

VPN Traffic Explorer

*Comprehensive MPLS VPN
Management Visibility*



Packet Design

Executive Summary

Considering that layer 3 MPLS VPNs are a high-growth component of most service provider WAN offerings today, and a major source of revenue, providers possess a striking lack of visibility into the operational state of their customers' MPLS VPN networks. This is due to historical limitations in the scalability of traditional network management approaches.

VPN Traffic Explorer is a layer 3 network management solution that leverages Packet Design's powerful route analytics technology to provide unprecedented visibility into network-wide and per-VPN routing and traffic operations. It delivers routing and traffic monitoring, troubleshooting, capacity planning, service analysis, and network change modeling/simulation capabilities, along with customer reporting and enhanced business intelligence. Network managers now have the tools to maximize efficiency, productivity and profitability in their MPLS VPN service offerings.

Lack of Network-Wide Visibility Impedes MPLS VPN Management

As well-established as layer 3 MPLS VPNs are, there has historically been no practical way to assemble a network-wide view of VPN service traffic for an individual customer's VPN, let alone for the provider's entire network. As a result, many critical service management questions go unanswered, such as:

- Which routers and links are (or were) carrying a specific VPN customer's traffic?
- Are all the sites of a customer's VPN connected and reachable (at the IP layer) through the VPN network?
- What is the breakdown of traffic by individual customer and/or Class of Service (CoS) on any given link in the network?
- What is the growth trend for a VPN customer? For a particular CoS offering?
- If current VPN traffic growth continues, will the network's current QoS configurations remain valid in the future, or will network changes or capacity upgrades be needed?
- If a core network link fails, or is congested, which customers are affected?
- Will adding a new customer or carrying a new, bandwidth-intensive application impact the ability to meet existing customer SLAs?

Today's MPLS VPN networks are operated with too many "intelligent guesses" about the current and historical state of the network. Productivity and customer satisfaction are squandered in trying to find the root causes of problems without timely monitoring data or adequate forensic information. Without accurate information on the network-wide effect of VPN traffic growth to provide a "big picture" context for network engineers, MPLS VPN networks are prone to change management and, planning errors and frantic responses in an effort to maintain customer service levels.

These well-known deficiencies of MPLS VPN management have led to questions about the ultimate feasibility of an MPLS-based network infrastructure. Some have gone so far as to

propose leaving behind layer 3 MPLS networks and services in favor of non-MPLS layer 2 service models. But the massive investments made by service providers and the huge shift over the last decade from Frame Relay and ATM to Layer 3 MPLS VPN services don't permit an easy retreat. And such a retreat is unnecessary if service providers can find a comprehensive way to gain visibility into their MPLS VPN network and service delivery and bring OA&M capabilities in line with customers' ever-increasing service-level expectations.

Historical MPLS VPN Management Approaches are Inadequate

Traditional MPLS VPN management technology hasn't met service providers' business needs because it hasn't given them visibility into layer 3 routing and traffic across an MPLS VPN network. Providers have had to settle for expensive, incomplete solutions that provide very limited, edge-only visibility to customer VPNs, with no insight into the core networks where changes and errors have the greatest impact on service levels.

For most of the history of MPLS VPNs, service providers have possessed management visibility only into PE router state and PE-to-CE interface utilization statistics based on periodic SNMP polling. More recently, approaches based on NetFlow or probes have delivered information on customer traffic entering the VPN network at the PE router interfaces. Yet even these flow-based approaches fall far short of addressing service provider needs:

