

TITLE OF THE INVENTION

Network Fault Analysis Tool

5

BACKGROUND OF THE INVENTION

Network tools are used to monitor and diagnose network faults. These tools typically monitor network traffic and make determinations regarding transfer times and packet loss. Most of these tools provide testing across Open System Interconnection (OSI) layer 1 and 2 (Physical Layer and Data Link Layer) only. Further, many of these
10 known tools are topology dependent, in that they must know the layout of the network in order to monitor and test the network. As the network changes, the tool information must be updated to keep up with the current network topology. Another problem associated with existing network tools is that they may generate heavy network loads in order to conduct tests and make measurements, which affect the network users. It would be
15 desirable to have a network tool which provides testing capabilities across multiple OSI layers, which is topology independent, and which only generates a minimal amount of network traffic necessary to obtain the desired results.

SUMMARY OF THE INVENTION

20

With the foregoing background in mind, it is an object of the present invention to provide a testing tool for Internet Service Provider (ISP) network engineers which is used to diagnose network faults, characterize network performance and evaluate new equipment and software releases. The tool can be used to schedule and run proactive tests to identify network problems before subscribers are affected. Further, the tool can
25 be used to provide testing on demand to quickly isolate the root cause of a problem identified by the tool or by network management systems or subscribers. The tool is topology independent and thus does not have to be reconfigured as the network changes. The tool only sends traffic as directed by the network engineer and thus does not generate undesirable heavy network traffic loads, unless such a heavy network loads are desired by
30 the network engineer.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be better understood by reference to the following more detailed description and accompanying drawings in which:

Fig. 1 is a block level diagram of the network fault analysis tool of the present invention;

Fig. 2 is a flowchart representing a web characterization application;

Fig. 3 is a flow chart representing a network performance characterization application; and

Fig. 4 is a flow chart representing a multi-size packet pinger.

DESCRIPTION OF THE PREFERRED EMBODIMENT

A tool for Internet Service Provider (ISP) engineers is presented. The tool provides network engineers with the ability to quickly write and deploy tests to diagnose network faults and to characterize network performance. Additionally, the tool is useful for evaluating new equipment and software releases.

The tool provides active testing capabilities across Open Systems Interconnection (OSI) layers two through seven (the data link layer, network layer, transport layer, session layer, presentation layer and application layer respectively). With the present invention, an ISP network engineer can test both basic connectivity and performance as well as common Internet applications and services such as HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP), Domain Naming System (DNS), Simple Mail Transfer Protocol (SMTP), and Post Office Protocol (POP). The network engineer can test the ISP network and can also test other locations accessible by the ISP's users, such as popular web sites.

The present invention can be used in two modes. In a first mode the tool is used to perform scheduled proactive testing and routining. In this manner network problems can be identified before subscribers are affected. In a second mode the tool is used to provide testing on demand in order to quickly isolate root causes of symptoms identified by the tool, reported by Internet subscribers or identified by network management systems.

Referring now to Fig. 1, the tool 10 comprises a hardware/software system specifically developed for Internet testing and fault isolation. The tool includes protocols 11, commands 12 and Internet test function libraries 13. The tool also includes test applications 14, user interfaces 15 and 18, and an Application Program Interface (API) 17.

Protocols 11 comprise custom developed, testing focused protocol stacks. Bit level and individual state transition-level control over the operation of all the protocols enable the users to quickly create tests that cannot be performed with standard protocol stacks.

Commands 12 allow the tool to perform protocol-level actions such as opening a Transmission Control Protocol (TCP) connection or requesting a HyperText Markup Language (HTML) file from a web server.

Test function libraries 13 provide convenient building blocks for developing test applications. A test function contains commands to execute a specific network test. For example, the "HTTP page access command" test function issues a GET request for a specified Uniform Resource Locator (URL), and then times and records important aspects of the response. In order to create a new test application, a user writes a script using the pre-written test functions. The test function library 13 includes the following functions.

The Internet Control Message Protocol (ICMP) Ping function sends a standard ICMP ping to the specified destination OSI (IP) address. Multiple pings can be sent with the retry option. Timing statistics are kept for each ping sent. By default, the number of responses and min/max/average round trip times are presented. Several standard error conditions are also reported.

