



# Testing Edge Aggregation Devices: The challenges of PPPoX

## Introduction

Point-to-Point Protocol (PPP) has long been used by millions of dial-up subscribers to connect to their ISP Point of Presence (POP). Designed to accommodate the interaction of a wide variety of hosts, bridges, and routers, PPP's strengths lie both in its ability to multiplex different network-layer protocols simultaneously over the same link and in its encapsulation and framing formats that are engineered for maximum compatibility with typical host/router hardware.

As new technologies emerge, PPP is being adapted to work with them. Thus, multiple link layers involving PPP can occur in various combinations in access networks, such as PPP on ATM links (PPPoA), PPP on 10/100 Ethernet links (PPPoE), and a hybrid combination of PPPoE sessions carried over ATM links, known as PPPoAoE. These and other PPP-based access methods are referred to generically as "PPPoX". All of these technologies co-exist in the complex environment of today's access networks to connect broadband residential and enterprise customers to the Internet – or to remote Virtual Private Network (VPN) sites via L2TP tunnels.

In today's competitive environment, service providers can no longer merely provide the "link": their offerings must extend beyond PPP and link-layer connections to include services such as VPN. In particular, Remote Access VPNs – wherein travelling employees (road warriors) and telecommuters are provided secure and reliable access to corporate resources – are an important source of revenue for service providers. And, given that the foundation of remote access VPN technology is PPP, service providers must provide the full complement of PPP-related technologies.

In order to meet customers' performance expectations of PPPoX implementations, including VPN services, both providers and equipment manufacturers must perform an exhaustive series of tests. This white paper examines the test challenges for PPPoX-enabled devices – such as access concentrators, edge aggregation routers, and L2TP network servers – and outlines the types of tests that are necessary to verify that these devices are able to provide all manner of PPP services.

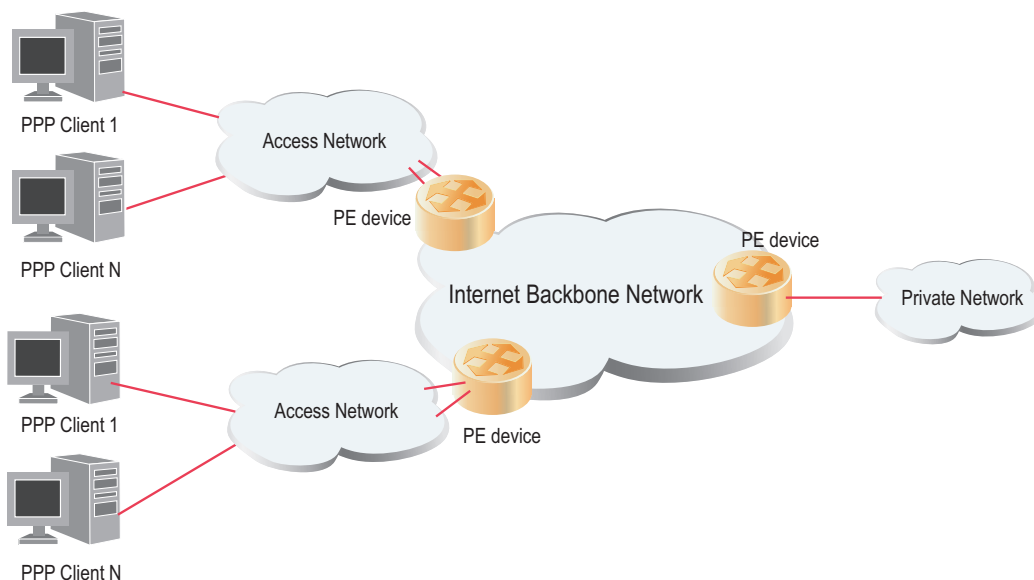
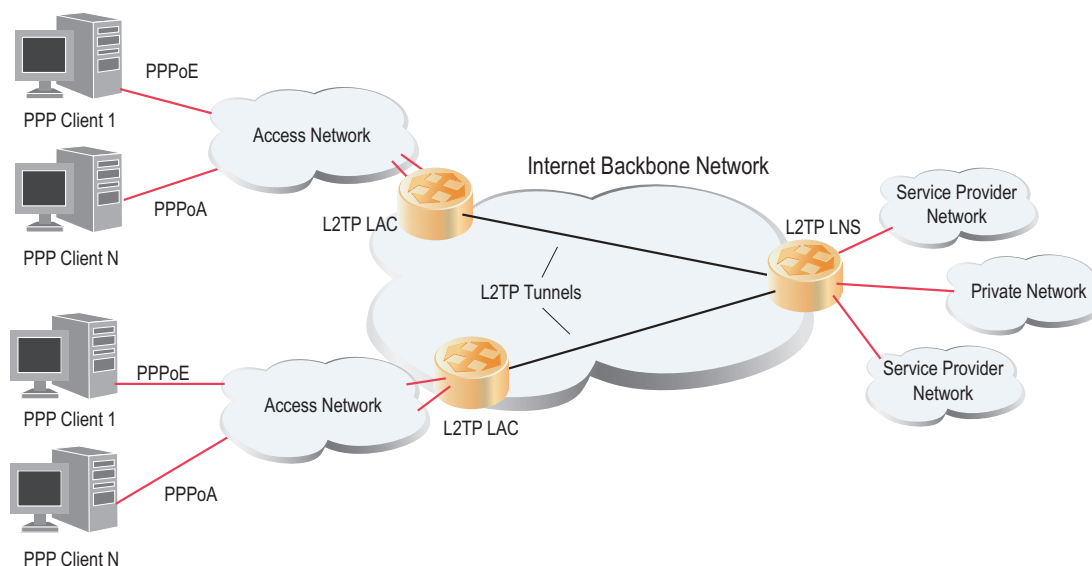


