

Agilent NetworkTester

IPv6 Test Software

N4193A

Technical Datasheet



Test the performance of next-generation IPv6 and IPv4 network security and content-switching devices, networks, and application services.



Agilent Technologies

Key Features

- **Seamless IPv6 and IPv4 integration - test next-generation layer 4-7 devices rapidly**
- **Broad range of application protocol bricks - emulate stateful traffic over IPv6**
- **Client and server IPv6 emulation - one system, one user interface, one Test Plan**
- **Named addresses and address ranges - no need to re-enter IPv6 addresses**
- **Integrated IPsecv6 emulation option - test IPv6 encryption and authentication**

Product Overview

The Agilent NetworkTester is the industry's most powerful test solution for 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.

The introduction of IPv6 support into IPv4 equipment and networks can severely impact scalability and degrade performance. Next-generation layer 4-7 devices need to process longer addresses, optional header parts, encryption and authentication, concurrent IPv6 / IPv4 operation, and new types of DoS attacks. To ensure reliability and verify performance, test labs need a powerful and flexible test solution that enables a broad range of IPv6 and IPv4 test cases to be rapidly designed and executed.

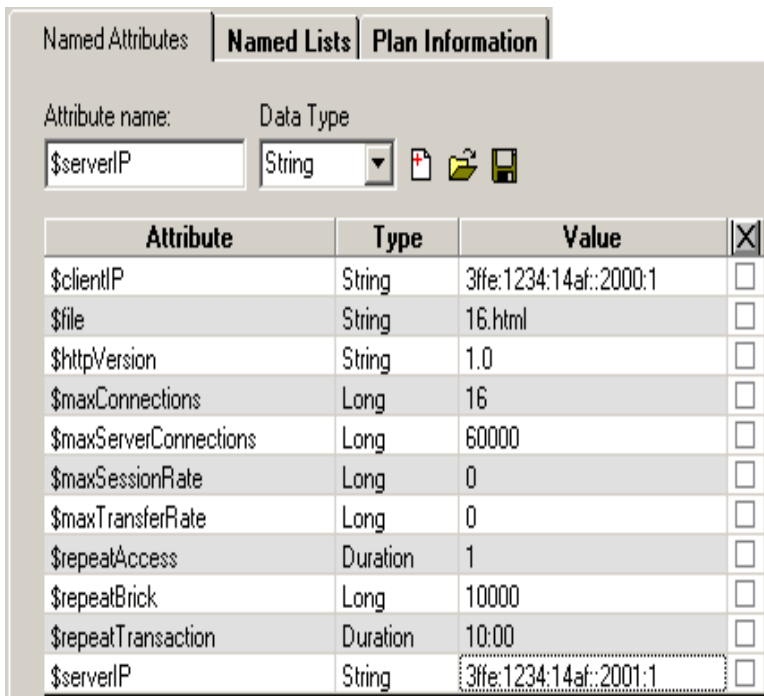


Figure 1: Named Attributes and Named Lists prevent the need to re-enter IPv6 addresses and address ranges

The N4193A NetPressure IPv6 Software License fully integrates IPv6 emulation into NetworkTester for testing next-generation IPv6 and IPv4 network security and content switching equipment and networks. Typical devices-under-test include firewalls; intrusion detection and prevention systems; virus and spam email filters; content switches; SSL accelerators; load balancers; and IPsec and IPsecv6 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 IPv6-capable 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.

Before introducing IPv6 infrastructure and services, NetworkTester is applied ahead of equipment purchases to verify vendor-reported networking capacity and performance, and to ensure that next-generation security devices will not become a network bottleneck or a single point of failure. After IPv6 deployment, NetworkTester is utilized to perform off-line testing of new network configurations prior to exposure to live customer traffic.

NetworkTester offers a complete environment for the development, management, execution and logging of performance test campaigns. The N4193A NetPressure IPv6 Software License seamlessly extends the highly flexible and extremely powerful NetPressure software application, allowing your team to easily build and run both simple and complex tests using a mixture of stateful traffic over both IPv6 and IPv4 - without the need to develop test tool scripts.

With the N4193A NetPressure IPv6 Software License, Agilent NetworkTester delivers realistic Internet-scale IPv6 and IPv4 traffic testing to your lab.

