User Guide:
Visualising and Scanning Network Information

Author
Leon Roy

Table of Contents

Table of Figures

1 Scanning the Network

1.1 Starting the program

The program can be started from *dev/bin/* by running the Linux or Windows version; *Visual.sh* and *Visual.bat* respectively.

(NB. The programme depends on a MySQL server containing a table of Nessus results (SQL server IP is set in DBManager.java), SQL table dump can be found at *dev/lib/nessus_dump.sql*).

1.2 Starting the scan

When you first start the program you will be confronted by a Window (Figure 1) containing the network view (A) and the user menu (B).

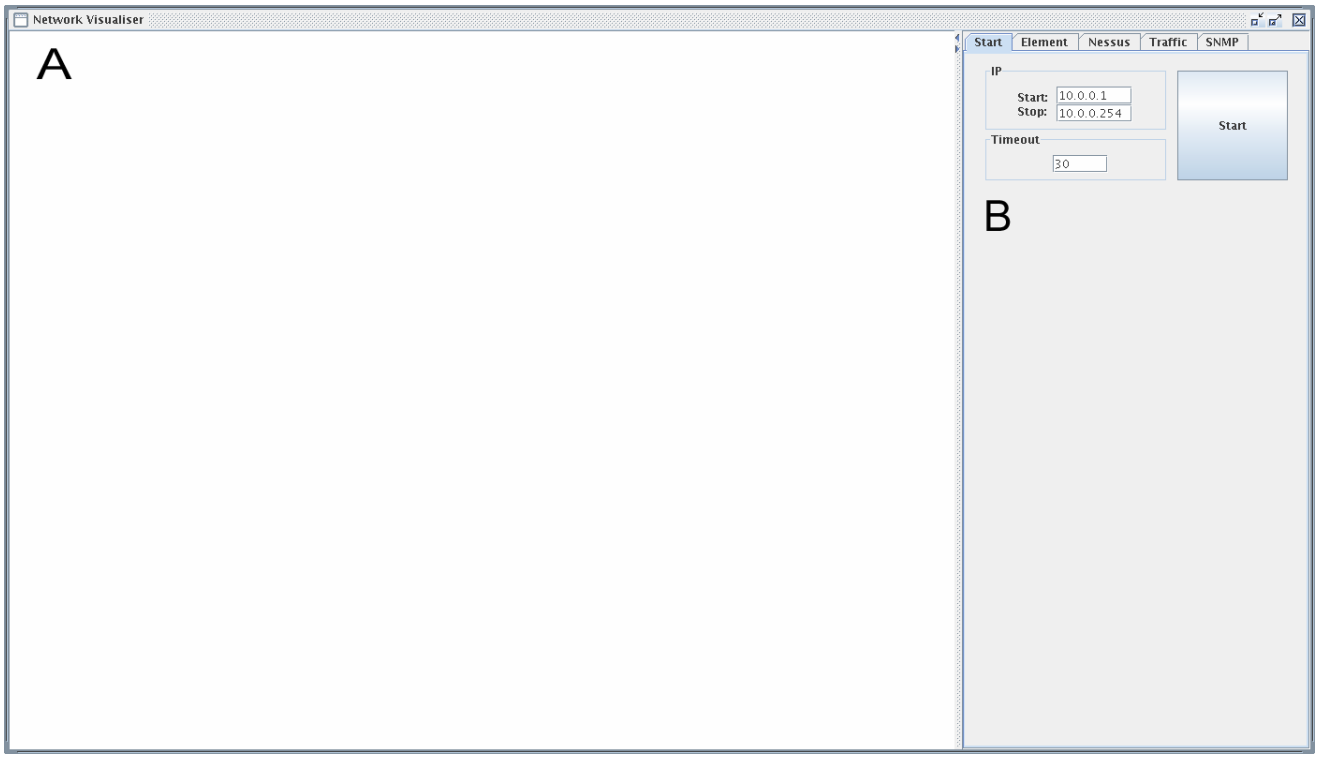

Figure 1 - Initial Window

To initiate a network scan enter the start IP address and end IP address you want to scan, and click on 'Start'.

You might need to increase the value of 'Timeout' to give more time for hosts to reply to the program. In Windows the timeout might need to be as much as 3000.

This can take a while, so please be patient. The programme's internal scanning status will

be displayed to standard output (Figure 2).

