

Práctica 1: Configuración de TCP/IP en Windows 7 y Linux

1. Introducción

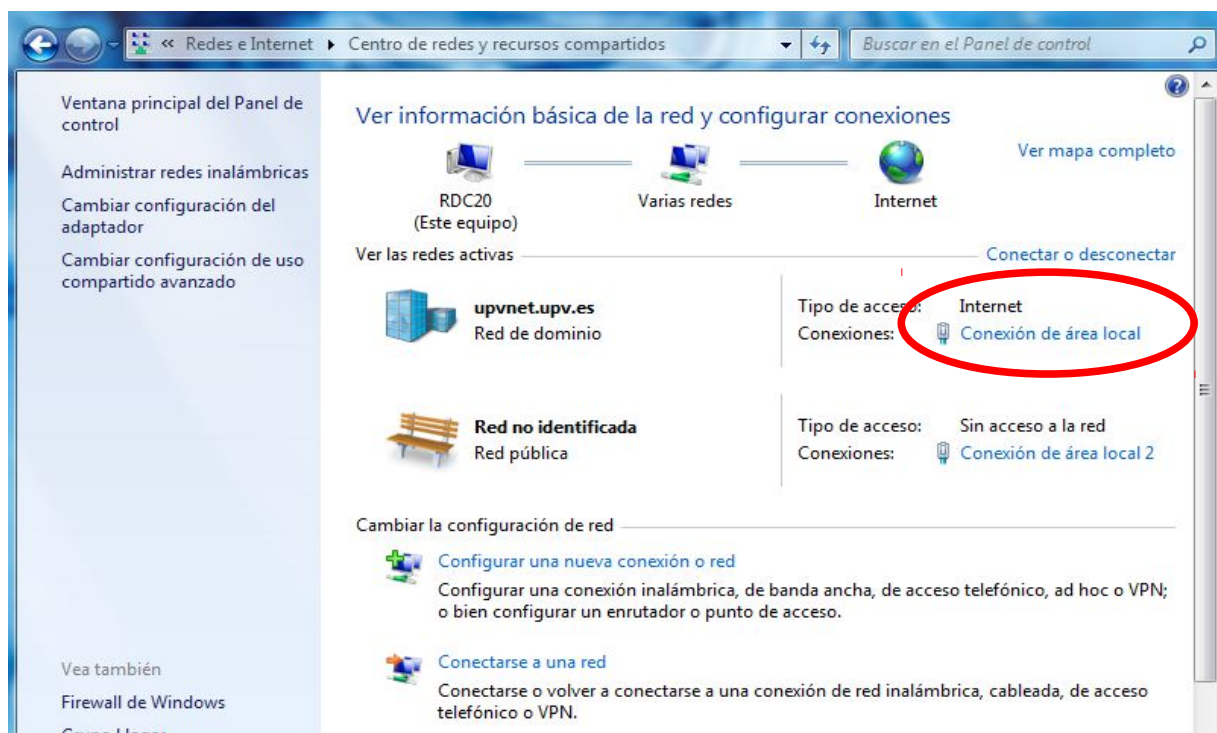
Esta práctica está dedicada a revisar el procedimiento básico de instalación y configuración de los protocolos TCP/IP en Windows 7 y Linux. Se muestra el uso de algunas herramientas útiles a la hora de resolver problemas con estos protocolos: configurar el software de red, verificar su funcionamiento y ajustar los parámetros relacionados con TCP/IP.

