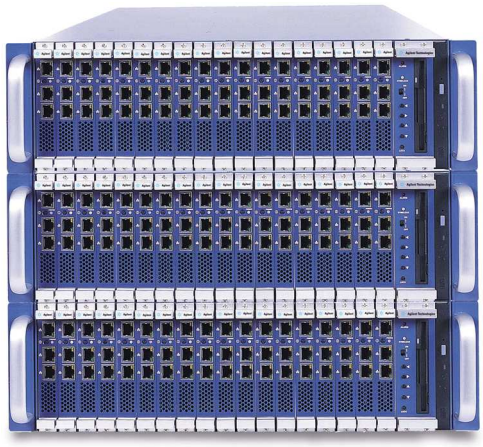
Agilent NetworkTester

Chassis-based Layer 4-7 Test Solution

N4180A/ N4181A/ N4182A

Technical Datasheet



Accelerate the development and deployment of network security and content-switching devices and networks.

Agilent Technologies

Key Features

- **Broad range of protocol bricks - simulate millions of real users**
- **Client and server emulation - one system, one user interface**
- **Powerful "Test Plan" design and management environment**
- **Stateful traffic over integrated IPSec, PPPoE, DHCP, 802.1x and VLANs**
- **Transaction Variability and Real-Time Control - no need for scripts**

Product Overview

The Agilent NetworkTester is a powerful test solution focused on performance testing of connection-aware and content-aware (Layer 4-7) devices and networks. NetworkTester offers Internet-scale, multi-protocol, multi-port client/server traffic emulation capabilities, delivering unprecedented realism, flexibility and control for your most complex test challenges.

Whether you are an equipment manufacturer, public network operator, or private enterprise network manager, you'll find NetworkTester applicable to a diverse set of network performance test problems.

Key product application areas include network security and content networking. Typical devices-under-test include firewalls, intrusion detection systems, virus, web and mail filters, content switches, SSL accelerators, load balancers and IPsec VPN concentrators. NetworkTester is specifically designed to test integrated devices where point test solutions fall short.

Equipment manufacturers use NetworkTester to load and stress test new products with Internet-scale traffic throughout the development lifecycle. Development costs and cycle times are reduced by finding complex traffic-related problems in the lab before deployment.

Public network operators and private enterprise network managers find NetworkTester an invaluable addition to their test labs. NetworkTester is applied before equipment purchases to verify vendor-reported networking capacity and performance. After equipment deployment, NetworkTester is utilized to perform off-line testing of new network configurations prior to exposure to live customer traffic.

Customer labs that have developed their own wall-of-PCs proprietary test solutions find that a migration to the NetworkTester reduces the total costs of solution ownership. Proprietary solutions take significant valuable resources to develop, maintain, upgrade and extend over time. NetworkTester makes the wall-of-PCs approach obsolete.

Agilent NetworkTester offers a complete multi-user environment for the development, management, execution and logging of performance test campaigns. The NetPressure software application is highly flexible and extremely powerful, allowing your team to easily build and run both simple and complex tests – without the need to develop test tool scripts.

Agilent NetworkTester delivers realistic Internet-scale traffic testing to your lab.

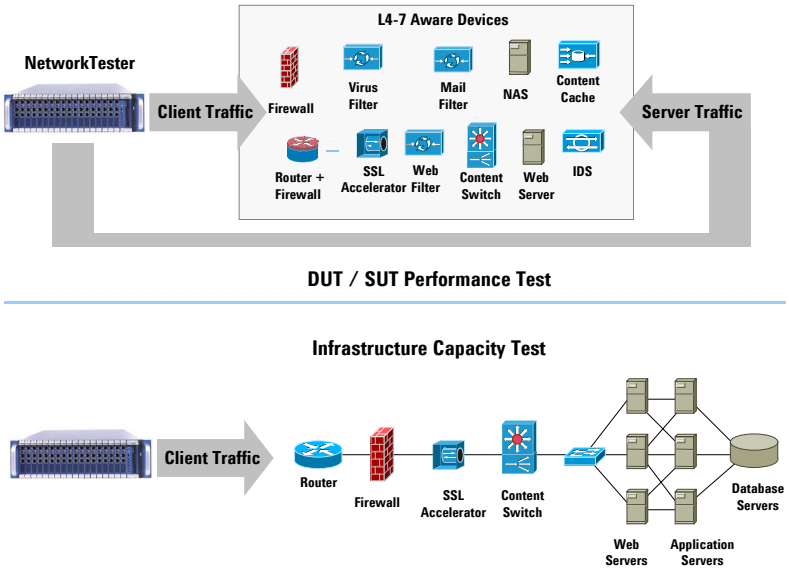


Figure 1: Agilent NetworkTester accelerates the development and deployment of network security and content-switching devices and networks.

