NS Lab 1 - Appendix 2
Ping and Traceroute

Chariklis Pittaras (c.pittaras@uva.nl)
Karel van der Veldt (k.vd.veldt@uva.nl)

Traceroute is a network diagnostic tool for displaying the route (path) (and transit delays times) between your machine and a remote network host. Traceroute is implemented in different ways in Unix/Linux/MacOS and in Windows. In Unix/Linux, the source sends UDP packets to the target destination; in Windows, the source sends ICMP packets to the target destination.

You can use the traceroute tool in a Windows machine typing *tracert* in the command prompt. A nicer Windows traceroute program is pingplotter, available both in free version and shareware versions at http://www.pingplotter.com. The size of the ICMP echo request message can be explicitly set in pingplotter by selecting the menu item Edit-> Options->Packet Options and then filling in the Packet Size field.

The Unix/MacOS traceroute command is *traceroute* and you can use it from the command line. The tool send by default UDP packet, but you can send ICMP packet using the –I argument. You can also indicate the size of the UDP datagram after the name or address of the destination. For example, to send traceroute datagrams of 2000 bytes towards www.google.com, the command would be: `traceroute www.google.com 2000`

You can read more about traceroute in section 1.4.3 of the book and section 3.4 of RFC 2151 [ftp://ftp.rfc-editor.org/in-notes/rfc2151.txt].

Ping program is simple tool that allows anyone (for example, a network administrator) to verify if a host is live or not. The Ping program in the source host sends a packet to the target IP address; if the target is live, the Ping program in the target host responds by sending a packet back to the source host. Both of these Ping packets are ICMP packets. The ping program (traceroute as well) reports also the RTT (Round-Trip Time) of each packet. The RTT is the length of time it takes for a packet to be sent (ICMP echo) plus the length of time it takes for an acknowledgment (ICMP Reply) of that packet to be received. In both Windows and Unix/MacOS the ping command is *ping.*

Furthermore, very useful commands are the **ipconf /all** for Windows and **ifconfig** for Linux/Mac, that display all the network interfaces (and information about them) that your computer has.

You can always find out how to use a command using the Unix man command 'man <commandName>', for instance to see the ping manual page you can type 'man ping' at the command line, and press enter to scroll down the page. You can exit the manual page by typing 'q'. For Windows you can use '<commandName> /?'