The TCP Ping function attempts to open a TCP connection to the specified TCP port on the machine with the specified destination address. Multiple pings can be sent with the retry option. If a response is seen to a TCP ping, the IDU then closes the TCP connection. Timing statistics are kept for each ping sent. By default, the number of normal responses and min/max/average round trip times are presented. Several standard error conditions are also reported.

The HTTP Ping function extends the TCP ping function. For each ping, if a TCP connection is established an HTTP HEAD command is sent, and HEAD data is expected in response. The path for the head request defaults to "/", but can be optionally specified, and the port defaults to the standard HTTP port, but can be overridden. The function
5 opens a TCP connection to the specified server and issues a HEAD request (with configurable HTTP version) for the root of the document tree. The function also records and times the response. In addition to standard timing and success statistics, details about headers in the data returned is available.

The HTTP page access function is similar to the HTTP ping function, but gets the
10 entire page at the specified URL, and does not have a retry option. The function opens a TCP connection to a specified server and issues a GET request for the specified URL. The function times and records important aspects of the response.

The UDP Traceroute function performs a standard traceroute to a specified host. The maximum time-to-live for the packets (which limits the number of hops the
15 traceroute can cover) defaults to 255, but can be optionally set to any legal value. The destination UDP port may be specified or it can default to a randomly selected port number in a suitable range. The size of the UDP packets sent can be controlled. For each hop detected in the route to the destination, timing and success information is available, as is error information for several standard errors that can occur.

The TCP Traceroute function is similar to the UDP traceroute function except that
20 instead of sending UDP packets, TCP SYN packets are sent to the specified port. When the traceroute has progressed to the point that a packet reaches the final destination, this will attempt to open a TCP connection. If successful, the connection is then closed.

SMTP Mail related functions include SMTP ping, SMTP test mail, SMTP-DNS,
25 SMTP performance and SMTP Rx Mail. The SMTP ping function makes a TCP connection to a specified server, times the response and observes an expected banner message. The SMTP test mail function connects to a specified server and verifies that a mail message to a specified username is accepted, and times individual pieces of the transaction. The SMTP -DNS function, for a given email address, performs a DNS MX
30 query (from root servers or from specified nameserver) to determine destination SMTP server, then performs "SMTP Test Mail". The SMTP performance function connects to a

specified server and begins transferring a bulk test message (optionally delivered/aborted), measuring server's response time, and any observed message limit. The SMTP Rx Mail function starts an SMTP server listening for a client connection. After the client connects, the function expects, times and records details of an email message transfer.

POP3 Mail related functions include POP Ping, POP Rx Mail, POP Mail Purge, POP Mail View, POP Serve and POP Performance. The POP Ping function makes a TCP connection to a specified server, times the response and observes/records expected POP3 banner. The POP Rx Mail function connects to a specified server, authenticates with a provided username/password, retrieves list of messages and sizes. The POP Mail Purge function connects to a specified server and authenticates. The function then deletes specified message(s) without retrieving. The POP Mail View function connects to a specified server and authenticates. The function also records and times the retrieval of a specified portion of a specified message. The POP Serve function starts a POP3 server listening for a client connection. After the client connects, the function accepts any authorization attempt and any attempt to list or retrieve message(s). The client is told there is a single message, and any attempt to retrieve a message or messages will get the test message text. The POP Performance function connects to a specified server and authenticates. The function selects the largest queued message and retrieves sufficient quantity of data to make performance measurement.

DNS functions include DNS Ping, DNS Lookup, and DNS server. The DNS Ping function sends a simple UDP based DNS request to the specified name server and times and observes a correct response. The DNS Lookup function sends an arbitrary single UDP based DNS request to either the specified server, or performs a recursive lookup itself starting at a root server(for comparison). The function also times the response and records the result. The DNS serve function starts a DNS server listening for a client request. Details of the client request are recorded, and the specified result is returned to the client.

