The Software Tools for Networking column contains brief presentations of software tools that are freely available on the Internet and could be useful for the readers of this magazine. Each presentation is based on an extended abstract submitted by the authors of the tools that was copy edited and checked for accuracy against the version of the tool available on the Internet. Authors willing to have their tools presented in this manner should send a 300-word description of their tool in ASCII format with the URL of the tool by e-mail to Olivier Bonaventure (Olivier.Bonaventure@info.fundp.ac.be) with an indication that the description is submitted for the *IEEE Network* Software Tools for Networking column. Appropriate tools will be presented in this column.

Olivier Bonaventure
Infonet Group,
University of Namur (FUNDP), Belgium

Pathrate

C. Dovrolis, http://www.pathrate.org

Pathrate is a tool that is able to measure the capacity of network paths. Two bandwidth metrics that are commonly associated with a path are the capacity and available bandwidth. The capacity is the maximum throughput the path can provide when there is no competing traffic load (cross traffic). The available bandwidth is the maximum throughput the path can provide to a flow, given the current cross traffic load.

Pathrate is based on the dispersion of packet pairs and packet trains. It uses many packet pairs (with packets of variable size) to uncover the generally multimodal bandwidth distribution characteristic of the path. The local modes in this distribution are possible values for the capacity of the path. Then pathrate uses long packet trains to estimate the so-called asymptotic dispersion rate (ADR). The capacity of the path is always larger than the ADR. Among the local modes that are higher than the ADR, pathrate chooses the strongest and narrowest mode as the final capacity estimate.

Pathrate was designed to be robust to cross traffic effects, meaning that it can measure the path capacity even when the path is significantly loaded. This is crucial, since the hardest paths to measure are the heavily loaded ones. Pathrate differs from other bandwidth estimation tools, such as pathchar, clink, pchar, nettimer, and pipechar, which attempt to measure the capacity of each link in the path. The technique they use, however, often provides wrong estimates when the path includes "hidden" layer 2 switches.

Pathrate is publicly available with source code, documentation, and installation instructions. The tool is actively maintained and runs on all major UNIX systems, and does not require superuser privileges.

SProbe

S. Saroiu, P. Krishna Gummadi, and S. Gribble, http://sprobe.cs.washington.edu

SProbe is a tool for measuring bottleneck bandwidth in an uncooperative environment (i.e., one in which measurement software is deployed only on the local measurement host). SProbe uses the packet pair technique and exploits properties of the TCP protocol in a manner inspired by Savage's Sting tool. SProbe takes no more than three round-trip times (RTTs) to produce a single estimate.

SProbe can measure bottleneck bandwidths in both directions of a network path. To measure bottleneck bandwidth to a remote host, using its default settings, SProbe sends six TCP SYN packets to an inactive port on the remote host and receives six TCP RST packets. Several heuristic tests check for abnormal packet arrival times to detect cross traffic — foreign traffic that can alter the accuracy of an estimate. For a single measurement, SProbe generates 3160 bytes and receives 240 bytes.

To measure bandwidth from a remote host, SProbe relies on application-level protocols. Currently, SProbe contains protocol modules for measuring bottleneck bandwidth from Web servers and Gnutella peers. For Web servers, SProbe generates an HTTP get request with a large TCP maximum segment size (MSS). SProbe waits for the Web server to send two large back-to-back packets and measures their interarrival times, producing a bottleneck bandwidth estimate.

SProbe is distributed with source code and installation instructions. It was tested on Linux platforms with kernel versions 2.2.x and higher, and FreeBSD 3.4 and 4.2 platforms. SProbe uses the up-to-date libpcap library (v. 0.6.2), included in SProbe's distribution. SProbe also uses a software firewall, ipfw, supported in typical installations of RedHat 7.x and FreeBSD 4.2. Finally, SProbe makes use of raw sockets, and therefore needs to execute under root privileges.

NEM

D. Magoni, http://www-r2.u-strasbg.fr/nem

NEM is a network topology generator, analyzer, and converter. It was developed to manipulate graphs that model the Internet topology.

The generator module creates graphs that comply with the power laws recently discovered in the Internet topology. It supports several techniques to generate graphs, including the map sampling algorithm, the extended scale-free model, or the power-law out-degree algorithm. NEM supports graphs of any size, but the presence of power laws is only possible in graphs having at least a few hundred nodes.

The analyzer module allows analysis of the topological properties of graphs and supports properties like the degree distribution (mean degree, max degree, degree exponent, rank exponent, etc.), the distance and eccentricity distributions (average path length, eccentricity, radius, diameter, ...), the connectivity, the biconnectivity if the graph is not directed (cut-points, bridges, biconnected components, etc.), and the number of distinct shortest path distributions.

The converter module allows NEM to be used in combination with other Internet topology modeling tools. NEM can import graphs produced by generators such as Tiers, GT-ITM, BRITE, or Inet2.x as well as maps like the AS maps produced by NLANR or Mercator. The graphs produced by NEM can be exported in the GT-IM alternate format or the LBNL ns-2 TCL format.

NEM is available with source code and is written in C++. It has been tested on Linux, Windows, and Solaris, but should be easily portable to other C++ compilers with full STL support and standard libraries. The NEM distribution contains a manual that describes the capabilities of the tool and a list of references.

bgptools

N. Feamster, http://nms.lcs.mit.edu/bgp/

Several researchers have analyzed the behavior of the BGP routing protocol on the basis of traces of BGP messages collected by routers running the zebra or MRT BGP implementation. The bgptools package provides a set of tools that can be used to automate this type of analysis. bgptools provides both a

standalone tool called bgpdump and the "libbgpdump.a" library that ease the parsing of BGP message traces in MRT format. bgpdump is also able to produce the graphics of the prefix trees corresponding to the parsed BGP messages, and is also able to insert the parsed BGP messages in an SQL database to allow more detailed analysis. A second application provided with the bgptools package is "traced," a daemon that can automatically perform a traceroute to a destination that appears in a BGP withdraw message. This tool can be used to track in real time the impact of the received BGP withdraw messages.

The bgptools package has been developed on RedHat Linux 7.1, but should be portable to other UNIX systems. The current package relies on the MySQL database and contains source code and installation instructions.