- **Lack of comprehensive per-VPN traffic analysis.** Although both NetFlow and traffic probe deployments provide insight into a customer's VPN traffic, this visibility is only available on a localized, per-interface or per-VRF basis. Since most customer VPNs are comprised of multiple VRFs, service providers have to look at many separate reports and manually correlate utilization statistics and specific flow data to gain a global understanding of the customer's VPN traffic. The lack of solutions that provide comprehensive, network-wide analysis of customer VPNs means that it takes more personnel and time to respond to customer issues.
- **Lack of VPN and core network topology awareness:** Since neither probes nor NetFlow information collected at the network edge reveal anything about the core network's topology or how a given VPN's traffic transits that core, traditional MPLS VPN solutions severely handicap network engineers, making it nearly impossible for them to correlate customer service issues with core network conditions such as link or router failures, traffic spikes and shifts, out-of-profile traffic on particular core links, or routing errors such as suboptimal paths, route flapping, and slow routing convergence. Given the size and complexity of MPLS VPN backbones, lack of visibility into an individual VPN's complete topology, including all PE to-PE paths connecting that customer's sites, means providers see the core network as a big dark "cloud" obscuring service-delivery conditions. They can't tell whether planned changes, new services, equipment failures or maintenance outages will affect existing VPN traffic, or how projected customer growth will impact their core network and customer service levels. The reason for this is more practical than technical. In order to "see" traffic on all links in the network, either probes must



be attached to a majority of the interfaces in the network, which is economically unfeasible, or NetFlow must be turned on ubiquitously, which would overwhelm the network with flow-record traffic.

- **Lack of insight into VPN routing reachability and integrity.** MPLS VPNs are layer 3 services, meaning that the service provider is responsible for delivering CE-to-CE prefix reachability. Service providers must also ensure that customer VPNs stay private and aren't exposed to security-compromising route leakages from other customer networks or potential outages due to overlapping private address spaces. Because current solutions don't monitor these conditions, service providers are blind to a critical aspect of service assurance.
- **No end-to-end service forensic history.** The traditional technique for troubleshooting historical problems is for an engineer to study a time range report showing traffic statistics for a given interface or VRF. This isolated analysis lacks the complete network view needed for effective troubleshooting and forensics. Solutions are needed that can present the actual state of the entire network, and the individual VPNs overlaid on that network, at the time when a problem was occurring.
- **No per-VPN or network-wide modeling and planning.** Today's MPLS VPN solutions provide only a "current" or "historical" view of VPN traffic on a small sub-set of links. To ensure service delivery in the face of dynamic network growth and activity, service providers also need the ability to interact with the state of the whole network, simulate network and service changes, and understand how those changes will affect traffic levels on an aggregate, per-customer and per-CoS basis across the entire network.

VPN Traffic Explorer: A New Approach to MPLS VPN Management

VPN Traffic Explorer brings a unique approach to MPLS VPN management by leveraging Packet Design's powerful route analytics technology to gain network-wide and per-VPN routing and traffic visibility with low network and operational overhead. Using information collected by passively monitoring the IP routing protocols that control delivery of MPLS VPN traffic (e.g., OSPF, IS-IS, and MP-BGP), VPN Traffic Explorer computes and maintains a real-time routing topology of the provider's entire network, as well as the individual VPNs overlaid on that network, including which PE's are participating in each VPN, the complete PE-to-PE paths through the core, and the customer prefixes that are reachable at each PE. It then employs a highly efficient and scalable NetFlow collection and analysis architecture that shows end-to-end traffic flows across all hops they traverse from edge to edge, as well as per-VPN and per-CoS traffic classification on every link in the provider's network.

VPN Traffic Explorer includes four types of appliances:

- VPN Explorer which passively monitors routing protocols (MP-BGP, OSPF, IS-IS) and computes real-time, network-wide and per-VPN topologies.

- Flow Recorders which efficiently collect NetFlow v9 flow records and LDP (Label Distribution Protocol) information at the PE-to-P router interfaces around the perimeter of the core network, rather than around the much larger CE-PE perimeter. Flow recorders intelligently associate inbound traffic flows with the VPN customer who sent the traffic and the exit PE router where it leaves the provider's network, to enable mapping of flows across their complete edge-to-edge path, while providing aggregate and per-customer traffic visibility (including bit rates, CoS, SRC/DST, port, protocol) on all links in the network core.
- Flow Analyzer which aggregates routing and traffic data from the VPN Explorer and Flow Recorders, generates and updates traffic reports (e.g. link utilization by CoS per customer, peering statistics) and issues alerts (e.g. utilization or CoS threshold exceeded).
- Modeling Engines provide simultaneous access to multiple users, allowing each to have an independent, customizable view of current or historical network state, from which they can analyze network activity, diagnose problems, or simulate network changes.