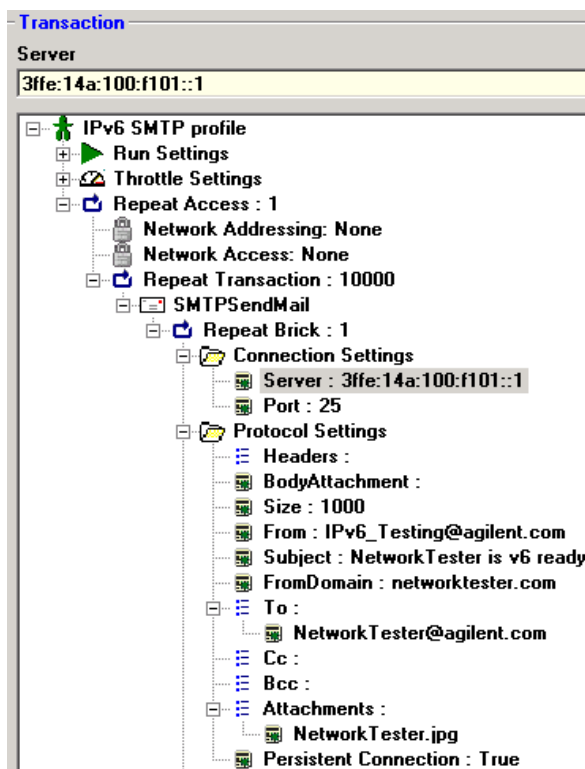


Figure 2: NetPressure allows you to easily create IPv6 Client Profiles and Services

Product Features

Seamless IPv6 and IPv4 integration - test next-generation layer 4-7 devices rapidly

NetworkTester fully integrates IPv6 and IPsecv6 (IPsec for IPv6) in exactly the same way as IPv4 and IPsec. You can generate and measure real, stateful traffic over both IPv6 and IPv4 in a single Test Plan.

Broad range of application protocol bricks - emulate stateful traffic over IPv6

NetworkTester supports a broad range of protocols over IPv6, such as TCP and UDP, HTTP, HTTPS, FTP, SNMP, H.323, SIP, SMTP and POP3, 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 IPv6 and TCP port addressing, extra headers, cookies, target URL lists, proxy server IPv6 addresses, and abort times. The HTTP server enables you to specify error codes and custom headers for specific IPv6 addresses, and emulates URL spoofing for 404 (Page Not Found) errors. This flexibility allows you to generate protocol traffic with the characteristics you need.

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 IPv6 and IPv4 user groups with differing 'think times'. This powerful feature allows you to create traffic patterns that accurately reflect the complexity of real world conditions.

Multiple protocols can be combined on any test port. For example, you can create realistic test scenarios that combine FTP, HTTP and HTTPS emulation all on the same port to test interactions and measure the performance impact on devices that process at the application layer.

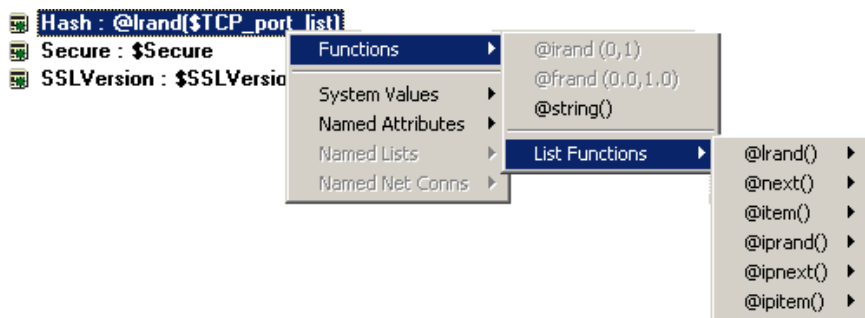


Figure 3: List functions cycle through and randomize parameters such as IPv6 address ranges

Client and server IPv6 emulation - one system, one user interface

NetworkTester combines emulation of IPv6 and IPv4 clients and servers into a single system with one user interface. Using the NetPressure software application, you can create a Test Plan in minutes that emulates stateful IPv6 and IPv4 clients and servers with a range of applications.