2. Configuración de TCP/IP en Windows 7

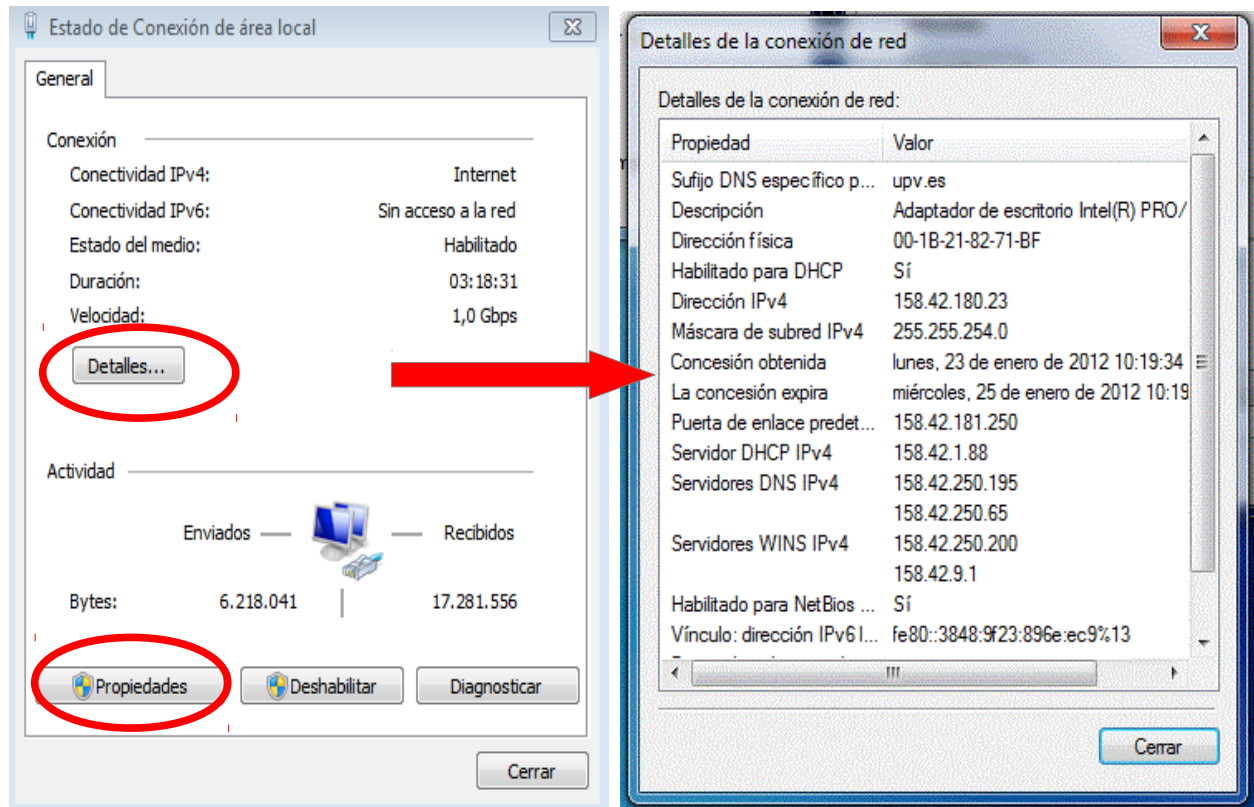
Para poder realizar este apartado debes arrancar tu ordenador en la partición de Windows 7, y utilizar para el acceso el nombre de usuario y la contraseña de tu cuenta de la UPV (dominio ALUMNO).

Para utilizar los protocolos TCP/IP desde una máquina Windows 7 conectada a una red de área local (Ethernet en nuestro caso) es necesario tener instalada una tarjeta adaptadora o NIC (*Network Interface Adapter*). En nuestros computadores esta tarjeta ya está instalada y configurada. Para ver la configuración de la tarjeta adaptadora Ethernet:

1. Pulsa el botón **Inicio**, y después **Panel de control, Redes e Internet**. En el apartado **Centro de redes y recursos compartidos** selecciona el enlace **Ver el estado y las tareas de Red**.
2. Como verás, aparecen dos conexiones de área local. Sólo nos interesa la primera (ver figura), que es la que proporciona acceso al resto de Internet. Haz clic sobre el enlace **Conexión de área local**.

