



VPN Explorer



Harnessing the Intelligence of IP

VPN Explorer is the first solution to overcome a critical operational blind spot in Service Provider MPLS VPN networks, providing network-wide and per-customer Layer 3 visibility, monitoring and analysis for RFC 4364 (RFC 2547bis) MPLS VPNs. Only VPN Explorer provides real-time knowledge about individual customers' VPN routed topology, VPN site-to-site reachability and routing policy enforcement, and inter-VPN privacy. By passively monitoring, recording and analyzing the information contained in the routing protocols (MP-BGP and IGP), a single VPN Explorer appliance can compute an accurate, real-time topology of each customer's VPN. It baselines each VPN and can alert the Service Provider whenever there are changes in routed topology, including whether they were caused by the customer. Powerful visualization, reporting, and diagnostic tools show the current state of each VPN, as well as provide a full historical audit trail of all VPN routing events. Based on Packet Design's patent-pending route processing algorithms and incorporating the industry-leading route analytics features of Route Explorer, VPN Explorer offers highly scalable and responsive OA&M capabilities for MPLS VPN services without the overhead or delays associated with traditional polling-based techniques. VPN Explorer speeds provisioning validation and time-to-revenue, and provides greater service assurance, uptime and customer satisfaction.

The Need for MPLS VPN Route Analysis

While the MPLS protocol controls the forwarding plane for RFC 4364 (RFC 2547bis) VPNs, it is the BGP routing protocol with multi-protocol extensions (MP-BGP) that manages customer VPN reachability and privacy for up to thousands of revenue-generating customer VPN sites. Service Providers need tools to:

- Quickly validate newly provisioned VPN services to speed deployment and time-to-revenue
- Maintain and monitor an accurate baseline of customer VPN routing operations
- Detect and correct site-to-site reachability problems before they impact services
- Avert privacy issues by assuring that Provider Edge (PE) router configurations do not cause "route leakage" between customers
- Rapidly respond to customer inquiries with accurate information on edge-to-edge VPN routing availability
- Collect and analyze critical forensic data for fast troubleshooting and data continuity during problem escalation

VPN Explorer Benefits

- Per-VPN baselining and monitoring of critical routing integrity:
 - Customer site-to-site address reachability
 - Provider Edge (PE) routers associated with each VPN
- IGP and BGP route analytics to provide core network routing monitoring, analysis, and modeling for increased service assurance
- Improved service forensics to determine the source of routing failures; including distinguishing whether reachability has been lost due to provider network or customer network issues
- Helps avoid outages and SLA pay-outs through modeling and simulation of planned network changes to ensure proper operation
- Small deployment footprint, minimal network load and continuous auto-discovery, delivering fast time-to-value and low management overhead

VPN Provisioning Validation

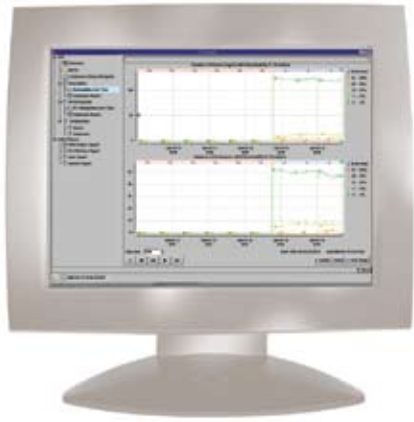
A key competitive factor for Service Providers is the speed of provisioning and deploying services. VPN Explorer allows operations groups to quickly assess the state and accuracy of newly provisioned MPLS VPN services, whether for a new customer or for a new site on an existing VPN. No other tool gives a real-time view of per-customer Layer 3 VPN status.