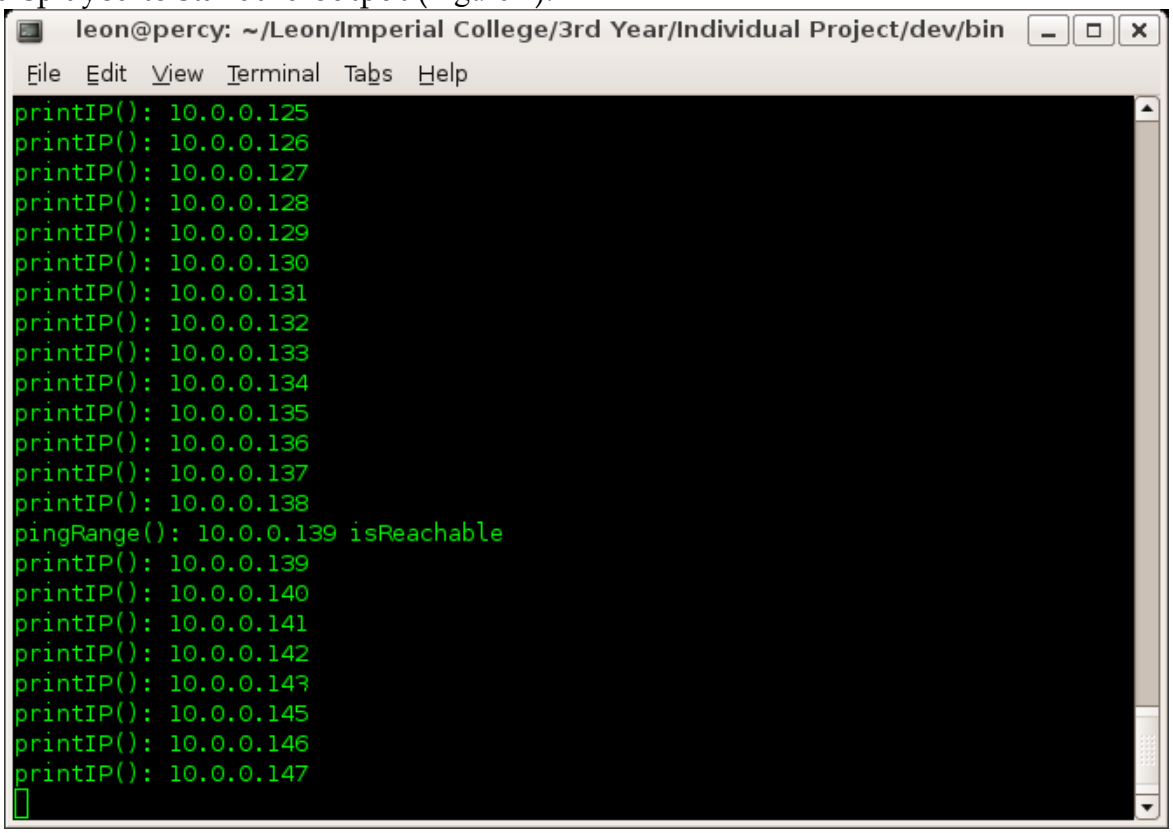

Figure 2 - Output of programme's internal scanning status

2 The Network Results

2.1 *Interpreting the network view*

Depending upon the data sources you have available your diagram will vary. The diagram below (Figure 3) was produced using two Level-2 SNMP capable switches, a simple SNMP capable router, and the results of a Nessus network scan (stored in a SQL server).

