

# Internet Toolbox

Ronn Ritke\*  
San Diego Supercomputer Center,  
University of California, San Diego,  
9500 Gilman Drive, La Jolla, CA 92093-0505  
ritke@nlanr.net

**Key words:** Internet Tools.

---

\*Ronn Ritke is the corresponding author, Fax: 1 858 534-5113

# 1 Introduction

Different network tools have been developed over the years for diagnostic and measurement purposes. There are a large number of available measurement tools, which were developed by individual researchers or by research organizations. The Cooperative Association for Internet Data Analysis (CAIDA) [5] has generated a comprehensive taxonomy which lists and organizes a broad collection of network measurement tools [4].

An organized listing and brief explanation is given for a number of Internet tools. The following categories are used to organize the Internet tools: Packet Collection Software, Bundled Packet Collection Software, Internet Measurement, Internet Throughput, ISP Measurements, Internet Cloud Measurements, High Performance Measurement Tools, Analysis Tools, and Traffic Generators.

## 2 Existing Tools

### (1) Packet Collection Software

These are tools which collect traffic measurements on a packet by packet basis. Key examples follow. **Tcpdump** [14] [38] is a Unix and Linux operating system portable packet collector that captures information from the packet traffic on a network. Tcpdump is a "passive" tool: it monitors the network traffic and does not inject traffic into the network. Other tools are active (they do inject traffic into the network). When tcpdump is used for traffic traces, the host computer is put in promiscuous mode and all packets (whether or not it was addressed to the host computer) is pulled into the host computer. A number of filtering options are offered by tcpdump. The tcpdump software can collect either the packet header or the whole packet and can capture all or some of the packet data (TCP, UDP, etc.). For example, filtering allows for the capture of only TCP traffic, only port 80 http traffic, etc. Tcpdump works in conjunction with **libpcap** [16] which is a packet dumping program. A sample libcap application **pcapture** [33] captures all the packet data to disk.

As network speeds increase and the amount of data also increases, the ability to take in

and store the desired information without overwhelming the host computer is an important issue. The BSD Packet Filter [17] does preprocessing below the application level in order to allow the host computer to take tcpdump traces on high speed networks which carry large amounts of data. The idea is to discard all unnecessary data (packets) as soon as possible (at a low level) in order to save CPU cycles. Processing packets at a lower level saves the CPU cycles that would be needed to move any discarded packets to the higher application level for processing.

**Packetman** [30] runs on Unix and DOS and is a LAN-oriented packet dump program. **IP-Traf** [11] is an IP LAN monitor which creates network statistics and provides post-processing perl scripts. Intended for general purpose packet analysis, **Argus** [1] provides a packet storage and analysis environment.

## (2) Bundled Packet Collection Software

This Bundled Packet Collection Software software collects packet traces and provides packet stream analysis and statistics. Some of the Bundled Packet Collection software comes with the Operating System. For example, the Sun Solaris OS contains a packet collector named **snoop** [36]. Likewise, **Iptrace** [13] is the IBM AIX packet collection program. There are also commercial Software Packet Analyzers which are not included in the OS and are not free. An example is **EtherPeek** [8], a Windows and Apple based Ethernet packet analyzer.

## (3) Internet Measurement

Internet measurement tools use “probing packets” which are injected into the network to gather various information including network performance measures. **Ping** [34] is probably the best known and most commonly used Internet measurement tool. It can determine if a machine is reachable, and may provide information on delay. Within the class of Internet measurement tools, the Hop by Hop characterization tools (also based on probing packets) determine Hop by Hop delay on a path from a source to a destination. An important example is Traceroute [40] [14], which is an Internet utility that sends UDP packets to a selected destination. The destination sends back an ICMP message. Traceroute sends out the first UDP packet with a hop count to destination of one and successively increases this

count by one. Each increase allows the UDP packet to travel one more hop to the destination see (Figure 1). An intermediate gateway will send an ICMP packet if the maximum hop count for the packet has been reached. In essence, each gateway on the way to a destination will send back an ICMP message. These messages give the hop count and the delay to each gateway on the path to the destination. Traceroute identifies each intermediate node on a route and the round trip delay to each node.

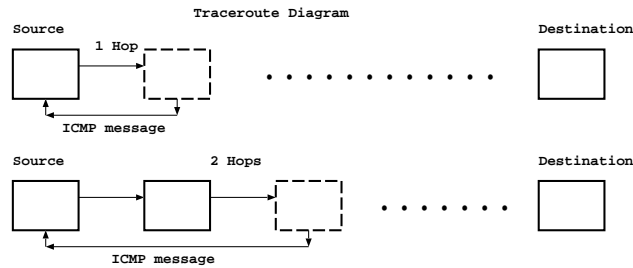


Figure 1:

**Nikhef traceroute** [25] is a traceroute variant that allows a number of options. The user may skip the first few hops, or request the min/ave/max round-trip times for each hop. **Pathchar** [31] sends a number of packet sizes to each hop in order to estimate performance characteristics for each hop as a function of packet length on a path from a source to destination.

