Tema 2.-Práctica5. Puertos y Servicios

El servicio DNS ***bind9***, ejecuta un proceso llamado ***named***

Procesos:

Para ver los procesos que tienen bind como ejecución

```
root@profesor:/home/usuario# ps -aux | grep bind
warning: bad ps syntax, perhaps a bogus '-'?
See http://gitorious.org/procps/procps/blobs/master/Documentation/FAQ
root      1652  0.0  0.0   2376   812 ?        Ss   11:58   0:00 /sbin/rpcbind -
w
bind      2082  0.0  0.9  41932  9852 ?        Ssl  11:58   0:00 /usr/sbin/named
 -u bind
root      2759  0.0  0.0   3568   840 pts/0    S+   12:09   0:00 grep bind
```

usuario que ejecuta el comando named

ejecución del comnado named

Se muestran 3 procesos:

El proceso que nos interesa es el segundo, el usuario bind ejecuta el comando de usuario /usr/sbin/named

Puertos:

Para ver los puertos abiertos por el servicio named

Netstat –atunp |grep named →

a→ todos los registros.

t→ TCP.

u→ UDP.

n→ números de IP y puertos en lugar de nombres.

p → procesos implicados.

```
root@profesor:/home/usuario# netstat -atunp |grep named
tcp        0      0 192.168.10.1:53         0.0.0.0:*               LISTEN      208
2/named
tcp        0      0 192.168.4.60:53         0.0.0.0:*               LISTEN      208
2/named
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      208
2/named
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      208
2/named
tcp6       0      0 :::53                   :::*                    LISTEN      208
2/named
tcp6       0      0 ::1:953                 :::*                    LISTEN      208
2/named
udp        0      0 192.168.10.1:53         0.0.0.0:*                           208
2/named
udp        0      0 192.168.4.60:53         0.0.0.0:*                           208
2/named
udp        0      0 127.0.0.1:53            0.0.0.0:*                           208
2/named
udp6       0      0 :::53                   :::*                                208
2/named
```

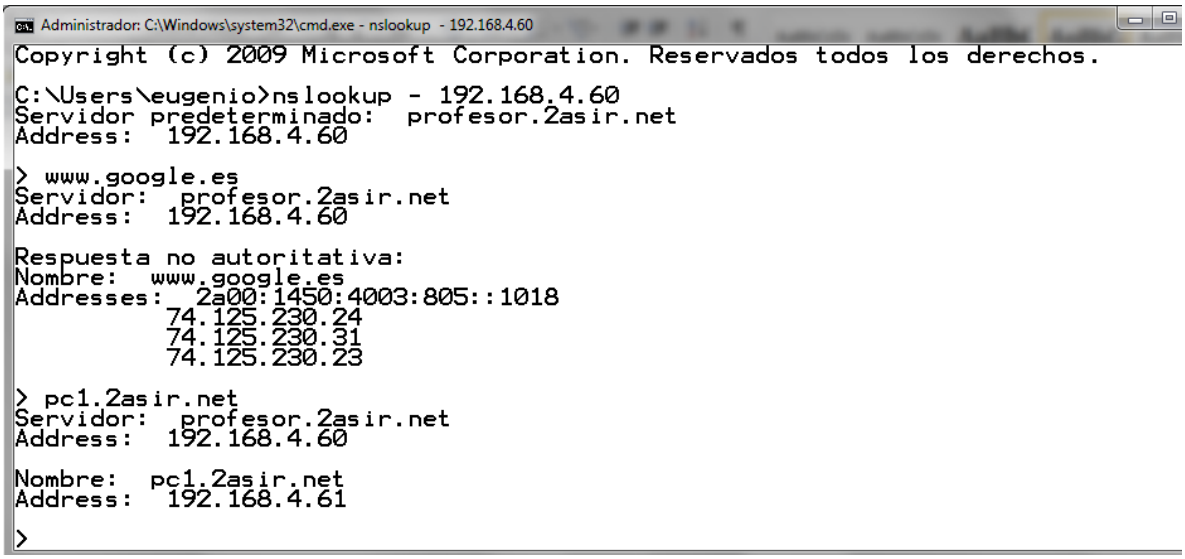
En este caso los puertos abiertos (53, puerto DNS) del proceso named para todas las interfaces de red.

