

Agilent RouterTester

L2TP Protocol Software

E5151A

Technical Datasheet



Agilent Technologies' L2TP Test Solution provides realistic Internet-scale simulation for testing the performance of edge aggregation devices that are involved in providing IP VPN services. Specifically, devices that act as L2TPv2 Network Servers (LNS) or L2TPv2 Access Concentrators (LAC) for delivering L2TPv2-based VPN services are fully stress tested by Agilent's RouterTester through emulation of the L2TP and the PPP protocols.



Agilent Technologies

Key Features

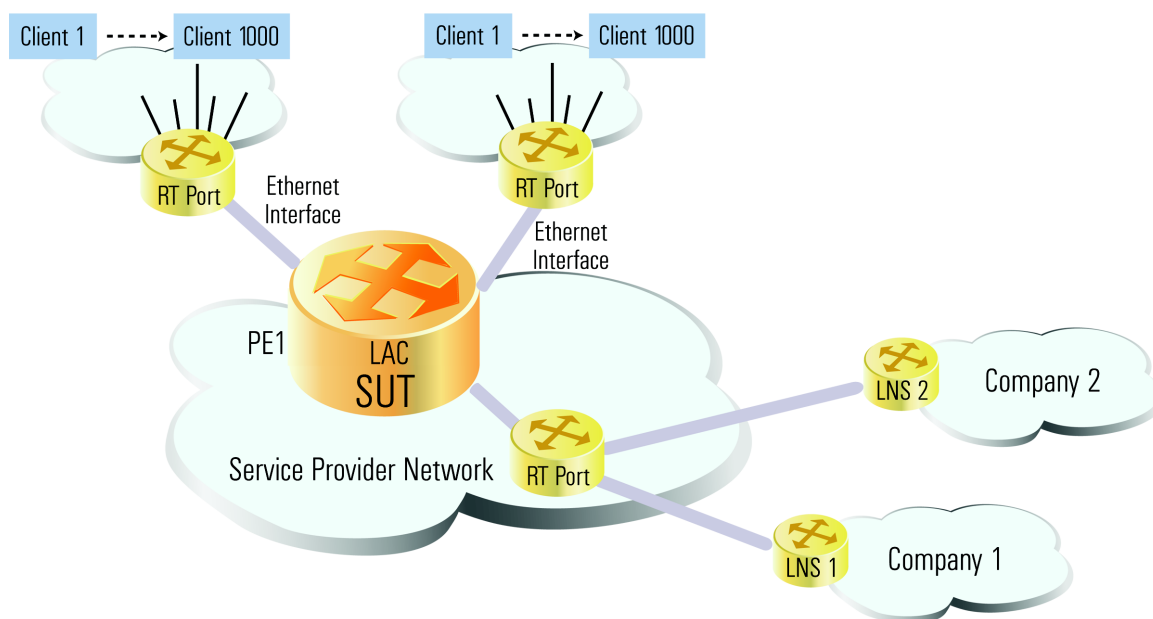
- Simulate real-world multiprotocol environments and measure performance related to VPN service offerings
- Establish thousands of L2TP tunnels and associated PPP sessions under varying conditions for stress-testing the SUT
- Measure tunnel and session capacity and tunnel/session set-up and tear-down rates of the SUT
- Tunnel/session flapping for testing the behavior of the SUT under real-life network conditions
- Verify protocol implementations
- Easy-to-use GUI that quickly configures physical interfaces and protocol parameters
- Includes pre-defined scripts (QuickTest) for automated measurement of performance metrics
- Tcl Application Programming Interface speeds the creation of custom test
- Vary protocol parameters (number of tunnels/sessions, sessions per tunnel, set-up rate, authentication) for testing under varying stress conditions

Product Overview

Agilent Technologies' L2TP Test Solution is ideally suited for control plane testing. The solution incorporates emulation of the both the L2TPv2 and the PPPoX (PPPoE and PPPoA) protocols. By varying set-up conditions, protocol parameters and authentication options and creating real-life network stress scenarios, testing L2TP-enabled devices becomes an easy task. Such comprehensive testing allows service provider and network equipment manufacturers to achieve their objective of verifying tunnel and session related performance of the edge aggregation devices.

Additionally, the companion product, the L2TP Conformance Test Suite (E7865A), completes L2TPv2 testing by verifying conformance of the implemented protocol software to published IETF standards through a comprehensive set of pre-scripted tests.