Web based functions include FTP Ping, HTTP Performance, HTTP Serve Test Page, HTTP Proxy Serve, HTTP Auth Looking-in and HTTP Auth Looking-out. The FTP Ping function opens a TCP connection to a specified server, time and records the

expected banner. The HTTP Performance function measures timing performance of web responses for several requests, in series and in parallel, for a specified URL. The HTTP Serve Test Page function starts an HTTP server listening as a proxy for a client request. The function records details of the request and returns the specified test page contents. 5 Optionally, the function will re-execute the request to the target server and return the actual content. The HTTP Auth Looking in function performs an HTTP Page Access, expecting an authentication request, and using the specified username/password. The function times and records each step of the process. The HTTP Auth Looking-out function starts an HTTP server listening for a client request. When the client request 10 arrives, the function requests and records authentication before delivering specified test page contents.

While a particular group of functions has been described, other functions may also be included. For example, the following functions could also be part of the Internet test function libraries 13. A Border Gateway Protocol V4 (BGP4) function comprises a 15 network to network routing protocol for autonomous systems. A Dynamic Host Configuration Protocol (DHCP) function is a protocol enabling dynamic addressing and configuration. An Internet Relay Chat (IRC) function establishes a protocol to implement chat functionality. A Network News Transport Protocol (NNTP) function enables news distribution from servers to subscribers. An Open Financial Exchange 20 (OFX) function enables electronic exchange of financial data over secure links (SET, SSL). An Open Shortest Path First (OSPF) function enables routing based on cost metrics.

Additional functions may include the following. A ReSerVation Protocol (RSVP) function enables reservation and prioritization of network paths. A Routing Information 25 Protocol (RIP) function enables routing based on a distance vector. A Remote Authentication Dial-In User Service (RADIUS) function provides authentication of remote dial-in users. A Real Time Streaming Protocol (RTSP) function enables continuous multi-media communications over the Internet. A Network Terminal Access (Telnet) function enables remote terminal access. A Voice over Internet Protocol (VoIP) 30 enables voice communication over the Internet.

The test application library 14 comprises Tcl scripts that use multiple test functions to perform a higher level task such as diagnosing a network fault or characterizing network performance. Test applications can be used in a proactive or reactive mode to identify network problems and diagnose and isolate their root causes.

5 Test application results can be made available to appropriate personnel via email or pager notification, enabling action to be taken as soon as possible. Example applications will be described in detail below.

Referring back to Fig. 1, the tool 10 also includes a Network Operations Center (NOC) Test WEB User Interface 15 which allows a network engineer to access the tool

10 from an authorized workstation 50. Access is done via a built-in Web-based user interface over a secure shell (SSH). Using the interface, the network engineer can run the tool applications and execute test functions

The tool 10 also includes a Tcl command line interface 16. Network engineers can run the tool applications and test functions from a Tcl command line interface via

15 secure shell (SSH).

The tool 10 also includes one or more custom application programming interfaces (API) 17. The API 17 may be used to interface the present tool with the APIs of existing monitoring and management systems. The API 17 is shown coupled to a workstation 40.

The tool 10 may additionally include an Administration Application 19 and a

20 User Interface 18. Administrative functions such as configuration and maintenance are performed using the administrative interface 18 secured via SSH.

As recited above, three examples of test applications of the test application library 14 are described in detail to show isolation and root cause analysis. The three described examples are a web characterization application, a network performance characterization

25 application, and a multi-size packet pinger application.

Referring to Fig. 2, a flow chart of the web characterization application 100 is shown. This application is executed on demand to assess network performance. This application is used to measure latency and packet loss behavior of the ISP, external networks, and a specified destination such as a web site. The following sequences of

30 tests are executed.

Initially, at step 110, the target web site is set. Next, as shown at step 115, the operational status of the target web site is ascertained and the appropriate test sequence is sent. While there are numerous test sequences, only a particular test sequence will be described in this embodiment. The following step, step 120, an HTTP ping of the target web site is performed. At step 125 the HTTP ping results are recorded.

The next step 130 involves a determination as to whether the HTTP ping results were positive. If the HTTP ping results are positive then a send HTTP page access command is issued as shown in step 135. The execution timing of the command and the data received are recorded as part of this step.

Upon obtaining negative results from step 130, step 140 is executed. Step 140 sends a TCP ping command. The execution timing and data received are recorded. Next, at step 145 a TCP Traceroute command is executed. The timing of this command and the data received are recorded.

The next step 150 involves a determination of whether the TCP Ping results are positive. If the results are positive, then step 155 is executed. Step 155 sends an ICMP Ping command. Following step 155, a Send UDP traceroute command is executed, as shown in step 160.