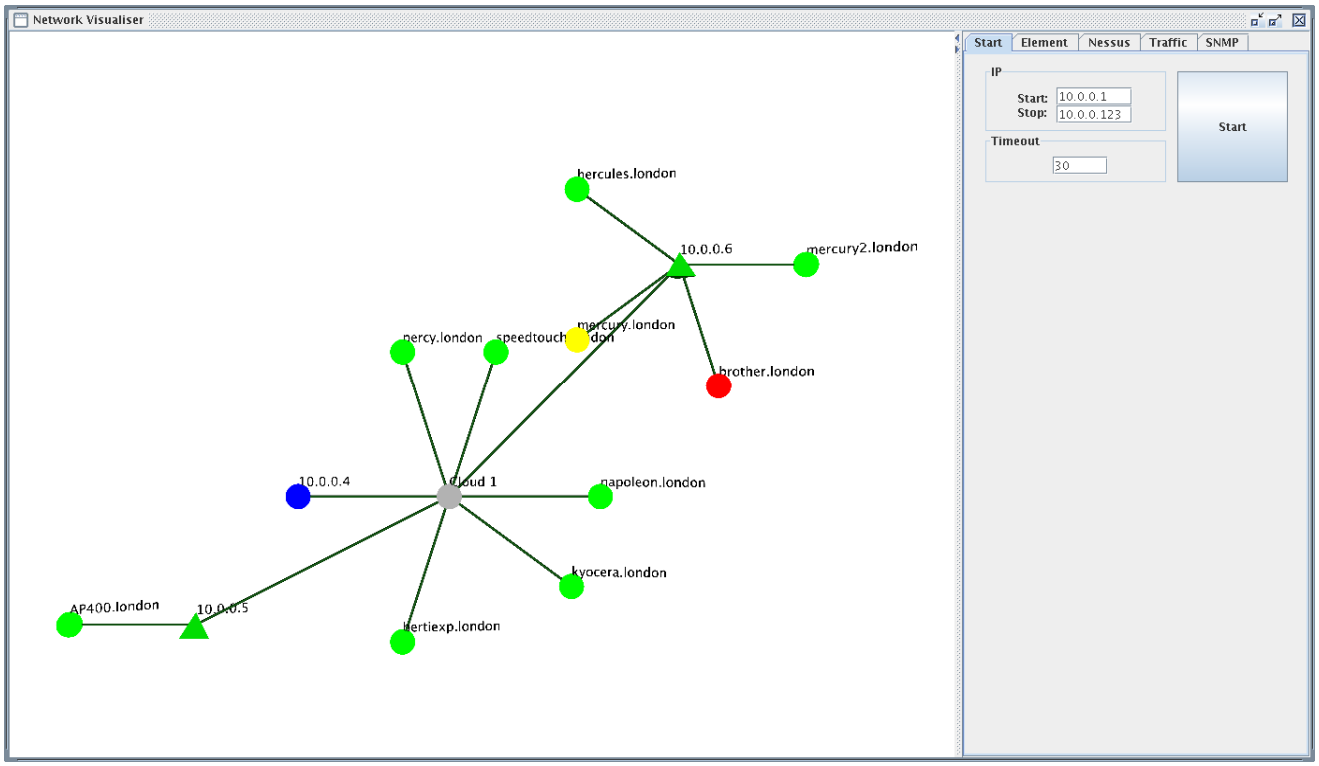

Figure 3 - Resulting output from the network scan

The network diagram here shows thirteen physically connected network elements (the individual nodes), one abstract element (the grey node labelled *Cloud 1*) and the links connecting the various elements (the green lines between the nodes).

Spheres depict network systems which are not network switches (ie. computers, IP phones, other network appliances, etc.), tetrahedrons depict network systems which are network switches, and the grey sphere represents the location of an indeterminable number of network switches which are not SNMP queryable.

Any elements for which the connectivity information cannot be determined by querying the network switches will be shown as unconnected. Without SNMP queryable switches, the links between network elements will indeterminable and individual, unconnected nodes will be returned.

The colour of the individual network nodes is determined using Nessus information about the network. Green signifies no problems detected, Blue signifies a Low risk problem, Yellow a Medium risk and Red a High risk problem.

A complete table of all Nessus results is provided under the tab marked ‘Nessus’ for further inspection.

3 Manipulating the View

3.1 Mouse

The main way in which the view of the network is manipulated is using the mouse. The Left mouse button is used to drag and rotate the network diagram about its origin. The Right mouse button is used to shift the view in the same direction. The Middle mouse button or mouse Wheel is used to zoom in and out of the diagram.

