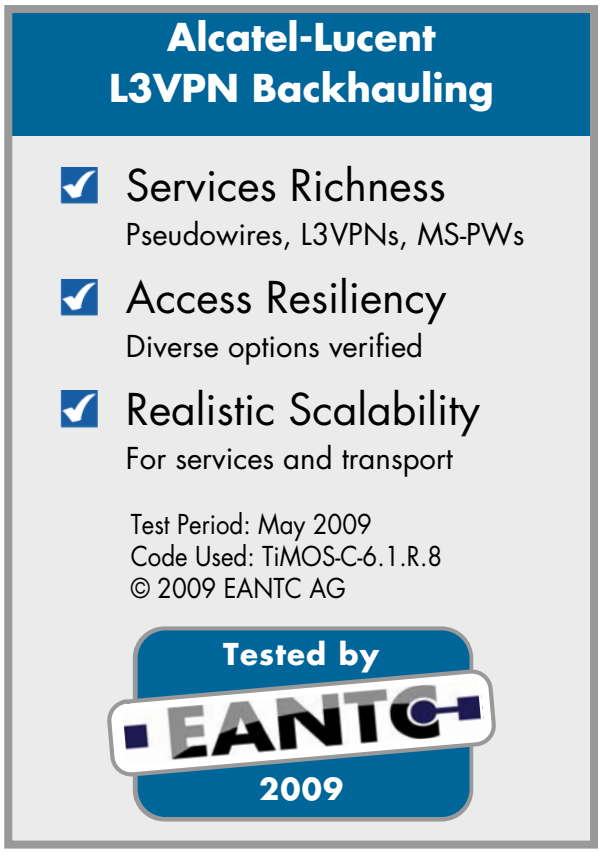
Alcatel-Lucent
Layer 3 VPN Backhauling Solution
Design Verification Test

Introduction

In Spring 2009 EANTC and Alcatel-Lucent performed a Design Verification test for a major European carrier. The test was completely independent – the carrier bore the cost of the testing while Alcatel-Lucent provided the facilities and the Solution Under Test. EANTC performed the testing using Ixia testers.

Provider-provisioned layer 3 virtual private networks (VPNs) have taken a central role in the majority of carriers networks over the last 10 years. While the core of the network retains its predominant IP focus, the edges — Metro and Aggregation, have been enjoying the benefits that cost-effective layer 2 based solutions have to offer, often in combination with MPLS.

Carrier-grade Ethernet is being used to keep the Metro and Aggregation networks simple and cost-effective. At the same time, these networks must connect between the device residing on the customer premise (called CE) with the starting point of the VPN (referred to as Provide Edge or PE). This utilization of layer 2 technologies to connect between two routing devices is referred to as Layer 3 VPNs backhauling.



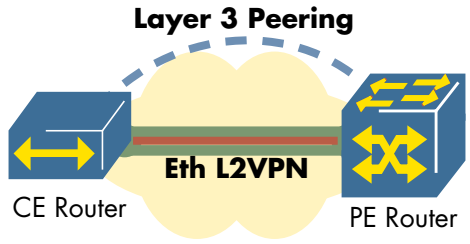
Why Layer 3 VPNs Backhauling?

Our customer wanted to use layer 3 VPN Backhauling which offers several attractive operational and cost benefits. The technology helps service providers scale down the dimension of the network core requiring fewer PE routers. This is possible by transporting customer edge router connections across a number of Metro areas to a central PE router. Reducing the number of PEs that a network needs to support has the following benefits:

- Cost reduction – both capital expenditures by requiring less routers and operational costs by reducing power consumption and support personnel
- Ease of operations – when an issue does occur it is much easier to localize, given a smaller core. In addition, the fewer devices a network needs to manage the more efficient the operations are

Service providers that are used to a two tiered operational structure – one for transport and one for services can maintain its systems. The backhauling of the service could still be managed by one group while the layer 3 service itself could continue being managed and offered by the same organization that has been supporting it thus far. This approach was taken by our customer, which is why it was important for us to verify that a clean and well defined interface could be defined between the transport and the service.