Client and server statistics can be graphed together and correlated in real time, allowing you to visualize system performance and rapidly diagnose performance bottlenecks and errors.

Each traffic module can be flexibly configured for either client or server emulation. There is no need to budget separately for client and server hardware. You can configure and place resources where you need them, according to your Test Plan.

Named addresses and address ranges - no need to re-enter IPv6 addresses

NetworkTester eases the painful configuration of long IPv6 addresses and address ranges. NetPressure's Named Attributes and Named Lists can be rapidly applied to both IPv6 and IPv4 addresses and address ranges. Create symbolic names for IPv6 parameters across all of your client and server emulations, and use NetPressure's List Functions to easily randomize and cycle through IPv6 address ranges.

Named Attributes can be changed in real time, allowing you to change the value of most parameters such as IPv6 addresses interactively, even while the test is running.

The string expression editor allows you to insert IPv6 addresses with other parameters into any place that you need a string, such as application header fields and payloads.

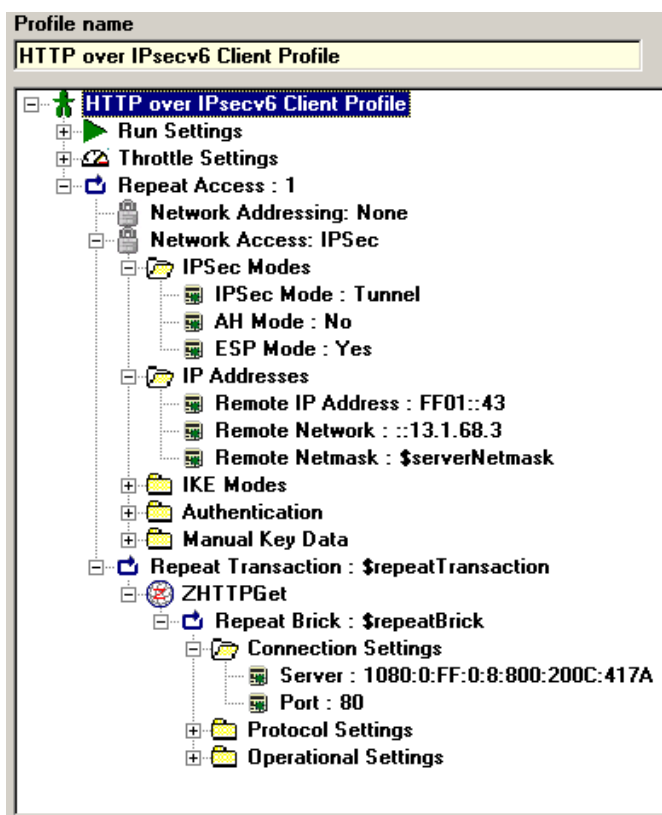


Figure 4: IPsecv6 protocols and encapsulation are easily configured

Integrated IPsecv6 emulation - test IPv6 encryption and authentication

IPsecv6 (IP Security for IPv6) is an integral component of IPv6 that provides security services such as encryption and authentication to maintain data confidentiality, data integrity and privacy. The testing of IPv6-capable systems would be incomplete without IPsecv6.

NetworkTester fully integrates emulation of both IPsec and IPsecv6, allowing you to quickly configure addresses and establish IPsec and IPsecv6 tunnels automatically. You can create powerful and realistic test cases that set up multiple tunnels and emulate real-world traffic using one or more service protocols (such as HTTP, FTP and SMTP) over the established tunnels.

IPsec, IPsecv6 and SSL hardware acceleration

The application traffic throughput of VPN concentrators, SSL accelerators and network security devices is often limited by their IPsec and SSL data encryption and decryption speeds. NetworkTester allows you to easily reach and exceed the performance limits of IPsec, SSL, and next-generation IPsecv6 (IPsec over IPv6) devices. NetworkTester test modules offer high IPsec and SSL (HTTPS) performance, surpassing the needs of the majority of test scenarios.

For the most demanding applications, test modules with hardware IPsec and SSL

acceleration are capable of even greater IPsec and IPsecv6 performance. Both IPsec and SSL can be accelerated at the same time, allowing high-speed emulation of HTTPS application traffic over IPsec or IPsecv6 tunnels.

