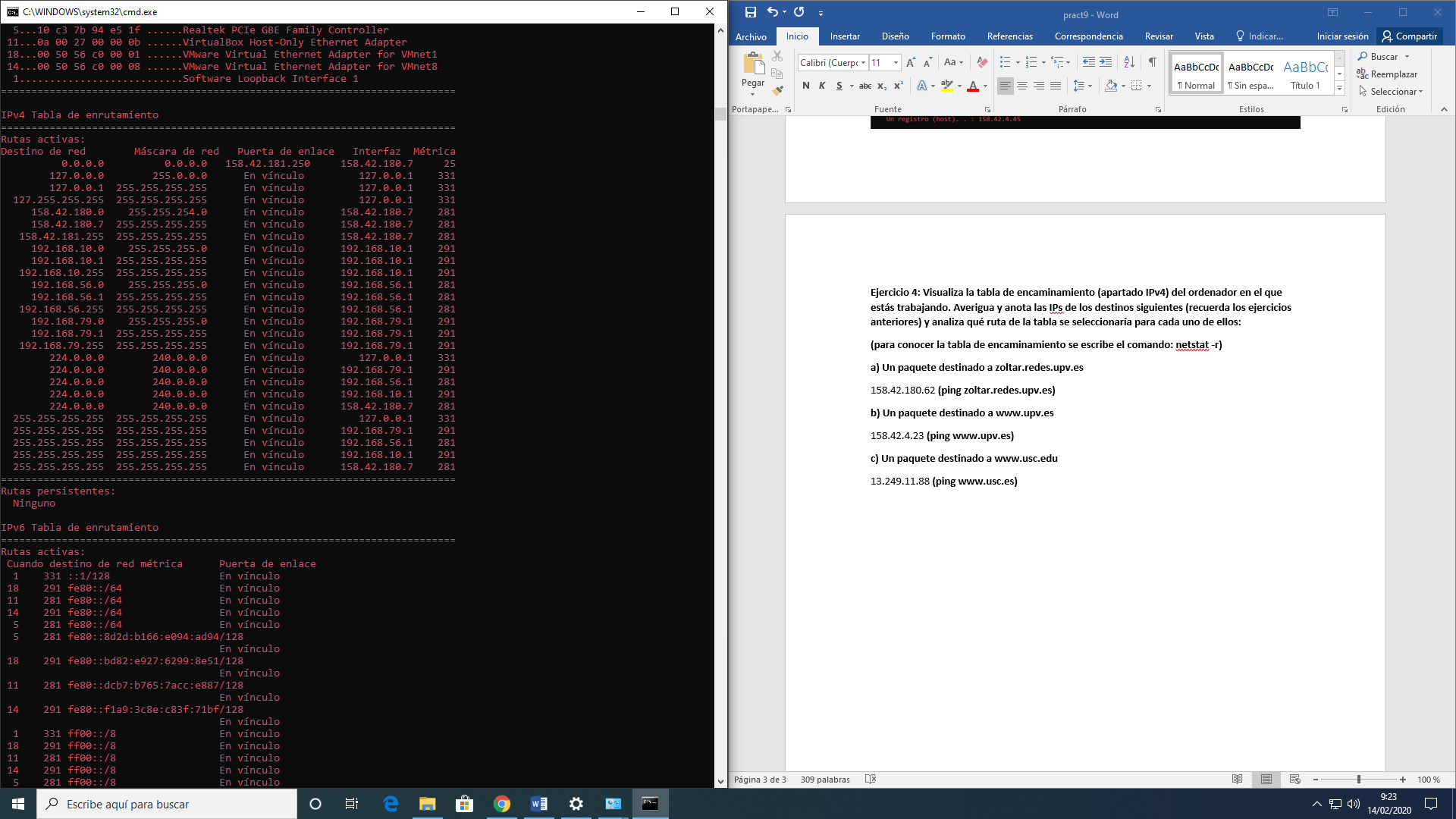
158.42.180.62 **(ping zoltar.redes.upv.es)** -> Se va por la interfaz 158.142.180.7

**b) Un paquete destinado a www.upv.es**

158.42.4.23 **(ping www.upv.es)**->Se va por la interfaz 158.142.180.7(Coincide solo con 0.0.0.0)

