

PRÁCTICA 5: CONFIGURACIÓN DE REDES TCP/IP (I)

Objetivo del laboratorio:

Aprender como conocer las características TCP/IP de un sistema.

Breve descripción:

Utilizando los ficheros y comandos que se describen en la primera parte de la documentación, se deben hacer los ejercicios de la segunda.

Primera parte: Descripción de ficheros y comandos

Ficheros

Todos ellos son ficheros Unix BSD. En otros sistemas Unix suelen estar ubicados en otros puntos, pero se mantienen links hacia las posiciones aquí indicadas para mantener compatibilidad con BSD. En Windows no siempre hay ficheros equivalentes. A menudo, la información que en Unix dan estos ficheros, debe conseguirse en Windows mediante el comando *winipcfg*.

/etc/hosts

Lista de direcciones IP y nombres de máquinas que les corresponden. En general, sólo contiene entradas para su máquina y tal vez alguna otra "importante", como servidores de nombres o encaminadores. El servidor de nombres de nuestra máquina lo usa para proporcionar a otras máquinas traducción de nuestro nombre a nuestra dirección IP. En este fichero siempre aparece una línea para el *loopback* (dirección 127.0.0.1).

/etc/networks

Contiene las direcciones de red que aparecen en la tabla de encaminamiento. No es la única fuente de información para construir esa tabla. Nuestro sistema no lo usa para ello.

/etc/netmasks

Contiene las máscaras de red de las redes conocidas.

/etc/ethers

Contiene las relaciones entre nombres de host y direcciones ethernet. Este fichero sólo es usado si nuestra máquina debe actuar como servidora de red para máquinas sin disco, para contestar a peticiones RARP.

/etc/protocols

Nombres y números identificadores de los protocolos implementados

/etc/services

Puerto que corresponde a cada aplicación.

Comandos

Los comandos que se dan a continuación corresponden a un sistema Unix, pero también los tienes disponibles en Windows (excepto el primero). Para conocer más sobre ellos, así como las opciones que ofrecen, usa el manual interactivo (`man comando`).

hostname

Da el nombre de nuestra máquina.

ping

Programa (no es un comando) usado para saber si un nodo está accesible o no. Para ello envía un mensaje *echo request* de ICMP.

arp

Muestra la situación actual de nuestra tabla ARP. También puede usarse para actualizar dicha tabla. Su nombre proviene del protocolo (*address resolution protocol*).

Segunda parte: Ejercicios

Haz los ejercicios con asterisco tanto sobre servidor.redes.uhu.es como sobre el PC. Si la respuesta es la misma en ambos casos (el método) simplemente indícalo. En todos los ejercicios hay que indicar cómo se ha llegado a la respuesta.

1) En tu PC, ¿dónde se sitúa el fichero que hace las funciones del fichero `/etc/services` de Unix? ¿Y los equivalentes a `/etc/protocols` y `/etc/networks` ?

2*) ¿Cuál es la dirección IP de tu máquina? `/etc/hosts` `C:\Windows\Hosts.sam`

`ifconfig -a`
PC: `windowsipconfig`

3*) ¿Qué máscara se aplica a tu máquina?

`/etc/netmasks`
`ifconfig -a`
PC: `windowsipconfig`

4*) ¿Cuáles son tus identificadores de red y máquina?

Se ve a través de la máscara y la dirección IP.

5*) ¿Qué contiene la tabla ARP de tu máquina? (no escribas la tabla completa, basta con decir cómo la ves)

arp -a

6*) ¿Cuál es la dirección ethernet de tu ordenador?

arp -a | grep nombre_maquina, o bien ifconfig -a (también con ifconfig le0, si conocemos las interfases).

PC: winipcfg

7*) ¿Cómo puedes saber cuál es la dirección física de otra máquina de tu misma red? Por ejemplo, ¿cuál es la dirección física de la máquina 10.0.0.2?

arp nombre_maquina. Si no aparece, hacer ping y de nuevo arp.

8*) ¿Cómo puedes saber si un ordenador (por ejemplo servidor_redes) está en tu red?