Product Features

Internet-scale client/server emulation

NetworkTester is an extremely high performance traffic emulator. NetworkTester can generate Gigabit line-rate HTTP traffic at rates exceeding 1 million Gets/second. Up to 3 chassis can be chained into a single test system to provide traffic emulation capabilities that can cost-effectively load and stress test the largest devices and networks.

Emulated traffic can be made to appear to be initiated by millions of independent clients and servers. This powerful capability adds to the realism of the generated traffic and in testing DUT/SUT (Device/System Under Test) connection management capabilities.

NetworkTester's traffic scalability is designed to provide you with the power you need to test and measure the performance of your DUT/SUT in establishing, maintaining, and tearing-down connections at the Transport Layer, plus its functional performance in filtering, modifying, and switching data at the Application Layer.

10/100/1000 Mbps Base-T Ethernet port scalability

NetworkTester can be configured with up to 36 10/100/1000 Mbps Base-T Ethernet test ports per chassis or 106 test ports in a three-chassis test system. Users with multiport devices or network configurations will find this invaluable for thorough performance testing.

Each traffic blade can be configured as a server or a client. This further reduces your testbed cost, complexity, and footprint.

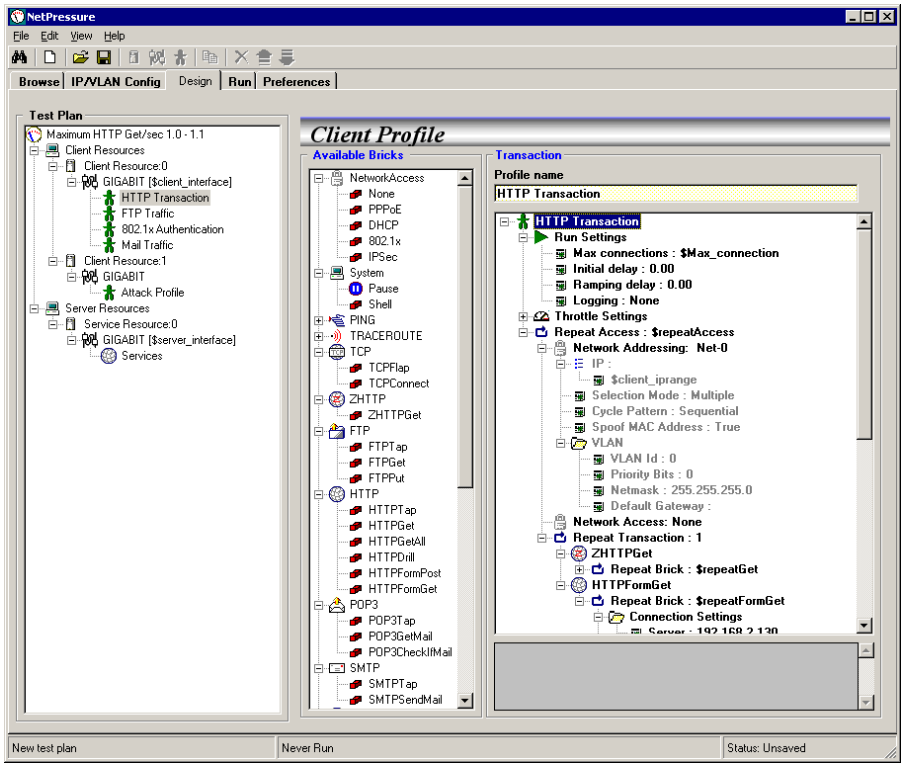


Figure 2: The NetPressure application provides a powerful and flexible test environment: Design, edit, manage and run realistic and complex tests, all through the graphical user interface.

Powerful test design and management environment

The NetPressure software application provides a complete environment for your layer 4-7 test and measurement needs that takes you far beyond traditional emulators.

From the NetPressure graphical user interface, you can graphically design, run, edit and manage your test plans. Common components and parameters such as URL lists can be defined independently and shared easily amongst test plans.

The powerful and flexible user interface allows you to create and run the complex and real-world scenarios that you always wanted to test – all without writing a single line of code.

