Agilent RouterTester

IP Analysis Test Software

E7852A

Technical Datasheet

The Agilent Technologies E7852A RouterTester IP Analysis Test Software adds powerful capture control, decode and analysis capabilities to RouterTester.

Agilent Technologies

Key Features

- **Extensive triggers, including performance threshold violations**
- **Synchronized capture control with powerful capture and analysis filters**
- **Multi-port correlated performance analysis by QoS/DS/TOS, Source-Destination pairs, Protocol type and more**
- **Acquisition, correlated visualization and analysis of large volumes of data with easy to use navigation tools**
- **Comprehensive protocol decodes**
- **Detailed analysis at fine resolution — per packet data and distributions of key measurements over time**

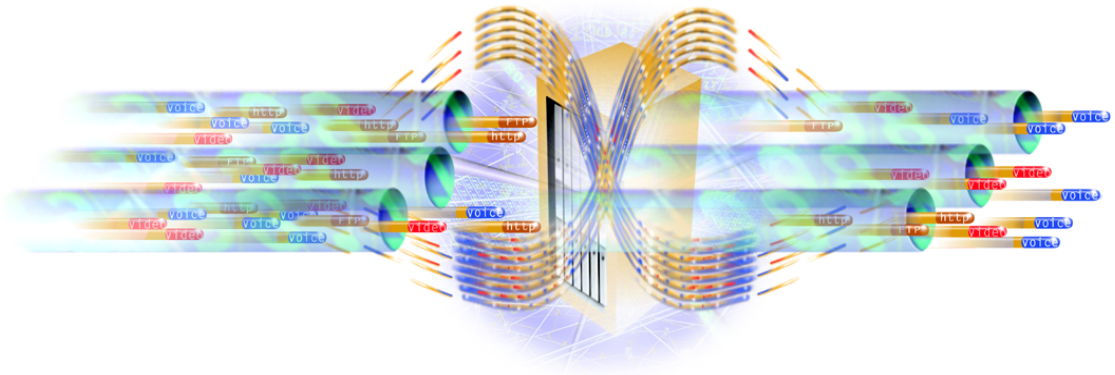
Product Overview

The high volume of data passing through today's routers intensifies the need to investigate performance and functional issues identified in real-time at fine resolution.

The Agilent Technologies E7852A RouterTester IP Analysis Test Software adds powerful capture control, decode and analysis capabilities to the RouterTester. This tool complements the real-time performance features already available in the RouterTester IP Performance Software, enabling you to:

- capture data and investigate performance issues at a finer resolution (per packet) than can be provided in real-time
- navigate to the point of interest within large volumes of captured data to help identify a specific problem
- view graphical representation and distribution of performance parameters at the resolution required to identify faults and diagnose router behaviour
- view detailed protocol decodes, including a comprehensive range of IP and routing protocols

To isolate specific performance criteria and events, RouterTester IP Analysis software defines performance thresholds and triggers that can capture packets to memory for detailed packet analysis. Powerful data reduction tools can be used to identify performance patterns and event sequences that reveal how the router responds to different traffic configurations and load profiles. Intelligent data reduction tools, protocol decodes and visual interpretations of captured data can be used to drill-down and thoroughly understand why the router was unable to deliver consistent service levels.



A fully configured RouterTester supports up to 128 ports, with up to 4 GB of capture memory. The IP Analysis Test Software helps you to find the needle of interest in the huge haystack of data.

Product Features

Extensive triggers

Capture can be started or stopped either manually or by a start or stop trigger. When capture is set to cyclic mode, the stop event will centre in the capture buffer, allowing you to analyse events both prior to and after the trigger.

There are a range of triggers available to start or stop capture or generate an external trigger including:

- layer 2/3 errors, such as TCP or UDP checksum error
- pattern match
- real-time latency, rate and count thresholds

Multiple triggers can be combined within and across modules to provide precise control over capture and stop conditions for correlated multiport capture and analysis.