Tienes que obtener su dirección IP, y mirar en esa dirección sin utilizar nslookup; Una forma de obtener la dirección IP es a través de ping -s

9*) ¿Cómo puedes saber qué puerto corresponde a una aplicación?

cat /etc/services | grep nombre_aplicación. También con netstat -a, pero sólo aparecerán los que están activos.

PC: Mirar en C:\Windows\Services

10*) ¿Cuánto tiempo necesitará un datagrama para llegar a su destino desde tu máquina? Calcula, por ejemplo, el tiempo necesario, más o menos, para alcanzar la máquina www.uhu.es.

ping ó ping -s

11*) ¿Qué camino sigue el datagrama anterior para llegar a su destino?

Traceroute / ping -sRv www.uhu.es

PC: Tracert / ping -r

12) Calcula, usando ping, la tasa de errores del camino entre dos ordenadores.

ping -I 1 dest tam num_env. Conviene ejecutar en paralelo varias veces.

PRÁCTICA 6: CONFIGURACIÓN DE REDES TCP/IP (II)

Objetivo del laboratorio: Aprender como conocer las características TCP/IP de un sistema.

Máquinas: servidor_redes y PC's de laboratorio.

Breve descripción:

Utilizando los ficheros y comandos que se describen en la primera parte de la documentación, se deben hacer los ejercicios de la segunda.

Bibliografía:

Manual on-line de Unix (comando *man*).

Primera parte: Descripción de comandos

Además de los comandos que se vieron en el primer laboratorio TCP/IP, son útiles los que se dan a continuación. Recuerda que corresponden a un sistema Unix, aunque algunos también están disponibles en Windows. Para conocer más sobre ellos, así como las opciones que ofrecen, usa el manual interactivo.

ndd

Se usa para consultar los parámetros de configuración de cualquier dispositivo del sistema. Entre esos dispositivos están *tcp* (referenciado como */dev/tcp*) y *udp* (referenciado como */dev/udp*). Para ver cuáles son los parámetros que el sistema define para un dispositivo cualquiera, como por ejemplo los puertos. Un ejemplo es el *tcp*, y para ello hay que ejecutar ***ndd /dev/tcp \?***

Este comando no está disponible en Windows.

ifconfig

Da información básica sobre la configuración de los interfaces. Se usa para detectar problemas con las direcciones IP, máscaras de subred, o direcciones de broadcast. Siendo superusuario, se usa para configurar los interfaces, activar o desactivar arp, o alterar el costo asociado a un interfaz en la tabla de encaminamiento.

Lo más aproximado en Windows es *winipcfg*.

netstat

Es el comando más usado para control de red. Puede ofrecer información sobre la tabla de encaminamiento, estado de los interfaces, actividad en cada puerto, contenido de la tabla ARP, etc.

route

Usado para ver y actualizar la tabla de encaminamiento. Sólo puede usarse con privilegios de superusuario.

Ejemplo:

/sbin/route

```
Kernel routing table
Destination Gateway Genmask Flags MSS Window Use Iface
localnet * 255.255.255.0 U 1500 0 23 eth0
loopback * 255.0.0.0 U 3584 0 2 lo
default si3101.si.ehu.es * UG 1500 0 19 eth0
```

traceroute

Sirve para hacer un seguimiento del camino seguido por los datagramas a través de la red hasta llegar a su destino. No lo tenemos disponible en servidor_redes, pero parte de su funcionalidad puede conseguirse con ping. En Windows hay una versión del mismo llamada *tracert*.

Ejemplo:

traceroute izar.eusnet.org

```
traceroute to 194.224.110.2 (194.224.110.2), 30 hops max, 40 byte packets
1 si3101.si.ehu.es (158.227.112.1) 1.316 ms 1.702 ms 2.778 ms
2 158.227.194.224 (158.227.194.224) 3.747 ms 3.591 ms 3.245 ms
3 S4-4.EB-Bilbao1.red.rediris.es (130.206.210.1) 4.982 ms 5.147 ms 4.396 ms
4 A1-0-6.EB-Madrid1.red.rediris.es (130.206.224.21) 13.108 ms 11.319 ms 10.832 ms
5 A1-0-1.EB-Madrid0.red.rediris.es (130.206.224.69) 12.726 ms 12.031 ms 12.295 ms
6 Ibertnet-2.red.rediris.es (130.206.192.238) 118.191 ms 72.564 ms 80.904 ms
7 194.179.3.130 (194.179.3.130) 147.024 ms 160.054 ms 228.512 ms
8 194.179.16.156 (194.179.16.156) 853.409 ms 814.393 ms 582.425 ms
9 194.224.110.2 (194.224.110.2) 1282.63 ms 965.919 ms *
```