Figure 1: PPPoX deployment in the network



**Figure 2: PPPoX/L2TP in the network**

## PPPoX in the Network

Figure 1 shows a typical PPPoX deployment scenario. PPPoX sessions typically originate at the subscriber's PC and are terminated at the edge of the service provider's network where the edge aggregation device extracts the IP payload and routes it over a public network to the destination.

Figure 2 shows the application of PPP in a typical VPN deployment scenario. In this case, PPP sessions are aggregated and carried inside an L2TP tunnel all the way across the public network to an L2TP Network Server (LNS). Typical PPP-based VPN testing scenarios include testing PPP on ATM or Ethernet links (PPPoA and PPPoE), and PPPoL2TP tunnels, as well as the correct implementation of PPPoL2TP in access concentrators and network servers.

## Testing PPPoX implementations

A PPPoX access concentrator (or edge router incorporating PPPoX aggregation functionality) must correctly implement a number of features. First, it must be able to accept incoming session requests and establish PPP sessions. Once sessions are established, the device must then be able to receive and forward traffic according to Quality of Service (QoS) parameters. Sessions must be maintained for the duration of the traffic and terminated gracefully when no longer needed. If links go down, the PPPoX device must be able to re-establish sessions quickly. Besides implementing all of the above, the device must also be able to handle hundreds of thousands of simultaneous PPP sessions/customers. This section outlines the implications of testing each of these tasks.

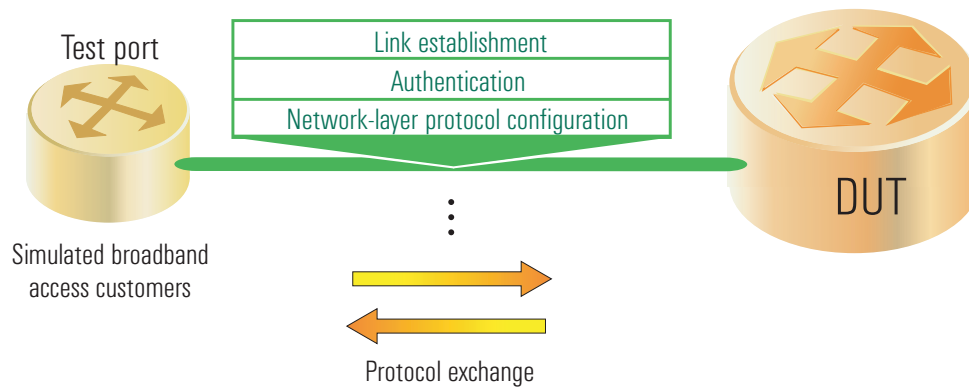
## Setting up PPP sessions

When testing PPPoX implementations, the first concern of network equipment manufacturers and service providers is to ensure that their device can successfully establish PPP sessions over a specific Layer 2 link. This procedure entails accepting incoming session requests and then successfully negotiating link establishment, authentication, and network protocol configuration. The device must also be able to terminate PPP links correctly. To establish (or terminate) a PPP session, a device goes through one or more discrete phases, each involving different types of protocol exchanges. These phases are outlined below.