Extensive range of IPv6 measurements

The NetPressure application offers the broadest range of real-time statistics available. These same statistics are available for measuring performance over IPv6 protocols and IPsecv6 tunnels. For each application protocol and each emulated client and server, you can graph and log metrics such as application transfer rates, transfer times, throughput, and tunnel set-up and tear down durations, giving you the ability to comprehensively characterize the performance of next-generation devices, networks and services.

Setting Name	IP Settings				VLAN Settings			
	IP Protocol	IP	Selection Mode	Spoof MAC Address	VLAN Id	Priority Bits	Netmask	Default Gateway
vlan-A	IPv4	192.168.0.1-192.168.3.254	\$cyclePattern	True	100-150	0	\$netmask	<input type="checkbox"/>
vlan-B	IPv6	2001::/16, size = 500	Random	False	1-4000	0	\$netmask	<input type="checkbox"/>
IPv6_range_C	IPv6	fec0::/12, size = 10000	Sequential	True	0	7	\$netmask	<input type="checkbox"/>
IPv6_range_D	IPv6	fe80::/10, size = 10000	Single	False	0	0	\$netmask	<input type="checkbox"/>

Figure 5: IPv6 and IPv4 addresses and VLAN pools can be represented symbolically to speed test configuration

Technical Specifications

Protocol Emulation

Network Access

The following Access protocols are supported.

Protocol	Comments
IPSecv6	<ul style="list-style-type: none"> Client only For further information please refer to N4190A IPsec Test Software Technical Datasheet

Encapsulation

The following VLAN encapsulation features are supported.

Protocol	Comments
802.1Q/VLAN	<ul style="list-style-type: none"> Client and Service support Support for VLAN range definition per client profile 4,096 VLANs per port

Transport

The following transport protocols are supported.

Protocol	Comments
TCP	<ul style="list-style-type: none"> Client and Service
UDP	<ul style="list-style-type: none"> Client and Service

Application

The following application protocols are supported.

Protocol	Comments
Attack Bricks	<ul style="list-style-type: none"> Client only IP, ICMP, UDP and TCP attacks Sample test plans for DoS attacks using these attack bricks are supplied.
FTP	<ul style="list-style-type: none"> Client and Service Active and Passive modes
H.323	<ul style="list-style-type: none"> Client (for client-to-client emulation) For further information please refer to N4195A VoIP Test Software Technical Datasheet
HTTP	<ul style="list-style-type: none"> Client and Service
HTTPS	<ul style="list-style-type: none"> Client and Service Secure modes supported: SSLv2, SSLv3, TLSv1
NNTP	<ul style="list-style-type: none"> Client only
POP3	<ul style="list-style-type: none"> Client and Service
RTP	<ul style="list-style-type: none"> Client (send, receive, and bidirectional for client-to-client emulation) RTCP emulation optional; configurable rate

SIP	<ul style="list-style-type: none"> Client (for client-to-client emulation) For further information please refer to N4195A VoIP Test Software Technical Datasheet
SMTP	<ul style="list-style-type: none"> Client and Service
SNMP	<ul style="list-style-type: none"> Client only SNMPv1, SNMPv2c
Telnet	<ul style="list-style-type: none"> Client and Service

Statistics

Measurement statistics collected during a test can be displayed numerically, graphically or saved to a file. Application statistics refer to the application protocol traffic - for example, for the HTTPGet Protocol Brick, application transfers/second refers to HTTP gets/second.

General Statistics

Statistic	Aspects	Units
Application Transfer Rate	<ul style="list-style-type: none"> Client profile Client interface Client resource Test plan Server interface Server resource 	Transfers/sec
Session Rate	<ul style="list-style-type: none"> Client profile Client interface Client resource Test plan Server interface Server resource 	Sessions/sec
Total sessions	<ul style="list-style-type: none"> Client profile Client interface Client resource Test plan Server interface Server resource 	Sessions
Access Rate (network access bricks)	<ul style="list-style-type: none"> Client profile Client interface Client resource Test plan 	Access/sec
Total accesses (network access bricks)	<ul style="list-style-type: none"> Client profile Client interface Client resource Test plan 	Access
L4-7 throughput	<ul style="list-style-type: none"> Client profile Client interface Client resource Test plan Server interface Server resource 	Kilobytes/sec Megabits/sec Megabytes/sec
Total errors	<ul style="list-style-type: none"> Client profile Client interface Client resource Test plan 	Errors