The fundamental test scenario involves the RouterTester simulating various network elements such as, LAC Clients, LNS, PPP clients as needed and then



Testing a LAC using the L2TP Protocol Software

setting up tunnels between the LAC and a LNS and tunneling PPP sessions through these tunnels. The concept of a Session/Tunnel Pool in RouterTester allows users to define a range of PPP clients and associate these sessions initiated by the simulated clients to individual tunnels from the tunnel pool. Through establishment of these tunnels and sessions, and by varying control plane parameters, devices supporting L2TP-based IP VPNs can be stressed fully to determine their performance under real network conditions involving thousands of VPN subscribers.

Typical Test Scenario: Testing a LAC

A typical test scenario for testing an L2TP Access Concentrator (LAC) is shown in the diagram opposite.

- Remote PPP Clients are simulated in two test ports and two L2TP Network Servers (LNS) are simulated in two test ports.
- The simulated Remote Client initiates PPP sessions to respective LNS through the SUT (LAC).
- The SUT sets up L2TP tunnels and incoming L2TP sessions with the LNS.
- Once the L2TP tunnels and sessions are in place, the end-to-end PPP session is established between the remote client and the LNS.

With this test set up, the following can be accomplished:

- Determine the LAC's (SUT) ability to establish L2TP tunnels with the right LNS.
- Measure tunnel set up and tear down rate.
- Measure tunnel and session per tunnel capacity of each LAC/LNS pair.
- By increasing the number of simulated LNSs more scalability testing can be done.

Similar constructs can be used for testing LNS with the test port simulating multiple LAC Clients.

Multi-Protocol emulation for testing IP VPN services

Testing of IP VPN services that rely on tunneling individual PPP sessions through L2TP tunnels requires the tester to implement both the L2TP and the PPP protocols with various encapsulations and authentication options. Along with protocol emulation, the tester also needs to simulate thousands of network elements such as the LAC, the LNS and PPP clients for testing under realistic Internet-scale conditions. Only by testing under these conditions can both the network equipment manufacturer and the VPN service provider feel confident that devices deployed can truly measure up to the requirements of VPN service subscribers. The RouterTester provides an easy way for creating these test scenarios through its comprehensive set of protocol emulations along with the ability to vary the pertinent parameters and user control of all aspects of the protocols' behavior. Below is a summary of various scenarios that can be simulated for testing L2TP-enabled edge aggregation devices:

- Establish thousands of L2TP tunnels to measure the tunnel capacity of the SUT and measure tunnel set-up and tear-down rates.
- Establish thousands of PPP sessions and tunnel these sessions through the L2TP tunnels and measure session per tunnel and session set-up and tear-down rate.
- Simulate link down condition and verify the ability of the SUT to handle abnormal network situations.
- Perform tunnel/session flapping to determine the performance of the SUT under realistic network load conditions.
- Set up and delete tunnels/sessions to simulate dynamic changes in the network.

Product Features

Verify and stress L2TP and PPP protocol implementations

The RouterTester provides an easy way to verify the robustness of the protocol implementations under various stress conditions. The L2TP protocol software follows the established standard (RFC 2661) and supports the transmission and reception of Hello packets to ensure that the L2TP tunnels and sessions continue to function after they are established. The PPP protocol software (RFC 1661) follows the link establishment options (LCP Phase) including CHAP/PAP (RFC 1994) authentication and establishes sessions after proper IPCP (RFC 1332) negotiation. Both PPPoE (RFC 2516) and PPPoA (RFC 2364) are supported. The tester can both initiate and respond to LCP Echo Requests and keep PPP sessions alive for user configured duration. All protocol options can be changed easily from both the GUI and the Tcl API to allow the user to set up various test conditions.

For testing robustness, various error conditions (tunnel ID mismatch, out of sequence packets, authentication error etc.) can be easily created by the user.

For users who require more formal conformance testing, the L2TP conformance test suite (E7865A) is recommended. This automated test suite comes pre-packaged with more than 180 test cases to completely test either the LAC or the LNS and verify adherence to published IETF specifications.

Easy-to-use graphical user Interface

A single dialog displays the complete status of the router test system. Physical/link layer status and alarms are highlighted. Traffic stream definitions, and statistics are displayed in real-time. The RouterTester configuration is easily saved to restore complex network and traffic simulations.

Tcl application programming interface

The Tcl-based API enables the user to create automated test sequences or pre-defined test configurations. It allows RouterTester to integrate with other instruments. Tcl scripts can run on the RouterTester System Controller, a remote PC, or Unix workstation attached to the Controller via a TCP/IP connection.