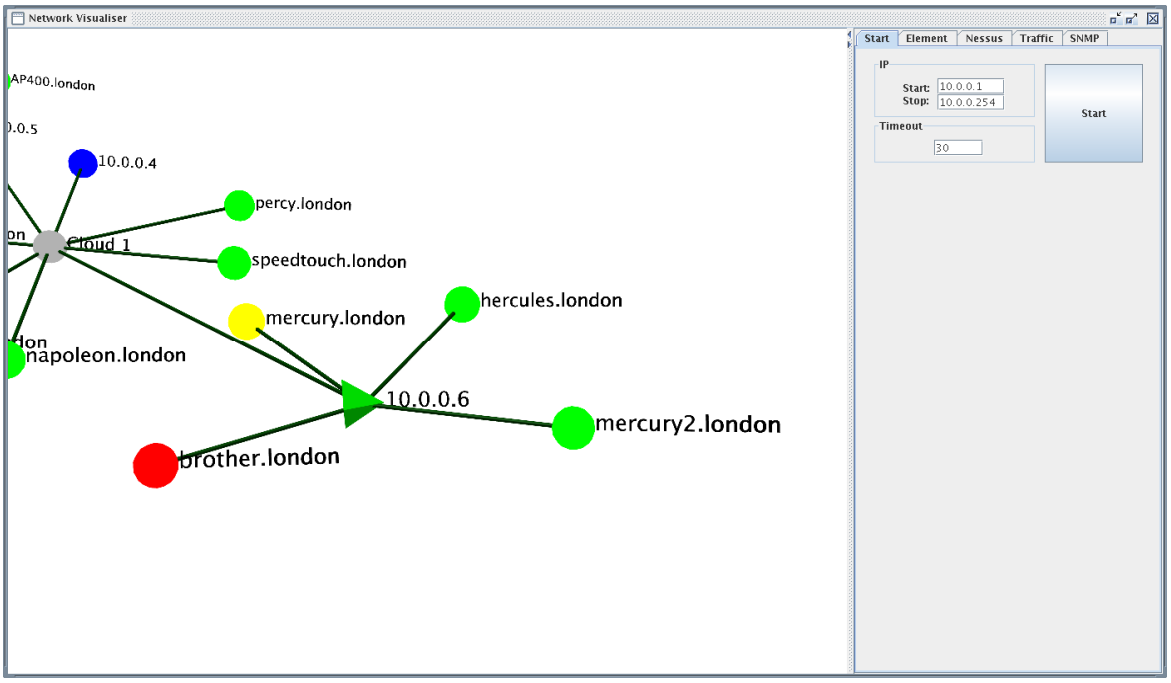

Figure 4 – Network view after being manipulated

3.2 Keyboard

The keyboard cursor keys offer basic navigation with Left and Right rotating the diagram in the X-Y plane about the origin.

Using these two input devices, the network view can be manipulated to focus on a particular point of the network that is of interest.

4 Network Traffic

Network traffic between an SNMP capable switch and a directly connected node can be monitored by clicking on the tab *Traffic*.

4.1 Initiating the traffic scan

First bring into view the link (or links) you want to check the traffic for. Enter the switch name as the *Start* entry and the node name as the *Stop* entry and click on the *Start* button to initiate the traffic diagram (Figure 5). All traffic data graphed is represented as the number of kilobytes outgoing from the Start node to the Stop node.