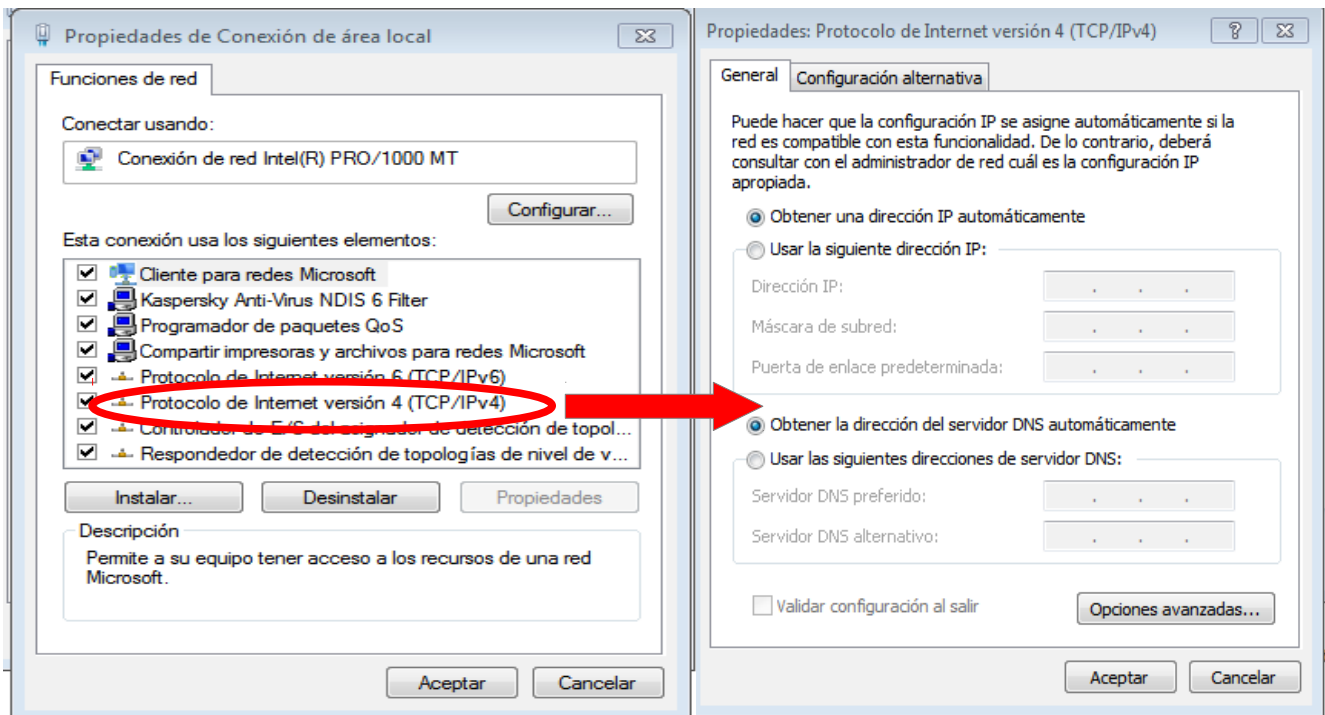


3. Se abrirá la ventana de **Estado de Conexión de área local**. En ella, al pulsar el botón **Detalles**, podemos ver las principales propiedades de la conexión de red asociada al adaptador: dirección física del adaptador de red, dirección IP asociada a ese interfaz, máscara de red, etc.



Además del adaptador de red, para poder utilizar aplicaciones Internet es necesario que estén instalados los protocolos TCP/IP. De nuevo, estos protocolos ya están instalados en nuestros ordenadores. Para comprobarlo podrías seguir los pasos siguientes (**si tuvieras los permisos necesarios**):

4. Desde la ventana **Estado de Conexión de área local** (que se muestra en el gráfico anterior a la izquierda), si se pulsa sobre el botón **Propiedades**, aparece la ventana de **Propiedades de Protocolo Internet (TCP/IP)** (página siguiente), donde se indican algunos datos relativos al funcionamiento de estos protocolos. Por motivos de seguridad al pulsar **el botón de Propiedades** se solicita usuario y contraseña, y no estamos autorizados. No es demasiado importante ya que la información que normalmente obtendremos es la que aparece en la figura de la página siguiente. Como podemos observar, la configuración más habitual consiste en que la mayoría de los parámetros necesarios para el funcionamiento de TCP/IP (¡incluyendo la propia dirección IP!) no se configuran manualmente, sino que se obtienen automáticamente durante el proceso de arranque de la máquina. Esto es posible gracias al protocolo DHCP (*Dynamic Host Configuration Protocol*) que permite a un cliente solicitar al servidor una dirección IP. Este protocolo, de empleo frecuente, se estudiará en una práctica posterior durante este cuatrimestre. Además de la dirección IP, el servidor DHCP proporciona información adicional necesaria para el funcionamiento de los protocolos TCP/IP (dirección IP del servidor DNS, dirección IP del router, etc.).



2.1 La orden ipconfig

Una vez que los protocolos TCP/IP están instalados, la orden **ipconfig** (se ejecuta desde una ventana de DOS -Símbolo del sistema- a la que puede accederse desde el menú “Accesorios”) proporciona información sobre la configuración de la red en nuestra máquina (para cada uno de los adaptadores de red instalados).