Since it doesn't rely on costly, broad deployments for NetFlow- or probe-based traffic collection, VPN Traffic Explorer consumes minimal overhead in providing network-wide MPLS VPN management visibility. Figure 1 illustrates VPN Traffic Explorer's architecture.

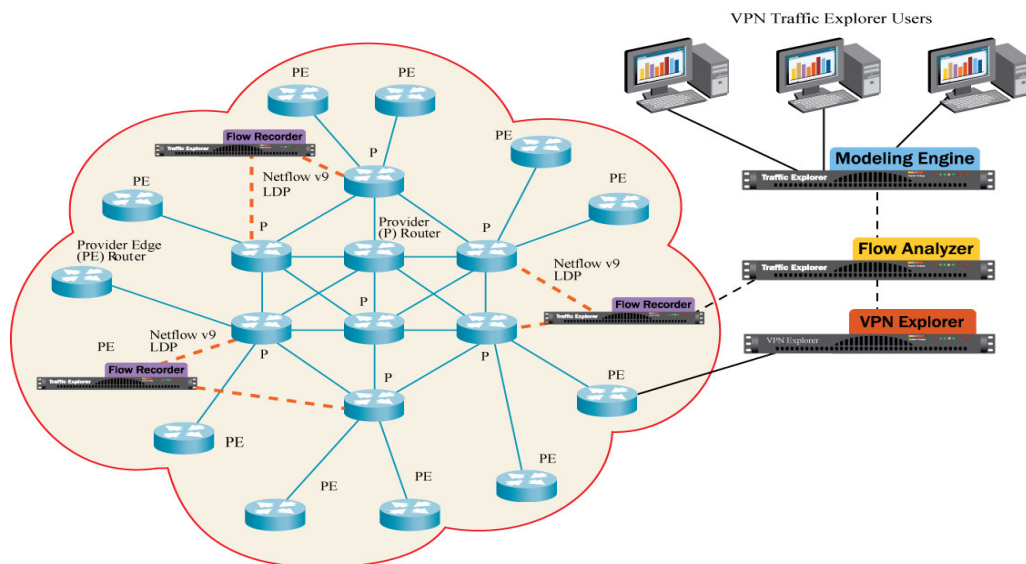


Figure 1: VPN Traffic Explorer efficiently collects NetFlow data only from the P routers at the perimeter of the core, providing network-wide traffic visibility with minimal cost or overhead.

Unprecedented Management Visibility for MPLS VPN Networks

VPN Traffic Explorer provides comprehensive MPLS VPN routing and traffic visibility along with extensive monitoring, analysis and planning capabilities to help service providers ensure the highest MPLS VPN service delivery:

Comprehensive VPN Monitoring and Alerting: On a network-wide and per-VPN basis, VPN Traffic Explorer monitors and alerts on such routing and traffic conditions as:

- VPN site to site routing reachability
- PEs participating in each VPN
- Total utilization, per-CoS and per-customer traffic crossing high/low thresholds on any link
- Per-VPN aggregate and per-CoS traffic high and low thresholds
- Network-wide router, route, or path changes or flaps
- BGP prefix floods or droughts

