

Traceroute Enhancements

Part 1: Describe the project and the objectives you are trying to accomplish.

traceroute is an indispensable network administration tool that probes the path between two machines on the Internet. The goal of this project is to improve the usability and functionality of this tool. This can be done by using administrative WHOIS information and by displaying the data in an enhanced format. The administrative contact and information regarding the physical location of a machine can be obtained from WHOIS information provided by sites like arin.net, and integrating this information into traceroute can be extremely helpful. Adding a graphical representation of ping times and trying to superimpose the nodes on a map will also help users get a new view into the routes being traversed. There are proprietary tools, like Neotrace, that provide such functionality, but no similar tool in the open source domain is up to date.

Part 2: Describe the methodology you used in working on your project.

There are three different tiers for this project:

- 1) Add relative and average ping information, as well as locational information to the existing traceroute code.
- 2) Create a graphical traceroute that provides the same information in a more concise manner.
- 3) Improve upon the graphical interface to give locations of servers on a map.

The existing traceroute application gives output in the following form:

```
traceroute to www.google.com (64.233.167.104), 30 hops max, 40 byte packets
 1  192.168.0.1 (192.168.0.1)  3.650 ms  3.596 ms  3.400 ms
 2  gw-63-239-72-1.watchtv.net (63.239.72.1)  16.204 ms  20.993 ms
23.067 ms
 3  gw-65-116-218-1.watchtv.net (65.116.218.1)  18.740 ms  279.233 ms
18.222 ms
 4  chi-edge-01.inet.qwest.net (65.123.106.113)  26.467 ms  26.850 ms
24.198 ms
 5  chi-core-02.inet.qwest.net (205.171.20.9)  31.276 ms  24.598 ms
37.868 ms
...
```

This is both cluttered and difficult to read. An example of output produced after Tier 1 would be similar to the following:

```
traceroute to www.google.com (64.233.167.104)
 1  192.168.0.1  3.650 ms  3.596 ms  3.400 ms
    Location: Local
    Average Ping: 3.54 ms
    Relative Ping Increase: 3.54 ms
 2  gw-63-239-72-1.watchtv.net  16.204 ms  20.993 ms  23.067 ms
    Location: Lima, OH
```

Average Ping: 20.09 ms
Relative Ping Increase: 16.55 ms

...

This more verbose output can help immensely when trying to troubleshoot network issues.

A tier 2 application would take the information provided by the tier 1 version and display it in a convenient graphical format. This would allow users to display or hide administrative details easily. It would also allow users to display a bar graph showing the relative ping times for each hop along the path allowing the user to quickly identify bottleneck links in the trace. A tier 3 application would take the locational information given from the WHOIS query and place it on a map of the world, providing a physical network map as well as a logical one from the trace. This can be done via a variety of mapping applications available today.

Part 3: Results you were able to achieve.

The information required for reaching tier 1 of this project is provided by simple math and a WHOIS lookup on a given server. The only difficulty presented here is the format of the WHOIS lookup. In general, the formatting is not consistent, making it difficult to glean the information directly from the lookup – requiring some interesting regular expressions. This was the first hurdle in completion of the overall project, and prevented any useful code from being generated. This points to a need for a standard format for WHOIS information to provide the ability for applications to have consistent access to this data. Regardless, a start would be to simply display the information returned from the WHOIS request. Only tier 3 really requires this information to be parsed out in detail.

Tier 2 follows fairly straightforwardly from tier 1, as it only displays the same information in a graphical format. There are a few graphical interfaces for existing traceroute tools (like the GNOME Network Tools) that can be used as examples.

The most difficult step is up to tier 3 – mapping the locational information onto a physical map of the world. There are plenty of open source mapping solutions (opensourcegis.org lists many), but unfortunately the data that they work on is not open source. There are also web-based Web Services applications that can provide the same information (mapblast.com, mapquest.com, among many others), but at a cost to the end user. This presented an extreme difficulty for this project. Generating data for these different applications to use was beyond the scope of this project, and even a small subset of data is not really available to make a proof-of-concept available. This points to a need for a non-proprietary map database to allow such projects to be written as open source. Regardless, this proposal presents many interesting improvements to the traceroute application that can be implemented in the future.