Broad suite of TCP/IP protocols with emulation realism

NetworkTester supports a broad range of TCP/IP suite protocols, such as HTTP, HTTPS, FTP, SMTP, POP3, DNS, and RTSP, with each protocol offering a rich set of capabilities for emulation control. For example, with the HTTP client protocol emulation you can control aspects such as IP and Port addressing, cookies, whether SSL is to be used and SSL version, target URL lists, proxy server addresses and abort times. This allows you to generate protocol traffic with the characteristics you need.

Some next-generation firewalls and security gateways are designed to detect or prevent Trojan Horse attacks and other threats generated from inside the protected network that exploit weaknesses in internal LAN/WAN protocols and host configurations. By emulating file and print sharing application protocols such as NFS and SAMBA (SMB/CIFS), NetworkTester can test the effectiveness and performance of these network security devices.

By manipulating emulation parameters, you can also perform negative testing to verify behavior under abnormal conditions such as illegal protocol fields, unexpected messages, or non-standard message sequences.

Additionally, you can create traffic from multiple independent user groups using the same protocol, but with different emulation characteristics – e.g. different abort times to simulate user groups with differing 'think times'. This powerful feature allows you to create traffic patterns that accurately reflect the complexity of real world conditions.

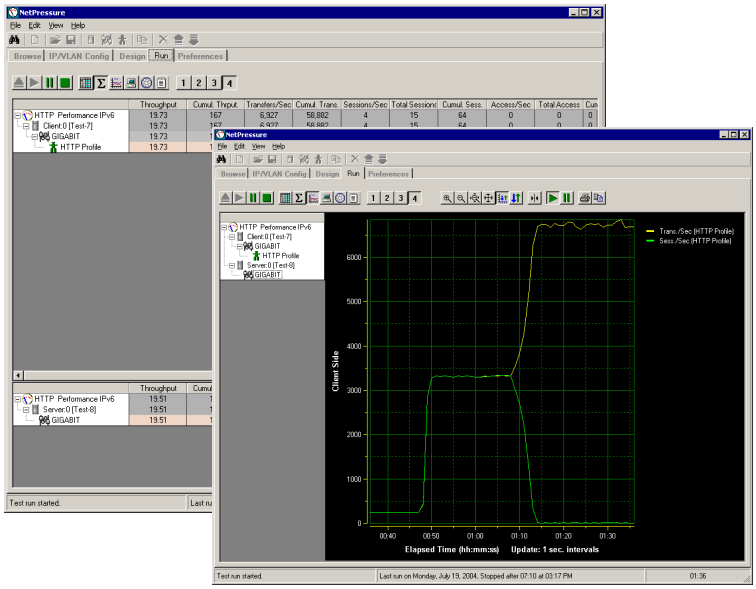


Figure 3: NetworkTester allows you to display results in both numerical and graphical formats

Broad range of access protocols including IPsec

Real-world test scenarios usually require one or more “access” or “support” protocols to set up connections. Network Tester integrates emulation of protocols such as IPsec, DHCP, PPPoE, and 802.1X, allowing you to configure addresses and establish connections automatically. You can create powerful and realistic test cases that set up multiple connections using access protocols (such as IPsec) and emulate real-world traffic using one or more service protocols (such as HTTP, FTP and SMTP) over the established connections.

Multi-protocol per port emulation

NetworkTester allows you to combine multiple protocols on any test port. For example, you can create realistic test scenarios that combine DHCP, DNS, HTTP and HTTPS emulation all on the same port.

Transaction Variability

The powerful NetPressure software application allows you to rapidly create powerful and realistic tests using named attributes, named lists, list functions, the string expression editor, and imported files. There is no need to develop scripts.

- All Parameters such as IP addresses that are used across multiple protocols, clients and servers can be set to variables known as named attributes. Set the value once and change it at will.
- Cycle through or randomize parameters such as IP addresses, port numbers and URLs from IP address ranges and named lists using built-in functions.
- Create "real" spam by varying the subject field and body for each message, based on named attributes and list functions, using the string expression editor.
- Attach files, such as your own web pages, email attachments and viruses. Filenames can also be varied.

Real-Time Control

Most parameters can be changed while the test is running -- there is no need to stop the test. This allows you to instantly observe the performance impact of almost any change you can dream of. For example, you can increase attack intensity, or change port numbers and IP addresses, or even the HTTP protocol version, while directly measuring session performance and application throughput.

