



Assignment 1 Value **10%**

Deadline: 08:10 am Tuesday, March 16th

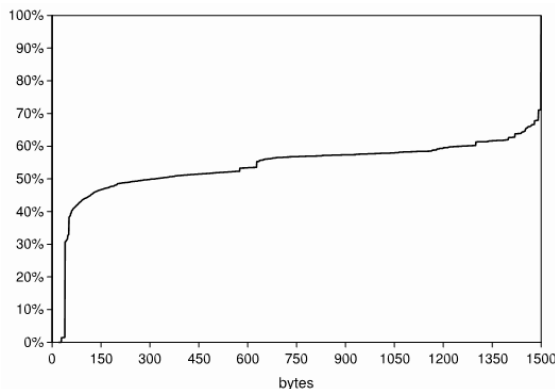
Eindagi: 08:10 f.h. Þriðjudagur, Mars 16.

Late assignments will not be marked.

### IPv4 Packets

#### Background

In their 2007 paper “Analysis of Internet Backbone Traffic and Header Anomalies Observed” Wolfgang John and Sven Tafvelin determined the packet size distribution of IPv4 packets and the frequency of protocols carried as payload (TCP, UDP, etc) – see below. The aim of this assignment is primarily to try and reproduce their findings. Their paper formed the basis of the lectures on “Measurements of internet traffic (IP)”.



	2AM	
	Pkts	Data
TCP	91.3	97.6
UDP	8.5	2.3
ICMP	0.2	0.02
ESP	0.01	0.00
GRE	0.01	0.01

#### Experimental parameters

Measure only IPv4 traffic to and from your own machine.

Truncate captures to the first 54 bytes.

Capture 50,000 truncated packets in a single trace.

Capture traffic specific to your use of one online application (e.g. doing searches with a search engine, playing a game, checking friend’s updates on a social networking site, checking flight and price availability with an airline).

#### Instructions

Create extra columns in Wireshark to capture specific measurements of IPv4 fields.

There is no requirement to anonymize IP addresses using cryptographic techniques.

Cumulative distribution plots can be created in Excel using:

Data>Data Analysis>Histogram>Cumulative Percentage+Chart Output.

You need to define the upper limit of each bin (bin range) plotted on the X-axis in a separate Excel column. Try using limits of 40, 50, 60, ... 1500 bytes (bin width 10 bytes) and using limits of 40, 41, 42, 43, ... 1500 bytes (bin width 1 byte).

(Use Add-Ins>Analysis Toolpack under Excel Options if you need to install Data Analysis.)



**IPv4 Packets report** The IPv4Packets report should be structured as follows:

**Title page** (-2% if not present)

The title should be “IPv4 Packets”. The title page must contain your name, the name of the course (NET0183 Networks and Communications) and the following statement: “This assignment is all my own work. This work has not been submitted for assessment in any other context. I have not knowingly allowed others to copy my work.” By including this statement, you are agreeing with it. If you plagiarize material your degree will be at risk.

**Platform & Experimental Parameters** (1%)

Describe the technology platform used for the packet sniffing experiment (hardware and software). Describe the network card used, the speed supported by the network card, and the speed of the link to the router. (0,5%) Describe the experimental parameters and describe the differences between your experimental parameters and the work of Wolfgang John and Sven Tafvelin choices. Note the time of day when the trace was captured. (0,5% )

**Size Distribution Graph** (4%)

Provide a graph (2,0%) showing the cumulative IPv4 packet size distribution. The X-axis is packet-size in bytes and the Y-axis is cumulative percentage. A line should be drawn through the points of the graph. Justify the bin width you have used (0,5%). Below the graph state: a) the percentage of packets between 40 and 100 bytes b) the percentage of packets between 1400 and 1500 bytes and c) the percentage of packets of exactly 576 bytes, the default IP datagram size (3\*0,5%).

**Protocol Breakdown Table** (4%)

Provide a table showing the frequency of protocols carried as payload (TCP, UDP, etc). Each row should represent data for one protocol. Data for the four most frequent protocols should be reported (4\*1,0%). Columns should represent the percentage of packets and the percentage of data carried by that protocol.

**Conclusions** (1%)

State your conclusions about the cumulative IPv4 packet size distribution (0,5%) and the frequency of protocols carried as payload (0,5%), comparing your results to those of Wolfgang John and Sven Tafvelin.

**Appendix A** The IPv4 packet trace (-2% if not submitted)

Submit an electronic copy of the IPv4 packet trace in pcap format.

**Appendix B** The Excel spreadsheet (-2% if not submitted)

Submit an electronic copy of the Excel spreadsheet used to analyse the packet trace.

**Submission instructions**

Submit a paper copy of your IPv4 Packets report (excluding appendices). One corner should be stapled. Do not enclose your submission in any folder or binder. Submit your paper copy at the start of the lecture hour 08:10 am, Tuesday, March 16th (or before). Also submit electronically via e-mail to [andy@unak.is](mailto:andy@unak.is) a copy of your IPv4 Packets report (Word), and electronic copies of



appendices A (IPv4 packet trace in pcap format) and B (Excel spreadsheet). The header of your e-mail message must be: "NET0183 Assignment 1 <your name>".

### **Bonus work**

A bonus of 2% is available. Students may attempt one of the following. Students may attempt more than one of the following exercises, but the maximum bonus achievable remains 2%. Create an appropriately named section in the report and use tables and graphs as necessary.

#### **(i) Unusual Features**

Explain the causes of any unusual features appearing in your packet size distribution graph.

#### **(ii) IP Flags**

Report on the usage of the various IP flags in your trace and compare your results with those of Wolfgang John and Sven Tafvelin.

#### **(iii) TOS field**

Report on the use of the TOS field in your trace and compare your results with those of Wolfgang John and Sven Tafvelin.

#### **(iv) Sanity Checks**

Report on several sanity checks performed on your trace.

#### **(v) BitTorrent**

Repeat the experiment capturing truncated packets while downloading a file using BitTorrent. (See the NET0183 website.) Provide a packet size distribution graph.

Should bonus work result in an assignment mark over 10%, the additional percentage points will be used in the overall grade calculation for NET0183.

### **Advice**

You are advised not to interrupt the work of the CPU by launching other applications while you sniff packets. Close down any unnecessary applications before you start Wireshark. Keep your technology platform (machine, operating system, network connection) in the same state as you perform packet sniffing. Prototype the approach doing a small capture of 100 truncated packets before doing a full capture of 50,000 truncated packets.

Because you are conducting an experiment, unexpected things might happen, so you are permitted **two** e-mail or phone or office consultations with the teacher.

Expect to work at least two hours for every 1% value of this assignment, i.e. 20 hours.

Dr Andy Brooks (andy@unak.is, GSM 869 3974)

27. febrúar 2010

<http://staff.unak.is/not/andy/Networks0910/networks.htm>