The next step to be executed is step 165. Step 165 is executed following step 160, by obtaining positive results from step 150, or upon completion of step 135. Step 165 organizes the test results, and step 170 displays the results.

Referring now to Fig. 3 a flowchart for a Network Performance Characterization application 200 is shown. This application 200 characterizes network performance by measuring latency and packet loss behavior of the ISP and the external networks to a specific destination server or router. The application accepts a list of systems to probe with a configurable ICMP or TCP pinger. The network performance characterization application 200 operates as follows.

A first step 210 sets a target list of routers or web sites to be characterized. The next step, step 220, sets the type, size and number of packets to send via each ping. At step 230 an ICMP/TCP ping of the targets is performed. The results of the pings are recorded in step 240. At step 250 the results are organized. The final step 260 involves displaying the network performance characterization results at the user web page.

Referring now to Fig. 4, a flow chart for a multi-size packet pinger 300 is shown. The multi-size packet pinger application 300 permits network engineers to send three simultaneous ICMP or TCP pings with each packet size set different from the others. For example, three ranges - small (1-192 bytes), medium (193 - 576 bytes) and large (577 - 1500 bytes). The purpose of this application 300 is to help identify routers in which packet loss increases due to the inbound packet size. The multiple-size packet pinger 300 operates as follows.

A first step 310 sets a target router or web site to be characterized. The next step, step 320, sets the type, size and number of packets to send via each ping. At step 330 ICMP/TCP pings of the target are performed. Pings having a packet size of 64, 256 and 1008 performed. The results of the pings are recorded in step 340. At step 350 the results are organized. The final step 360 involves displaying the results at the user web page.

By way of the above-described invention an ISP network engineer can diagnose network faults, characterize network performance and evaluate new equipment and software releases. The tool can be used to schedule and run proactive tests to identify network problems before subscribers are affected. Further, the tool can be used to provide testing on demand to quickly isolate the root cause of a problem identified by the tool or by network management systems or subscribers. The tool is topology independent and thus does not have to be reconfigured as the network changes. The tool only sends traffic as directed by the network engineer and thus does not generate heavy network traffic loads.

Having described preferred embodiments of the invention it will now become apparent to those of ordinary skill in the art that other embodiments incorporating these concepts may be used. Additionally, the software included as part of the tool may be embodied in a computer program product that includes a computer useable medium. For example, such a computer usable medium can include a readable memory device, such as a hard drive device, a CD-ROM, a DVD-ROM, or a computer diskette, having computer readable program code segments stored thereon. The computer readable medium can also include a communications link, either optical, wired, or wireless, having program code segments carried thereon as digital or analog signals. Accordingly, it is submitted

that that the invention should not be limited to the described embodiments but rather should be limited only by the spirit and scope of the appended claims.

What is claimed is:

- 1 1. A method comprising the steps of:
2 providing a processor capable of being coupled to a data network;
3 providing processor-readable storage for storing instructions and data;
4 performing with said processor at least one of testing said data network,
5 diagnosing a network fault and characterizing network performance of said data network;
6 and
7 wherein said instructions and data include at least one of protocol stacks,
8 commands for performing protocol-level actions, a test function library, a test application
9 library, a user interface, a command line interface, a custom API, and an administration
10 user interface.
- 1 2. The method of claim 1 wherein said step of performing includes the step of
2 scheduling proactive testing to identify problems before subscribers of said data network
3 are affected.
- 1 3. The method of claim 1 wherein said step of performing includes testing on
2 demand of said data network to isolate root causes of symptoms identified by at least one
3 of said tool, a subscriber of said data network, and a network management system.
- 1 4. The method of claim 1 further comprising the step of performing bit-level and
2 individual state transition level control over protocols.
- 1 5. The method of claim 1 wherein said test application library includes at least one
2 of a web characterization application, a network performance characterization
3 application, and a multisize packet pinger.
- 1 6. The method of claim 1 wherein said step of performing includes the step of
2 testing with protocols selected from the group consisting of IP, TCP, UDP, HTTP, ICMP,
3 SMTP, DNS, POP, FTP, RADIUS, HTTPS and PPP.

1 7. The method of claim 1 wherein said step of performing includes the step of
2 testing across at least one of OSI layers two through seven.