Concurrent connections	<ul style="list-style-type: none"> Client profile Client interface Client resource Test plan 	Connections
------------------------	--	-------------

Timing Statistics

Statistic	Aspects	Units
Response time (min, max, avg)	<ul style="list-style-type: none"> Client profile Client interface Client resource Test plan 	Seconds
Access connect time (min, max, avg)	<ul style="list-style-type: none"> Client profile Client interface Client resource Test plan 	Seconds
Connect time (min, max, avg)	<ul style="list-style-type: none"> Client profile Client interface Client resource Test plan 	Seconds
Authorization time (min, max, avg)	<ul style="list-style-type: none"> Client profile Client interface Client resource Test plan 	Seconds
Transfer time (clients) (min, max, avg)	<ul style="list-style-type: none"> Client profile Client interface Client resource Test plan 	Seconds
Transfer time (servers) (min, max, avg)	<ul style="list-style-type: none"> Server interface Server resource 	Seconds
Disconnect time (min, max, avg)	<ul style="list-style-type: none"> Client profile Client interface Client resource Test plan 	Seconds
Access destroy time (min, max, avg)	<ul style="list-style-type: none"> Client profile Client interface Client resource Test plan 	Seconds

Interface Statistics

Statistic	Aspects	Units
Interface throughput (Total Mb/s)	<ul style="list-style-type: none"> Client interface Client resource Test plan Server interface Server resource 	Megabits/sec
Interface throughput (Mb/s received)	<ul style="list-style-type: none"> Client interface Server interface 	Megabits/sec
Interface throughput (Mb/s transmitted)	<ul style="list-style-type: none"> Client interface Server interface 	Megabits/sec

Interface throughput (Total packets/s)	<ul style="list-style-type: none"> Client interface Client resource Test plan Server interface Server resource 	Packets/sec
--	---	-------------

Interface throughput (Packets/s received)	<ul style="list-style-type: none"> Client interface Server interface 	Packets/sec
---	--	-------------

Interface throughput (Packets/s transmitted)	<ul style="list-style-type: none"> Client interface Server interface 	Packets/sec
--	--	-------------

Interface errors	<ul style="list-style-type: none"> Client interface Client resource Test plan Server interface Server resource 	Errors
------------------	---	--------

Interface collisions	<ul style="list-style-type: none"> Client interface Client resource Test plan Server interface Server resource 	Collisions
----------------------	---	------------

Additional Log Statistics

Statistic	Aspects	Units
Cumulative transfers	<ul style="list-style-type: none"> Client profile Client interface Client resource Test plan Server interface Server resource 	Transfers
Cumulative sessions	<ul style="list-style-type: none"> Client profile Client interface Client resource Test plan Server interface Server resource 	Sessions
Cumulative accesses	<ul style="list-style-type: none"> Client profile Client interface Client resource Test plan 	Access
Cumulative throughput	<ul style="list-style-type: none"> Client profile Client interface Client resource Test plan Server interface Server resource 	Kilobytes/sec Megabits/sec Megabytes/sec
Error summary	<ul style="list-style-type: none"> Client profile Client interface Client resource Test plan 	NA

Application Programming Interface

Fully functioned Tcl (Tool Command Language) scripting environment.

Configuration

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

Product Numbers

N4193A - NetPressure IPv6 Software License

Adds integrated IPv6 support, including IPv6 protocol emulation, to the NetworkTester NetPressure application for one NetworkTester system.

N4194A - NetworkTester IPSec Software License for IPv4/v6

Adds integrated IPsecv4 (IPsec for IPv4) protocol emulation to the NetworkTester NetPressure application for one NetworkTester system. When combined with the N4193A IPv6 software license, IPsecv6 (IPsec for IPv6) is also supported.

N4195A NetworkTester VoIP Software License

Adds VoIP protocol emulation to the NetworkTester system. When combined with the IPv6 software license, VoIPv6 is also provided. When combined with the IPsec software license, VoIPsec (VoIP over IPsec) is also provided. When combined with both the IPv6 and IPsecv6 software licenses, VoIPsecv6 (VoIP over IPsecv6) is also provided.

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