In the heart of this idea actually lie the benefits of using Ethernet as access mechanism for network services. Ethernet allows, after all, slicing of bandwidth to chunks as small as one Mbit/s, therefore allowing a service provider to use its expensive router ports more economically. This, in combination with the cost effectiveness of Ethernet ports, makes for an attractive proposition.



L3VPN Backhauling

The Test – Introduction

The test verified Alcatel-Lucent's solution for aggregation Ethernet backhauling of Layer 3 VPN services (L3VPNs), both of which MPLS-based. Together with the carrier we had set several goals for the testing, all of them aimed at making sure that the design, which was based on L3VPN backhauling, would work in a real world deployment. Three key aspects that apply to the majority of large service providers were tested:

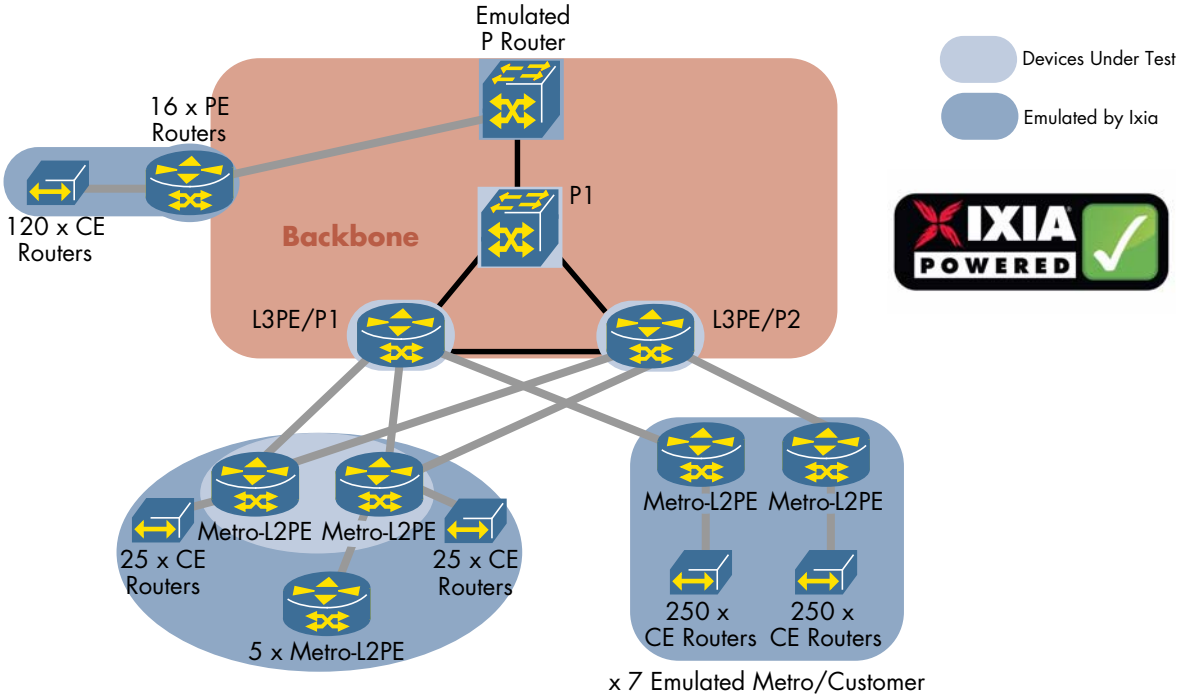
- The ability to offer Layer 3 VPN services, backhauled over layer 2 services, to a large number of sites and customers
- Matching appropriate resiliency scenarios with the solution
- Demonstrating the independence of the transport solution from the service itself and the potential to extend the service over network boundaries

We used a realistic number of services and devices for the test according to requirements set forth by our carrier customer.

