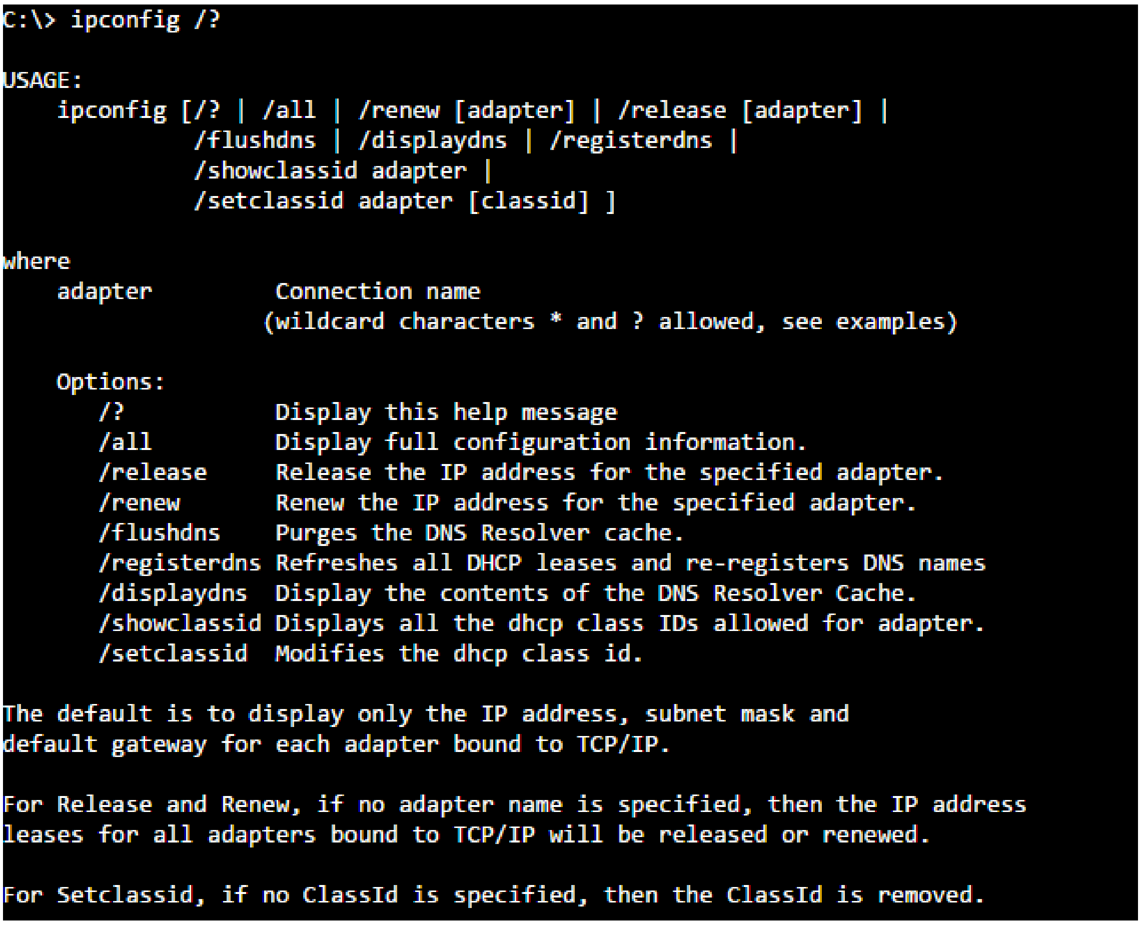
Lab 1 – TCP/IP Configuration

Windows 7 TCP/IP Configuration

To carry out this section you must boot your computer into Windows 7 partition and access using the username and password of your account at the UPV (ALUMNO domain).