**c) Un paquete destinado a www.usc.edu**

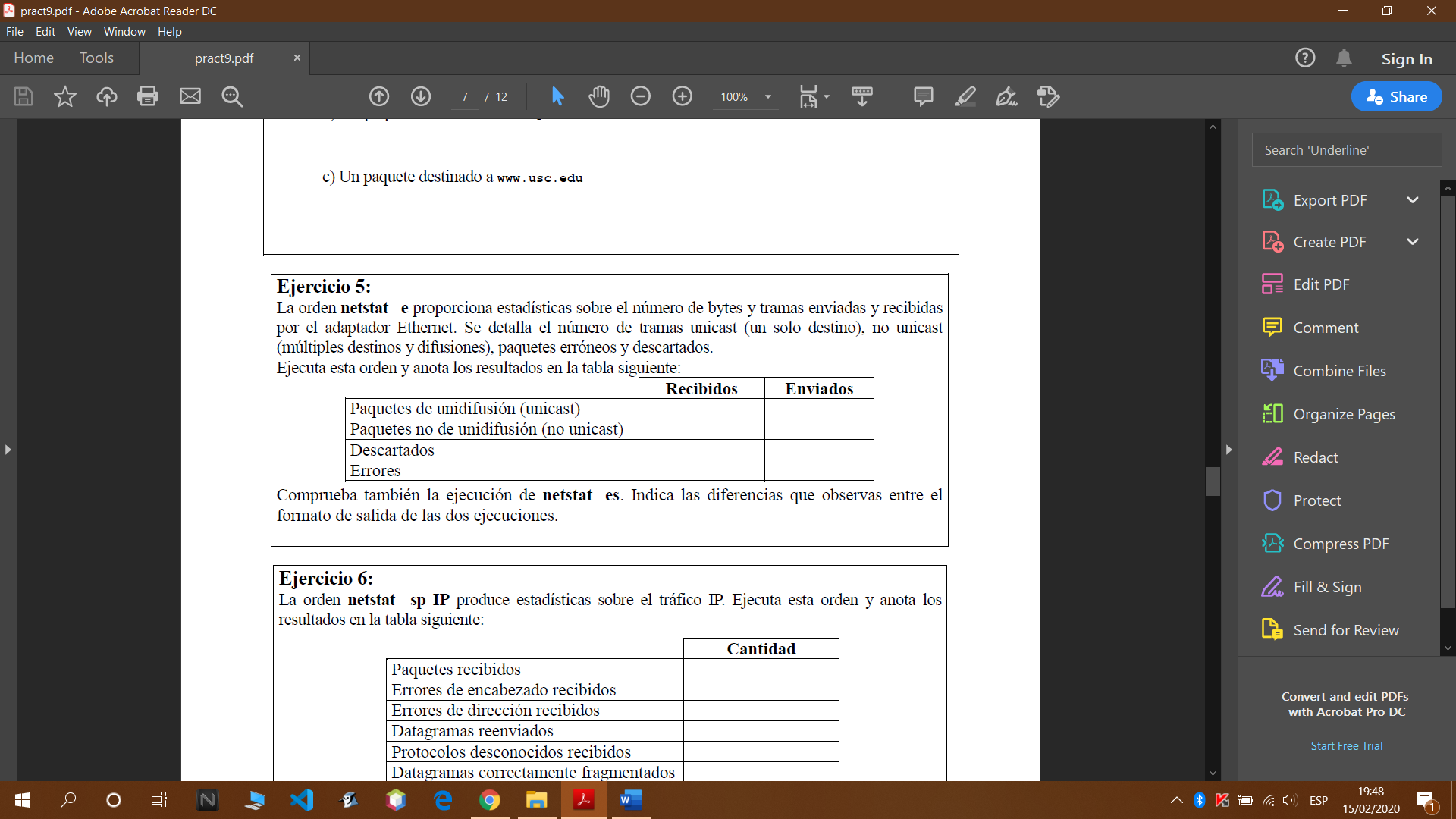
13.249.11.88 **(ping www.usc.es)**->Se va por la interfaz 158.142.180.7(Coincide solo con 0.0.0.0)



Para ver por cuál de las direcciones IP de la lista de arriba viajan estos tres paquetes realizamos la operación and con la dirección IP destino de donde se quieren enviar los paquetes y las máscaras respectivas y nos quedamos con el mayor prefijo coincidente con la IP destino de red mostradas en la tabla de arriba.