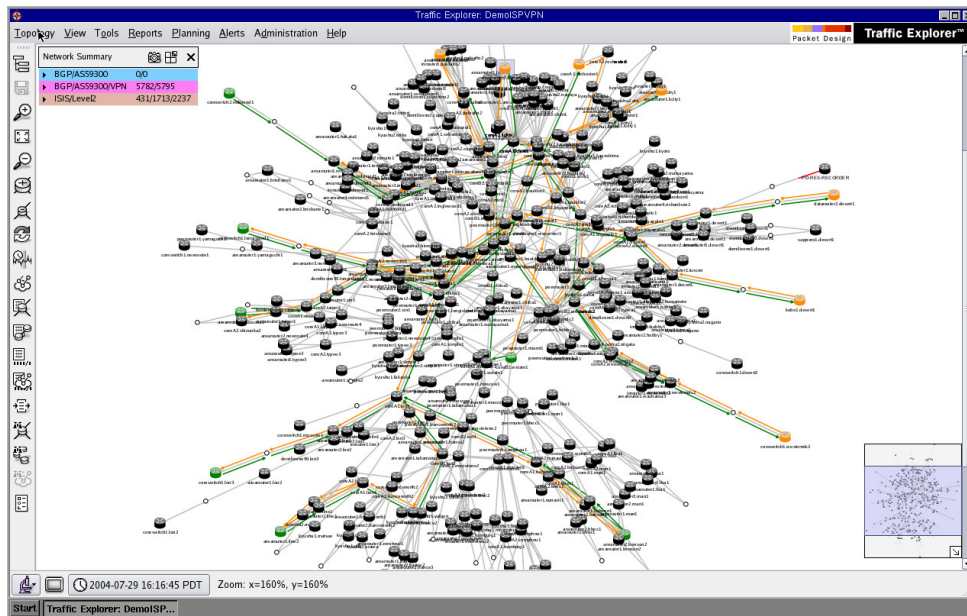


Figure 2: VPN Traffic Explorer monitors the status of MPLS VPN routing and traffic on all links in the network, not just CE-to-PE perimeter links.

Deep, Historical Troubleshooting: By recording every routing change and VPN traffic flow over time, VPN Traffic Explorer can provide a complete history of network state that is



invaluable in troubleshooting problems and revealing customer forensics. VPN Explorer's troubleshooting capabilities include:

- The ability to “rewind” the entire network model using a “History Navigator” (as seen in Figure 3) to see the exact state of network-wide and per-VPN routing and traffic at a given moment in the past
- Views of aggregate, per-CoS and per-customer bandwidth and utilization on any link across the entire network
- Quick identification of over- and under-utilized links
- Visibility into the PE-to-PE traffic matrix or a subset of the matrix broken down by VPNs, CoS or other criteria
- Understanding of all customers affected by a link failure
- End-to-end path highlighting between any PE pair
- Traffic loads between any PE pair
- Powerful and flexible drill-downs from any traffic report, allowing engineers to recursively refine their analyses (as seen in Figure 4) by further criteria such as:
 - Links (with aggregate traffic or broken down by VPN or IPv4 traffic)
 - VPN customers
 - Ingress or egress PE
 - Class of service
 - Detailed flow records
- Detailed views into traffic flow records at any historical point in time

