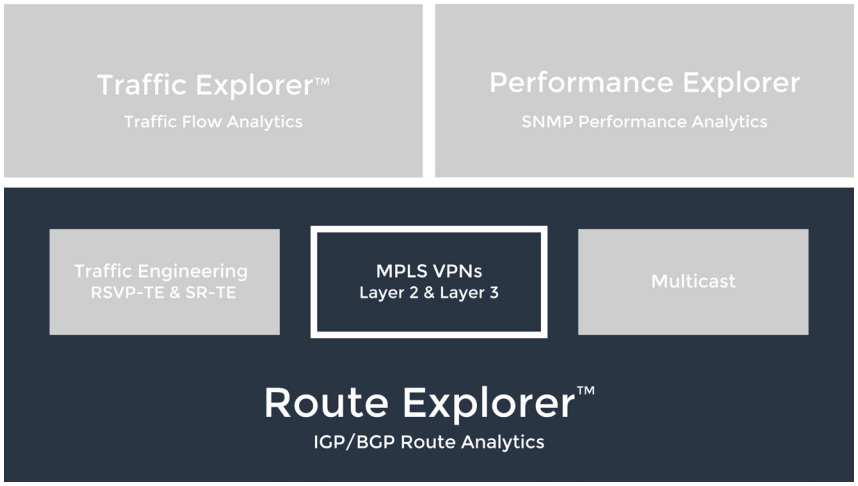
ROUTE EXPLORER™ FOR MPLS VPN WANS

The Route Explorer™ MPLS VPN WAN module is the first solution to deliver end-to-end network visibility across outsourced Layer 3 (L3) MPLS VPNs, helping enterprises ensure the availability, performance, and security of their wide area network (WAN), while keeping service providers accountable. Packet Design's industry leading route analytics technology provides an unprecedented view beyond the traditional boundaries of enterprise networks, encompassing both IP routing within the enterprise, as well as site-to-site reachability across the L3 MPLS VPN service. Route Explorer fills an important gap in enterprise WAN management, reducing network operations and engineering costs, while helping IT departments achieve their service quality goals.

Layer 3 MPLS VPN – An Outsourced IP Routing Service

When enterprises take advantage of L3 MPLS VPNs, they are relying on the service provider not only for connectivity and traffic delivery, but also for proper IP backbone routing between the VPN-connected sites. This includes ensuring that easily misconfigured routing between the enterprise's customer edge (CE) routers and the service provider's provider edge (PE) routers is stable and compliant with the enterprise's specified routing policies, as well as maintaining accurate exchange of critical IP network reachability information across the VPN between all connected sites.



The MPLS VPN WAN module is an optional extension to the Route Explorer base product.

Route Explorer for MPLS VPN WANs Benefits

- Ensure L3 MPLS VPN service providers deliver quality WAN service. VPN-aware route analytics baseline, monitor, report and alert on changes in site-to-site reachability that could impact network services.
- Quickly isolate site reachability problems while saving time, lowering costs and improving end-user satisfaction. A rich set of analytical tools helps diagnose the root cause of complex WAN outages, isolating it within the enterprise network or to the service provider's infrastructure.
- Easily maintain network integrity. Visualize, understand and verify WAN architecture and policies across one or more VPNs and service providers.
- Resolve historical or intermittent problems once and for all with complete historical data and the ability to rewind network state to any previous point in time for forensic troubleshooting.
- Analyze VPN usage trends for accurate network planning. Works with Traffic Explorer to readily show site-level, link-level and site-to-site VPN traffic reports broken down by ingress/egress, Class of Service (CoS) or user-defined traffic groups.
- Small deployment footprint, minimal network load and low management overhead delivers fast time-to-value and a low Total Cost of Ownership (TCO).

Since enterprises have no routing visibility into the VPN network connecting their sites, network managers are forced to carry out monitoring and troubleshooting processes without any knowledge of the outsourced IP routing service that comprises their WAN.