**Ejercicio 5 La orden netstat –e proporciona estadísticas sobre el número de bytes y tramas enviadas y recibidas por el adaptador Ethernet. Se detalla el número de tramas unicast (un solo destino), no unicast (múltiples destinos y difusiones), paquetes erróneos y descartados.**

**Ejecuta esta orden y anota los resultados en la tabla siguiente:**



**0**

**0**

**0**

**3542**

**97680**

**1837**

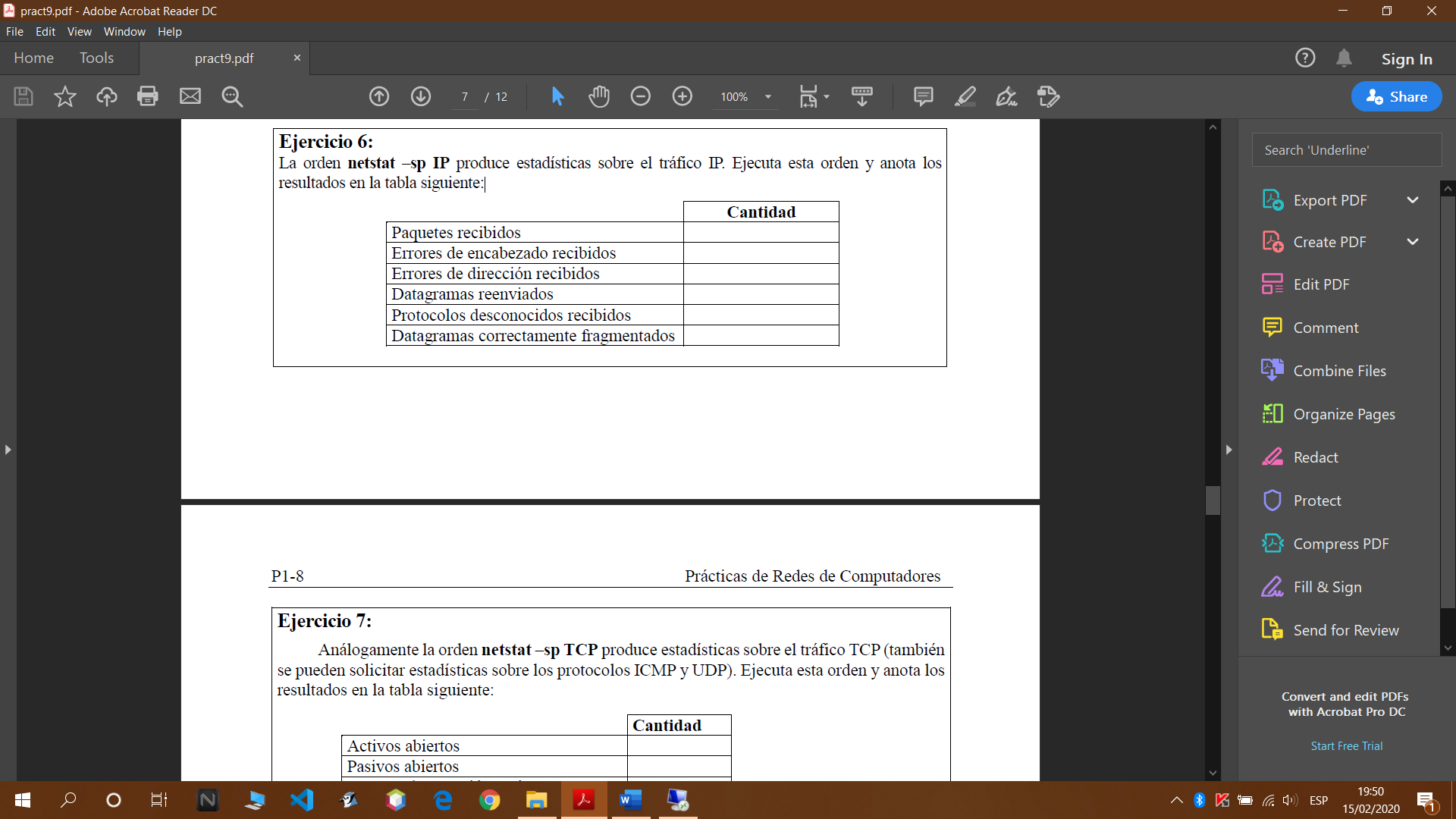
**439530**

**389736**

**Comprueba también la ejecución de netstat -es. Indica las diferencias que observas entre el formato de salida de las dos ejecuciones.**