1 8. The method of claim 1 wherein said step of performing includes the step of
2 testing an ISP network.

1 9. The method of claim 1 wherein said step of performing includes the step of
2 testing of web sites accessible by users of said data network.

1 10. The method of claim 1 wherein said step of performing includes the step of
2 testing with a test application library comprising scripts using multiple test functions.

1 11. A tool comprising:
2 a processor capable of being coupled to a data network;
3 processor-readable storage for storing instructions and data for causing the
4 processor to perform at least one of testing said data network, diagnosing a network fault
5 and characterizing network performance of said data network; and
6 wherein said instructions and data include at least one of protocol stacks,
7 commands for performing protocol-level actions, a test function library, a test application
8 library, a user interface, a command line interface, a custom API, and an administration
9 user interface.

1 12. The tool of claim 11 wherein said instructions and data include commands for
2 scheduling proactive testing to identify problems before subscribers of said data network
3 are affected.

1 13. The tool of claim 11 wherein said instructions and data include commands for
2 performing testing on demand of said data network to isolate root causes of symptoms
3 identified by at least one of said tool, said subscribers, and a network management
4 system.

- 1 14. The tool of claim 11 wherein said tool is non topology-dependent of said data
2 network.
- 1 15. The tool of claim 11 wherein said protocol stacks allow bit-level and individual
2 state transition level control over protocols.
- 1 16. The tool of claim 11 wherein said test application library includes at least one of a
2 web characterization application, a network performance characterization application,
3 and a multisize packet pinger.
- 1 17. The tool of claim 11 wherein testing protocols are selected from the group
2 consisting of IP, TCP, UDP, HTTP, ICMP, SMTP, DNS, POP, FTP, RADIUS, HTTPS
3 and PPP.
- 1 18. The tool of claim 11 wherein testing occurs across at least one of OSI layers two
2 through seven.
- 1 19. The tool of claim 11 wherein said processor performs testing of an ISP network.
- 1 20. The tool of claim 11 wherein said processor performs testing of web sites
2 accessible by users of said data network.
- 1 21. The tool of claim 11 wherein said test application library comprises scripts using
2 multiple test functions.
- 1 22. The tool of claim 11 wherein said applications are integrated with an Application
2 Programming Interface (API) of an existing monitoring and management system.
- 1 23. A computer program product for a Fault Analysis Tool, the computer program
2 product comprising a computer usable medium having computer readable code thereon,
3 including program code comprising:

4 instructions and data for causing a processor to perform at least one of testing a
5 data network, diagnosing a network fault, and characterizing network performance of a
6 data network.

1 24. The computer program product of claim 23 wherein said instructions and data
2 include at least one of protocol stacks, commands for performing protocol-level actions, a
3 test function library, a test application library, a user interface, a command line interface,
4 a custom API, and an administration user interface.

1 25. The computer program product of claim 23 wherein said instructions and data
2 include commands for scheduling proactive testing to identify problems before
3 subscribers of a data network are affected.

1 26. The computer program product of claim 23 wherein said instructions and data
2 include commands for performing testing on demand of a data network.

1 27. The computer program product of claim 24 wherein said protocol stacks allow
2 bit-level and individual state transition level control over protocols.

1 28. The computer program product of claim 24 wherein said test application library
2 includes at least one of a web characterization application, a network performance
3 characterization application, and a multi-size packet pinger application.

1 29. The computer program product of claim 24 wherein testing protocols are selected
2 from the group consisting of IP, TCP, UDP, HTTP, ICMP, SMTP, DNS, POP, FTP,
3 RADIUS, HTTPS, PPP.

1 30. The computer program product of claim 23 wherein testing occurs across at least
2 one of OSI layers two through seven.

1 31. The computer program product of claim 23 wherein said data network comprises
2 an ISP network.

1 32. The computer program product of claim 23 wherein said data network includes
2 web sites accessible by users of said data network.

1 33. The computer program product of claim 24 wherein said test application library
2 comprises scripts using multiple test functions.

1 34. The computer program product of claim 24 wherein said applications are
2 integrated with an Application Programming Interface (API) of an existing monitoring
3 and management system.

1 35. The computer program product of claim 23 wherein said computer program
2 product is topology independent of said data network.