The flexibility of these triggers supports an extensive range of scenarios, enabling you to capture data associated with an event of interest. Some examples would be:

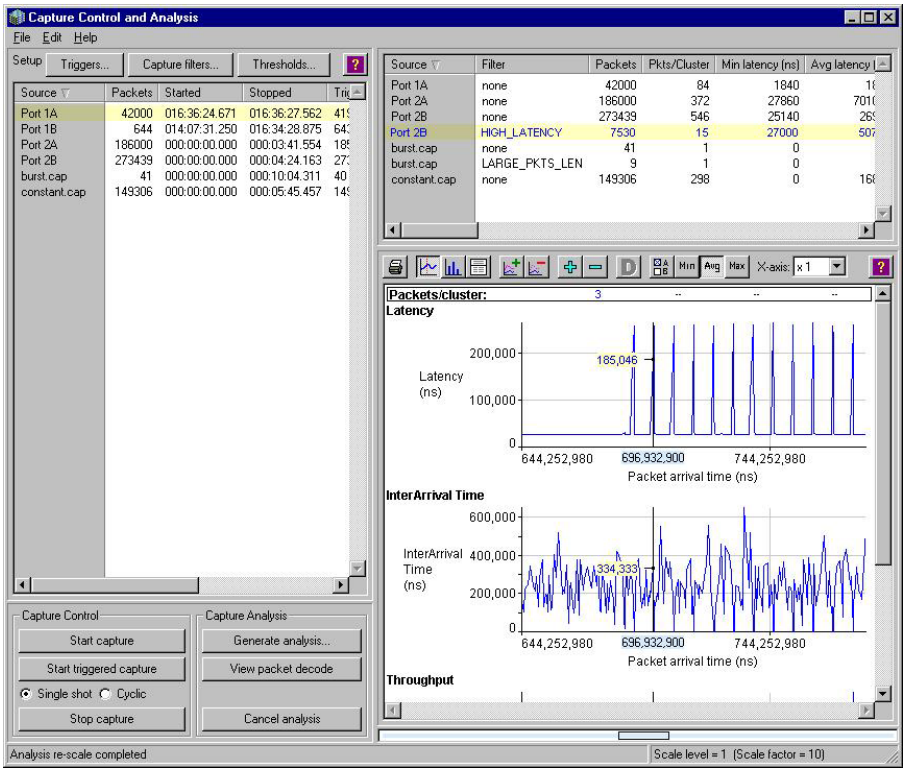
- a single-shot capture could be started when a measurement, such as latency, falls outside a user-defined threshold range
- a cyclic-capture could be halted when the rate of IP header errors exceeds a specified number of packets per second with a user-defined burst tolerance.

Powerful capture filters

Capture filters allow the user to optimize the use of capture memory by selectively storing or discarding packets according to pattern match and/or stream status criteria.

Comprehensive analysis filters

Analysis filters allow the user to select only those packets of interest out of the set of captured packets.



The IP Analysis Software clearly displays any anomalies in the analysis set and allows you to drill down to the packet level for further investigation.

This can significantly reduce the volume of data to be analysed and enables the generation of diverse comparative analyses from the same data. Typical applications include plotting latency by QoS (DS) type for SLA validation.

Multi-port correlated performance analysis

The IP analysis software enables you to capture data for performance measurements.

- Acquisition, analysis and correlated visualization
  - up to 4 GB of capture data across up to 128 ports
  - performance measurements over time and measurement distributions
  - packet decode viewer including major Internet routing protocols
- High performance post-processing analysis at fine resolution: Per packet measurements over time (16 statistics) and distributions of key measurements including latency, packet length and interarrival time
- Graphical visualization and troubleshooting using line graphs showing performance measurements over time and distribution charts showing the distribution of a range of values

The IP Analysis tool provides you with a graphical picture of an entire RouterTester capture buffer. You can select a point of interest, such as a spike in latency, then "drill down" by re-analysing the location around the selected point at a much finer resolution. You can continue to scale further until you have located a single packet of interest out of the possible several million packets in the capture buffer. It is this ability to "find the needle in the haystack" that makes the IP Analysis software unique in the industry.