The screenshot displays two windows from the RouterTester application. The 'Statistics' window on the left shows a tree view on the left with expandable sections for L2TP (Packets, Tunnels, Sessions, Tunnel Timing, Session Timing), PPPoE (Packets, Sessions, Timing), and PPP (Packets, Sessions, Timing). The main area of the 'Statistics' window contains a table with the following data:

Session Pool Name	SCCRQ Rx/Tx	SCCRP Rx/Tx	SCCDN Rx/Tx	ICRQ Rx/Tx	ICRP Rx/Tx	ICDN Rx/Tx	OCRQ Rx/Tx
1A	0/1	1/0	0/1	0/1	1/0	0/1	0/0
1B							
1C							
1D	1/0	0/1	1/0	1/0			

The 'Routing' window on the right shows a 'Summary' tab with a table of selected ports. The table has columns for Port, State, E., Link Layer, #Sessions, #Active Sessions, Tester Address, and SUT Address. The data is as follows:

Port	State	E.	Link Layer	#Sessions	#Active Sessions	Tester Address	SUT Address
1A	Ready	<input checked="" type="checkbox"/>	L2TP	1	1	192.1.1.2	192.1.1.1
1B							
1C	Enabled	<input checked="" type="checkbox"/>	L2TP	1	1	192.1.1.1	192.1.1.2
1D							

The 'Routing' window also includes buttons for 'Routing Log...', 'Stop Routing Engine', 'IP Errors...', 'Enable All Session Pools', 'Disable All Session Pools', and 'Statistics...'. At the bottom are 'Close' and 'Help' buttons.

Session: Port 1A

Session Type: # Session: ☐ One per VLAN Address Pool

Pool Definition | **PPP Options** | **Link Layer Options**

Pool Definition

Pool Name:

Mode: ☒ Initiate Calls ☐ Respond to Incoming calls

Number of Sessions:

Session Lifetime: Min: Max: seconds

Session Initiation Rate: sessions every milliseconds

Traffic

Endpoint Address:

PPP Options

LCP Options

MRU: bytes ☐ Negotiate Address and Control Field Compression

LCP Echo Request Interval: seconds

Max Configure: seconds Max Terminate: seconds

Restart Timer: seconds Max Failure: seconds

Authentication

Authentication Protocol: ☒ CHAP ☐ PAP ☐ None

Username:

Password: ☐ Authenticate SUT

Base Domain Name: Number of Domains:

Assigning IP Addresses

Starting Address:

Modifier:

Link Layer Options

Type:

Identity: ☒ LAC Client ☐ LNS

Tester IP Address:

SUT IP Address:

Number of Calls per Tunnel: Hello Interval: seconds

R/W/S: Shared Secret:

Maximum Tx Retries: Initial Ack Timeout: seconds

Source UDP Port: Authenticate SUT: ☐

Called Number:

Bearer Capabilities: ☐ Analog ☐ Digital ☒ Both

Bearer Type: ☒ Analog ☐ Digital

Only Synchronous Framing is supported.

OK Cancel Help

Online Help

An extensive online help system provides complete descriptions and detailed usage instructions for every component of the RouterTester. Dialog-level, context-sensitive help provides rapid access to the relevant sections of the online help.

Applicable Standards

- CHAP (RFC 1994)
- IPCP (RFC 1332)
- L2TPv2 (RFC 2661)
- PAP (RFC 1334)
- PPP (RFC 1661)
- PPPoA (RFC 2364)
- PPPoE (RFC 2516)

Configurations

The system controller manages the test module and provides the common point of control for the multiport test system. All test modules are connected to the system controller through a Fast Ethernet Hub.

RouterTester

Hardware: A system controller and two test ports.

Product Number: E5151A L2TP Protocol Software (includes PPP emulation)

QA Robot

Hardware: A system controller with two test ports.

Product Number: E5151A L2TP Software (Only PPPoE software support is available on QA Robot.)

Technical Specifications

The following protocol-specific parameters are configurable through the GUI or the Tcl application.