El formato de la orden es el siguiente:

W:\>**ipconfig /?**

```
USO: ipconfig [/allcompartments] [/? | /all |
        /renew [adaptador] | /release [adaptador] |
        /renew6 [adaptador] | /release6 [adaptador] |
        /flushdns | /displaydns | /registerdns |
        /showclassid adaptador |
        /setclassid adaptador [id._clase] |
        /showclassid6 adaptador |
        /setclassid6 adaptador [id._clase] ]
```

donde:

adaptador Nombre de conexión (se permiten los caracteres comodín * y ?; consulte los ejemplos)

Opciones

/? Muestra este mensaje de ayuda.
/all Muestra toda la información de configuración.
/release Libera la dirección IPv4 para el adaptador especificado.
/release6 Libera la dirección IPv6 para el adaptador especificado.
/renew Renueva la dirección IPv4 para el adaptador especificado.

| | |
|---------------------|---|
| /renew6 | Renueva la dirección IPv6 para el adaptador especificado. |
| /flushdns | Purga la caché de resolución de DNS. |
| /registerdns | Actualiza todas las concesiones DHCP y vuelve a registrar los nombres DNS |
| /displaydns | Muestra el contenido de la caché de resolución de DNS. |
| /showclassid | Muestra todos los Id. de clase DHCP permitidos para el adaptador. |

Tecleando simplemente **ipconfig** obtenemos información para cada uno de los adaptadores de red instalados en nuestro ordenador sobre:

- **Dirección IPv4 e IPv6:** direcciones IP asignadas a nuestra máquina, en nuestro caso de forma dinámica mediante el protocolo DHCP.
- **Máscara de subred:** indica qué parte de la dirección IPv4 identifica la red, y qué parte identifica al computador (a un adaptador de red). La red de la UPV globalmente tiene asignado el bloque de direcciones IPv4 158.42.0.0/16, que se ha desglosado en una serie de subredes. La máscara de subred (255.255.254.0) indica que, en el caso de la subred del laboratorio, los 23 bits más significativos de cada dirección IPv4 (bits a 1 en la máscara) deben considerarse identificador de red, y los 9 últimos (bits a 0 en la máscara) identificador de *host*.
- **Puerta de enlace predeterminada:** dirección IP del router que conecta nuestra subred con el resto de la red de la UPV y con el exterior (Internet).

Si ejecutamos la orden **ipconfig /all** obtenemos información adicional, entre la cual destaca:

- **Dirección física:** es la dirección física que corresponde a la tarjeta adaptadora de red (Ethernet en nuestro caso) que está instalada en nuestro computador y nos permite el acceso a la red.
- **Servidores DNS:** la dirección IP de la(s) máquina(s) que realiza(n) las traducciones de nombres a direcciones IP (servidor de nombres).
- **Servidor DHCP:** dirección IP de la máquina que nos ha asignado la dirección IP y la mayoría de parámetros que aparecen en esta ventana.
- **Concesión obtenida (la concesión expira):** fecha en la que fue obtenida (caducará) la dirección IP actual. Aplicable únicamente en el caso de información obtenida por DHCP.

Las órdenes **ipconfig /release** e **ipconfig /renew** permiten liberar y renovar la dirección IPv4 obtenida mediante DHCP (se verán en la práctica de DHCP).

Ejemplos:

- > ipconfig /renew ... Renueva todos los adaptadores.
- > ipconfig /renew EL* ... Renueva cualquier conexión cuyo nombre comience con EL.
- > ipconfig /release *Con* ... Libera todas las conexiones coincidentes, por ejemplo: "Conexión de área local 2".

Ejercicio 1

Ejecuta la orden **ipconfig /all** y completa la información siguiente relativa a la “Conexión de área local” que tenga asociada una dirección IP que empiece por “158.42” (la conexión 2¹ no nos interesa):

| | |
|--|------------------------------|
| Dirección física del adaptador Ethernet conexión de área local | 10:C3:7B:94:E5:1F |
| Dirección IPv4 | 158.42.180.7 |
| Máscara de subred | 255.255.254.0 |
| Dirección IP del router (puerta de enlace) | 158.42.181.250 |
| Servidores DNS | 158.42.250.195 158.42.250.65 |
| Servidor DHCP | 158.42.1.8 |

Según la información obtenida:

- ¿Cuál es la dirección IP de la red a la que está conectado tu equipo? 158.42.180.0
- Los servidores DNS y DHCP, ¿están en la misma subred que el computador de prácticas? ¿Por qué? No, ya que su ip no esta en el rango de nuestra mascara de subred. porque los bits del identificador de red no coinciden

Ejercicio 2

Comprueba el contenido de la caché DNS mediante la orden **ipconfig /displaydns**. Anota en la tabla los valores de uno de los registros que aparecen que sea de tipo 1:

| | |
|-------------------------------------|-------------------------|
| Nombre registro | discasvr16.disca.upv.es |
| Valor registro (un registro <host>) | 158.42.53.97 |

Mira las diferencias con algún registro del tipo 28. es un host con ipv6

2.2 La orden ping

Mediante la orden **ping** (que se ejecuta desde una ventana DOS) se obtiene una estimación del tiempo de ida y vuelta de un paquete (RTT, *Round Trip Time*), desde la estación donde se ejecuta la orden a la estación destino que se especifica. El funcionamiento de la orden **ping** se basa en el uso de mensajes ICMP de eco, que se estudiarán en una práctica posterior.