**La instrucción netstat -es, muestra las estadísticas del adaptador ethernet pero por protocolos a diferencia del netstat -e.**

**Ejercicio 6 La orden netstat –sp IP produce estadísticas sobre el tráfico IP. Ejecuta esta orden y anota los resultados en la tabla siguiente:**



**0**

**0**

**0**

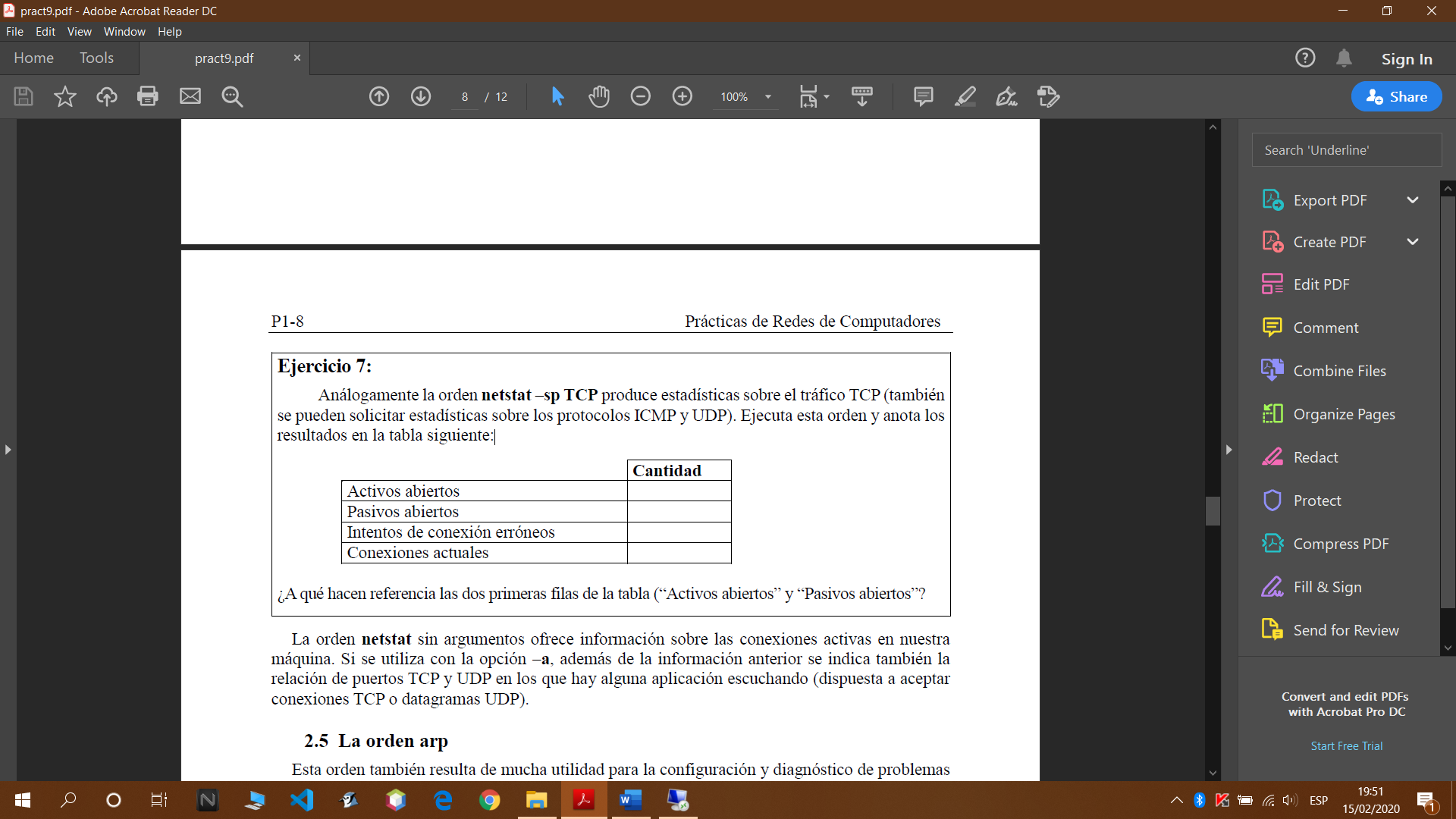
**167**

**0**

**139154**

(al unir s con p se muestran estadísticas del protocolo pasado como parámetro a la instrucción netstat, en este caso al ser IP será del protocolo IP)