L2TP Parameters

Parameter	Type	Range	Default
• Identity	Enumerated	LAC Client or LNS	LAC Client
• Source UDP Port	Integer	1 - 65,535	1701
• Number of callers per tunnel	Integer	1 - 65,535	1
• Hello Interval	Seconds	1 - 999,999	10
• Shared Secret	String	256 characters	"secret"
• Receive Window Size	Integer	1 - 10,000	4
• Bearer Capabilities	Enumerated	Analog, Digital, Both	Both
• Bearer Type	Enumerated	Analog or Digital	Analog
• SUT Authentication	Boolean	True/False	False
• Initial Ack Timeout	Seconds	1 - 999,999	2
• Maximum Tx Retries	Integer	1 - 999,999	5

PPP Parameters

Parameter	Type	Range	Default
• MRU	Integer	1 - 65,535	1500
• Address and Control Field Compression	Boolean	True/False	False
• Authentication Protocol	Enumerated	CHAP, PAP, none	CHAP
• Authentication Username	String	256 characters	"user"
• Authentication Domain Name	String	256 characters	"company.com"
• Number of Domains	Integer	0 - 65,535	1
• Authentication Password	String	256 characters	"password"
• Starting IP address for IPCP address management	IP address	Valid IP address values	192.1.1.2
• IP address modifier for IPCP address assignment	Integer	0 - 65,535	1
• Restart Timer	Seconds	0 - 999,999	3
• Max-Configure	Integer	0 - 999,999	10

Parameter	Type	Range	Default
• Max-Failure	Integer	0 - 999,999	5
• Max-Terminate	Integer	0 - 999,999	2
• LCP Echo Request Interval	Seconds	0 - 999,999	0

PPPoA Parameters

Item	Description
• Encapsulation	Both LLC Encapsulation and VC-based Multiplexing are supported.
• Starting VC Number	Max VPI is 255 Max VCI is 16,383 Default is VPI=0, VCI=32
• Modifier	Default is VCI=1
• Last VC Number	This is read-only. Computed using Starting VC Number, Number of VCs, and Modifier

PPPoE Parameters

Parameter	Type	Range	Default
• Number of sessions per source MAC address	Integer	1 - 65,535	1
• Service Name	String	256 characters	"AGILENT"
• Initial Ack Timeout	Seconds	1 - 999,999	2
• Maximum Tx Retries	Integer	1 - 999,999	5

Types of Statistics

L2TP Statistics

Types of packets	Transmitted/Received
• SCCRQ, SCCRP, SCCCN	Yes
• Hello	Yes
• StopCCN	Yes
• ICRQ, ICRP, ICCN	Yes
• OCRP, OCRQ, OCCN	Yes
• CDN	Yes
• ZLBAck	Yes
• Number of Tunnels	Attempted, failed, set-up, deleted
• Tunnel Timing	Min, Max and Average set-up time and set-up rate
• Tunnel Lifetime	Min, Max and Average
• Number of sessions	Attempted, failed, set-up, deleted
• Session Timing	Min, Max and Average set-up time and set-up rate
• Session Lifetime	Min, Max and Average

PPP Statistics

Types of packets	Transmitted/Received
<ul style="list-style-type: none"> • LCP <ul style="list-style-type: none"> – Config Req – Config Ack – Config Nak – Config Reject – Terminate – Echo Req – Echo Reply • CHAP <ul style="list-style-type: none"> – Challenge – Response – Success – Failure • PAP <ul style="list-style-type: none"> – Authentication Request – Auth Response • IPCP <ul style="list-style-type: none"> – Config Req – Config Ack – Config Nak – Config Reject • Number of sessions • Session Timing • Session Lifetime 	<ul style="list-style-type: none"> Yes Yes Yes Yes Attempted, failed, set-up, deleted Min, Max and Average set-up time and set-up rate Min, Max and Average

PPPoE Statistics

Types of packets	Transmitted/Received
<ul style="list-style-type: none"> • PPPoE <ul style="list-style-type: none"> – PADI – PADO – PADR – PADT • Number of sessions • Session Timing • Session Lifetime 	<ul style="list-style-type: none"> Yes Attempted, failed, set-up, deleted Min, Max and Average set-up time and set-up rate Min, Max and Average

Acronyms

API	Application Programming Interface
CHAP	Challenge Handshake Authentication Protocol
GUI	Graphical User Interface
IETF	Internet Engineering Task Force
IPCP	Internet Protocol Control Protocol
L2TP	Layer-2 Tunneling Protocol
LAC	L2TP Access Concentrators
LCP	Link Control Protocol
LNS	L2TP Network Server
PAP	Password Authentication Protocol
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
PPPoX	PPP over Any Link Layer (ATM, Ethernet or L2TP)
RFC	Request for Comment
SUT	System Under Test
Tcl	Tool Command Language
VC	Virtual Channel
VCI	Virtual Channel Identifier
VPI	Virtual Path Identifier
VPN	Virtual Private Network

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