1. The ipconfig Command

ipconfig is used to find out your current TCP/IP settings. With IPCONFIG you can find out your IP Address, find your Default Gateway and find your Subnet Mask. The command format is as follow:

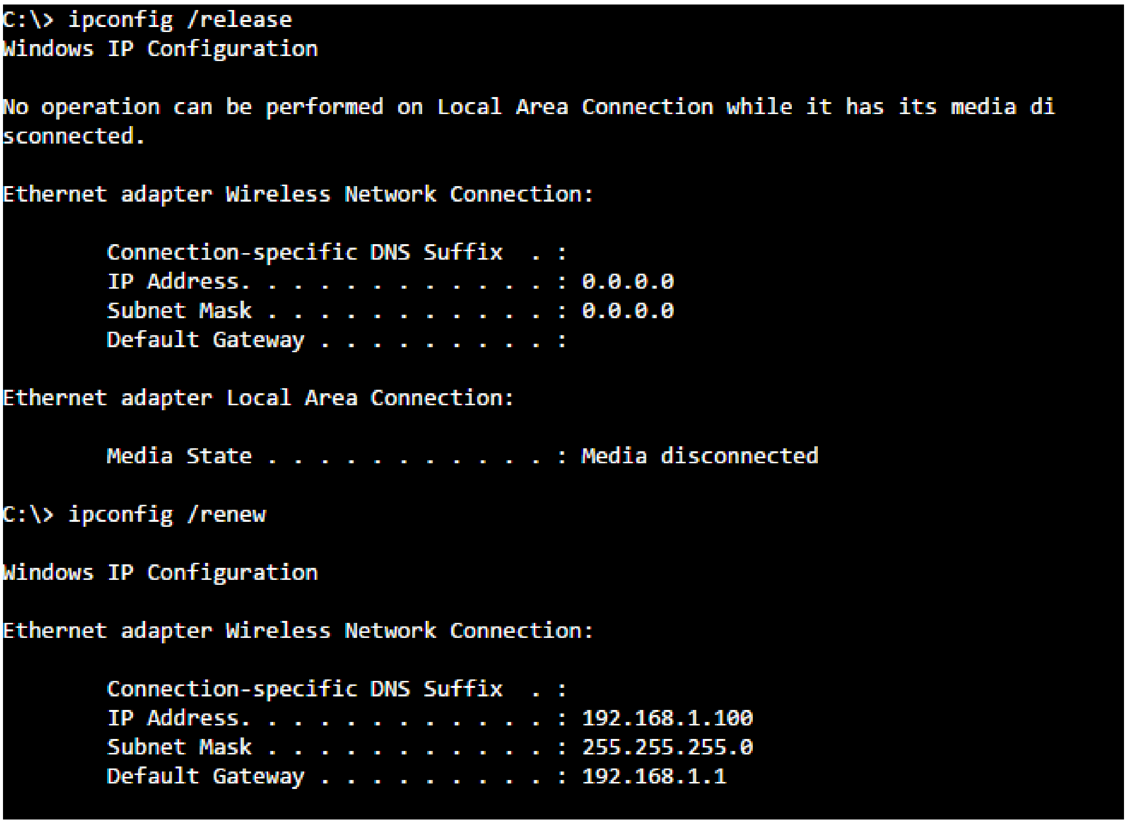


```
C:\> ipconfig /?

USAGE:
    ipconfig [/? | /all | /renew [adapter] | /release [adapter] |
              /flushdns | /displaydns | /registerdns |
              /showclassid adapter |
              /setclassid adapter [classid] ]

where
    adapter         Connection name
                   (wildcard characters * and ? allowed, see examples)

    Options:
       /?           Display this help message
       /all         Display full configuration information.
       /release     Release the IP address for the specified adapter.
       /renew       Renew the IP address for the specified adapter.
       /flushdns    Purges the DNS Resolver cache.
       /registerdns Refreshes all DHCP leases and re-registers DNS names
       /displaydns  Display the contents of the DNS Resolver Cache.
       /showclassid Displays all the dhcp class IDs allowed for adapter.
       /setclassid  Modifies the dhcp class id.

The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid, if no ClassId is specified, then the ClassId is removed.
```

ipconfig /all
To display all your IP information for all adapters. With ipconfig /all you can also find out your DNS Server and MAC Address. This will show your full TCP/IP configuration for all adapters on your Windows machine.
You can find out your own IP Address as well as your default gateway.

ipconfig /release
To release your current IP information and obtain a new IP Address from the DHCP server.