Ejemplo:

```
W:\>ping www.upc.es
```

```
Haciendo ping a www.upc.es [147.83.2.135] con 32 bytes de datos:
```

```
Respuesta desde 147.83.2.135: bytes=32 tiempo=31ms TTL=110
```

```
Respuesta desde 147.83.2.135: bytes=32 tiempo=31ms TTL=110
```

```
. . .
```

¹ Puede que en algunos de los equipos del laboratorio la conexión 2 se haya numerado como conexión 3.

La orden **ping** admite un serie de opciones, la única que nos interesa de momento se muestra a continuación:

ping [-n cantidad] destino

-n cantidad número de solicitudes de eco a enviar.

Esta orden se analizará con detalle en la práctica destinada al estudio del protocolo ICMP. Hasta ese momento la emplearemos únicamente con el propósito de saber si un destino determinado puede alcanzarse o no a través de la red y cuál es su dirección IP.

2.3 La orden tracert

La orden **tracert** (se ejecuta desde una ventana DOS) permite conocer el camino (secuencia de routers) que debe atravesar un paquete para llegar desde la estación origen a la estación destino. Se basa en el empleo de mensajes ICMP y, por lo tanto, también se estudiará en la práctica destinada a este protocolo.

2.4 La orden netstat

La orden **netstat** (desde **Símbolo del sistema**) ofrece diversa información sobre el estado y estadísticas de los protocolos de red. Se pueden obtener datos sobre los principales sucesos Ethernet, IP, ICMP, UDP y TCP. El formato de la orden, que puedes ver tecleando **netstat -h**, es el que se muestra a continuación:

netstat [-a] [-e] [-n] [-s] [-p proto] [-r]

-a Muestra todas las conexiones y puertos escucha.

-e Muestra estadísticas Ethernet. Se puede combinar con **-s**.

-n Muestra números de puertos y direcciones en formato numérico.

-p proto Muestra conexiones del protocolo especificado por **proto**; que puede ser TCP, UDP, TCPv6 o UDPv6. Si se usa con la opción **-s** para mostrar estadísticas por protocolo, **proto** puede ser TCP, UDP, TCPv6 o UDPv6.

-r Muestra el contenido de la tabla de rutas.

-s Muestra estadísticas por protocolo. De forma predeterminada, se muestran para los protocolos IP, IPv6, TCP, UDP e IP; se puede utilizar la opción **-p** para especificar un subconjunto de los valores predeterminados.

Mediante la orden **netstat -r** obtenemos información sobre la tabla de encaminamiento (produce la misma salida que la orden **route print**).

Cuando hay que encaminar un datagrama, para averiguar la ruta se sigue el proceso siguiente:

1. Para cada línea de la tabla de encaminamiento, se realiza un AND lógico entre la **dirección IP destino** del datagrama y la **máscara de red**. IP compara el resultado con la **Red destino** y marca todas las rutas en las que se produce coincidencia.
2. De la lista de rutas coincidentes IP selecciona la ruta que tiene más bits en la máscara. Esta es la ruta más específica y se conoce como la **ruta de máxima coincidencia** (*longest matching*).
3. Si hay varias rutas de máxima coincidencia, se usa la ruta con menor **métrica**. Si hay varias con la misma métrica se usa una cualquiera de ellas.