VPN Baseline and Health Monitoring

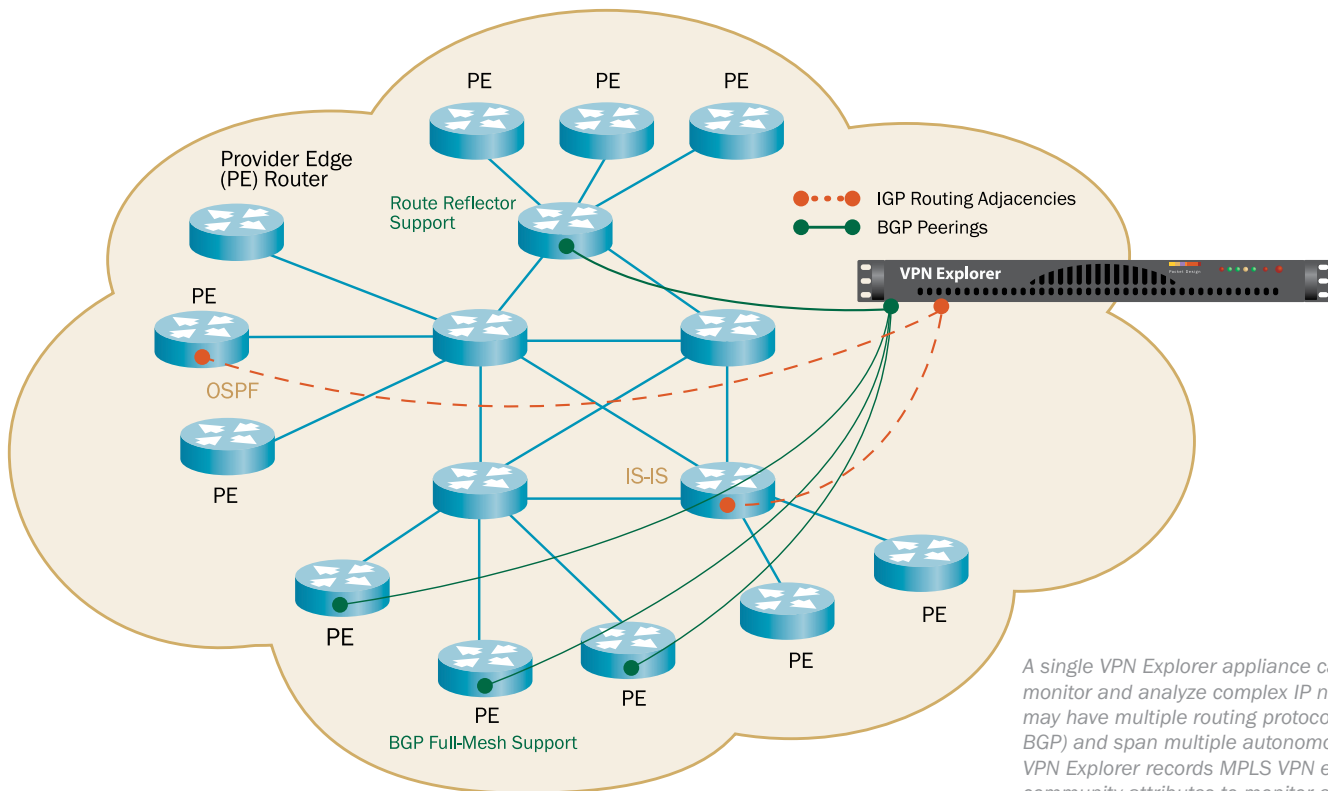
VPN Explorer passively monitors and records the MP-BGP and IGP routing protocols in the Service Provider's network to compute real-time and historical routed topologies for each customer VPN. Baselines of each VPN are automatically generated across multiple data attributes, including:

- PE routers participating in each customer's VPN
- Network prefixes advertised by each customer VPN site