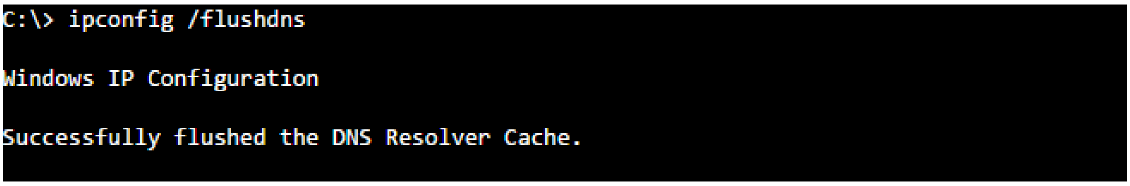
ipconfig /renew
Used to renew your IP Address if you have it set to obtain IP Address automatically.



```
C:\> ipconfig /release
Windows IP Configuration

No operation can be performed on Local Area Connection while it has its media di
sconnected.

Ethernet adapter Wireless Network Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . . :

Ethernet adapter Local Area Connection:

        Media State . . . . . . . . . . . : Media disconnected

C:\> ipconfig /renew

Windows IP Configuration

Ethernet adapter Wireless Network Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
```

ipconfig /displaydns
This shows your current DNS Resolver Cache Logs.

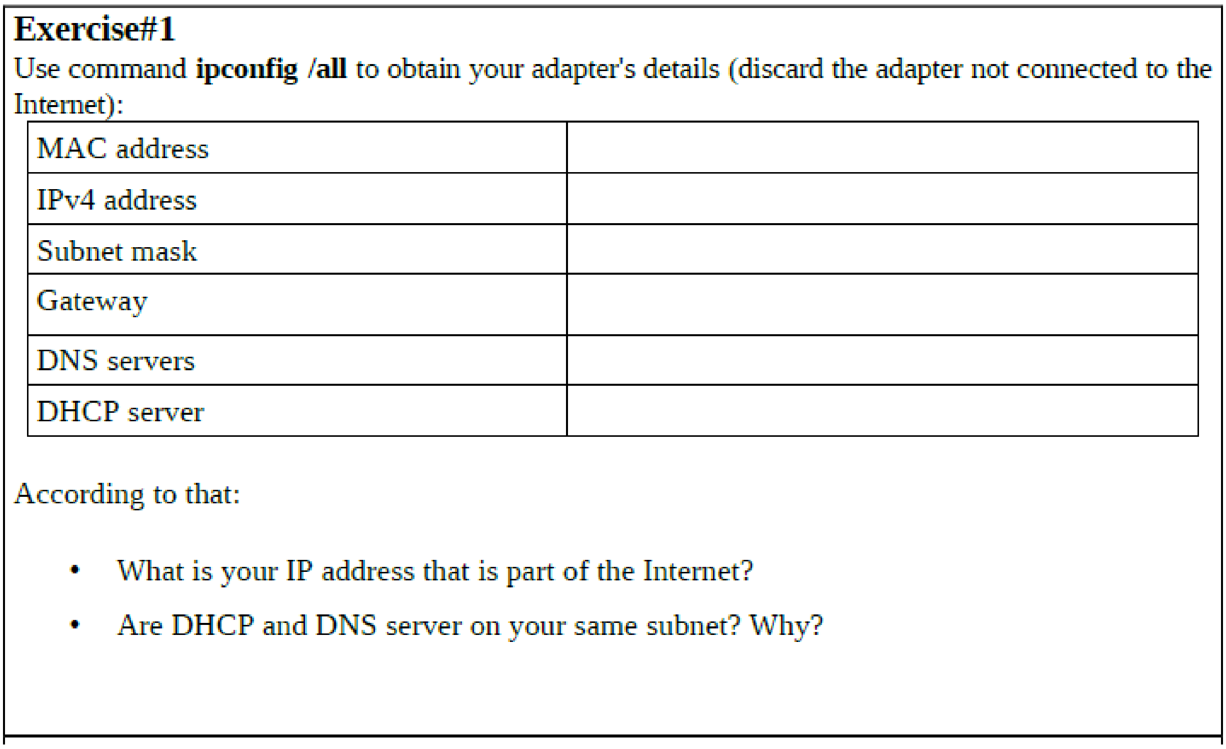
ipconfig /flushdns
This flushes or clears your current DNS Resolver Cache Logs. DNS uses TTL (Time-To-Live) value which let the intermediate name servers to cache DNS information. If you changed your DNS settings, and your computer doesn't see the change immediately, you may perform "ipconfig /flushdns" to clear the DNS cache. If you changed your DNS settings, and your computer doesn't see the change immediately, you may perform "ipconfig /flushdns" to clear the DNS cache.



```
C:\> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

ipconfig /registerdns

The register DNS command updates the DNS settings on the Windows computer. It doesn't just access the local DNS cache, it initiates communication with the DNS server and the DHCP server so it can re-register the network address. You can use this for troubleshooting problems with connection to the ISP (Internet Service Provider), like failing to obtain a dynamic IP address from the DHCP Server or failing to connect to the ISP DNS server.



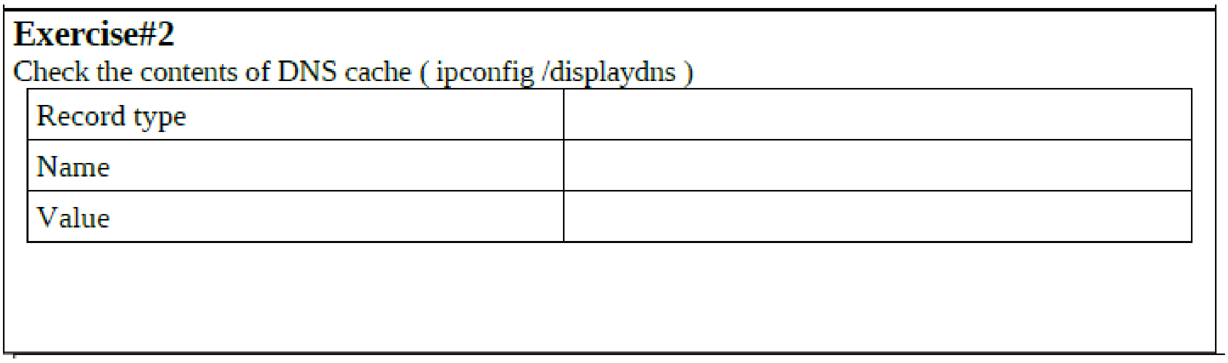
Exercise#1

Use command **ipconfig /all** to obtain your adapter's details (discard the adapter not connected to the Internet):

MAC address	
IPv4 address	
Subnet mask	
Gateway	
DNS servers	
DHCP server	

According to that:

- What is your IP address that is part of the Internet?
- Are DHCP and DNS server on your same subnet? Why?



Exercise#2

Check the contents of DNS cache (ipconfig /displaydns)

Record type	
Name	
Value	

2. The Ping Command

