Lab#4B: ICMP Protocol

Read Kurose's 4.4.3 section. You can this video too:
http://www.youtube.com/watch?
v=FprZF9agJJI

1. IP header analysis

Start your computer with Linux.

Theoretical exercise

Computer B has received the following datagrams whose origin was computer A. Only TCP ports 22 and 30,000 are opened in B when the IP datagrams arrive.

Num.	Indentified	More Fragments	Offset	Total Length	Protocol	Type if icmp/Port if UDP or TCP
1	1340	1	185	1500	ICMP	8
2	1341	0	0	877	UDP	8000
3	1342	1	0	1500	TCP	22
4	1340	0	370	78	ICMP	8
5	1342	1	185	1500	TCP	22

Which data will the transport layer receive? Justify the answer.

Will ICMP messages be generated? Justify the answer. If yes, indicate which

datagram(s) generated it (them).

Exercise#1:

Start wireshark software and launch a capture of network traffic (IP packets) of any access to server www.ua.es.
Using your broswer access www.ua.es to get just the front page. You can stop the capture now and fill-in the form below just looking at the IP headers of the first four packets of the capture:

	Id	***TTL***	***Source IP***	***Destination IP***
Pkt#1				
Pkt#2				
Pkt#3				
Pkt#4				

a) Explain how TTL value changes, why? How does Id field change? Why?
b) Look at the field Protocol, what value does it hold? What does it mean?

2. Ping command

The ping command uses ICMP messages to assess the rount-trip time to a certain host. It uses ICMP messages type 0 (*Echo reply*) and 8 (*Echo request*). To stop the program press Cltr+C.

ping [**-b**] [**-c** *count*] [**-i** *interval*] [**-l** *preload*] [**-p** *pattern*] [**-s** *packetsize*] [**-t** *ttl*] [**-w** *deadline*] [**-F** *flowlabel*] [**-I** *interface*] [**-M** *hint*] [**-Q** *tos*] [**-S** *sndbuf*] [**-T** *timestamp option*] [**-W** *timeout*] [*hop ...*] *destination*

-b		**Allow pinging a broadcast address.**
-c	***Count***	**Stop after sending *count* ECHO_REQUEST packets. With *deadline* option,** ping **waits for *count* ECHO_REPLY packets, until the timeout expires.**
-s	***packetsize***	**Specifies the number of data bytes to be sent. The default is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data.**
-t	***Ttl***	**Set the IP Time to Live.**
-Q	***Tos***	**Set Quality of Service -related bits in ICMP datagrams. *tos* can be either decimal or hex number.**

Exercise#2:

Ping three times (-c 3) the following addresses and write down the time.

	Round-trip time (ms)		
	Min	**Max**	**Average**
zoltar.redes.upv.es			
www.upv.es			
www.rediris.es			
www.uq.edu.au			
www.berkeley.edu			

Ping results are sometimes difficult to interpret. Why does round-trip time change?

Exercise#3:

1) Start a capture filter for IMCP traffic (icmp) and issue the following command `ping -c 3 zoltar.redes.upv.es` Run it twice.
2) Stop the capture and review the ICMP messages, paying special attention to type, code and data fields.
3) Look at the IP header, header length, total length and data.
4) Why ICMP messages do not have port numbers?
5) What are sequence number and identifier fields for?

3. Traceroute command

It sends a special message (either ICMP or UDP) with a specially crafted TTL value that will cause all the routers along the path to the destination to send back an ICMP message of time exceeded when the TTL value reaches zero. When arriving at the destination a different type of answered will be triggered making the sender aware that no more hops are needed to reach the destination.
While Unxix-like ping sends a UPD datagram to an unlikely port on the destination, Windows sends an ICMP echo-request. Destination will react differently to these. The former will trigger an ICMP destination port unreachable while the latter will cause an ICMP echo-response by the destination host.

```
Syntax
      traceroute [options] host [packetsize]

Some options:

   -n    Show numerical addresses; do not look up hostnames.
         (Useful if DNS is not functioning properly.)

   -N squeries
         The number of probe packets sent out simultaneously. Sending
         several probes concurrently can speed up traceroute
         considerably. Default = 16
         Note that some routers and hosts can use ICMP rate
         throttling. In such a situation specifying too large number
        can lead to loss of some responses.

   -q nqueries
         Set the number of probe packets per hop. Default = 3
```

Exercise#4:

Try traceroute, using the paramenters: -q 1and –N 1, to the following destinations and write down the number of hops:
(e.g. traceroute –q 1 –N 1 www.upv.es)

	hops
www.upv.es	
www.ua.es	
www.usc.edu	

Why `traceroute www.ua.es` causes a different result?
Why in *traceroute* a www.usc.edu, important time differences happen?

Exercise#5:

1) Point your browser to **https://www.telstra.net/cgi-bin/trace**
2) Request a traceroute to your own computer in the lab.

4) Do you obtain the same path than if you traceroute www.usc.edu from your computer? Why?

Exercise#6:

1) Whith wireshark capture the traffic created when running this command: traceroute –q 1 –N 1 www.upv.es. To capture only the traffic generated for that command use the filter “icmp or (udp && host 158.42.4.23)” being 158.42.4.23 the IP address of www.upv.es.
2) List the different types of packets captured. What are they for?
3) What is the value of the TTL field of the IP packets sent?
4) Note that responses may arrive out of order. What information can you use to match responses with requests?
5) What is the value of ICMP code field on the messages you have captured?
6) Do ICMP error messages contain more fields than echo messages? Why?