Network Under Test

The network constructed for the test proved to be advanced and demanding. The routers provided and configured by Alcatel-Lucent were positioned in the exact network locations that were the focal point of the test, namely the Layer 3 VPN PE and the Layer 2 PE routers as is depicted in the figure below. In addition to these two functions Alcatel-Lucent provided a router to serve as a Provider (P) device. Two Alcatel-Lucent device types participated in the test:

- *7750 SR-7* – This router served as the MPLS layer 3 VPN workhorse positioned in the center of the provider backbone as well as the P router in the core. The *7750 SR-7* peered with all the emulated Customer Edge (CE) routers, maintained the virtual routing and forwarding instances for the layer 3 VPNs, stitched all the multi-segment pseudowires and terminated virtual private wire services (VPWS) directly into its VRFs.
- *7450 ESS-7* – This device was used as an MPLS layer 2 VPN router in the metro area. All multi-segment pseudowires and resilient CE-PE interfaces were being supported by this device.



Logical Network Under Test Setup

Key Architectural Aspects Tested

The engagement started with test cases verifying single functionality and culminated in a test that had all services and transport options active at the same time. As the tests progressed we added more configuration, more emulated control state and more services resulting in a realistically large number whose parameters are highlighted later in the report.

Metro to Backbone Interface Flexibility

There are a number of solutions for Metro Ethernet networks, some of which are using MPLS or IEEE standards such as Provider Bridges as defined in the IEEE specification 802.1ad (often referred to as Q-in-Q). Our service provider customer focused the initial design verification testing on the PE functionality. He wished to verify that the options for transport remain open – that both native Ethernet and MPLS technologies could be used to connect between CE and PEs.

The test was setup so that we were able to investigate two technologies that could be used as an interface between the metro devices and the backbone: provider bridges and VPWS. eBGP peering were set between the emulated CE router and the Devices Under Test (DUTs, in this case Alcatel-Lucent 7750 SR-7) regardless of the underlaying transport mechanisms. We verified that the DUTs were able to terminate the various access mechanisms by sending traffic between the emulated CEs belonging to the same VRFs.

The setup allowed us to simultaneously test several potential configurations. One emulated metro area used 802.1ad tags to directly terminate the customer connections into the router's VRF. A second emulated Metro PE used MPLS pseudowires directly terminating into VRFs on a second router. Both DUTs had emulated customers connected to them belonging to the same VRF.

Test Results

The test results were positive. We were able to terminate both provider bridges and MPLS pseudowires directly into our configured VRFs and recorded no difference in the performance of the layer 3 routers between the two access methods. No frames were lost in our traffic streams crossing the network and low latency was recorded.

The test showed that Alcatel-Lucent's 7750 SR-7 routers give service provider a flexible choice between at least the two different metro to backbone interfaces. The connectivity between the customer and backbone routers remained stable for the duration of the test. An additional benefit of the setup has been the fact that the CE router always had the same configuration – eBGP to the PE router and a VLAN tag on the interface to the network. The difference in the backhauling mechanisms were only visible to the carrier and not to the customer.

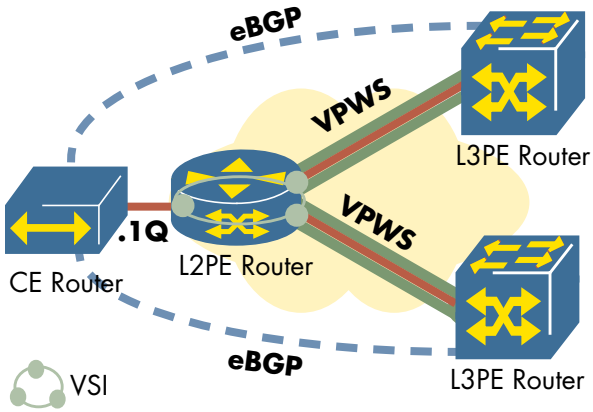
Customer Access Resiliency

While customers are often connected using a single interface to the network, the network itself must remain available, according to Service Level Agreements (SLA) up to 99.999% of a given year. In essence a business customer with several sites connected to the same network must be able to reach its neighboring sites at all times.

A CE router can maintain Dual Homed eBGP connections to two separate PE routers guaranteeing that if one PE fails the other will still provide network access. While this step is considered perhaps trivial these days, the underlying infrastructure connecting the CE router to the PE must also facilitate this resiliency mechanism by having a diverse set of paths through the network.