Regression test support

The ability to load and analyse saved capture data allows you to compare current performance with previously established reference standards. This allows rapid validation of hardware and software upgrades against prior releases or investigation of the impact of changes to traffic engineering parameters.

Easy to use graphical interface

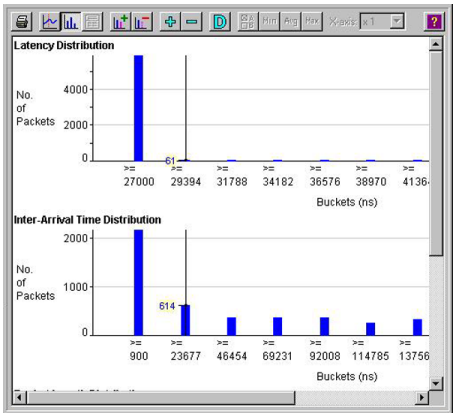
Keeping in line with the RouterTester IP Performance Software, the IP Analysis software also uses a single window to display the complete control and analysis application; physical ports, capture files, analysis sets, statistics and graphs.

Tcl/Tk application programming interface

The Tcl (Tool Command Language) based API enables you to create automated test sequences to set up and control data capture and retrieve and analyse captured data. It also allows you to integrate RouterTester with other instruments. Tcl Scripts can run on the RouterTester System Controller or can run on a remote PC or Unix workstation attached to the RouterTester System Controller via a TCP/IP connection.

Online Help

An extensive online help system provides complete descriptions and detailed usage instructions for every component of RouterTester. Dialog-level context-sensitive help provides rapid access to the relevant sections of the online help. A technology reference section provides a complete library of background information pertaining to gigabit and terabit router performance testing.



Generating a Latency Distribution bar chart allows you to see what proportion of packets are violating the SLA.

Technical Specifications

Capture Triggers

Any of the trigger events can fire any or all of the trigger actions: Start capture, Stop capture, Generate external trigger.

Layer 2 (any or all)

HDLC FCS error
HDLC aborted frame
Any packet
Emulation packet
MPLS packet

IP (any or all)

Any IPv4 packet
IPv4 header checksum error
IPv4 fragmented datagram
IPv4 TCP or UDP checksum error

Stream (any or all)

Above upper real-time latency threshold (ns)
Below lower real-time latency threshold (ns)
Sequence error
Severe sequence error
Misdirected packet

Pattern

Eight 128-octet wide pattern matchers are shared amongst protocol emulation, capture filters and triggers.

Rate threshold

A single real-time leaky-bucket rate threshold can be defined. The threshold is expressed as a rate and associated burst tolerance.

Stream sequence error	(error/s)
Stream packet	(pkt/s)
Stream octet	(octet/s)
Stream misdirected packet	(pkt/s)
Any packet	(pkt/s)
Any octet	(octet/s)
MPLS packet	(pkt/s)
IPv4 header checksum error	(error/s)
IPv4 fragmented datagram	(pkt/s)
IPv4 packet	(pkt/s)
IPv4 octet	(octet/s)
IPv4 TCP or UDP checksum error	(error/s)

Count threshold

A single real-time count threshold can be defined. The threshold is specified as a count of the specified event.

Stream sequence error
Stream packet
Stream octet
Stream misdirected packet
Any packet
Any octet
MPLS packet
IPv4 header checksum error
IPv4 fragmented datagram
IPv4 packet
IPv4 octet
IPv4 TCP or UDP checksum error

Module

External trigger in

Pattern Library

Patterns are used for triggers, capture filters and analysis filters. A pattern editor is provided for creating and modifying patterns at the bit level or by protocol field values. Patterns are either pre-defined or user-defined. As PDUs are created in the IP Performance application corresponding patterns are made available in the pattern library.