The Ping command allows you to test the connection speed between you and another network node. You can use it to tell the strength, distance, and availability of a connection, either in your own network or over the internet. You can also use the Ping command to return the IP address of a given host name.

Ping Command Syntax

ping [**-t**] [**-a**] [**-n** *count*] [**-l** *size*] [**-f**] [**-i** *TTL*] [**-v** *TOS*] [**-r** *count*] [**-s** *count*] [**-w** *timeout*] [**-R**] [**-S** *srcaddr*] [**-4**] [**-6**] *target* [**/?**]

This command will be studied in detail in Labs 2 and 4.

3. The Netstat Command

The netstat command is used to display *very* detailed information about how your computer is communicating with other computers or network devices. Specifically, the netstat command can show details about individual network connections, overall and protocol-specific networking statistics, your host forwarding table and much more, all of which could help troubleshoot certain kinds of networking issues.

Syntax and switches

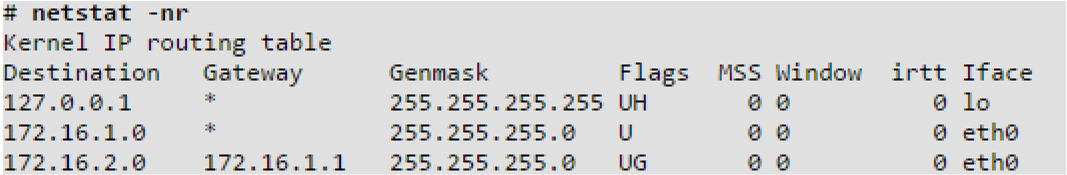
The command syntax is netstat [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-v] [interval]

Switch	Description
-a	Displays all connections and listening ports
-b	Displays the executable involved in creating each connection or listening port. (Added in XP SP2.)
-e	**Displays Ethernet statistics**
-f	Displays Fully Qualified Domain Names for foreign addresses. (In Windows Vista/7 only)
-n	**Displays addresses and port numbers in numerical form**
-o	Displays the owning process ID associated with each connection
-p proto	**Shows connections for the protocol specified by proto; proto may be any of: TCP, UDP, TCPv6, or UDPv6.**
-r	**Displays the routing table**
-s	**Displays per-protocol statistics**

-t	Displays the current connection offload state, (Windows Vista/7)
-v	When used in conjunction with -b, will display sequence of components involved in creating the connection or listening port for all executables. (Windows XP SP2, SP3)
[interval]	An integer used to display results multiple times with specified number of seconds between displays. Continues until stopped by command *ctrl+c*. Default setting is to display once,

Displaying the Forwarding Table

When you invoke **netstat** with the –r flag, it displays the kernel routing.