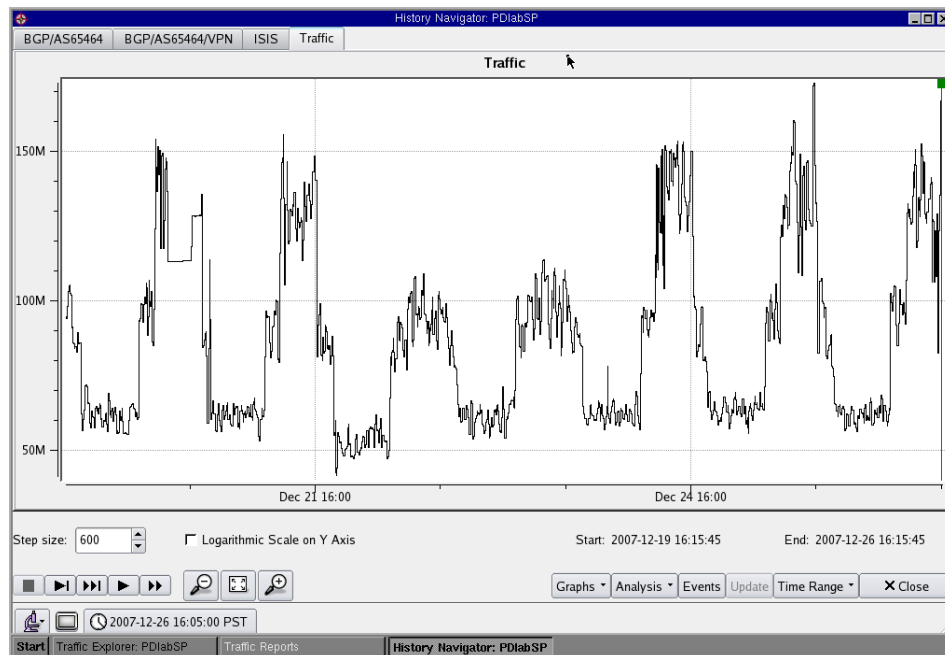


Figure 3: The History Navigator makes it easy for engineers to “rewind” the network and analyze traffic and routing conditions at the exact time a problem was occurring, greatly speeding troubleshooting.

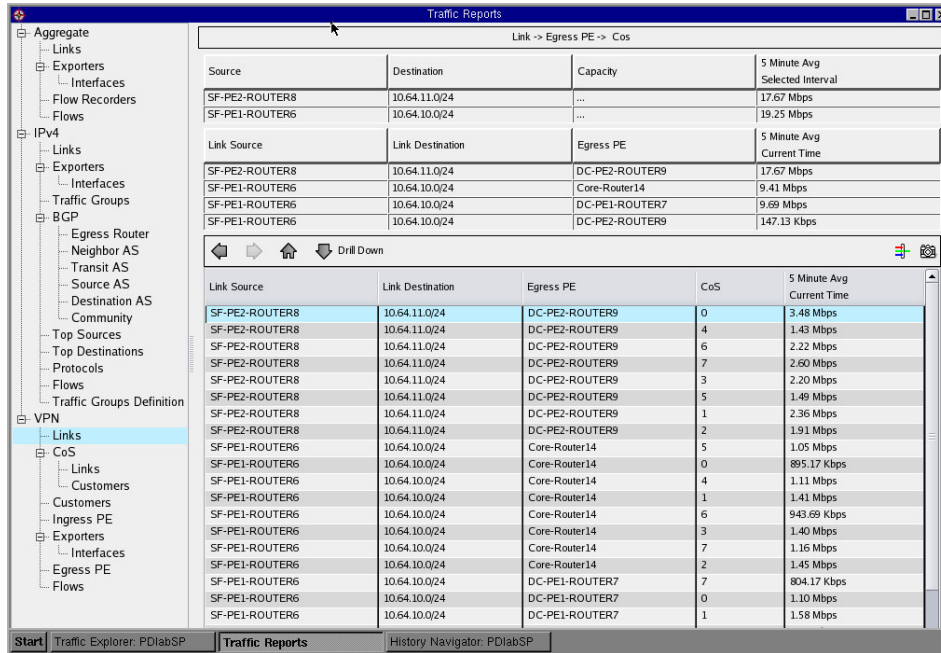


Figure 4: Engineers can flexibly analyze MPLS VPN (as well as aggregate and IPv4) traffic using VPN Traffic Explorer’s powerful traffic reports. Recursive drill-downs classify traffic according to selected criteria. In this case, an engineer can select a core link and view the per-CoS traffic matrix between a set of PEs whose traffic is transiting the link.