Pattern	(128 octets)
Mask	(128 octets)

Capture Filters

The filters provide both hardware status and pattern matching which can be used to store or exclude data to or from the capture.

Status

Above upper real-time latency threshold
Below lower real-time latency threshold
Sequence error
Severe sequence error
Misdirected packet
IPv6 valid packet
IPv4 header checksum error
IPv4 fragmented datagram
IPv4 TCP or UDP checksum error
Any Layer 2 packet
Layer 2 emulation packet
MPLS packet
Streams selected
Stream not selected

Patterns

Eight 128-octet wide pattern matchers are shared amongst protocol emulation, capture filters and triggers.

Capture Modes

The location of the start and stop trigger packets within the capture buffer can be controlled by selection of the appropriate capture mode. In Single-shot mode, the capture will automatically stop if the buffer fills. In Cyclic mode, the stop trigger packet will be centered within the buffer.

Single-shot	Stops capturing if buffer fills
Cyclic	Automatically centers stop trigger packet in the capture buffer

Capture Control

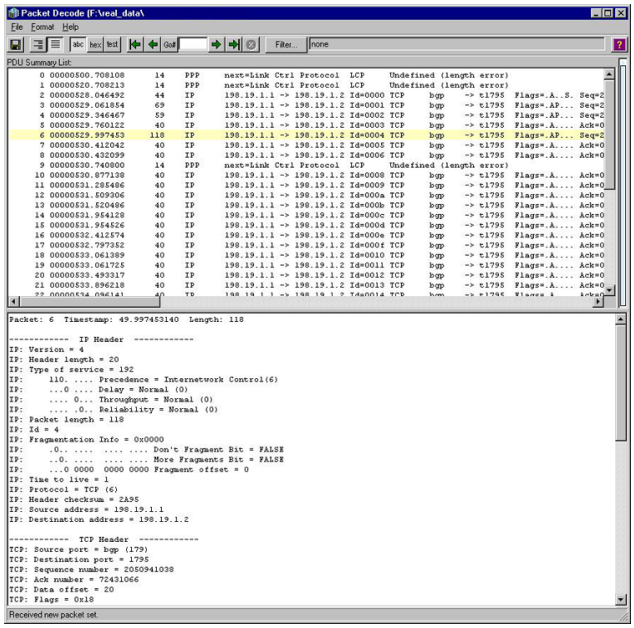
Capture can be started or stopped either manually or via triggers. Start triggers are enabled by using the start triggered capture control. Stop triggers are always active.

Start capture	(Stop triggers are active)
Start triggered capture	(Start and stop triggers are active)
Stop capture	(Immediate stop)

Analysis Control

Generate analysis

When performing an analysis on either a capture buffer or a file, an optional analysis filter can be specified. Repeated analyses can be made using different filters and the results overlaid and compared.



View packet decode

An unlimited number of protocol decode windows can be opened on one or more capture buffers or files to allow comparative analysis of the data. Extensive control is provided over the decode formatting and powerful navigation and filtering tools accelerate the task of locating and diagnosing faults.

Packet Decode Viewer

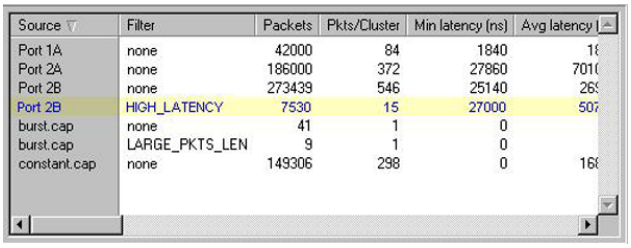
Each Packet Decode window shows protocol decodes from a single source (port or file). Both Summary and Detailed decode views are provided. The Summary view shows a brief decode for a window of 100 packets from the capture source. Navigation controls allow rapid movement of the window to anywhere in the capture data.