```
# netstat -nr
Kernel IP routing table
Destination   Gateway       Genmask          Flags  MSS Window  irtt Iface
127.0.0.1     *             255.255.255.255 UH       0 0           0 lo
172.16.1.0    *             255.255.255.0   U        0 0           0 eth0
172.16.2.0    172.16.1.1    255.255.255.0   UG       0 0           0 eth0
```

The –n option makes **netstat** print addresses as dotted quad IP numbers rather than the symbolic host and network names.

The second column of **netstat** 's output shows the gateway to which the routing entry points. If no gateway is used, an asterisk is printed instead. The third column shows the network mask for this route. When given an IP address to find a suitable route for, the kernel steps through each of the routing table entries, taking the bitwise AND of the address and the genmask before comparing it to the target of the route.

The fourth column displays the following flags that describe the route:

G

The route uses a gateway.

U

The interface to be used is up.

H

Only a single host can be reached through the route.

D

This route is dynamically created. It is set if the table entry has been generated by a routing daemon like **gated** or by an ICMP redirect message

M

This route is set if the table entry was modified by an ICMP redirect message.

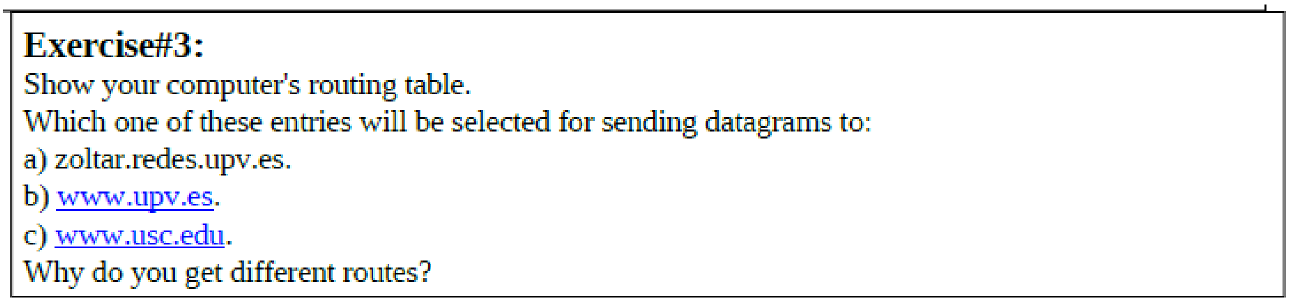
!

The route is a reject route and datagrams will be dropped.

The next three columns show the MSS, Window and irtt that will be applied to TCP connections established via this route. The MSS is the Maximum Segment