**Ejercicio 7 Análogamente la orden netstat –sp TCP produce estadísticas sobre el tráfico TCP (también se pueden solicitar estadísticas sobre los protocolos ICMP y UDP). Ejecuta esta orden y anota los resultados en la tabla siguiente:**



**15**

**17**

**13**

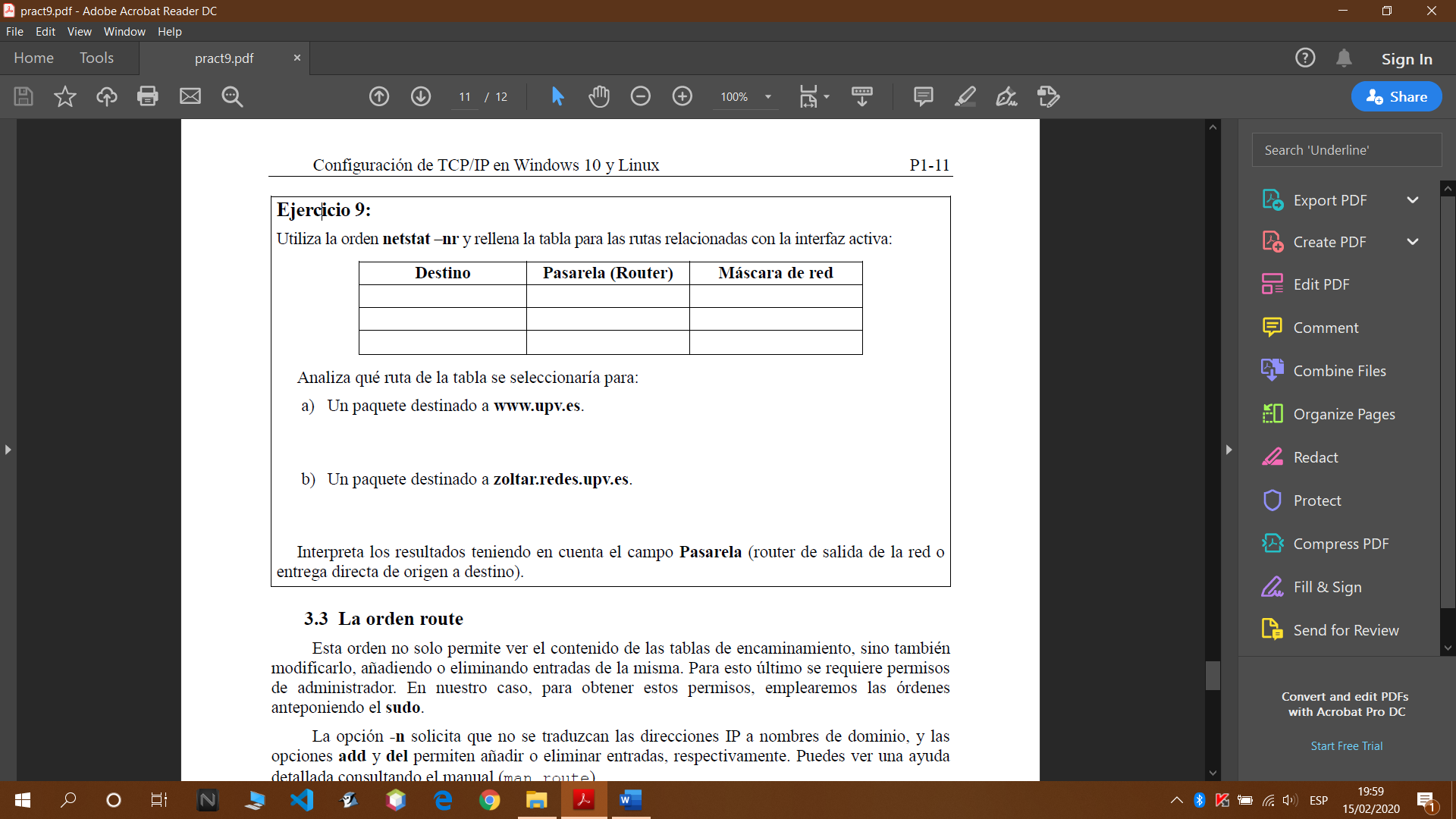
**652**

**¿A qué hacen referencia las dos primeras filas de la tabla (“Activos abiertos” y “Pasivos abiertos”?**

**Activos abiertos** hace referencia a aquellos puertos que están abiertos para establecer conexiones y que están siendo usados y **pasivos abiertos** son los que están a la espera para ser usados.