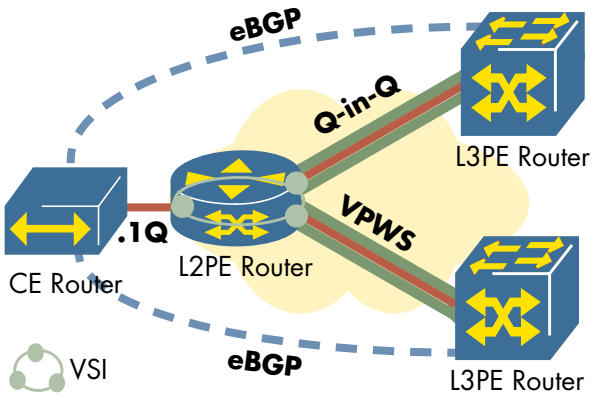
In our tests resilient CE to PE connections were set in one Metro area with Dual Homed eBGP peerings between the customer CE and two PEs. The underlying layer 2 transport used two mechanisms to provide diverse paths:

- Both links set as H-VPLS Spoke connections with the L2VPN router configuring a Virtual Switching Instance (VSI) for the access circuit and two uplinks spokes as depicted below



CE to PE Resiliency using VPLS Spokes

- One link between L2PE and L3PE set to use Q-in-Q and the second link using Ethernet Virtual Private Wire Service (VPWS). The option is depicted below:



CE to PE Resiliency using Q-in-Q and VPWS

Test Results

Both resilient access methods worked well. We emulated 250 resilient customer connections in one Metro area, verifying that all traffic sent for the dual homed CEs correctly reached its destination CE ports.

Complete Concept Use Case

Once the above concepts had been verified we created one massive configuration that mirrored the expected deployment scenario in a carrier's network. In addition to the dual homed CE routers and the 7 Metro areas, we configured 6,500 multi-segment pseudowires between several of the metros. All pseudowires were stitched by the L3PE/P1, terminated at the L3PE/P2 and emulated L2PEs.

We ended up with a network of the scale depicted in the test highlights listed in the table below. Alcatel-Lucent engineers configured Access Control Lists (ACLs) including 10,000 rules on one of the layer 3 PEs for all VPN traffic.

Once all the configuration was done we sent traffic for the majority of the routes within the VRFs as well as traffic traversing the multi-segment pseudowires. We monitored the test traffic for frame loss and latency as well as capturing the routers CPU and memory utilization.

Test Results

The test revealed a stable and robust solution. We recorded no frame loss over the duration of the test. The system resources (memory and CPU) were stable and ranged between 5.6% for the system and 35.4% for the BGP process (maintaining 2,000 eBGP sessions in addition to 16 mp-BGP sessions). The delay through the network was also recorded at an average of 59.1 microseconds.

Test Highlights

- → 2,000 eBGP sessions per PE router
- → eBGP sessions using Q-in-Q and Ethernet Pseudowires
- → 250 resilient customer connections
- → 120 VRFs per PE router
- → 6,500 Multi-segment Pseudowires

Summary

Configuring such a massive scale test is no small feat. In every step of the test process we added more and more features to the network and scaled them. At no stage did we encounter problems of the routers supporting our requirements.

The results showed that carriers can easily use Alcatel-Lucent's 7750 SR-7 and 7740 ESS-7 devices to support L3VPNs backhauling over a diverse set of transport methods, while still maintaining the access resiliency. The scale reached in the test mimicked a realistic service provider's needs and requirements showing that even with a minimal number of PEs in the core (two were used for the test) a large number of customers can be supported.

About EANTC

The European Advanced Networking Test Center (EANTC) offers vendor-neutral network test services for manufacturers, service providers and enterprise customers. Primary business areas include interoperability, conformance and performance testing for IP, MPLS, Mobile Backhaul, VoIP, Carrier Ethernet, Triple Play, and IP applications.

EANTC AG Einsteinufer 17, 10587 Berlin, Germany
info@eantc.com, http://www.eantc.com/