

European Service Provider Enhances MPLS VPN Service Delivery with VPN Explorer

VPN Explorer Service Benefits

- Improves service levels, customer satisfaction and retention, and reduces SLA credits to customers through:
 - Proactive monitoring and identification of emerging network and service health issues
 - Faster troubleshooting and problem resolution
 - Replayable forensic history to pinpoint root causes and isolate customer origination of issues
 - Accurate simulation of failure scenarios to ensure functionality of redundant PE to CE connectivity

Ensuring Higher MPLS VPN Customer Satisfaction

Some of the world's largest enterprises – from electronics manufacturers to automobile makers to worldwide delivery services – rely on a single European global service provider for their virtual private network (VPN) services. That provider delivers services over a backbone offering end-to-end MPLS connectivity, with all traffic encapsulated in MPLS once it enters the backbone. Many enterprise customers have embraced provider-managed MPLS VPNs because they offer simple and flexible layer 3 connectivity for multiple distributed sites.

But for service providers, successful MPLS VPN operation depends heavily on their network's routing, which controls site-to-site reachability and policy – not to mention the critical issue of customer-to-customer privacy. And MPLS VPNs today incorporate the IETF RFC 2547bis standard, which uses the notoriously hard-to-manage Border Gateway Protocol (BGP) to distribute the layer 3 VPN information that defines which customer sites can talk to each other across the provider's core network.

According to this provider's MPLS backbone engineering manager, there are two fundamental challenges in managing MPLS VPNs. One is that router configuration is a tedious manual process prone to errors. The other is the nature of the BGP protocol, which can generate thousands, even millions, of updates following a peering loss or other significant routing event. "If some BGP event happens on the network, you cannot go back later and see what took place unless you recorded that event at the moment it happened," he said. Lacking visibility into layer 3 routing topology and activity, service providers have had no reliable way of knowing when routing errors occurred or how to find and fix them once they did.

When he was first hired, this engineering manager quickly saw the potential applicability to the provider's backbone of a technology he'd deployed at his former job as an network architect at one of the leading North American Internet Service Providers. That technology, route analytics, could sit passively on the IP/MPLS backbone, "listening" to IP routing-protocol exchanges, creating an accurate, real-time, end-to-end layer 3 topology map and logging all routing events in a local data store. Route analytics solutions that incorporate the IETF RFC 2547bis standard can provide full visibility into the VPN infrastructure, giving the service provider instant knowledge of both reachability within individual customers' VPNs and privacy between VPNs.

VPN Explorer Operational Benefits

- Enhances productivity by:
 - Maintaining an always-accurate routing map and automating identification of service paths for trouble shooting, and redundancy planning
 - Providing per-VPN views of Layer 3 service health
 - Increasing accuracy of network change operations through highly accurate change modeling using the as-running network as recorded from the live network



VPN Explorer Provides Layer 3 Visibility for Layer 3 MPLS VPNs

Proven, Market Leading Solutions: Based in Palo Alto, Packet Design Inc. is the pioneer and market leader in routing-aware network management solutions. Find out more at www.packetdesign.com



Technology
Developer
Partner



MPLS VPN Service Provider Case Study

In mid-2005 the provider deployed VPN Explorer, one of a family of route analytics products from Packet Design, Inc., of Palo Alto, Calif. VPN Explorer incorporates a BGP root-cause analysis capability that can quickly analyze huge numbers of BGP messages to single out the key routing events behind major routing activity.

So the engineering manager was ready when one of his customers, a major electronics manufacturing firm, started reporting outages at its VPN sites. Using VPN Explorer's History Navigator feature – which lets the user "rewind" and "replay" his network topology map from any point in time since the device began logging data – he was able to review all BGP routing events around the time of the outage to see how traffic was rerouted to cause the problem. What he learned was that, just before the outages started, one of the customer premises routers had been misconfigured to propagate a new default route into the VPN; this new default route was overriding the correct one. The root cause of the problem was quickly identified: an operator at a third-party managed service provider (MSP) had inadvertently made a configuration error and "injected" the incorrect route into the system.

The engineering manager quickly found that VPN Explorer's benefits extended beyond just day-to-day troubleshooting to proactive monitoring of VPN instabilities that could help prevent problems from occurring in the first place.

For example, in looking at VPN Explorer's graph of historical network activity for one enterprise customer, a large financial services firm, he noticed a higher than normal level of background routing events. "No outages had been reported, and we hadn't suspected a problem," he said. "But the graph should be pretty level, with occasional event spikes, so the sustained high rate of routing activity indicated a situation such as a route flap or routing loop. Even though this situation hadn't yet affected the customer, it had the potential to stress our CPU and memory resources to the limit." He was able to use VPN Explorer to set an event threshold for this customer and others; whenever a threshold was exceeded, VPN Explorer would send him an alert.

Problems linked to ensuring redundancy are another area where route analytics technology can be proactively useful. "Customers deploy redundant routers and peerings to their critical VPN-connected sites, but the redundancy will work only if the routing is properly configured such that both redundant routers announce the same routes to the VPN," the manager said. "At initial setup, everything may be fine. But somewhere down the line, unrelated changes may be made, and configuration errors or incorrect design assumptions may creep in that cause the two redundant routers to announce different routes. This leads to a loss of actual redundancy. Often, until a partial or full outage occurs, no one knows anything is wrong – but by then it's too late. VPN Explorer provides 100 percent visibility into the backup routes and generates a daily report for BGP route redundancy. We can monitor all our redundant service customers and catch any issues before the complaints start to come in. In addition, we can use VPN Explorer's modeling capabilities to proactively simulate link failures and see exactly how the redundant connectivity would behave."

The combination of reactive analysis and proactive monitoring and modeling is the key to VPN Explorer's utility, according to the engineering manager. "There are things every service provider can do to increase the satisfaction of its MPLS VPN customers. But those things are often hard to pinpoint because the vulnerabilities created by transparent peering between customers and providers are hidden in the complexities of the network. VPN Explorer gives us all the evidence we need to troubleshoot customer problems and to minimize the chances that those problems will crop up again. And it does all this while sitting passively on the network, generating no traffic of its own."

Service Providers Using Packet Design Solutions and technology

