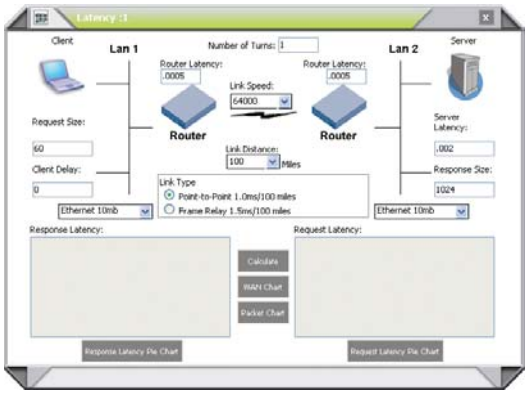
NETWORK PERFORMANCE TOOLKIT

There are hundreds of free tools that claim to help network professionals do their jobs. But how do you sort out the toys from the power tools? Respected NetAnalyst and network performance advisor Bill Alderson recommends the following free tools for Network Engineers interested in improving the performance of their enterprise networks and the applications that run on them.

Latency Calculator

Meet the Swiss Army knife for network and performance tasks! The NetPerformance.com calculator offers 10 different tools. The most powerful and complex of these is the Latency Calculator. It models a client-server environment, where both client and server are attached to local area networks, and each network is attached to a router, where the client-side and server-side routers are attached through some kind of wide area link. To calculate latency times, the tool also lets you input arbitrary request and response sizes, and lets you set delays for the client itself. Then, for each of a pair of routers, you can set router latency, wide area link speed and distance, to model the WAN portion of the connection. On the server side, you can set Server Latency and response size. You can then click the Calculate button to produce response latency and request latency values, with accompanying pie charts to show how overall delay breaks across the various input values provided. You can also use the input data to produce a WAN bar chart that helps model variable data rates for frame relay or constant bit rates on T1 links. Taken all together, this is a valuable tool for modeling network latency and playing what-if games as values change. The other tools include subnet and multicast address calculators, a link speed calculator, a decimal to/from hex converter, an OUI lookup tool, and more. Register for free to receive this tool at *www.netperformance.com/calculator/index.html*.



Latency Calculator

Start Using it Now.

Jperf Gives Iperf a GUI, and Makes Modeling IP Network Traffic Easy

Iperf is a well-known TCP and UDP bandwidth modeling and performance measurement tool, developed at and copyrighted by the University of Illinois, and freely available to the general public. Iperf's roots lie deep in the Unix/Linux world, and explain why this program operates exclusively from the command line. Though powerful and capable, this character-mode, keyboard driven interface makes it difficult for some and clunky for others to use. In coming to the rescue, Jperf not only provides a Java-based graphical front end to Iperf that makes it easier to use, it also produces nice charts and graphs to report the results of the tests performed between a client machine and a server machine (both of which must run the software to make this tool work). The Iperf-Jperf combination proved to be just the thing to help us model mixes of small-packet UDP traffic and large-packet TCP traffic, just like you'd see when both VoIP and TCP applications are active on a single cable segment or VLAN. It also lets us observe the effects that occur when two or more TCP clients share a cable segment and establish connections with a server, through the handshake, through Slow Start, into congestion avoidance behavior, and even back into Slow Start when two or more segments were dropped. Here again, Jperf's charts and graphs provided great visualizations to let us see how traffic behaved on the network. Together, Jperf and Iperf make a great toolset, one that is best addressed by grabbing the so-called Iperf distribution, which combines both Iperf and Jperf in a single Windows installer package. Grab Iperf by visiting the projects page for Iperf, and searching on Iperf or Kperf; this page resides at *http://dast.nlanr.net/Projects/Iperf/*.

More than Reachability:

Using a TCP Traceroute Utility

TCP Traceroute sends TCP segments instead of ICMP messages between pairs of routers as they work their way from the original sender to the designated receiver. This helps model real network latency more effectively than an ordinary traceroute utility, not only because of the TCP connection set-up time that is automatically included, but also because segment sizes may be set at will (1500 is a typical max, and represents applications that transfer larger amounts of data quite nicely, but anything as small as 48 bytes is valid). As an added benefit, using TCP traceroute also sidesteps issues that can occur when ICMP traceroute packets are rejected by intermediate routers. For security reasons, this occurs all too frequently on the public Internet, as service providers lock down devices to protect them from potential threats, and to extract as much performance out of them as they can. This article features the tracetcp utility from SourceForge.net (*tracetcp.sourceforge.net*) which in turn requires the promiscuous mode packet capture driver known as WinPcap,

WinPcap

www.winpcap.org, to be pre-installed to work properly. Both items are free, easy to find, install and use, and make a useful addition to any network engineer's box of software tools. When working with tracetcp, we had to increase the number of pings per hop to five to produce at least one response from the intermediate routers between the sending client and the target host. We also had to dig up the readme.txt file bundled with the program to learn that "-?" displays its help information (something that proved very helpful as we learned how to use this nice little tool).

SysInternals TCPView

SysInternals TCPView is the brainchild of well-known Windows guru Mark Russinovich, who has honed this tool into its current final shape from 1997 through 2002. It's a very capable software TCP monitor that provides the same kind of information that netstat makes available at the Windows command line. The biggest differences between the two tools is that TCPView runs as a standalone graphical Windows application so that its output appears in tabular format inside a window pane that gets dynamically updated every second which is a default setting that you can alter, should you wish to do so.

You will also find several added bonuses in TCPView. For example, the process name that owns each TCP connection and UDP endpoint is listed in its own column. You can also capture the entire content in the display pane in tab-separated text format using a nice text snapshot facility. As new TCP connections are created or UDP endpoints are opened, they are highlighted in green during the polling interval during which they appear. Likewise, old TCP connections or UDP endpoints show up in red just before they are torn down or endpoints are closed. You can also toggle unconnected endpoints on and off inside the display pane, when unconnected endpoints are toggled off. This limits the display so that only to active TCP endpoints are shown; which in turn effectively shuts off all UDP endpoints and all inactive TCP endpoints as well. This thoroughly useful and informative tool is available as a free download from the Sysinternals Networking Utilities download page at *http://www.sysinternals.com/NetworkingUtilities.html*.

SysInternals TCPView

More Tools and Resources

There are more tools and resources available for Network Engineers and Administrators at *www.netperformance.com*.