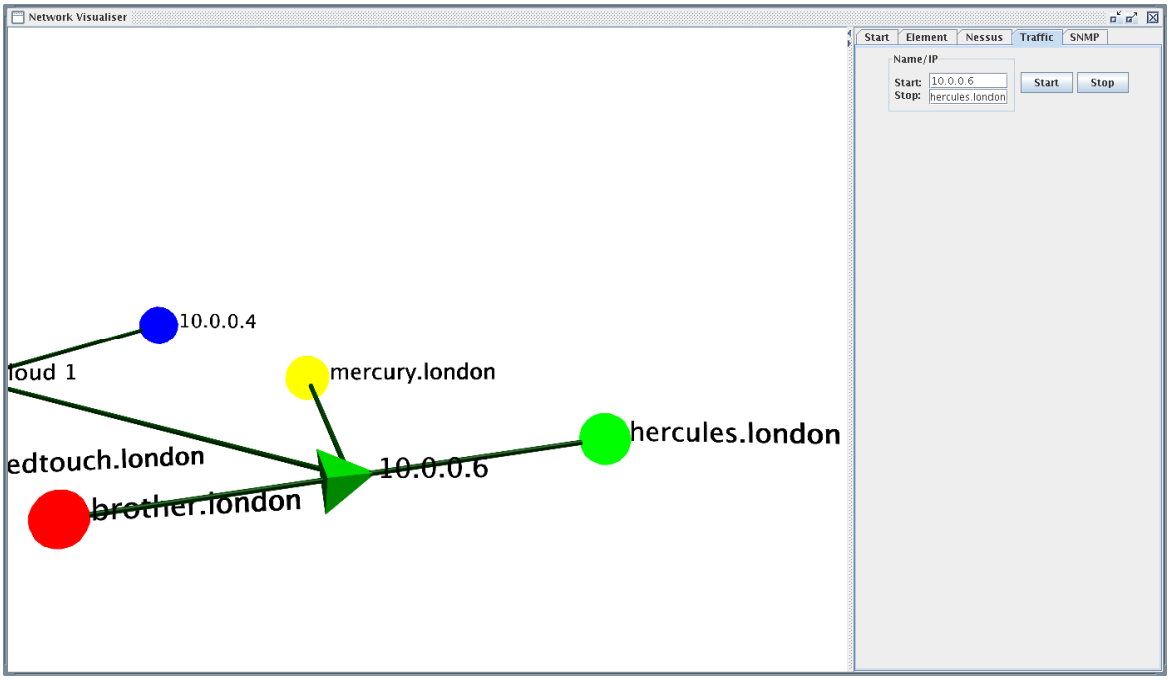

Figure 5 - Portion of the network brought into view and Start and Stop values entered

4.2 *Interpreting the traffic scan*

The traffic scan is drawn along the length of the connection between the start node and the end node. The y-axis is represented as a vertical magenta line. The half way line is also drawn to aid readability, as is the maximum value line, alongside which is a number which shows the current highest value displayed in kilobytes per 3 seconds (the update speed - Figure 6).

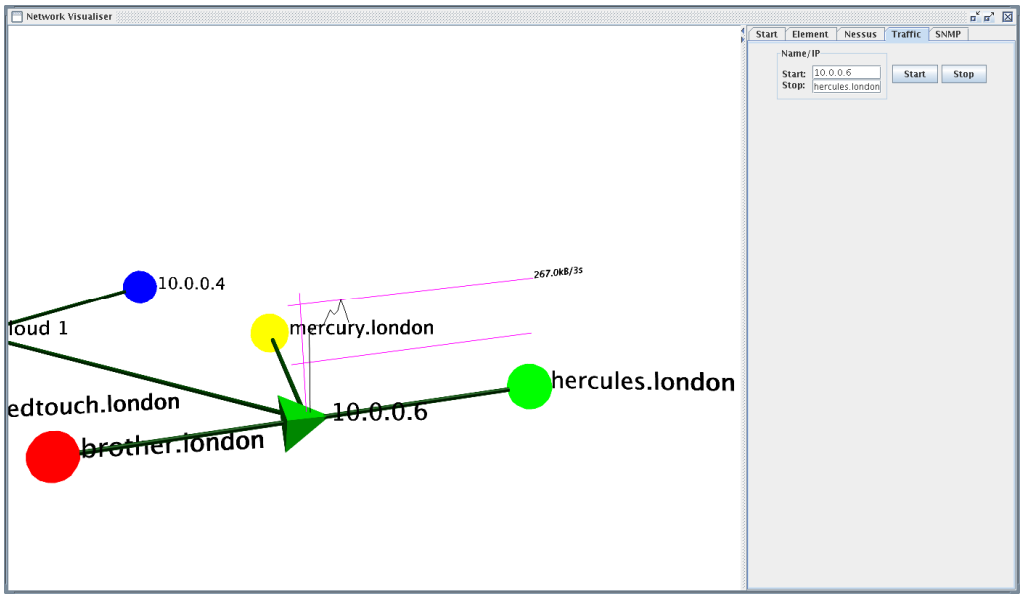

Figure 6 - Traffic scan invoked

The diagram above (Figure 6) shows the current peak value, with any subsequent peak value causing the traffic graph to be rescaled so that the new peak value is drawn as the maximum (Figure 7).