Ejercicio 3:

Visualiza la tabla de encaminamiento (apartado IPv4) del ordenador en el que estás trabajando. Anota las IPs de los destinos y analiza qué ruta de la tabla se seleccionaría para:

- a) Un paquete destinado a zoltar.redes.upv.es. 158.42.180.0 => interfaz 158.42.180.7
 b) Un paquete destinado a www.upv.es. 158.42.181.250 => interfaz 158.42.180.7
 c) Un paquete destinado a www.usc.edu. 158.42.181.250 => interfaz 158.42.180.7

Interpreta los resultados obtenidos, ¿por qué se obtienen diferentes rutas?

porque zoltar esta en la misma red que nosotros sin embargo los otros estan en otra red

Ejercicio 4:

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:

| | Recibidos | Enviados |
|---|-----------|----------|
| Paquetes de unidifusión (unicast) | 28423 | 3177848 |
| Paquetes no de unidifusión (no unicast) | 49375 | 1530 |
| Descartados | 0 | 0 |
| Errores | 58 | 0 |

Comprueba también la ejecución de **netstat -es**. Indica las diferencias que observas entre el formato de salida de las dos ejecuciones. [este comando indica las estadísticas de cada protocolo](#)

Ejercicio 5:

La orden **netstat -sp IP** produce estadísticas sobre el tráfico IP. Ejecuta esta orden y comprueba los valores de los conceptos indicados en la tabla siguiente:

| | Cantidad |
|---------------------------------------|----------|
| Paquetes recibidos | 12982 |
| Errores de encabezado recibidos | 0 |
| Errores de dirección recibidos | 1051 |
| Datagramas reenviados | 0 |
| Protocolos desconocidos recibidos | 1 |
| Datagramas correctamente fragmentados | 0 |

Ejercicio 6:

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 comprueba los valores de los conceptos indicados en la tabla siguiente:

| | Cantidad |
|-------------------------------|----------|
| Activos abiertos | 191 |
| Pasivos abiertos | 49 |
| Intentos de conexión erróneos | 229 |
| Conexiones actuales | 1 |

Puertos abiertos por nosotros para conexión
puertos abiertos a la espera de conexión

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

La orden **netstat** sin argumentos ofrece información sobre las conexiones activas en nuestra máquina. Si se utiliza con la opción **-a**, además de la información anterior se indica también la relación de puertos TCP y UDP en los que hay alguna aplicación escuchando (dispuesta a aceptar conexiones TCP o datagramas UDP).

2.5 La orden arp

Esta orden también resulta de mucha utilidad para la configuración y diagnóstico de problemas en redes. Para analizarla de forma detallada, se dedicará una práctica al protocolo ARP más adelante durante este cuatrimestre.

3. Configuración de TCP/IP en Linux

Para este apartado debes arrancar en la partición “Practicas RedLocal”. Tu profesor te indicará la contraseña necesaria.

En Linux encontramos las mismas órdenes que acabamos de estudiar dentro del entorno Windows 7, en particular:

- Orden **tracert**, equivale a la orden **tracert** de Windows
- Orden **arp**, equivale a la orden de Windows del mismo nombre.
- Orden **netstat**, equivalente a la que hemos estudiado para Windows.

Por ello, aquí sólo revisaremos algunas diferencias significativas entre los dos sistemas operativos.

3.1 La orden ifconfig

La orden **ifconfig**, que puedes ejecutar desde un terminal de red, permite configurar y obtener información sobre la configuración de red. Utilizando esta orden con las opciones adecuadas podemos configurar todo el software de TCP/IP. En nuestro caso el software ya está instalado y, además, no tenemos permisos de administración para modificar los parámetros. Así que nos limitaremos a inspeccionar la información mediante **ifconfig**.

Si ejecutamos **ifconfig** seguido del nombre de una interfaz (**eth1** en nuestro caso) obtendremos información sobre la configuración de ésta. Si se ejecuta sin parámetros, presenta las características de todas las interfaces que se hayan configurado. A modo de ejemplo, la consulta de la configuración de la interfaz Ethernet **eth0**² sería:

```
#alumno@rdc20:~$ ifconfig eth0
eth1      Link encap:Ethernet  Hwaddr 00:04:75:C8:F0:86
inet addr:158.42.180.20 Bcast:158.42.181.255
        Mask:255.255.254.0
inet6 addr: fe80::12c3:7bff:fe94:e54e/64 Alcance:Enlace
ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
Paquetes RX:88220 errores:0 perdidos:0 overruns:0 frame:0
Paquetes TX:50640 errores:0 perdidos:0 overruns:0 carrier:0
colisiones:0 long.colatX:1000
Bytes RX:107112019 (107.1 MB)  TX bytes:52937680 (52.9 MB)
```

² Puede ocurrir que en algunos puestos del laboratorio la información similar a la que se muestra corresponda a la interfaz 1 (eth1) en lugar de a la 0 (eth0).