Segunda parte: Ejercicios

Haz los ejercicios con asterisco tanto sobre servidor_redes como sobre el PC. Si la respuesta es la misma en ambos casos (el método) simplemente indícalo. En todos los ejercicios hay que indicar cómo se ha llegado a la respuesta. Apunta tus respuestas en hoja aparte, para ser entregadas al final de la sesión.

1) ¿Cuál es el mínimo número de puerto libre (denominados *no private* en Unix) en servidor_redes?

`ndd /dev/tcp tcp_smallest_nonpriv_port`

2) ¿Cuál es el valor del ttl (Time To Live) usado en servidor_redes?

`ndd /dev/tcp tcp_ip_ttl`

3) ¿Cuál es el valor del temporizador de inactividad (keepalive)?

`idem tcp_keepalive_interval`

4*) ¿Cuántos interfaces de red tiene tu máquina? ¿Cuáles son sus direcciones físicas? ¿Y sus direcciones IP?

`ifconfig -a. netstat -in .`

con `winipcfg` solo aparece un interfaz. No referencia al local.

5) En un interfaz que esté funcionando con normalidad no debe haber tramas encoladas pendientes de envío (eso sería señal de que o el cable no está bien conectado o la tarjeta no funciona bien). Revisa ese parámetro en los interfaces de tu máquina (no tengas en cuenta el *loopback*)

`netstat -i . Queue`

Sobre el PC no se puede saber, no saca esas estadísticas

6) Una tasa de errores demasiado elevada (más de 100 puede ser una cifra orientativa) en la entrada o salida de un interfaz es un síntoma de problemas. Si hay muchos errores de salida, quiere decir que la red está saturada o que hay un problema físico en la conexión con la red. Si son muchos los de entrada, puede ocurrir alguna de las dos cosas anteriores, o que la máquina local está sobresaturada de trabajo. Revisa esos parámetros en los interfaces de tu máquina (no tengas en cuenta el *loopback*). Si sospechas que la red está saturada (más de un 5% de colisiones) ¿Cómo comprobarás cual es la tasa de colisiones que se están dando?

`netstat -i . Ierrs Oerrs. Collis Opkts`

Sobre el PC no se puede saber, no saca esas estadísticas

7*) Mirando en el fichero /etc/services podemos ver cuáles son los puertos que corresponden a cada servidor de aplicaciones. Pero eso no nos sirve para saber qué puertos son los que están usando los clientes que estemos ejecutando. ¿Cómo puedes saber eso?

netstat -a

8) En la sesión pasada vimos la tabla ARP usando el comando arp. Haz lo mismo usando netstat.

netstat -p

9*) ¿Con qué otras redes está conectada tu red? ¿A través de qué encaminadores se pasa a esas otras redes?

netstat -nr, edo netstat -r (este último saca también los nombres).

En Windows sólo se puede utilizar el último.

10) ¿Cómo podemos saber si en un puerto concreto hay alguna actividad? ¿Y para saber qué conexiones hay abiertas en un momento dado en un puerto?

netstat -a

11*) ¿Por qué encaminadores pasa un datagrama hasta alcanzar su destino? Haz la prueba con www.uhu.es

En unix: ping -sRv o bien traceroute

En W95:tracert, o bien ping -r 4 www.uhu.es

12) Analizando la ejecución de traceroute dada en el ejemplo, responde las siguientes preguntas:

-¿Cuántos encaminadores de la UHU se atraviesan en el camino?

-¿Qué paso del camino lleva más tiempo recorrer?

13) Sitúate en la URL <http://www.slac.stanford.edu/comp/net/wan-mon/traceroute-srv.html> y analiza a partir de las facilidades que en ella se ofrecen los caminos que siguen los datagramas provenientes de distintas partes del mundo para llegar hasta la red de la UPV. Estudia cuáles son los puntos críticos en esos caminos.