Network Capacity Planning: Using VPN Traffic Explorer’s continuously-updated model of all VPN service routing and traffic, engineers can perform accurate trending and capacity planning analyses to estimate future capacity needs, as shown in Figure 5. Capabilities include:

- Flexible analyses on:
 - Aggregate, IPv4 or VPN traffic, across all links or a selected subset of links
 - VPN customers
 - CoS: aggregate, per-customer, or per link or groups of links
- Trending based on a user-defined historical window defined in days, weeks, months or years
- Trend calculation using daily minimum, maximum, average or 95% traffic levels
- Support for linear or exponential projection models

- Projection to a bandwidth threshold, to let engineers understand when a link or links will hit a utilization level that requires additional capacity
- Projection to a specific future date to tell engineers whether, based on current trends, their short-, medium- or long-term capacity requirements are covered by existing bandwidth

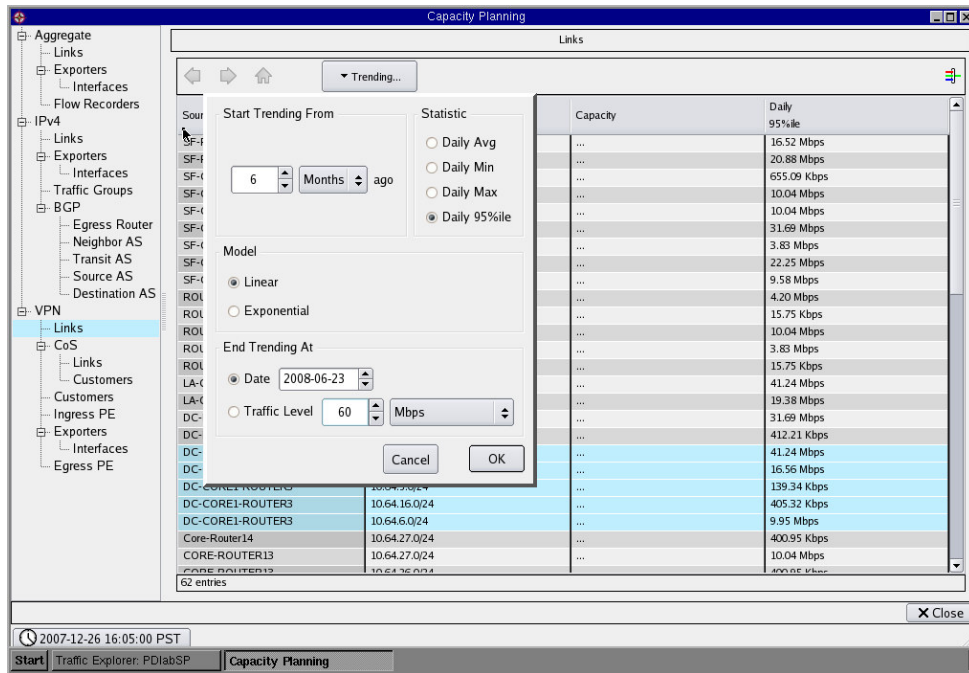


Figure 5: Engineers can perform capacity planning trend analyses on traffic categorized by links, customer, CoS and many other criteria.

Highly Accurate Routing and Traffic Modeling: VPN Traffic Explorer provides a “design mode” where engineers can simulate changes to the “as-running” routing and traffic, then perform “before and after” analyses to understand the network-wide effects of the changes. VPN Traffic Explorer allows engineers to add, down or change:

- Routers and links
- IGP metrics and BGP peering attributes
- New customer VPNs, VRFs and prefixes and traffic loads
- Traffic for an existing VPN customer
- Single or multiple traffic flows, including the ability to manipulate the entire traffic matrix

By granting engineers a global view of the effects of proposed or planned changes, VPN Traffic Explorer helps ensure that routine maintenance and new customer provisioning won't impact existing service levels. For example, engineers can simulate the addition of a new VPN and analyze its effects on traffic across all links and CoS levels, as seen in Figures 6 through 8.