A number of sites around the world are part of the Surveyor [37] project. This tool has the ability to monitor one-way delays by using timestamps and Global Positioning Satellite (GPS) technology to obtain accurate transit interval measurement by virtue of time synchronization (via GPS). Surveyor machines periodically send ping packets to each other (full mesh coverage). Two key network performance metrics are measured; packet loss and one-way delay between the 61+ different Surveyor sites. Surveyor can also conduct passive tests.

NLANR has an active monitor program [27] that provides round trip information (min, mean, max, etc.) and packet loss percentages from the 124+ active monitor sites.

#### (4) Internet Throughput

These tools give bandwidth information for an end to end path. **TReno** [42] creates a very simplified, user level implementation of a TCP-like transport protocol. This allows for the measurement of throughput independent of the actual TCP implementation used in the Host. It is a good reference platform for prototyping TCP changes and determining the bandwidth a process would get if it were running over the most recent TCP version. Another interesting end-to-end tool is **bing** [3]. While keeping the amount of extra traffic low, bing compares round trip time for different packet lengths and determines link bandwidth. **{b|c}probe** [2] is really two programs. Bprobe can be used to check the capacity of a bottleneck link. Cprobe sends out a small stream of packets, measures the packet separation upon return and from this determines the amount of bandwidth available taking into account the bandwidth demands of competing traffic. Other tools widely used in the Internet and related to the above are:

(a) **Systematic Pinging**: the periodic or systematic use of the ping mechanism for Internet response times.

(b) **Internet Traffic Reports** [9]. These provide a 7 day 24 hour graph of Internet response times.

(c) **MIDS Internet Weather Report** [18] shows latency data over long time scales. It displays latency distributions on mercator-projection maps across time.

(d) **Traceping** [41] uses traceroute and ping to determine packet loss rates to different destinations.

#### (5) ISP Measurements

This class of tools is used to measure the performance of the various Internet Service Providers along an end-to-end internet path. **ClearInk Weather Report** [6] periodically pings different sites to help determine in which Internet provider problems lie. It attempts to measure performance on the Internet. **Inverse Internet Measurement Service** [10] creates ISP performance profiles. This allows for the comparison of performance for different ISPs. **National Internet Measurement Infrastructure** [20] is based on Vern Paxson's

Network Probe Daemon (discussed below). It is designed to measure the global Internet.

#### (6) Internet Cloud Measurements

**Network Probe Daemon** [21] is a prototype of Internet measurement infrastructure. Used by Vern Paxson to characterize end-to-end Internet routing. **NetNow** [22] measures packet loss and latency across components of the Internet. **IPMA** [12] has a number of monitors in over 10 different countries. It collects statistics on latency, packet loss and routing.

#### (7) High Performance Measurement Tools

In this category one finds tools typically used to measure throughput and other key performance parameters in high performance networks. **Netperf** [23] can measure LAN based network performance such as latency, throughput and TCP transaction speed. This is done on a point-to-point basis. **Ttcp** [43] can also be included in this class. It can be used as a throughput benchmark as well as a load generator. **NetSpec** [24] is a scripting language for writing throughput benchmarks with complex communication and workload patterns.

#### (8) Analysis Tools

The network trace data is typically processed and analyzed using a variety of traffic analysis tools in order to extract various types of views. Important examples follow.

**Tcptrace** [29]: this program reconstructs individual TCP connections from different format packet traces (tcpdump, etherpeek, etc.) and provides detailed connection information.

**Tcpanaly** [32] analyzes packet traces from tcpdump. This analysis includes diagnosing performance and congestion problems.

**Tracelook** [39]: allows the user to graphically view tcpdump trace files that use the -w tcpdump option.

**Xplot** [44]: this tool is used by tcptrace to graphically display its outputs.

#### (9) Traffic Generator

Sugih Jamin applied the idea of creating a TCP network traffic generator (tcplib) [7] that was based on the characterization of the well known port applications from empirical data. Network traffic traces were used to identify the core applications that have the largest

percentage of the total packets sent. Each of the core well known port applications was then analyzed and modeled. The output of tcplib is the combined output of each modeled application. HTTP traffic was less than 1% of the total traffic at the time and so it was not included in the tcplib traffic generator [7].