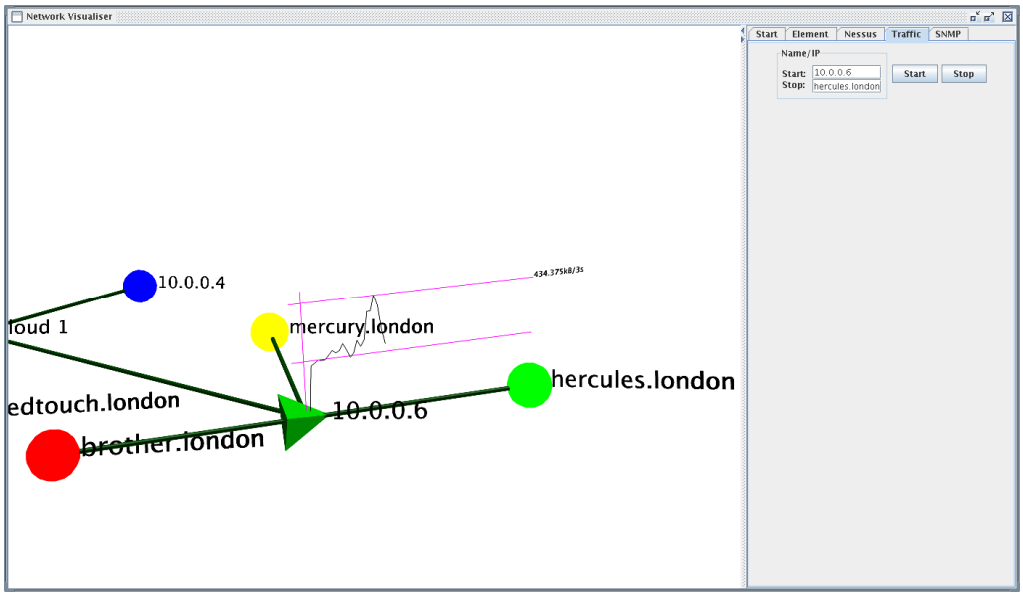

Figure 7 - Traffic graph readjusted to account for new peak value

The reverse also happens as the graph is drawn with any old peak values removed (causing the traffic graph to readjust to take account of the new peak value.

