

University of London International Programmes
Computing and Information Systems and Creative Computing
CO2222 Data communications and enterprise networking
Coursework assignment 1 2017–18

Introduction

This assignment aims to develop your experimental, data handling, presentation and analytical skills and your understanding of the causes of network delays and how utilities such as ping and traceroute can be used to analyze network performance.

Learning objectives

You should be able to:

- carry out experiments using different features of the ping utility
- carry out experiments using different features of the traceroute utility
- enter and display experimental results using spreadsheets
- analyze data, particularly relating measurements made to the different main types of network delay (propagation, transmission and queuing delays).

Tasks

Task 1: Research and write a short report describing the main features and operation of the ping and traceroute utilities, explaining how they may be used to analyze network performance.

Task 2: Using a PC at home or at your institution, find a host near you that responds to a ping command, and carry out Activity 6.3 of Volume 1 of the CO2222 subject guide to determine the Maximum Transfer Unit (MTU) size. Start by sending an ICMP echo request with 1500 bytes of data that has the Don't Fragment bit set. Then send another similar ICMP echo request with 500 bytes of data. You will probably find that the first ping fails because the 'packet needs fragmenting but DF bit set' while the second one succeeds. This means that the maximum data size lies somewhere between 500 and 1499. Continue using a Binary Search until you find the largest amount of data that can be transmitted without fragmentation. This is the largest amount of data an ICMP packet can carry which is less than the MTU size. Indicate what you think this MTU size is and why. Explain why the MTU size has been set to this value.

Task 3: Using a PC at home or at your institution, study the correlation between Round Trip Time (RTT) and distance. Identify three host sites, each one on a different continent, that respond to ICMP echo requests generated by ping commands. Please see the advice section for guidance. Ping each of the three sites you found above and record the average RTT from the ping replies. Using an on-line distance calculator (such as www.indo.com/distance or <http://www.geobytes.com/CityDistanceTool.htm>) or an atlas, calculate the distance between your own location and the host sites. Enter the hostnames, RTTs and distances onto a spreadsheet table and draw an XY (Scatter) Graph to show the relationship between RTT and distance. Draw the trend line and calculate the correlation between RTT and distance. Comment on your results, and explain why a positive correlation might exist between RTT and distance, with reference to the different components that might contribute to RTT (propagation, transmission and queuing delays).

Task 4: Carry out traceroutes (the command is `tracert` in DOS/Windows) to each of the three hosts you pinged in Task 3 above. Your report should include a list of the IP addresses (and hostnames, if given) of all of the devices that make up the route. Study the routes followed by the packets to these hosts and record the location of the routers. These can often be found within the domain name of the router, or by a 'whois' search (<http://www.whois.net/>) to find the owner of the router. Comment on any peculiarities that may account for some of anomalous results you may have obtained in Task 3.

Task 5: 'Wireshark is the world's foremost network protocol analyser. It lets you see what's happening on your network at a microscopic level. It is the *de facto* (and often *de jure*) standard across many industries and educational institutions.' Download Wireshark (<https://www.wireshark.org/>) and install on your computer. Using online help (e.g. <http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/>) configure Wireshark to 'Follow a TCP Stream' and access one of the hosts used in Tasks 3 and 4 above. Provide a screenshot of the output obtained. Identify a DNS packet and examine it in more detail. Provide a screenshot and comment on the data obtained.

Please note: Many organisations don't allow Wireshark and similar tools on their networks. You should not use this tool at work or on your Institution's network unless you have permission. Why do you think this restriction might be in place?

Advice

Finding sites to ping is getting harder, as many network managers have responded to security concerns by filtering ICMP echo request packets. However, there are still many sites that do respond to pings, particularly on academic networks. You can obtain the website URLs for universities from <http://www.univ.cc/> by selecting appropriate countries. If the site is filtering ICMP echo request packets, ping will time out. If replies are received, you should note the domain name for subsequent use.

In order to capture the output of ping and traceroute commands, you can use the `>` or `>>` operators provided on most operating systems that use a command line to direct output of commands into files. If during any experiment, any packets are lost, repeat the experiment, as the lost packets will affect the average RTT calculation.

Sometimes routers do not issue TTL expired messages. When this happens, a line with three stars appears in the traceroute output. If this happens, you should label the routers as unknown. If the host has not been reached before traceroute gives up, then find another host instead which can be reached.

Deliverables and Marking

Your report should contain between 2,000 and 3,000 words and be submitted in **.pdf format**.

Please submit **one** pdf document, which is named using the following convention:

YourName_SRN_COxxxxcw#.pdf (e.g. MarkZuckerberg_920000000_CO2222cw1.pdf)

- **YourName** is your full name as it appears on your student record (check your student portal)
- **SRN** is your Student Reference Number, for example 920000000
- **COXXXX** is the course number, for example CO2222, and
- **cw#** is either cw1 (coursework 1) or cw2 (coursework 2).

For each experiment you should describe the method, display the results in a well-formatted table and, where appropriate, in graphical form and analyse the results you have obtained. Finally you should write a conclusion summarising what you have learnt from the experiments.

It is important that your submitted assignment is your own individual work and, for the most part, written in your own words. You must provide appropriate in-text citation for both paraphrase and quotation, with a detailed reference section at the end of your assignment (this should not be included in the word count). Copying, plagiarism and unaccredited and wholesale reproduction of material from books or from any online source is unacceptable, and will be penalised (see: [How to avoid plagiarism](#)).

The report must contain the following section headings and numbering scheme:

Section No	Heading	Contents	Marks
1	Introduction	Brief description of the ping and traceroute utilities.	5%
2	MTU Size	Method, results and analysis.	20%
3	RTT vs Distance	Method, results and analysis.	25%
4	Traceroute	Method, results and analysis.	25%
5	Wireshark	Installation, operation, results and analysis.	20%
6	Conclusions	Summary of what you have learnt from the Assignment	5%
		Total	100%

[END OF COURSEWORK ASSIGNMENT 1]