**Link establishment phase.** Link Control Protocol (LCP) is used to exchange Configure packets that establish, configure, and test the data link connection. LCP negotiates such options as encapsulation format, packet size limit, error detection method, and link quality monitoring protocols. Successful completion of this phase results in an "LCP Opened" state.

**Authentication phase.** Once the session is open, this phase negotiates which authentication protocol will be used, if a peer is required to authenticate itself. Currently two protocols are recognized: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

**Network-layer protocol phase.** During this phase, each network-layer protocol (e.g., IP, IPX, and AppleTalk) is configured by the appropriate Network Control Protocol (NCP) to resolve LAN-specific problems, such as the assignment and management of IP addresses. For data encapsulated in IP, which is by far the most common network protocol, the NCP is Internet Protocol Control Protocol (IPCP).



**Figure 3: PPPoX setup rate test configuration**

**Link termination phase.** When a PPP link needs to be terminated, an exchange of LCP Terminate packets is necessary to close the link.

Besides implementing all of these protocols correctly, the rate at which a PPPoX-enabled device is able to establish authenticated PPPoX sessions is of vital importance, since thousands of customers may need to be reconnected quickly if a link goes down. Test equipment should provide the necessary link-layer interfaces (e.g., ATM, Ethernet), support the full PPP protocol stack (e.g., LCP, IPCP, PAP, CHAP), and be capable of scaling to setup rates beyond those of the device under test.

The PPPoX session setup rate test should determine the percentage of successful, authenticated sessions the device can establish at various setup rates – 25 sessions per second, 50 sessions per second, etc. Figure 3 illustrates a basic test configuration in which a single test port simulates many broadband access customers and initiates a user-specified number of PPP sessions at a given setup rate. Besides measuring the number of successful sessions for each setup rate, the test should also measure each session’s actual setup time as well as the average setup time at that rate.

### PPPoX session scalability

In today’s competitive environment, a service provider’s viability depends on the number of customers it can attract. With the broadband access market still expanding rapidly, this translates as the ability of a PPPoX edge aggregation device to scale to hundreds of thousands of individual, concurrent sessions. Testing the number of simultaneous PPPoX sessions a device can set up and maintain requires highly scalable test equipment that supports thousands of sessions per port to simulate realistic broadband access numbers.

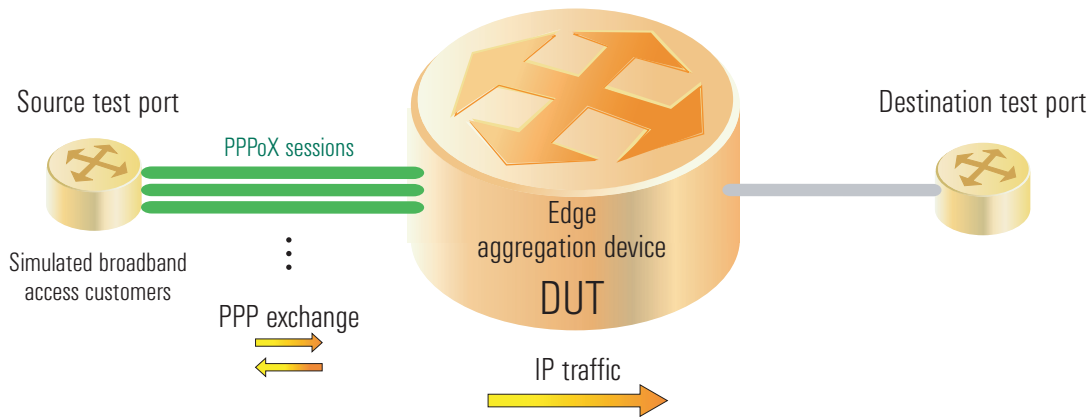
When testing PPPoX session scalability, the tester should initiate a large number of PPP sessions over ATM or Ethernet links with the device under test. After completing all the necessary setup phases and protocol exchanges, the device’s ability to remove the PPP header and forward native IP traffic should then be

verified. As illustrated in Figure 4, this test requires at least two test ports – one to set the PPP sessions with the device under test (DUT) and send PPP-encapsulated IP packets over each session, and a second port to receive and analyze the IP traffic. More source test ports can be added as the test is repeated with an ever-increasing number of PPPoX session setup attempts. For each iteration, the test should report the percentage of successfully established sessions. The number of PPPoX sessions, packet size of the IP traffic, and offered load are all user-specified variables.