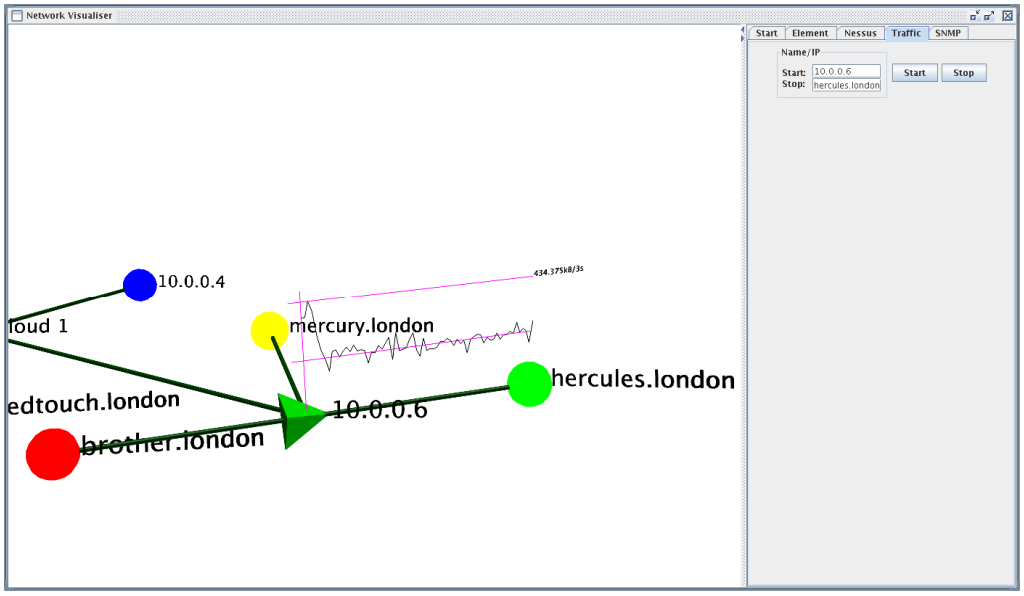

Figure 8 - Old peak value to be removed

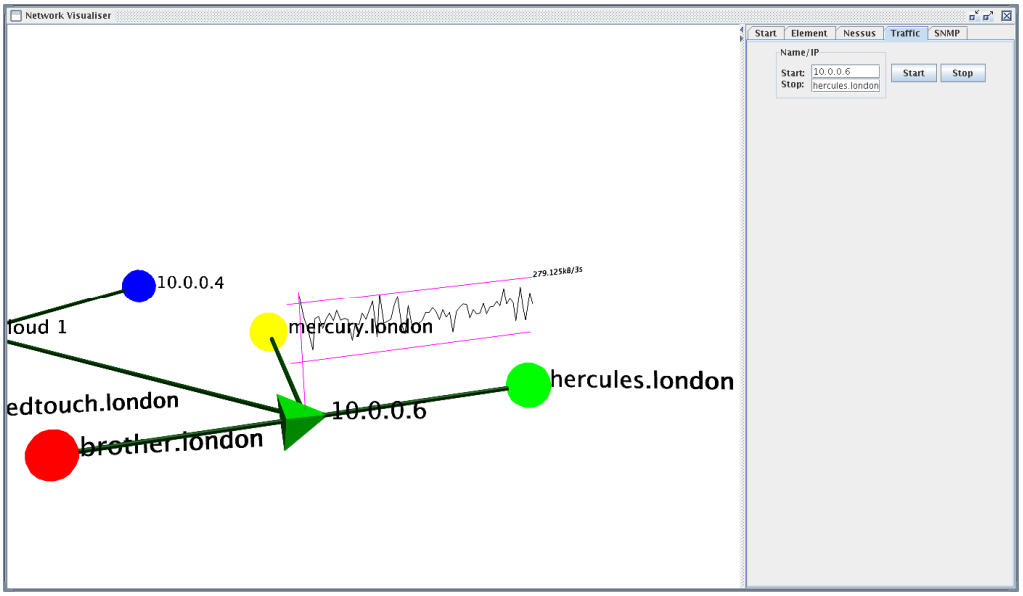

Figure 9 - Old peak value removed and traffic graph readjusted to account for new peak value

4.3 *Multiple traffic scans*

Multiple traffic scans can be drawn, each new diagram being drawn as normal along the network connection between the Start and Stop nodes.

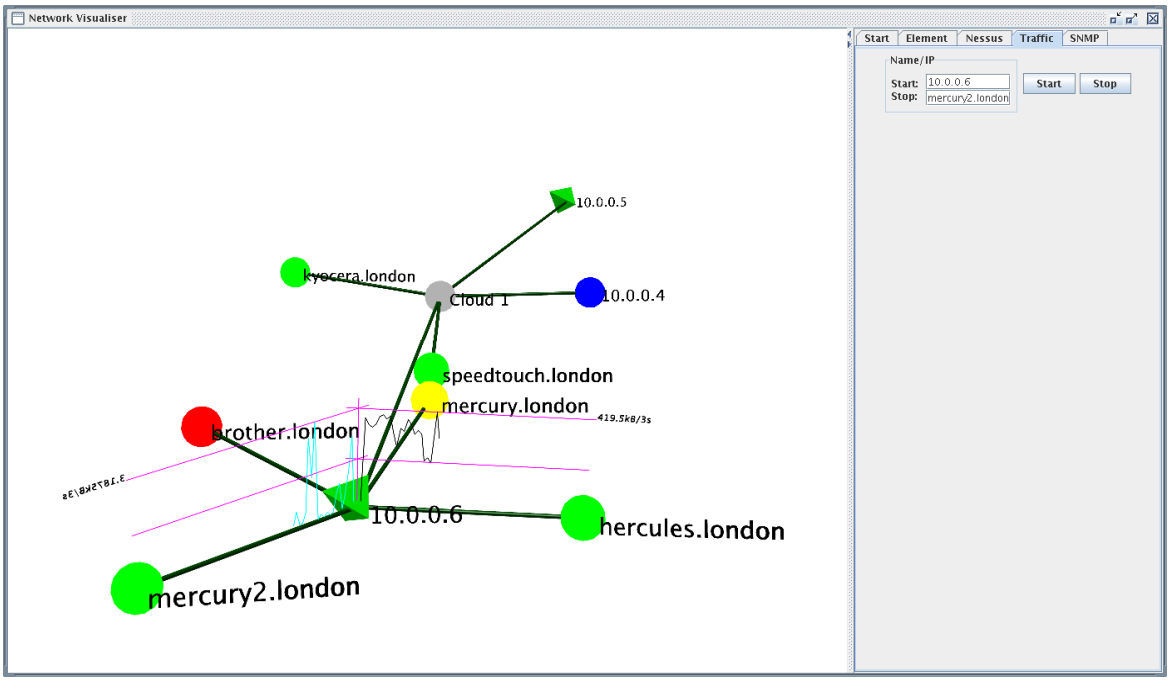

Figure 10 - Multiple traffic diagrams

4.4 *Stopping traffic scans*

Pressing the *Stop* button will stop all traffic scans.