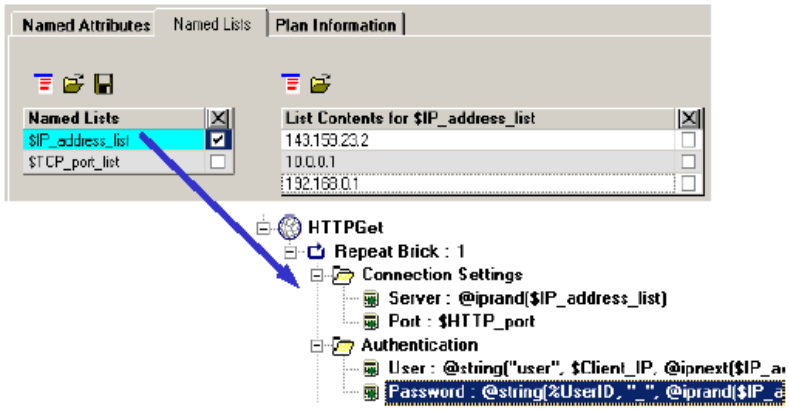


Figure 4: Create powerful tests using named attributes and lists, system values, list functions and the string editor.

Graphical and numerical measurement displays

NetworkTester allows you to view measurements during test execution in both numeric and graphical formats. Performance statistics such as messages per second, connections per second and total sustained connections are viewable for individually defined user groups and for the test system. Logging to a CSV format file is also supported for more detailed off-line analysis and record keeping.

Also provided are various windows for connection monitoring, system resource monitoring, and fault-finding. Together they provide a rich information source for rapid fault finding and trouble-shooting.

Stateful Transaction Spy

Traditional test tools allow you to capture, decode, and view protocol packets in their sequence of arrival. Network Tester goes one step further with its Stateful Transaction Spy. Because it is state-aware, you can determine the state of any connection or session – in real-time, without waiting for your test to complete.

The Stateful Transaction Spy speeds up your test creation, aids real-time monitoring during testing, and helps you find and solve problems while you analyze test results. For example, your test may have frozen and you could be waiting 30 seconds or longer for a HTTP session to time-out. This can be very frustrating, especially if it takes several attempts to diagnose the problem. With the Stateful Transaction Spy, you can instantly see that the HTTP session is timing out and you can rectify the problem fast.

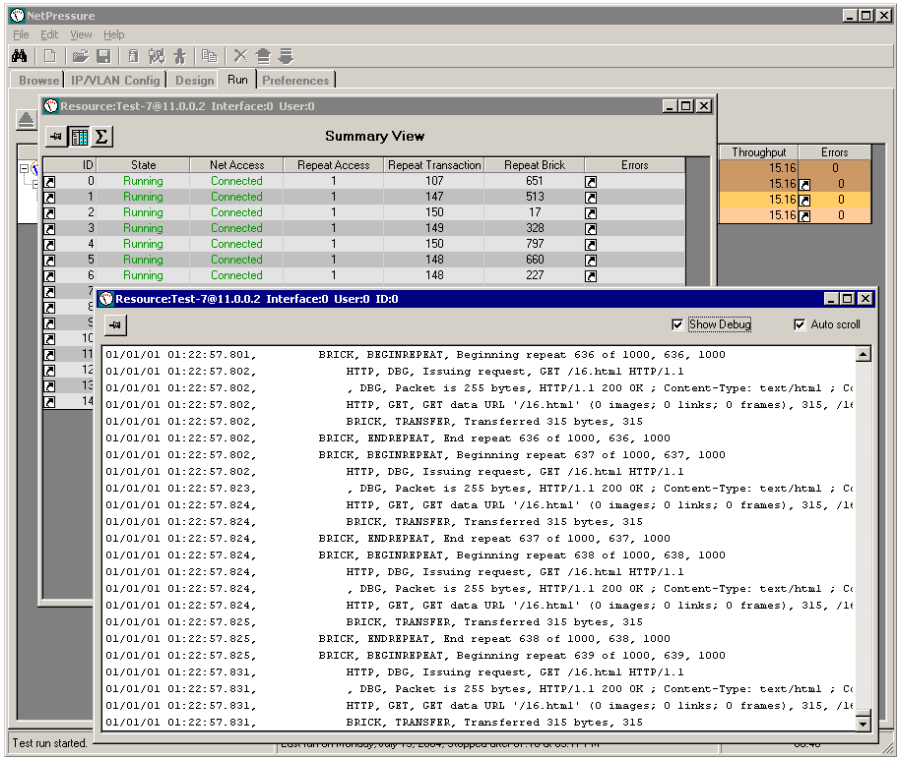


Figure 5: The Stateful Transaction Spy monitors the state of each emulated transaction in real-time

Multi-user remote access

NetworkTester can be used in either local or remote modes. Local operation can be carried out through a directly attached peripheral (rackmoutable keyboard, mouse, monitor optionally supplied).