Size and is the size of the largest datagram the kernel will construct for transmission via this route. The Window is the maximum amount of data the system will accept in a single burst from a remote host. The acronym irtt stands for “initial round trip time.” The irtt value can be set using the **route** command. Values of zero in these fields mean that the default is being used.

Finally, the last field displays the network interface that this route will use.



Exercise#3:

Show your computer's routing table.

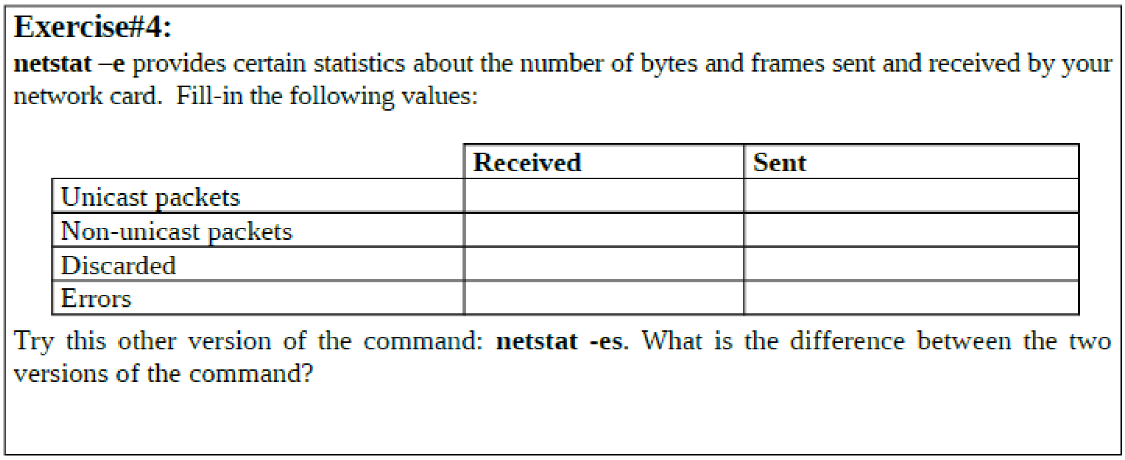
Which one of these entries will be selected for sending datagrams to:

a) zoltar.redes.upv.es.

b) www.upv.es.

c) www.usc.edu.

Why do you get different routes?

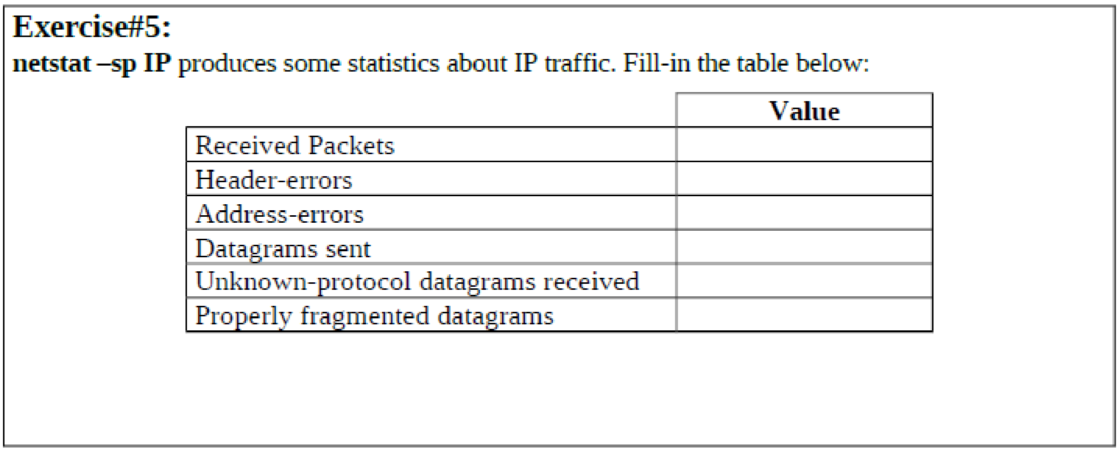


Exercise#4:

netstat –e provides certain statistics about the number of bytes and frames sent and received by your network card. Fill-in the following values:

	Received	**Sent**
Unicast packets		
Non-unicast packets		
Discarded		
Errors		

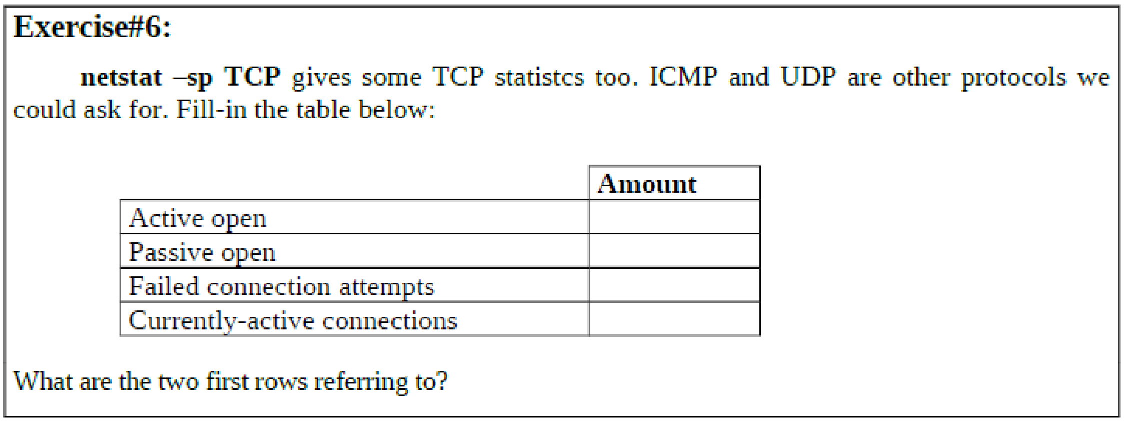
Try this other version of the command: **netstat -es**. What is the difference between the two versions of the command?



Exercise#5:

netstat –sp IP produces some statistics about IP traffic. Fill-in the table below:

	Value
Received Packets	
Header-errors	
Address-errors	
Datagrams sent	
Unknown-protocol datagrams received	
Properly fragmented datagrams	



Exercise#6:

netstat –sp TCP gives some TCP statistcs too. ICMP and UDP are other protocols we could ask for. Fill-in the table below:

	Amount