Los campos **MTU** y **Metric** informan sobre los valores actuales de la MTU (Unidad Máxima de Transferencia) y de la métrica para una interfaz dada. Algunos sistemas operativos usan el valor **Metric** para calcular el coste de una ruta. Linux no usa este valor por el momento, pero lo define por razones de compatibilidad.

Las líneas **RX packets** y **TX packets** dan información sobre de los paquetes recibidos o transmitidos sin errores, del número de errores ocurridos, de cuántos paquetes han sido descartados, seguramente por memoria insuficiente, y cuántos se han perdido por desbordamiento, condición que ocurre cuando la recepción de paquetes es demasiado rápida y el sistema operativo es incapaz de dar servicio al paquete anterior antes de la llegada del nuevo paquete. Los nombres de los campos que genera **ifconfig** coinciden más o menos con los parámetros con los que se puede ejecutar esta orden.

A continuación tenemos una lista de algunos parámetros reconocidos por **ifconfig** (puedes visualizar todas las opciones disponibles mediante la orden **man ifconfig**). Las opciones que simplemente activan alguna característica pueden usarse para desactivarla anteponiendo un guión (-).

La utilización de estos parámetros nos permitiría cambiar la configuración de la interfaz (si tuviésemos los privilegios necesarios).

- **up**: marca la interfaz como "up" o activa, es decir, disponible para que sea usada por el nivel IP. (Esta opción corresponde a los indicadores UP RUNNING).
- **down**: marca la interfaz como "down" o inactiva, es decir, inaccesible al nivel IP.
- **netmask máscara**: asigna una máscara de subred a una interfaz.
- **metric número**: puede ser usada para asignar un valor de métrica a la tabla de encaminamiento creada para la interfaz.
- **mtu bytes**: fija la unidad máxima de transferencia, o lo que es lo mismo, el máximo número de octetos que la interfaz es capaz de manejar en una única transacción. Para Ethernet, la MTU toma el valor 1500 por defecto.
- **arp**: esta opción es específica de redes de difusión como Ethernet. Permite el uso de ARP, el Protocolo de Resolución de Direcciones, para detectar la dirección física de las máquinas conectadas a la red. Para redes de difusión, esta opción es habilitada por defecto. **ifconfig** avisa que ARP ha sido inhabilitado mediante el indicador NOARP. **-arp** inhabilita el uso de ARP para esta interfaz.
- **promisc**: pone la interfaz en modo promiscuo. En una red de difusión, esto hace que la interfaz reciba todos los paquetes, independientemente de si están dirigidos a ella o no. Esto permite el análisis del tráfico de red mediante utilidades como filtros de paquetes. Se trata de una buena técnica para localizar problemas de red que de otra forma resultan difíciles. Por otro lado, esto también posibilita ataques, permitiendo al atacante analizar el tráfico de la red en busca de claves u otras cosas peligrosas. (Esta opción corresponde al indicador PROMISC). **-promisc** desactiva el modo promiscuo.

Ejercicio 7:

Ejecuta la orden **ifconfig eth0³** y, basándote en la descripción anterior, analiza la información obtenida. [nuestra ip](#), [la puerta de enlace](#), [la mascara de red](#), [la mac ...](#)

³Recuerda que en tu puesto podría ser la eth1.

3.2 La orden netstat

La orden **netstat** tiene un funcionamiento muy similar al descrito para Windows 7. Describiremos únicamente la opción de esta orden que permite consultar la tabla de encaminamiento para ver las diferencias de formato de ambas tablas.

Si se ejecuta **netstat** usando el indicador **-nr**, se puede ver la información de la tabla de encaminamiento del núcleo (produce una salida muy similar a la orden **route**). Por ejemplo:

```
alumno@rdc20:~$ netstat -nr
```

Tabla de rutas del núcleo

| Destino | Pasarela | Genmask | Indic | MSS | Ventana | irrt | Interfaz |
|--------------|----------------|---------------|-------|------|---------|------|----------|
| 0.0.0.0 | 158.42.181.250 | 0.0.0.0 | UG | 1500 | 0 | 0 | eth0 |
| 158.42.180.0 | 0.0.0.0 | 255.255.254.0 | U | 1500 | 0 | 0 | eth0 |
| 169.254.0.0 | 0.0.0.0 | 255.255.0.0 | U | 1000 | 0 | 0 | eth1 |

La segunda columna de la salida producida por **netstat** informa sobre los routers a los que apunta la información de encaminamiento. Si una ruta no usa router, el programa indica la dirección 0.0.0.0. La tercera columna muestra el nivel de generalización de una ruta. Dada una dirección IP, el núcleo recorre la tabla registro a registro haciendo un AND lógico de la dirección IP destino y la máscara de nivel de generalización (**Genmask**) antes de compararla con el destino que muestra dicho registro (**Destino**). La ruta por defecto tiene máscara 0.0.0.0. Al igual que ocurre en windows, de todas las rutas en las que se produzca coincidencia con el destino se selecciona la que tenga más bits a uno en la máscara.