Summary format options

Mode	Multi-line/single line
Port number	On/Off
Packet number	On/Off
Packet length	On/Off
Timestamp	Absolute/Relative/Interval/Off
Latency	On/Off
Time resolution	µs/ns
Status flags	On/Off

Detail format modes

Protocol decode
Hex
Test payload decode



Source	Filter	Packets	Pkts/Cluster	Min latency (ns)	Avg latency
Port 1A	none	42000	84	1840	18
Port 2A	none	186000	372	27860	7010
Port 2B	none	273439	546	25140	269
Port 2B	HIGH_LATENCY	7530	15	27000	507
burst.cap	none	41	1	0	
burst.cap	LARGE_PKTS_LEN	9	1	0	
constant.cap	none	149306	298	0	168

Navigation controls

First page
Last page
Previous page
Next page
Goto packet number

Filters

Analysis filters can be defined and applied to select out only packets of interest and reduce the volume of decode data.

Analysis Filters

The user can define detailed filters for selecting packets of interest from the captured data. An analysis filter may be constructed from any combination of patterns, value threshold or status conditions. When a filter is applied, a captured packet must match any of the patterns selected together with all specified threshold and status conditions.

Pattern filter

A packet must match any one of the specified 128-octet patterns.

Value filter

A packet must match all activated value filters.

Stream ID	RouterTester stream identifier
MPLS label	(value)
Latency ≥	(ns)
Latency ≤	(ns)
Packet length ≥	(octets)
Packet length ≤	(octets)

Status filter (true or false match)

A packet must match all activated status filters.

Above upper real-time latency threshold
Below lower real-time latency threshold
New highest latency
New lowest latency
Sequence error
Severe sequence error
Misdirected packet
IPv4 header error
IPv4 fragmented datagram
TCP packet
UDP packet
IPv4 TCP or UDP checksum error
Layer 2 emulation packet
IPv4 packet
MPLS packet
Ethernet Packet with VLAN tag
AAL5 CRC Error
AAL5 Length Error
AAL5 Encapsulation Error
Not instrumented packet
Stream not selected
Caused stop capture trigger

Analysis Results

The result of an analysis is an Analysis Set that identifies the capture data source (port or file), the filter that was applied, the packets that passed the filter (and hence were analysed) and the derived measurements.

Measurements taken over the entire analysis set are available in a table while measurements from the cluster down to the per-packet level are available as graphs.

Analysis set data

Capture source name

Analysis filter name

Number of packets in the set

Packet statistics

All packet statistics are available as Minimum, Average and Maximum values.

Latency	(ns)
Interarrival time	(ns)
Packet length	(octets)

Cluster statistics

Top level data reduction is achieved by collecting packets into clusters and providing measurements on a per-cluster basis. Powerful tools are provided for repeating analysis at ever finer detail, down to the per-packet level (i.e. one packet/cluster).

Pkts/cluster	(packets)
Throughput	(pkt/s)
Bandwidth	(kb/s)
Lost packets	(packets)
MPLS packets	(packets)
TCP packets	(packets)
UDP packets	(packets)
Checksum errors	(packets)
Misdirected packets	(packets)
Unselected stream packets	(packets)
Sequence errors	(packets)
Severe sequence error count	(packets)
IPv4 header error	(packets)
IPv4 Fragmented packets	(packets)
VLAN packets	(packets)
AAL5 CRC Errors	(packets)
AAL5 Length Errors	(packets)
AAL5 Encapsulation Errors	(packets)
Not instrumented packet	(packets)

Available Graphs and Statistics

Up to six of the Packet or Cluster statistics can be graphed over time with data from up to four analysis sets being simultaneously plotted. Value distributions of the Packet statistics are presented as bar graphs. Color printing of the graphs is supported.