Active open	
Passive open	
Failed connection attempts	
Currently-active connections	

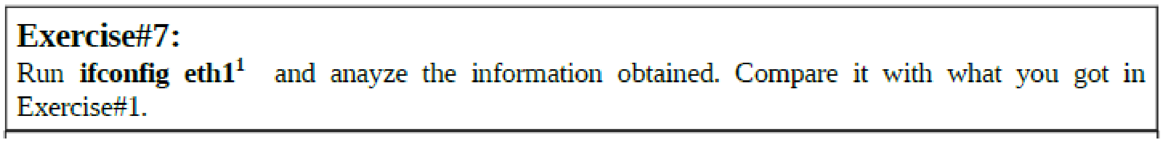
What are the two first rows referring to?

Linux Configuration

Please reboot your computer to Linux.

4. The Ifconfig Command

ifconfig is used to configure, or view the configuration of, a network interface on your system. Running the **ifconfig** command with no arguments will display information about all network interfaces currently in operation. To view the configuration of a specific interface, specify its name (eth0, eth1,lo, wlan0,…) as an option.



Exercise#7:
Run **ifconfig eth1**[1] and anayze the information obtained. Compare it with what you got in Exercise#1.

5. The Netstat Command

The netstat command is similar to that described for Windows 7 in section 3.

Exercise#8:

Run **netstat –nr** and fill in the routes related to device eth0:

dest	gateway	mask

Which one will be select for a datagram destinated to:

a) www.upv.es

b) zoltar.redes.upv.es.

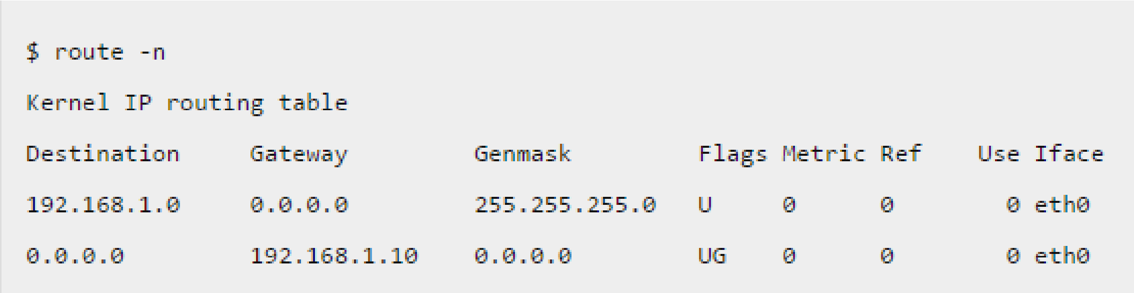
Is it a different gateway in both cases? Why?

6. Route Command

Route command is used to show/manipulate the IP routing table. It is primarily used to setup static routes to specific host or networks via an interface.

Display Existing Routes

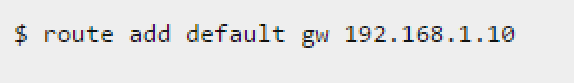
route command by default will show the details of the kernel routing table entries. By default route command displays the host name in its output. We can request it to display the numerical IP address using -n option as shown below.