La cuarta columna muestra varios indicadores que describen la ruta:

- G La ruta utiliza un router.
- U La interfaz está activa.
- H Esta interfaz permite el acceso a una sola máquina.

Las columnas **MSS**, **Ventana** e **irrt** indican los valores iniciales de algunos parámetros que se utilizan en las conexiones TCP que se establecen a través de esta ruta. La columna **Interfaz** indica a través de qué interfaz se accede a estas rutas. En nuestro caso solo estamos interesados en las rutas que se establecen a través de la interfaz Ethernet (**eth0**).

Ejercicio 8:

Utiliza la orden **netstat -nr** y rellena la tabla para las rutas relacionadas con la interfaz **eth0**:

| Destino | Pasarela (Router) | Máscara de red |
|--------------|-------------------|----------------|
| 0.0.0.0 | 158.42.181.250 | 0.0.0.0 |
| 158.42.180.0 | 0.0.0.0 | 255.255.254.0 |
| 169.254.0.0 | 0.0.0.0 | 255.255.0.0 |

Analiza qué ruta de la tabla se seleccionaría para:

- a) Un paquete destinado a www.upv.es 158.42.181.250
- b) Un paquete destinado a zoltar.redes.upv.es 0.0.0.0

Interpreta los resultados teniendo en cuenta el campo **Pasarela** (router de salida de la red o entrega directa de origen a destino). Compara los resultados con los que obtienes al ejecutar la misma orden sin el parámetro **-n** (**netstat -r**).

uno dice la ip de la puerta de enlace y el otro el nombre

3.3 La orden route

Esta orden permite además de ver el contenido de las tablas de encaminamiento, modificarlo, añadiendo o eliminando entradas de la misma. Para esto último se requiere permisos de administrador, en nuestro caso emplearemos las órdenes anteponiendo el **sudo**.

La opción **-n** solicita que no se traduzcan las direcciones IP a nombres de dominio, y las opciones **add** y **del** permiten añadir o eliminar entradas, respectivamente. Puedes ver una ayuda detallada consultando el man (man route).

```
alumno@rdc20:~$ route -n
```

Tabla de rutas IP del núcleo

| Destino | Pasarela | Genmask | Indic | Métric | Ref | Uso | Interfaz |
|--------------|----------------|---------------|-------|--------|-----|-----|----------|
| 0.0.0.0 | 158.42.181.250 | 0.0.0.0 | UG | 0 | 0 | 0 | eth0 |
| 158.42.180.0 | 0.0.0.0 | 255.255.254.0 | U | 0 | 0 | 0 | eth0 |
| 169.254.0.0 | 0.0.0.0 | 255.255.0.0 | U | 1000 | 0 | 0 | eth1 |

En este apartado emplearemos la posibilidad de modificar las tablas para ver cómo afectan las entradas más importantes al encaminamiento de los paquetes. En particular, analizaremos dos entradas de la tabla. La que indica cómo enviar paquetes a destinos que están en la misma red que nuestro computador, y la entrada por defecto, que nos permite alcanzar el resto de Internet.

Ejercicio 9:

- 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**). Visualiza la tabla de encaminamiento.

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

ping -c 2 www.upv.es

Explica que pasa. [que nuestro pc no sabe como encaminar el paquete fuera de la red debido a que no tiene el registro en la tabla de encaminamiento](#)

Vuelve a probar el ping empleando ahora la dirección destino (anotada en el ejercicio 3b).

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.

- 4) 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.
- 5) Comprueba el estado de la tabla de encaminamiento. Debe ser el mismo que era antes de eliminar la ruta.

Ejercicio 10:

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

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

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

Intenta acceder a destinos fuera de tu red IP. Por ejemplo, **ping -c 2 www.upv.es** y **ping -c 2 www.google.es**. que hemos eliminado el registro de la tabla de encaminamiento ha nuestra red

Explica lo que has observado y a qué se debe.

- 2) Restaura el estado original de la tabla de encaminamiento:

sudo route del -net 158.42.180.0 netmask 255.255.254.0 reject

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