Alternatively, NetworkTester can be connected to your corporate LAN so that multiple users can have concurrent remote access to test system resources, resulting in a very economical solution.

Test automation

With NetworkTester's powerful and flexible NetPressure software application, you do not need to develop test programs or edit scripts – even for realistic and complex test scenarios. However, if you do need to integrate Network Tester into a regression test environment, you can use its Tcl API (Application Programming Interface). Tool Command Language has become the defacto standard for test system control.

Using the API, you only need a few lines of code to load and run Test Plans (test configuration files) that you have created previously using the graphical user interface. This is, by far, the easiest way to automate your testing.

Negative Testing

To ensure the robustness of your device or system, NetworkTester's Packet Disruptor enables you to test under abnormal and adverse conditions using unexpected or incorrectly formed packet sequences. You can modify traffic generated from each port before it is transmitted using a range of useful packet filters to drop packets, fragment packets, resequence and replay packets, and corrupt checksums. Modified traffic can be specified by destination port number (TCP or UDP) and destination IP address so that you can simulate errors and attacks (such as packet fragmentation) that target individual users or services.

Technical Specifications

System Characteristics

Features	
Scalability	Internet-scale load and stress test Multi-port, multi-chassis
Usability	Highly intuitive graphical user interface Complete integrated test environment
Realism	Broad TCP/IP protocol emulation suite Multi-protocol emulation per port
Measurements	Numeric and graphical

Protocol Emulation

Network Access	
802.1x	Clients
DHCP	Clients
IPSec	Clients
• Mode	Transport, tunnel
• Authentication header mode	MD5, SHA1
• Encapsulated security payload	3DES, DES, Blowfish, AES
• Authentication method	Pre-shared secret, RSA DSS, Manual keys
PPPoE	Clients
Encapsulation	
802.1Q/VLAN	Clients and Servers (supporting all protocols over VLAN except NFS and SAMBA)
Utility	
Ping	Clients
TraceRoute	Clients
Transport	
TCP	Full stack
UDP	
Application	
DNS	Clients and Servers
FTP	Clients and Servers
HTTP	Clients and Servers, v.10, v.1.1 authentication, cookies, proxies, URLs, aborts
HTTPS	Clients; SSL v2, v3; TLS v1
IM	Clients & Servers
NFS	Clients
NNTP	Clients
POP3	Clients and Servers
RTSP	Clients and Servers (MPEG-II, MPEG-III, MOV)
SAMBA	Clients
SMTP	Clients and Servers
Telnet	Clients and Servers

Hardware Components

Chassis	
Quantity	1-3 per system
Slots	18 per chassis for blades
FDD	Integrated
CD	Integrated
Rackmountable	2-post mounts natively
Traffic Blade	
Quantity	1-53 per system; width of 1 chassis slot
Test Ports	2 per traffic blade
Test Port Types	10/100/1000 Base-T Ethernet
Test Port Connectors	RJ-45
Configurations	Swappable Client or Server Emulation
Controller Blade	
Quantity	1 per system
Location	Chassis 1 slot 1
Users	Up to 3 concurrent remote users
Ethernet Switch	(Optionally supplied)
Quantity	1 (24 port, 1U switch offered) per chassis
Rackmountable	Yes; kit not included
KVM	(Keyboard, Video, Mouse) - optionally supplied
Quantity	1 (1U) offered for local operation
Rackmountable	Yes; kit not included
Cables	
Quantity	1 per controller or traffic blade
Type	Shielded Ethernet; RJ-45

Mechanical and Electrical	
Chassis	
Physical	
Slots	18 (for blades)
Width	427.40 mm (19" rack mountable)
Depth	672.25 mm
Height	132.60 mm
Weight	~ 50 kgs (dependant on configuration)
Electrical	
AC Voltage	100 to 120V nominal 200 to 240V nominal
Frequency	50/60 Hz
Power Consumption	500 W maximum
Environmental Specifications	
Location	Indoor use only Altitude up to 2000 m
Operating Temperature	5° to 35C
Storage Temperature	-20° to 80C
Cooling Requirements	Gap of 2 mm required around vents Maximum 80% for up to 31°C Decreasing linearly to 50% at 40°C
Safety	Installation category: II Pollution degree: 2
Regulatory Approvals	
CSA	
CE	
ISM 1-A	

Configuration

Please see the NetworkTester Ordering and Configuration Guide for more information.