### PPPoX session performance

While the number of PPP sessions that an edge device can handle is important for attracting customers, the quality of each individual session ensures that each broadband access customer will be satisfied enough to maintain their service contracts. To ensure the highest quality PPP session, traffic-related performance – or Quality of Service – must be measured on both an aggregate and a per-session basis. That means testing a PPPoX-enabled device’s ability to forward traffic at a high rate with minimal packet loss.

The configuration of the PPP session performance test is shown in Figure 4. The test begins with the tester opening a relatively small number of PPP sessions with the DUT, to which more sessions (and test ports, if needed) are added incrementally up to the maximum number of sessions that the DUT can support. For each iteration, the test should report the number of packets transmitted and received for each session, the packet rate (in packets per second and the percentage of the maximum rate), and the minimum, maximum, and average latency. These measurements will then be used to establish service-level agreements (SLAs) with key broadband access customers.



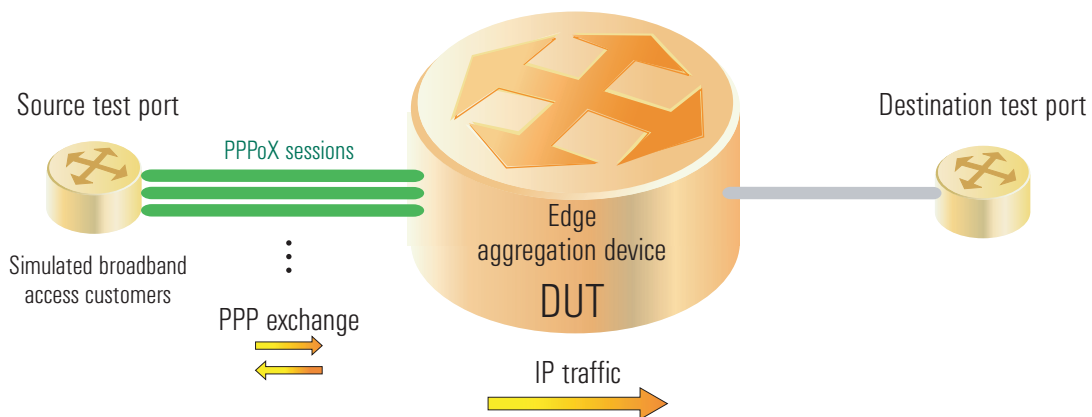
**Figure 4: PPPoX session scalability and performance test configuration**

### Performance impact of PPPoX session flapping

Once basic testing – measuring setup rate and session scalability limits – has been performed, it is important to subject the DUT to stress testing under real network conditions. By subjecting the edge device to session flapping, wherein the number of active sessions varies over the course of the test, the device's ability to handle simultaneous session initiation and termination at varying rates can be gauged.

The configuration of the PPP session flapping test is shown in Figure 5. After a given number of sessions have been established, the tester terminates a subset of the sessions already established (according to the PPP protocol specification) and then establishes a new number of sessions. This process is

repeated and the results recorded in terms of number of sessions terminated and number of sessions established at each iteration. Over a number of iterations, this test provides data on the DUT's ability to handle session termination/re-establishment (session flapping) requests. The test can be made somewhat more complex by also varying the session setup rate at each iteration, which would further indicate the DUT's ability to handle session flapping at fast setup rates.