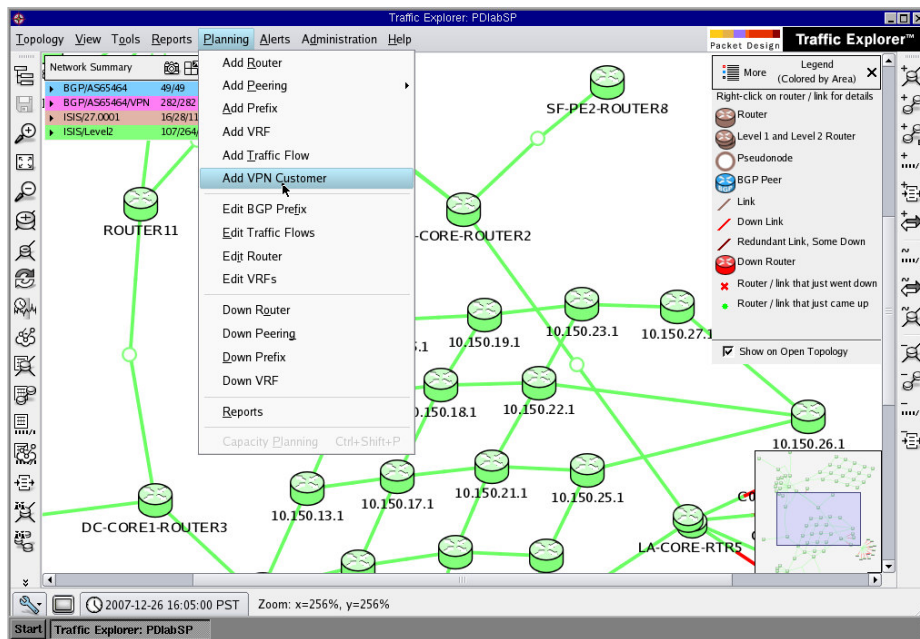


Figure 6: VPN Traffic Explorer provides powerful network modeling for adding, downing or changing routing and traffic elements in the network. An easy-to-use wizard can be used to simulate the addition of a new customer VPN.

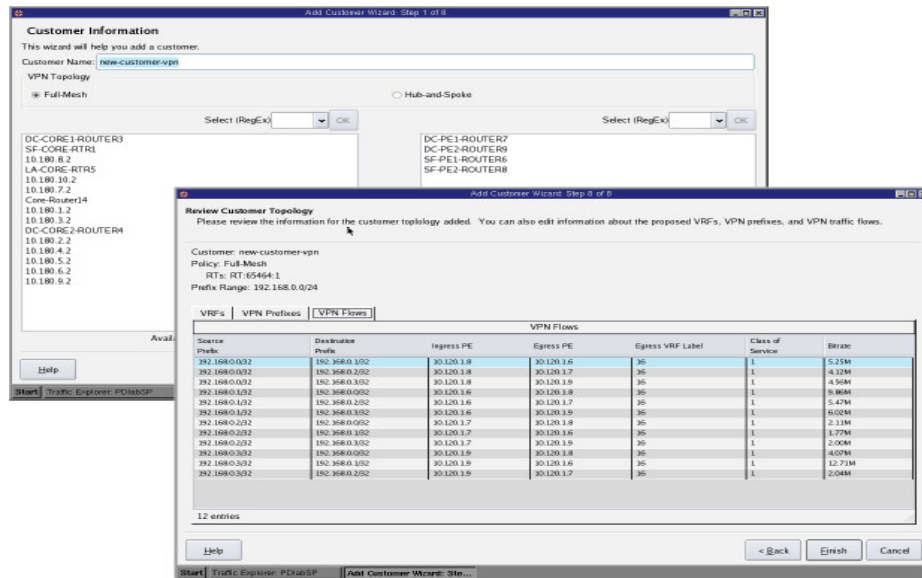


Figure 7: The “Add New VPN Customer” wizard allows engineers to define PEs, VPN routing topology, and PE-to-PE traffic matrix by CoS.