Product Numbers

N4180A - NetworkTester

Contains all the components to configure an initial complete system

N4180A-100 - NetworkTester Chassis

N4180A-001 - NetworkTester 10/100/1000 Base-T Ethernet Blade

Multi-rate Ethernet traffic blade, including NetPressure application software license for the blade

N4180A-002 - NetworkTester IPSec Software License

Adds IPsec protocol emulation to the NetworkTester system

N4181A - NetworkTester Chassis

Additional chassis for system expansion with optional accessories

N4182A - NetworkTester 10/100/100 Base-T Ethernet Blade

Additional traffic blade, including NetPressure application software license, for system expansion

This page intentionally left blank.

This page intentionally left blank.

Agilent's NetworkTester Solution

Agilent's NetworkTester solution offers a powerful and versatile test platform to address the evolving test needs of connection and content aware devices and networks. NetworkTester provides Network Equipment Manufacturers, Public Network Operators and Private Enterprise Network Managers with the industry's leading solution for multi-protocol, multi-port traffic emulation for performance analysis of today's L4-7 networking devices.

Warranty and Support

Hardware Warranty

Agilent warrants all NetworkTester hardware against defects in materials and workmanship for a period of 1 year from the date of delivery. Agilent further warrants that the NetworkTester will conform to specifications. During the warranty period, Agilent will, at its option, repair or replace the defective hardware. Services provided under this warranty will normally require return of the hardware to Agilent.

Software Warranty

Agilent warrants all NetworkTester software for a period of 90 days. Agilent warrants that the software will not fail to execute its programming instructions due to defects in materials and workmanship when properly installed and used on the hardware designated by Agilent. This warranty only covers physical defects in the media, whereby the media is replaced at no charge during the warranty period.

Software Updates

With the purchase of any new system controller Agilent will provide 1 year of complimentary software updates. At the end of the first year you can enroll into the Software Enhancement Service (SES) for continuing software product enhancements.

Support

Technical support is available throughout the support life of the product. Support is available to verify that the equipment works properly, to help with product operation, and to provide basic measurement assistance for the use of the specified capabilities, at no extra cost, upon request.

Ordering Information

To order and configure the test solution consult your local Agilent field engineer.

United States:

Agilent Technologies
Test and Measurement Call Center
P.O. Box 4026
Englewood, CO 80155-4026
1-800-452-4844

Canada:

Agilent Technologies Canada Inc.
5150 Spectrum Way
Mississauga, Ontario
L4W 5G1
1-877-894-4414

Europe:

Agilent Technologies
European Marketing Organisation
P.O. Box 999
1180 AZ Amstelveen
The Netherlands
(31 20) 547-2323

United Kingdom
07004 666666

Japan:

Agilent Technologies Japan Ltd.
Measurement Assistance Center
9-1, Takakura-Cho, Hachioji-Shi,
Tokyo 192-8510, Japan
Tel: (81) 426-56-7832
Fax: (81) 426-56-7840

Latin America:

Agilent Technologies
Latin American Region Headquarters
5200 Blue Lagoon Drive, Suite #950
Miami, Florida 33126
U.S.A.
Tel: (305) 269-7500
Fax: (305) 267-4286

Asia Pacific:

Agilent Technologies
19/F, Cityplaza One, 1111 King's Road,
Taikoo Shing, Hong Kong, SAR
Tel: (852) 3197-7777
Fax: (852) 2506-9233

Australia/New Zealand:

Agilent Technologies Australia Pty Ltd
347 Burwood Highway
Forest Hill, Victoria 3131
Tel: 1-800-629-485 (Australia)
Fax: (61-3) 9272-0749
Tel: 0-800-738-378 (New Zealand)
Fax: (64-4) 802-6881

www.agilent.com/comms/NetworkTester

August 3, 2004.
5988-9330EN Rev B

Agilent Technologies