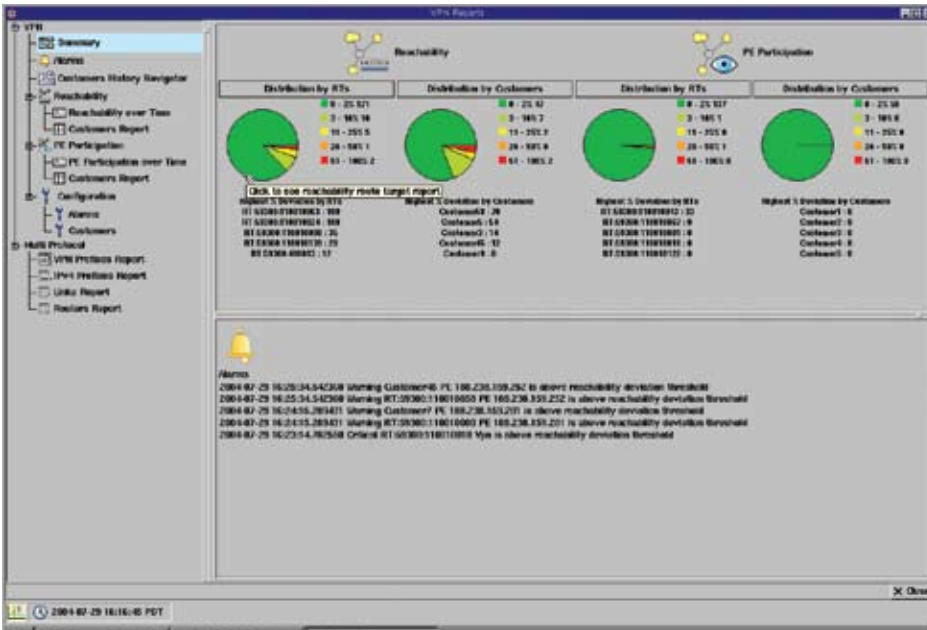
Using these baselines, VPN Explorer can provide network-wide and per-customer monitoring, reporting and alerting on the most significant changes in customers' VPN service. Instead of having to manually "hunt and peck" for this information by logging into multiple routers, users can easily visualize the Layer 3 status of each customer's VPN network. A VPN Explorer summary view provides the network administrator with overall VPN service health, individual customer VPN site-to-site reachability and PE participation, and status indicators showing deviation from customer baselines. Potential VPN "hot spots" are pinpointed, along with a list of customers whose VPNs have potential problems as indicated by an unusually high percentage of change in their VPN status.



VPN Explorer allows network managers to quickly view routing reachability deviations from baseline state for each of their customers' VPNs.



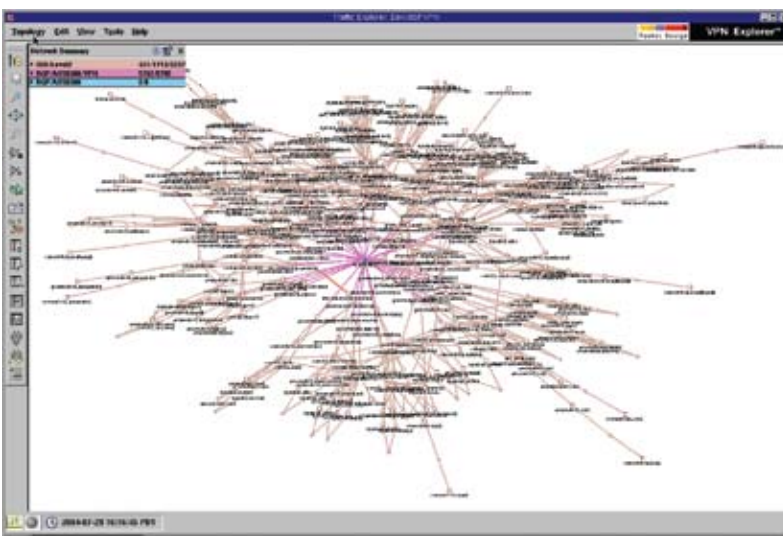
A single VPN Explorer appliance can concurrently monitor and analyze complex IP networks which may have multiple routing protocols (OSPF, IS-IS, BGP) and span multiple autonomous systems. VPN Explorer records MPLS VPN extended BGP community attributes to monitor each VPN's routing reachability and PE membership.