**Figure 5: Performance impact of PPPoX session flapping test configuration**

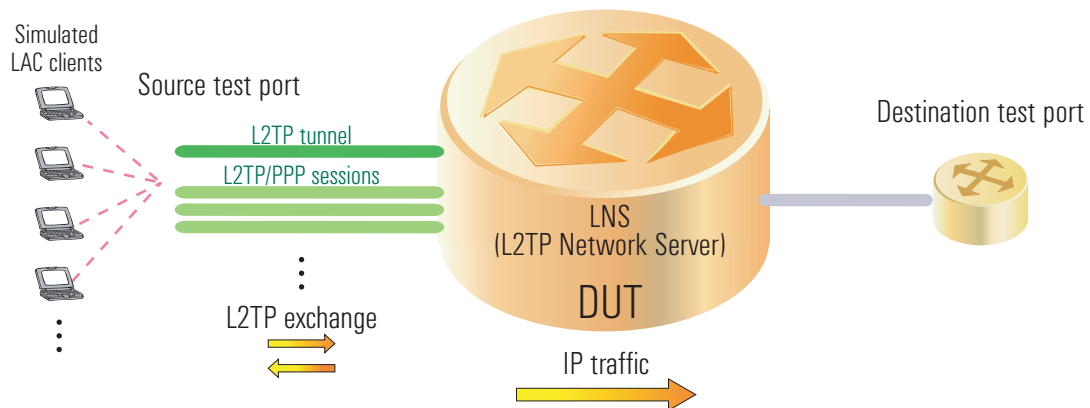
## Testing PPPoL2TP VPNs

Using L2TP tunnels to carry PPP sessions over a non-point-to-point public network is especially useful for VPN services, where network security and efficiency are critical. Known as PPPoL2TP, this technology aggregates thousands of PPP sessions into one tunnel, thus avoiding the need to terminate sessions at the edge and route each individual IP packet through the network.

The network device that connects to a corporate VPN site and serves as the L2TP tunnel endpoint (with an L2TP access concentrator (LAC) as the tunnel's starting point) is called an L2TP Network Server (LNS). As with PPPoX edge aggregation devices, two issues are especially important when testing an LNS – the device's ability to establish many simultaneous L2TP tunnels and L2TP/PPP sessions, and the rate at which it can set up and tear down those tunnels and sessions. Test equipment

must be able to simulate an LAC or many LAC clients (i.e., PCs with built-in LAC functionality) to serve as the other endpoint of the L2TP tunnel. It must also be able to generate PPP-encapsulated traffic through each tunnel to verify tunnel viability.

The L2TP LNS tunnel scalability test is illustrated in Figure 6. A large number of L2TP tunnels are set up with a varying number of L2TP/PPP sessions in each tunnel. PPP-encapsulated IP packets are then sent from a source test port through the device to a destination test port to verify that the tunnels/sessions were correctly set up and that the device can remove the PPP header and forward the IP traffic. At test completion, the percentage of successfully established tunnels/sessions is measured. A second test repeatedly sets up and tears down a specified number of L2TP tunnels and L2TP/PPP sessions, then measures setup and tear-down rates for each one and calculates the average rate for that number of tunnels/sessions.



**Figure 6: PPPoL2TP tunnel scalability test configuration**

## Conclusion

With all of its associated authentication requirements, PPP is indeed a complex protocol. Setting up a single PPP session incorporates a minimum of thirteen protocol exchanges (including four for LCP, three for CHAP, and six for IPCP), plus additional exchanges, if any special LCP options are used. The termination phase also has its own minimum set of packet exchanges. When L2TP tunnels are involved or PPP sessions are layered over Ethernet or ATM, the number of protocol exchanges involved grows even greater. Any device supporting such a complex compendium of protocols must be thoroughly tested under real networking conditions, including the deliberate introduction of error conditions.

Beyond the testing associated with setting up tunnels and sessions, and the measured rates thereof, a service provider must also ensure reasonable QoS levels – especially low packet loss and latency. That means sending traffic with a mix of packet sizes and variable bandwidth all the way up to wirespeed, and then measuring QoS parameters. All of these put a premium on the tester in terms of providing not only protocol state machines and traffic generation capability, but also control over protocol elements, including test automation tools.

The demands of testing PPPoX implementations on edge devices require robust test equipment. Such equipment must have high port density to be able to simulate hundreds of PPP clients and receive IP packets. It must also be capable of simulating full protocol stacks for PPP, L2TP, and IP, as well as capturing and analyzing packets in order to produce QoS measurements for SLAs.