**Ejercicio 8 Ejecuta la orden ifconfig eth02 y, basándote en la descripción anterior, analiza la información obtenida.**

**Ejercicio 9 Utiliza la orden netstat –nr y rellena la tabla para las rutas relacionadas con la interfaz activa:**



**255.255.0.0**

**0.0.0.0**

**0.0.0.0**

**255.255.254.0**

**0.0.0.0**

**158.42.181.250**

**169.254.0.0**

**158.42.180.0**

**0.0.0.0**

**Analiza qué ruta de la tabla se seleccionaría para:**

1. **Un paquete destinado a** [**www.upv.es**](http://www.upv.es)**.**

Un paquete destinado a [www.upv.es](http://www.upv.es) tendrá una dirección ip destino de 158.42.4.23(al hacer ping [www.upv.es](http://www.upv.es) sale su dirección ip), al aplicarle las máscaras de vemos que solo coincide con la 0.0.0.0 con destino 0.0.0.0, por lo que tomará este destino.

1. **Un paquete destinado a zoltar.redes.upv.es.**

Un paquete destinado a zoltar.redes.upv.es tendrá una dirección ip destino de 158.42.180.62, al aplicarle la máscara de red más larga que es 255.255.254.0, esta coincide con el destino 158.42.180.0 por lo que tomara este destino.

**Interpreta los resultados teniendo en cuenta el campo Pasarela (router de salida de la red o entrega directa de origen a destino).**

**Ejercicio 10**

**1) Visualiza la tabla de encaminamiento de tu ordenador (orden route -n).**

**2) Anota la dirección del router de salida de la red. Nos referiremos a ella como dir\_IP\_de\_tu\_router.**

158.42.181.250

**3) Elimina la entrada de la dirección de red por defecto (sudo route del default) y visualiza la tabla de encaminamiento.**

**4) Intenta acceder a un destino fuera de tu red IP. Por ejemplo, mediante la orden**

**ping -c 2 www.upv.es**

**Explica que pasa.**

Al eliminar el dafault elimina la interfaz hacia el router por lo que no se encuentra un destino al que se le pueda enviar los paquetes que envía la orden ping

**5) Vuelve a probar el ping empleando ahora la dirección destino (que anotaste en el ejercicio 4b) en vez del nombre del servidor.**

Igual

**6) Intenta acceder a un destino que esté en la misma red IP que tu ordenador. Por ejemplo, mediante la orden ping -c 2 158.42.180.62, (es la IP de zoltar.redes.upv.es), o haciendo ping al ordenador de algún compañero (158.42.180.<puesto>).**

**7) Restaura la línea de la tabla de encaminamiento que habías eliminado (sudo route add default gw dir\_IP\_de\_tu\_router). Al ejecutar la orden puede que el sistema dé un mensaje de aviso porque no tiene acceso al DNS, pero no tiene mayor importancia.**

**8) Comprueba el estado de la tabla de encaminamiento. Debe ser el mismo que era antes de eliminar la ruta. Verifica también que ahora sí funcionan los pings a computadores fuera de tu red.**

**Ejercicio 11 Lo ideal para comprobar cómo afecta al encaminamiento la entrada local sería eliminar de la tabla la entrada que corresponde a la red IP de tu equipo, pero no está permitido. Así es que vamos a emplear un truco para conseguir algo similar, la mantendremos en la tabla, pero impediremos su uso.**

**1) Ejecuta la orden sudo route add -net 158.42.180.0 netmask 255.255.254.0 reject.**

**2) Visualiza el estado de la tabla de encaminamiento (route -n)**

**3) Intenta acceder a un destino de tu red IP. Por ejemplo, mediante la orden ping -c 2 zoltar.redes.upv.es.**

**4) Intenta acceder a destinos fuera de tu red IP. Por ejemplo,**

**ping -c 2 www.upv.es**

**ping -c 2 www.google.es.**

**5) Comprueba lo que has observado y observa a qué se debe.**

**6) Restaura el estado original de la tabla de encaminamiento:**

**sudo route del -net 158.42.180.0**

**7) Comprueba el estado de la tabla de encaminamiento. Debe ser el que había antes de eliminar la ruta.**

Pin /dir ip/