Latency	(ns)
Interarrival time	(ns)
Packet length	(octets)
Throughput	(pkt/s)
Bandwidth	(kb/s)
Packet loss	(packets)
MPLS packet count	(packets)
TCP packet count	(packets)
UDP packet count	(packets)
Checksum error count	(packets)
Misdirected count	(packets)
Unselected streamID count	(packets)
Sequence error count	(packets)
Severe sequence error count	(packets)
IPv4 header error count	(packets)
IPv4Fragmented count	(packets)
VLAN packets	(packets)
AAL5 CRC Errors	(packets)
AAL5 Length Errors	(packets)
AAL5 Encapsulation Errors	(packets)
Not instrumented packet count	

Data Export

Entire capture buffers or selected packet ranges can be saved to disk for later, offline analysis.

Tabular data can be exported in comma-separated value (CSV) format via the Windows clipboard.

Protocol decode data can also be selectively exported via the clipboard.

Graphs can be printed (in color) to any installed printer.

Decoded Protocols

Cisco	**EIGRP**	Enhanced IGRP
	IGMP	RFC 2236; Internet Gateway Routing Protocol
	IGMPv2	RFC 2236; Internet Group Management Protocol
	IGRP	Internet Gateway Routing Protocol
IETF - XoIP	**MGCP**	Media Gateway Control Protocol
	SAP	Session Announcement Protocol
	SDP	Simple Gateway Control Protocol
	SGCP	Session Description Protocol
	SIP	Session Initiation Protocol
IETF - VoIP	**H.248**	MEGACO I ETF MEGACO WG. Voting: Feb '00, ITU-T H
ITU-T XoIP	H.225.0 Version 2	
	H.225.0 Version 3	H225V3WCM5/99
	H.235	Security and encryption for H.323 ITU-H H.235 (2/98)
	H.245 Version 1	Call Control for H.323 ITU-T H.245 (1996)
	H.245 Version 2	Call signaling for H.323 logical channels; ITU-T H.245 (1997)
	H.245 Version 3	Call signaling for H.323 logical channels; ITU-T H.245 (1998)
	H.245 Version 5	Control Protocol for Multimedia Communication; H245V5WCMI6/99
	H.261	Video CODEC used in H.323; ITU-T H.261
	H.450.1	Call control for supplementary services; ITU-T H.450.1 (Sept. 1997)
	H.450.2	Call transfer supplementary service for H.323; ITU-T H.450.2 (Sept. 1997)
	H.450.3	Call diversion supplementary service for H.323; ITU-T H.450.3 (Sept. 1997)
	Q.931 (H.225.0 V1)	Signaling for H.323; ITU-T H.225.0 (1996)
	RAS (H.225.0 V1)	Registration, Admission, Status for H.323; ITU-T H.225.0 (1996)
	RTCP	Real-time Transport Control Protocol; RFC 1889
	RTP	Real-time Transport Protocol; RFC 1889, RFC 1890
SUN	**MOUNT**	Mount
	NFS Version 2	Network File System; RFC 1094
	NIS	Network Information Services
	PMAP	Port Mapper
	RPC	Remote Procedure Call; RFC 1057
	RSTAT	RSTAT
TCP/IP	**ARP**	Address Resolution Protocol; RFC 826
	ATM ARP	
	BGP	Border Gateway Protocol; RFC 1577
	BGP-4	Border Gateway Protocol version 4; RFC 1771
	BOOTP	BOOT Protocol; RFC 951
	DHCP	Dynamic Host Configuration Protocol
	DISP	Dispatching for SNMP; RFC 2572
	DNS	Domain Name Service; RFC 1035
	DVMRPv3	Distance Vector Multicast Routing Protocol; Draft v3-08exp8/99
	EGP	Exterior Gateway Protocol; RFC 904
	Finger	Finger User Information; RFC 1196
	FTP	File Transfer Protocol; RFC 959
	GGP	Gateway to Gateway Protocol; RFC 823
	GTP	General Packet Radio Service (GPRS) Tunnelling Protocol; ETSI EN 301 347 V7.1.1 (2000-01)
	HTTP	Hypertext Transfer Protocol
	HTTP 1.1	Hypertext Transfer Protocol Version 1.1
	ICMP	ICMP Router Discovery Protocol; RFC 1256
	ICMP IRDP	Internet Control Message Protocol; RFC 792
	ICMPv6	Internet Control Message Protocol version 6; RFC 1885
	IP	Internet Protocol; RFC 791
	IP-SEC	IP-Security Authentication Header; RFC 2402, RFC 2406-9
	IPinIP	Minimum IP Encapsulation; RFC 2004
	IPv6	IP Version 6; RFC 1883, RFC 1884
	LDAP	Lightweight Directory Access Protocol; RFC 1777
	LPP	ISO Presentation Services on top of TCP/IP; RFC 1085
	MBGP	Multiprotocol BGP; RFC 2283
	MIP	Mobil IP; RFC 2002, RFC 2344 and extensions
	MOSPF	Multicast OSPF; RFC 1584
	NetBIOS	NetBIOS
	NTP	Network Time Protocol; RFC 1119
	OSPF	Open Shortest Path First; RFC 2328
	PIM-DM	Protocol Independent Multicast - Dense Mode; Draft v2-dm-00
	PIM-SM	Protocol Independent Multicast - Sparse Mode; RFC 2362
	RARP	Reverse Address Resolution Protocol; RFC 903
	REXEC	Remote Exec