The importance of proper routing and reachability as managed aspects of a L3 MPLS VPN network cannot be underestimated. It is possible for all WAN interfaces to be reported as “up” using traditional management techniques, yet enterprises can experience down or unstable VPN routing, site-to-site IP reachability outages, compromised routing policies, route leakage from other VPNs, and even entire VPN failures that go undetected by traditional network management systems, yet severely impact application traffic delivery.

Layer 3 MPLS VPN-Aware Route Analytics Restores Network Management Visibility

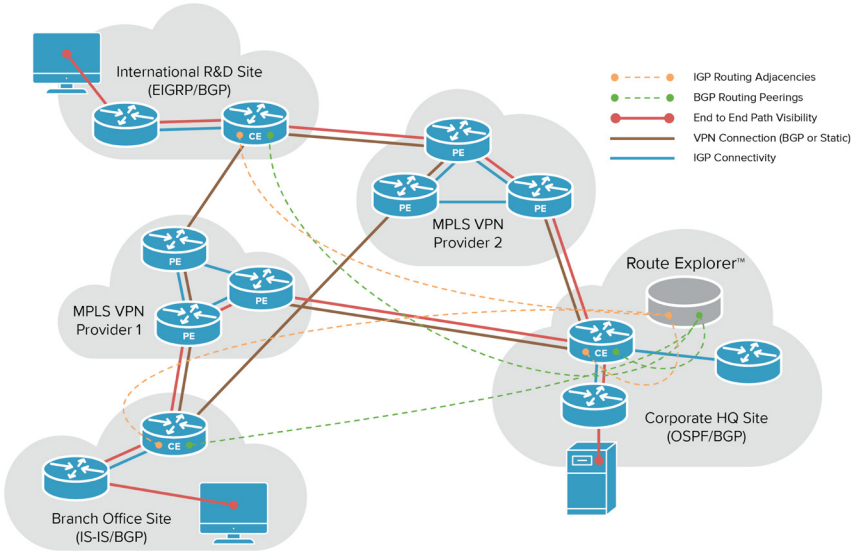
Route Explorer works by passively recording routing protocols such as OSPF, IS-IS, EIGRP and BGP to compute, monitor and analyze network-wide routing behavior. It delivers a real-time view of enterprise WAN architecture, showing site-to-site paths across one or more outsourced L3 MPLS VPN services, while monitoring reachability between all sites.

Real-Time Network Visualization

- View an accurate map of WAN routing architecture to understand and monitor VPN policy and status
- Not dependent on multi-minute SNMP polling cycles; helps IT respond faster to emerging issues

Monitor and Alert on Changes in WAN Reachability

- Easily create a baseline of site-to-site reachability specifying prefixes to be exchanged between sites
- Monitor active prefixes and alert on any deviations from baseline to identify reachability problems



End-to-end path awareness through the VPN provider cloud allows visual verification as well as alerting for hard to detect routing issues.

Enforce Service Provider Accountability

- Know when your Service Provider is responsible for WAN outages
- Ensure you are receiving the service quality you’re paying for

Accurately Simulate Changes on an Always Up-to-Date Network Model

- Simulate changes in routing or traffic for failure analysis or when planning network changes
- Understand the impact of adding new sites or deploying new applications before making changes

Works with Traffic Explorer to Deliver VPN Traffic Reports

- Analyze VPN traffic usage by WAN link, site, Class of Service, traffic group or Top-N reports
- Monitor and trend traffic loads to perform accurate WAN planning

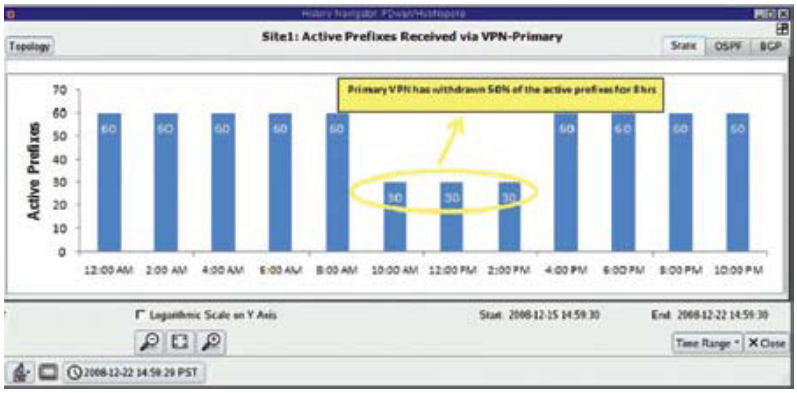
Highly Scalable Architecture

- A single Route Explorer physical or virtual system can manage an entire enterprise network including multiple L3 MPLS VPNs from multiple service providers
- Monitors full IGP network domains within all major sites (e.g. data centers), as well as reachability through the VPN to all “satellite sites” with no IGP domain (e.g. branch offices with a single router)