VPN Explorer records every routing event in the network. Engineers can “go back in time” and look at a stream of routing events pertaining to any particular customer VPN.

VPN Explorer provides at-a-glance visualizations of the overall health of the VPN service, and the customers who require the most attention.

VPN Explorer provides at-a-glance, network-wide, customer VPN monitoring and alerting and can be integrated into other operations systems. A topology map that can be viewed in real-time or historical mode shows the state of the network as of the specified time. By selecting an individual customer’s VPN, the user can see an overlay of the links and routers that comprise that customer’s VPN at the selected time on a topology map of the Service Provider’s entire network. Details including the prefixes advertised by each site and a complete list of all routing events pertaining to a single customer’s VPN can also be rapidly analyzed. Powerful event analysis and filtering tools let the network engineer quickly diagnose and resolve potential problems.



VPN Explorer allows network operators to easily drill down from summary views to per-VPN reachability and PE membership histograms and related routing event details.

VPN Explorer provides real-time, network-wide routing visibility across the Service Provider’s entire network, along with per-customer MPLS VPN monitoring and analyses.



VPN Explorer provides a comprehensive repository of network-wide routing information that network engineers need to speed troubleshooting and find the root causes of customer issues.



Network operators can be alerted if any customer VPN's reachability or PE membership deviates beyond pre-set thresholds from baseline state. Alerts can be sent via SNMP traps or Syslog messages.

Detailed Analysis and Diagnosis of MPLS VPN Problems

When problems occur, VPN Explorer not only detects them in real time, but helps the operator rapidly diagnose complex Layer 3 problems that typically go undetected by traditional network management products. Any deviation from baseline VPN operation is immediately detected, and historical graphs of prefix reachability and PE router participation let the administrator identify the exact moment when these changes occurred. Administrators can view a complete and accurate audit trail per customer VPN, drill down to see every relevant event, and leverage VPN Explorer's powerful sorting and filtering functions to isolate the root cause.

Change Modeling and Simulation on the As-Running Network

A large percentage of service-affecting problems are caused by misconfigurations. VPN Explorer allows engineers to model network changes before they're implemented, preventing outages from simple misconfigurations and even from network architecture errors that only become apparent when routing is altered. Since changes are simulated on an always up-to-date model of the network, engineers can be confident about the outcome of any planned maintenance operations or network upgrades.

Reports

Web-based reports can be generated for any historical time period, providing an overall understanding of network performance, while allowing quick identification of potential problem areas. In many instances, network problems can be averted or quickly isolated and resolved due to early awareness of anomalies. Data from reports can be useful in network maintenance and planning to understand trends, plan for network changes and growth, and verify changes made during scheduled maintenance. The breadth of VPN Explorer reports ranges from overall network health to reports that provide analysis of individual customer service history.

MPLS-VPN and BGP Reports

- VPN Site-to-Site Reachability
- PE Participation by VPN
- VPN Prefixes
- Links Report
- VPN Reachability over Time
- PE Participation over Time
- IPv4 Prefixes
- Routers Report

Alerts

VPN Explorer provides a range of alerts that can be enabled selectively, allowing for monitoring of specific routing events or problem areas and early notification of potential failures. Alert notifications can be viewed on the VPN Explorer console, sent to an SNMP-based network management system, or recorded to Syslog, for consolidated problem reporting and management.

MPLS-VPN Alerts

- Reachability Deviation by Customer or RT
- PE Participation Deviation by Customer or RT
- Reachability Deviation by specific Prefix(es)
- PE Participation Deviation by specific PE(s)
- Reachability Deviation by specific PE(s)



Packet Design

2455 Augustine Drive
Santa Clara, CA 95054
Tel: 408-490-1000
Fax: 408-562-0080
Email: info@packetdesign.com
www.packetdesign.com