TCP/IP (cont.)	**RIP**	Routing Information Protocol
	RIP-2	Routing Information Protocol version 2
	RLOGIN	Remote Login; RFC 1282
	RLPR	Remote Print
	Routed	Route daemon Protocol; RFC1993
	RSHELL	Remote Shell
	RSVP	Resource Reservation Protocol; RFC 2205
	RWHO	Remote Who; RFC 954
	SMB	Server Message Block
	SMTP	Simple Mail Transport Protocol; RFC 821
	SNMP	Simple Network Management Protocol; RFC 1157
	SNMP-2	Simple Network Management Protocol version 2
	SNMP-3	Simple Network Management Protocol version 3; RFC 2271-4
	SNMPv2c	Simple Network Management Protocol Hybrid; RFC 1905
	TCP	Transport Control Protocol; RFC 793
	TDS	SyBase Tabular Data StreamSyBase TDS 5.0 Reference
	TELNET	Telnet; RFC 854
	Teradata	NCR Teradata; NCR,1995
	TFTP	Trivial File Transfer Protocol; RFC 873
	TIMED	Time Daemon Protocol
	TNS	Oracle Transparent Network Substrate Oracle Version 6
	UDP	User Datagram Protocol; RFC 768
	XTP	Xpress Transfer Protocol; XTP Forum Rev. 4 March 1, 1995
	XWIN	X-Windows
WAN	**L2TP**	Layer 2 Tunnelling Protocol
	PPP	Point to Point Protocol

This page intentionally left blank.

This page intentionally left blank.

Agilent's RouterTester system

Agilent's RouterTester system offers a powerful and versatile test platform to address the evolving test needs of metro/edge platforms, core routers and optical switches. RouterTester provides Network Equipment Manufacturers and Service Providers with the industry's leading tools for wire speed, multiport traffic generation and performance analysis of today's networking devices.

Warranty and Support

Hardware Warranty

Agilent warrants all RouterTester and QA Robot hardware against defects in materials and workmanship for a period of 3 years from the date of delivery. Agilent further warrants that the RouterTester and QA Robot hardware 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 RouterTester and QA Robot 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 RouterTester system 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 system 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.
2660 Matheson Blvd. E
Mississauga, Ontario
L4W 5M2
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/RouterTester

5980-1707E, Rev C

Agilent Technologies