## References

- [1] Argus <ftp://ftp.sei.cmu.edu/pub/argus-1.5/>.
- [2] {b|c} probe <http://www.cs.bu.edu/students/grads/carter/tools/Tools.html>
- [3] bing <http://spengler.econ.duke.edu/ferizs/bing.html>
- [4] CAIDA Measurement Tool Taxonomy <http://www.caida.org/tools>.
- [5] CAIDA <http://www.caida.org>.
- [6] ClearInk Weather Report <http://www.internetweather.com/>
- [7] P. Danzig and S. Jamin, 1991: tcplib: A Library of TCP internetwork Traffic Characteristics. Report CS-Sys-91-01, Computer Science Department, University of Southern California, 1991.
- [8] EtherPeek <http://www.aggroup.com/prodinfo/products.html>.
- [9] Internet Traffic Reports <http://www.internettrafficreport.com>
- [10] Inverse Internet Measurement Service <http://www.inversenet.com/products/index.html>
- [11] IPTraf <http://cebu.mozcom.com/riker/iptraf/index.html>.
- [12] IPMA <http://www.merit.edu/ipma>
- [13] iptrace IBM
- [14] V. Jacobson, "traceroute", V. Jacobson, <ftp://ftp.ee.lbl.gov/traceroute.tar.Z>.

- [15] Van Jacobson, Craig Leres and S. McCanne, 1989: The Tcpdump Manual Page. *Lawrence Berkeley Laboratory*, <http://ee.lbl.gov/>, <ftp://ftp.ee.lbl.gov/tcpdump.tar.Z>.
- [16] libpcap <http://ee.lbl.gov/>.
- [17] Steven McCanne and Van Jacobson, The BSD Packet Filter: A New Architecture for User-level Packet Capture. *USENIX conference*, Jan. 25-29, 1993, San Diego, CA. Available using anonymous <ftp://ftp.ee.lbl.gov/bpf.tar.Z>.
- [18] MIDS Internet Weather Report <http://www.mids.org/weather/>
- [19] Multi Router Traffic Grapher (MRTG)  
<http://ee-staff.ethz.ch/oetiker/webtools/mrtg/mrtg.html>.
- [20] National Internet Measurement Infrastructure (NIMI)  
<http://www.psc.edu/networking/nimi/ure>
- [21] Network Probe Daemon <http://nic.merit.edu/ipma/npd/>
- [22] NetNow <http://nic.merit.edu/ipma/netnow/>
- [23] netperf <http://www.cup.hp.com/netperf/NetperfPage.html>
- [24] NetSpec <http://www.ittc.ukans.edu/Projects/AAI/products/netspec/>
- [25] Nikhef traceroute <ftp://ftp.nikhef.nl/pub/network/traceroute/>
- [26] NLANR Measurement & Operations Analysis Team Web Page. <http://moat.nlanr.net/>.
- [27] NLANR AMP Project for HPC sites <http://amp.nlanr.net/AMP/>.
- [28] NLANR packet traces and tools <http://moat.nlanr.net/Traces/>.
- [29] Shawn Ostermann, Tcptrace Software Web Page.  
<http://jarok.cs.ohiou.edu/software/tcptrace/tcptrace.html>.
- [30] Packetman <http://www.cs.curtin.edu.au/netman/etherman.html>.

- [31] pathchar <ftp://ftp.ee.lbl.gov/pathchar/>
- [32] V. Paxson, 1997: Automated Packet Trace Analysis of TCP Implementations. *Proc. SIGCOMM 97*, available from <ftp://ftp.ee.lbl.gov/papers/vp-tcpanaly-sigcomm97.ps.Z>.
- [33] pcapure <http://ee.lbl.gov/>.
- [34] Ping <ftp://ftp.arl.mil/pub/ping.shar>.
- [35] RIPE NCC <http://www.ripe.net/>.
- [36] snoop Sun Comes with Sun Solaris OS.
- [37] Surveyor Home Page <http://io.advanced.org/csg-ippm/>
- [38] tcpdump <http://ee.lbl.gov/>.
- [39] Tracelook <http://ita.ee.lbl.gov/html/contrib/tracelook.html>.
- [40] Traceroute <ftp://ftp.ee.lbl.gov/traceroute.tar.Z>
- [41] Traceping <http://www-nplvms.physics.ox.ac.uk/>
- [42] TReno <http://www.psc.edu/networking/treno>
- [43] ttcp <ftp://ftp.arl.mil/pub/ttcp/>
- [44] xplot <ftp://mercury.lcs.mit.edu/pub/shep/xplot.tar.gz>.