Critical Layer 3 Monitoring Keeps Service Providers Accountable

Layer 3 MPLS VPN problems can impact application delivery and increase costs due to lost productivity. Route Explorer monitors and alerts on VPN routing and reachability problems that otherwise go undetected, including:

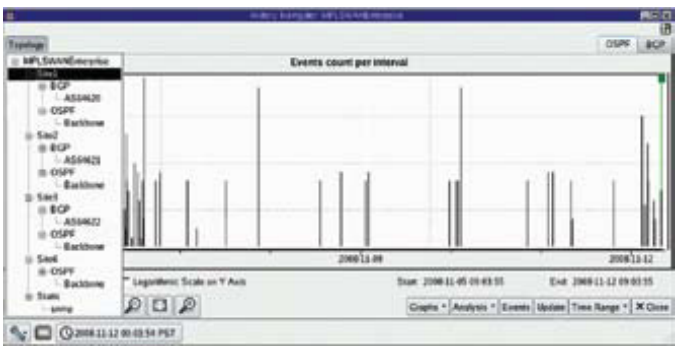
- Loss of site-to-site IP prefix reachability, such as when a key data center resource becomes unreachable from remote sites
- Routing instabilities or loss of IP peering between a site and the service provider network, even though the connection is still reported as “up” by traditional network management systems
- Failover of sites from primary to backup VPN connections and the resulting loss of redundancy
- Policy violations, such as when branch offices are directly connected over a VPN rather than through a specified hub-and-spoke architecture
- Compromised security resulting from route leakage between separate VPNs due to misconfigurations in the service provider network



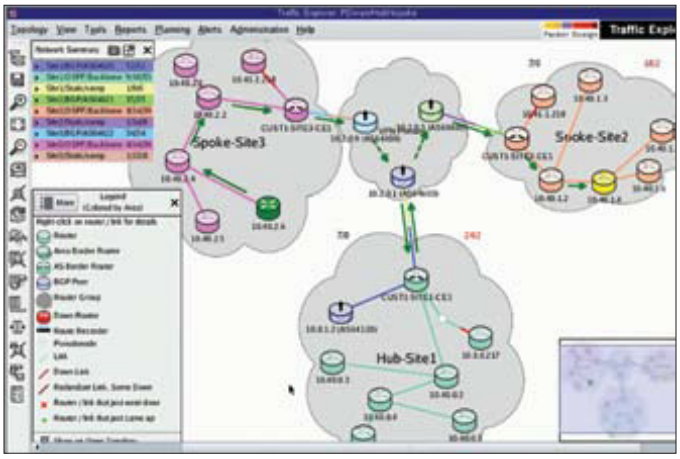
Understand the performance of VPN service providers and know when a provider is not meeting their SLA. Easily view the history of reachability to/from any site for each VPN provider.

Historical Analysis and Path Tracing Speed Troubleshooting

- Continuous recording of all routing events enables detailed forensic analysis of historical or intermittent problems
- Easy-to-use “network DVR” feature allows engineers to “rewind the network” to the point in time when a problem occurred
- Visual path tracing of application traffic between routed prefixes, and across the VPN, lets users quickly localize the problem and speed resolution



The “network DVR” feature window lets engineers see routing activity by protocol for each site, while moving the time cursor will “rewind” the network view to the time a problem occured.



Operators can view the network topology at any point in time, and see the path of application traffic within each site and across the VPN, to speed problem localization, diagnosis and resolution.