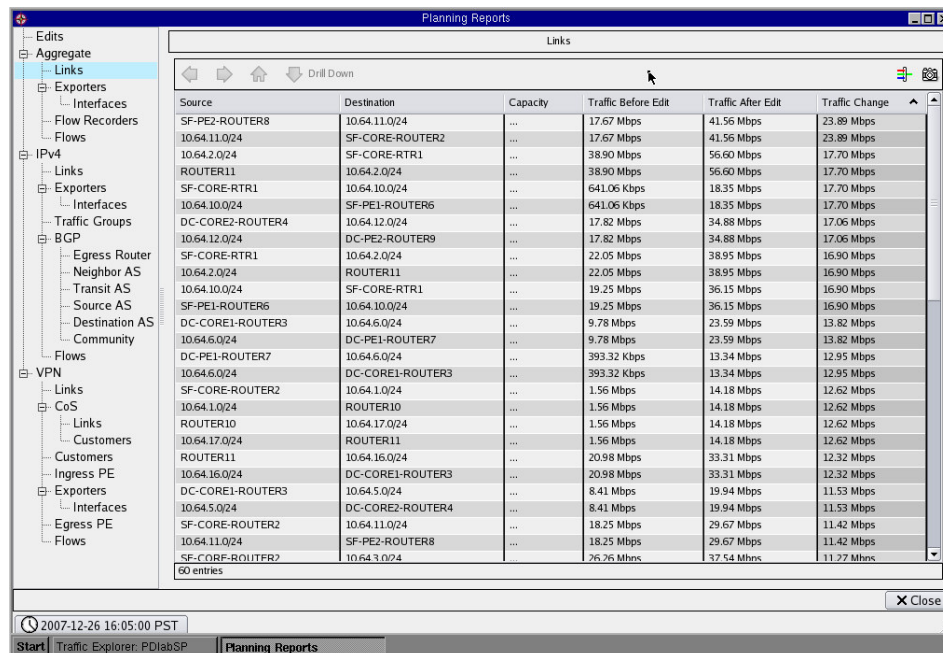


Figure 8: After modeling a network change (e.g., addition of a new customer VPN), comprehensive before-and-after analysis reports allow engineers to accurately assess the projected impact of the change (e.g., increase in utilization on all links).

Customer Reporting and Business Intelligence

VPN Traffic Explorer's rich VPN routing and traffic data support the creation of customer-facing routing and traffic reports through an XML API, providing additional value and differentiation for VPN services. VPN Traffic Explorer also provides product managers and sales departments with a rich source of intelligence for understanding individual and overall customer trends, allowing them to respond with optimized service plans for key customers and more competitive service offerings to capitalize on market trends.

VPN Traffic Explorer Benefits

VPN Traffic Explorer provides numerous key benefits to service providers and other MPLS VPN operators:

- Dramatically expanded management visibility into the network-wide routing and traffic operation of MPLS VPN service networks
- Much more timely and accurate fault notification and correlation on VPN service-affecting issues than that available from traditional network management tools
- Dramatically faster and more comprehensive troubleshooting, root cause analyses and customer forensics to achieve higher service uptime and customer satisfaction
- Powerful capacity planning and modeling tools allowing them to optimize use of existing network infrastructure to satisfy customer needs while reducing operational expenses
- Increased accuracy of daily, weekly and monthly maintenance and change operations reduces mistakes and customer service impacts, leading to higher service reliability
- Improved business intelligence based on the ability to analyze network-wide VPN service statistics to help drive innovative service creation and increased competitiveness that result in higher customer satisfaction and revenue

Conclusion

VPN Traffic Explorer delivers an extraordinary ROI to network managers looking to ensure the reliable delivery of business-critical MPLS VPN services. With unprecedented global visibility into MPLS VPN networks and services, service providers can bring MPLS VPN management capabilities in line with customer and market needs and expectations. For more information about Packet Design's technology and solutions, please visit our website at <http://www.packetdesign.com>.