Consulta a un servidor:

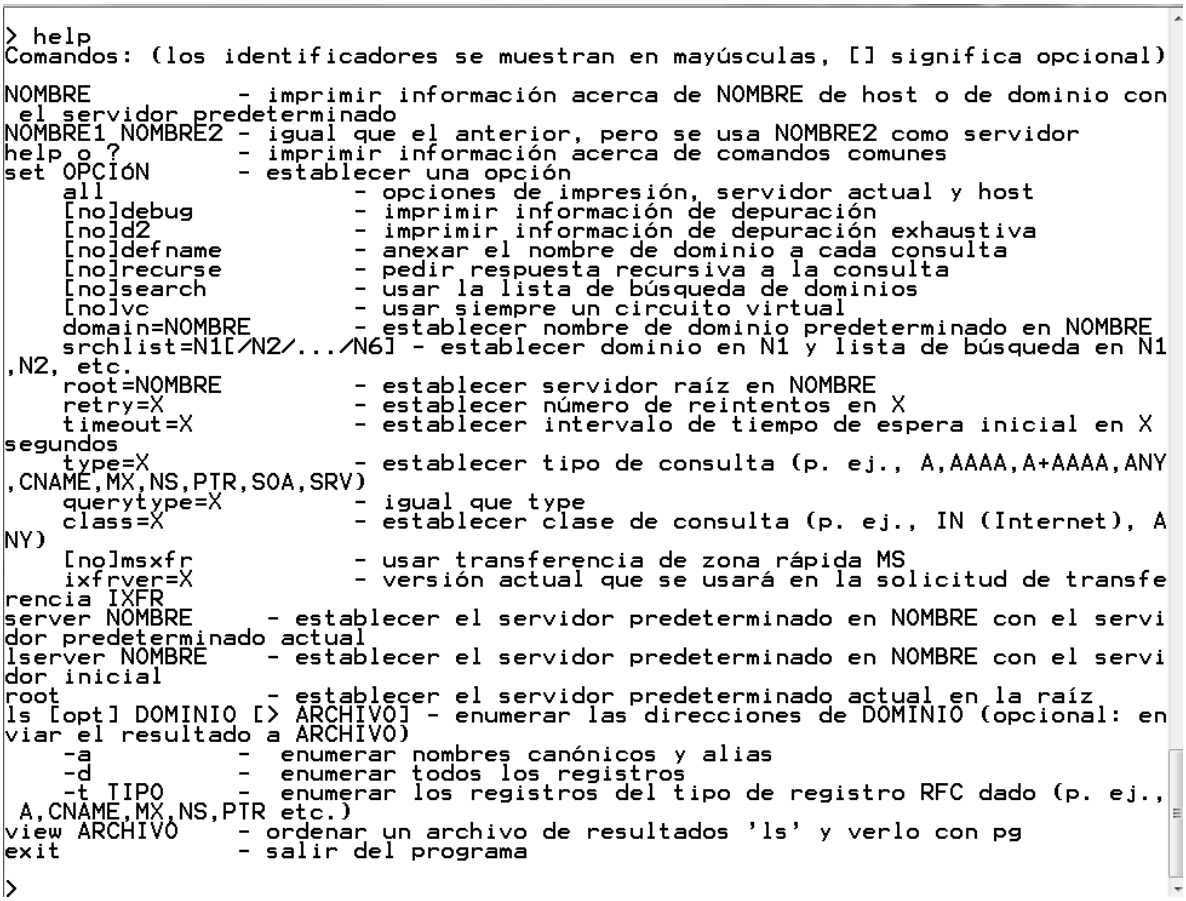
Desde el windows 7 hacemos establecemos una conexión con el servidor DNS 192.168.4.60, aunque dicho sistema tenga como Servidores DNS otros:

```
C:\Users\eugenio>ipconfig /all

Configuración IP de Windows

   Nombre de host. . . . . . . . . . : Profesor
   Sufijo DNS principal  . . . . . . :
   Tipo de nodo. . . . . . . . . . . : híbrido
   Enrutamiento IP habilitado. . . . : no
   Proxy WINS habilitado . . . . . . : no

Adaptador de Ethernet Conexión de área local:

   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . : Atheros AR8151 PCI-E Gigabit Ethe
rnet Controller (NDIS 6.20)
   Dirección física. . . . . . . . . . . . . : 50-E5-49-41-B3-4B
   DHCP habilitado . . . . . . . . . . . . . : no
   Configuración automática habilitada . . . : sí
   Vínculo: dirección IPv6 local. . . : fe80::71c1:dc21:b696:ac37%10(Preferido)

   Dirección IPv4. . . . . . . . . . . . . . : 192.168.4.16(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.4.253
   IAID DHCPv6 . . . . . . . . . . . . . . . : 240182601
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-1B-3C-8D-74-50-E5-49-
41-B3-4B
   Servidores DNS. . . . . . . . . . . . . . : 194.179.1.100
                                       194.179.1.101
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado
```

Conexióncon el servidor 192.168.4.60:



Podemos ver los distintas consultas a hacer mediante las opciones



Para ver los distintos tipos de registro, el el fichero T2_Registros_Recursos.pdf