Comprehensive Reporting Helps Pinpoint the Root Cause of Problems

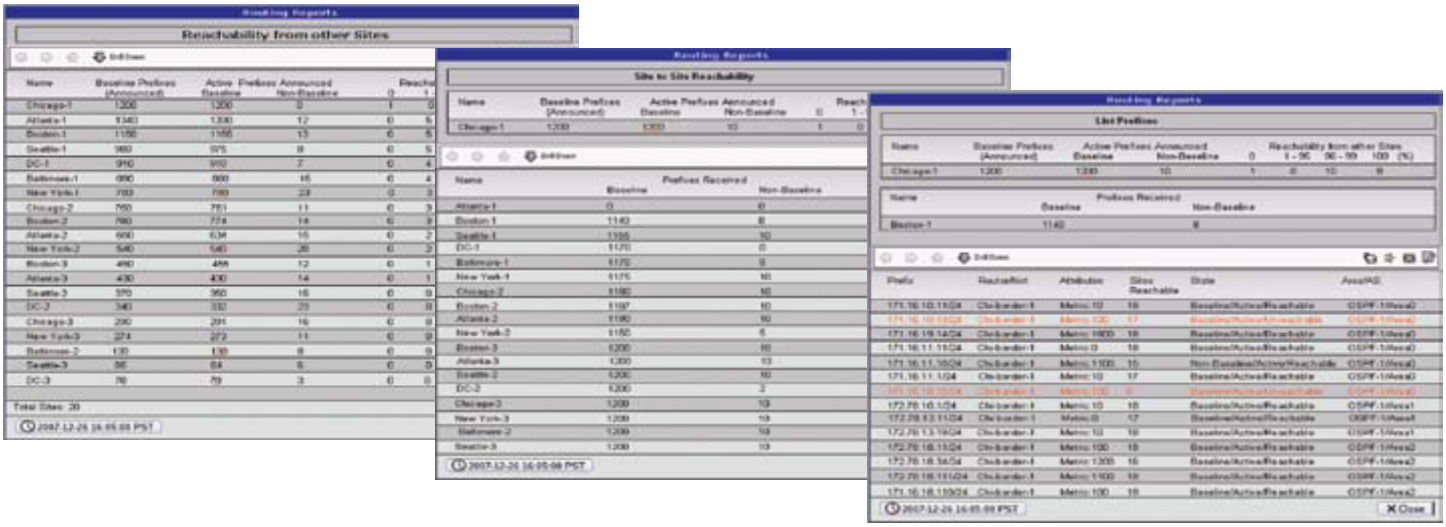
Route Explorer provides easily navigable reports and charts, from summary-level views of overall WAN reachability to per-VPN, per-site, per-prefix, down to the detailed routing events. WAN managers can create reachability baselines, specifying exactly how routing prefixes are to be exchanged between sites, and be alerted on any deviations from that baseline. Route Explorer's comprehensive VPN monitoring capabilities let enterprises know when their WAN service is compromised, and helps them quickly determine the cause of the problem.

Route Explorer Reports

- Overall reachability by VPN
- Site reachability from other sites
- Site reachability to other sites
- Reachability to satellite sites (small sites with minimal routing)
- Reachability by prefix
- Routing event details

Traffic Reports (when used with Traffic Explorer):

- Site-to-site traffic
- Ingress/egress traffic by site
- Ingress/egress traffic by WAN link
- Traffic classification by CoS and user-defined groups
- Top-N traffic reports (talkers, listeners, protocols)



Engineers can drill down from summary reachability reports to more detailed per-site and per-prefix analyses, and even examine historical routing events records.

Improve Application Delivery, Lower Operation Costs

Route Explorer's network-wide visibility increases the speed and accuracy of network operations and engineering processes, while ensuring the quality of WAN service to enterprise users.

- Real-time detection of changes in site-to-site reachability that affect network services
- Quickly isolate WAN problems and diagnose root-cause to minimize impact
- Monitor service provider performance to ensure they meet SLAs
- Visualize WAN architecture; verify policy and design of outsourced VPN service
- Improve accuracy of network change and maintenance processes
- Increase quality of WAN application delivery, end-user productivity and satisfaction