```
$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
0.0.0.0         192.168.1.10    0.0.0.0         UG    0      0        0 eth0
```

Adding a Default Gateway

We can specify that the packets that are not within the network have to be forwarded to a Gateway address. The following route “add command” will set the default gateway as 192.168.1.10.



```
$ route add default gw 192.168.1.10
```

Exercise#9:

1) **route -n**
2) Write down your default gateway.
3) Remove that entry (**sudo route del default**). Check your table now.

   Try reaching out of your subnet ...

   ping -c 2 www.upv.es

   What does it happen?

   Try pinging again but now using www.upv.es IP address instead of its name(you wrote it down in exercise 3).

   Now try a destination on your same subnet: **ping -c 2 158.42.180.62**
4) Restore things as they were before (**sudo route add default gw dir_IP_de_tu_router**). Ignore a possible warning about DNS.
5) Check that you now have full connectivity.

Reject Routing to a Particular Host or Network

Sometimes we may want to reject routing the packets to a particular host/network. To do that, add the following entry.

```
$ route add -host 192.168.1.51 reject
```

we cannot access that particular host, however we can still access other hosts in the network .

If you want to reject an entire network (192.168.1.1 – 192.168.1.255), then add the following entry.

```
$ route add -net 192.168.1.0 netmask 255.255.255.0 reject
```

Now, you cannot access any of the host in that network.

Exercise#10:

1) Run **sudo route add -net 158.42.180.0 netmask 255.255.254.0 reject**.

   Now try **ping -c 2 zoltar.redes.upv.es**.

   And next **ping -c 2 www.upv.es** and **ping -c 2 www.google.es**.

   What does it happen?

2) Restore initial config:

```
sudo route del -net 158.42.180.0 netmask 255.255.254.0 reject
```

Double-check local and remote networks are accessible again.