Real-Time
Traffic Engineering Management
With Route Analytics
Executive Summary

Increasing numbers of service providers and mobile operators are using RSVP-TE based traffic engineering to provide bandwidth reservation and data-loss protection for MPLS tunnels, and to increase the predictability of traffic delivery. Deployments range from low numbers of ad-hoc TE tunnels to full tunnel meshes between core or edge routers.

Unfortunately, while providing network managers with the means to implement specific routing policies, traffic engineering today suffers from a lack of visibility into the real-time, dynamically changing states of traffic engineering (TE) tunnels. This lack of visibility has a profoundly negative impact on network operations and engineering. Monitoring and troubleshooting processes are delayed for lack of timely information, driving up mean time to repair (MTTR) and operating expenses. Change processes are more error-prone without up to date information on the true state of the network, affecting customer service delivery and triggering SLA payouts. And capacity planning is less accurate, wasting infrastructure investments and causing out of plan capital expenditures.

Fortunately, a solution exists to bring real-time, deep insight not only to TE tunnels but to the underlying IGP routing, overlaid Internet or MPLS VPN service routing, and network-wide traffic flows. Route analytics technology—which uses live routing protocol peerings as a source of unique intelligence into the dynamic behavior of IP networks, provides a way to understand the constantly changing behavior of all IP/MPLS routing and traffic, including RSVP-TE.

This white paper provides a brief overview of IP/MPLS traffic engineering and its common applications, explores the most important sources of tunnel dynamics, assesses current limitations to TE tunnel management visibility, explains how route analytics provides real-time visibility into TE tunnel dynamics, and demonstrates the advantages that network operations and engineering can gain by utilizing route analytics to monitor, analyze, troubleshoot and plan IP/MPLS traffic engineering networks.

A Brief IP/MPLS Traffic Engineering Overview

Traffic engineering is the practice of mapping traffic onto particular paths and links in order to optimize network resource allocation and enforce traffic policies. The most common way to do this is by:

- Implementing MPLS
- Configuring routers and links to support RSVP-TE
- Enabling OSPF or IS-IS traffic engineering extensions to propagate per-link traffic engineering information, such as link capacity, available bandwidth, and configured link group membership (link coloring and “Shared Risk Link Group” membership)
- Specifying path “constraints” such as required bandwidth and routing policies (such as including or excluding certain link groups, or even specifying which routers should be part of the path)
- Utilizing the RSVP-TE label distribution protocol to set up traffic engineered paths, also known as TE tunnels, that are calculated by the constraint-based shortest path first (CSPF) routing algorithm based on the specified constraints.
Common deployment use cases for MPLS traffic engineering include:

- Maximizing the utilization and redundancy of core links by enabling a full mesh of TE tunnels between core routers
- Leveraging Fast Re-Route (FRR) to achieve path restoration by avoiding IGP recalculation upon path changes or failures
- Specifying optimized edge-to-edge paths for specific customer transit traffic
- Ensuring that redundant paths don’t share common infrastructure facilities
- Routing traffic only through parts of a network to meet regulatory or other traffic policy requirements

**TE Tunnel Dynamics and the Limits of Current TE Visibility**

Since traffic engineered tunnels are calculated using constraint extensions to normal SPF routing algorithms, they can experience dynamic changes like other routed paths for a variety of reasons:

- Re-optimization: Tunnel re-optimization calculations are run by all head-end routers (the entry point of traffic into tunnels) on a regular basis—typically hourly—in order to ensure that changes in the network are accounted for.
- Failovers from primary to FRRs or to secondary tunnels due to IGP or router link failures
- Re-routing of tunnels based on changes in bandwidth availability and tunnel hold priorities
- Fast Re-Route tunnels that become permanent
- Auto-bandwidth: Head-end routers can be configured to periodically change tunnel bandwidth constraints based on growth or reduction in tunnel utilization
- Tunnels that go down due to network inability to meet specified constraints
- Changes to tunnel metrics that affect SPF calculations by routers, when tunnels are injected into the core IGP as links

Unfortunately, current methods of managing traffic engineering tunnels aren’t suited to tracking tunnel dynamics in real-time. First of all, while tunnel path shifts can happen very quickly and continuously, particularly due to IGP and auto-bandwidth changes, traditional methods for monitoring traffic engineering tunnels are based on relatively infrequent SNMP polling (no more frequently than once every five minutes) or on very occasional configuration file downloads (usually once a day). This means that only a fraction of tunnel changes are captured, severely limiting the data available for sound network monitoring and problem resolution. It’s not only the frequency of traffic engineering monitoring but also the depth of monitoring that’s limited via traditional methods. Due to limitations in vendor implementations, most routers don’t provide very much detail on tunnels via SNMP—so that in most cases, SNMP polling doesn’t reveal the path of the tunnel, which is crucial to understand the impact of the tunnel change. Worse, most traditional tools don’t provide insight into critical tunnel protection (via secondary tunnels or FRRs). Even in cases where more data is available, traditional tools store very limited or no history of network changes besides summary statistics, making it difficult to analyze problems after the fact, which means that engineers must wait for problems to reoccur before being able to effectively troubleshoot it—hardly the recipe for delivering a best in class quality of experience to end users. Finally, most traditional approaches have no way to show tunnels in their critical context—the rest of the dynamic IP-layer network topology which involves core IGP routing.
Network-Wide Traffic Engineering Management

Internet BGP routing, MPLS VPN routing as well as end-to-end traffic flows traversing the whole matrix of tunneled and non-tunneled paths.

The Cost of Insufficient Traffic Engineering Visibility

As is the case with other IP network technologies, lack of proper management visibility doesn’t prevent the deployment, provisioning and fundamental operation of traffic engineering, since aside from initial configuration, it is the routers themselves that run the algorithms and protocols that actually implement and realize TE tunnel operations in the network. However, lack of proper visibility significantly raises the cost of operating, troubleshooting, maintaining and planning traffic engineered networks, for the following reasons:

- Insufficient monitoring: Without real-time, detailed monitoring of TE tunnels, network operators can’t easily detect critical network issues that may affect large sets of customers. This means that network operators must take much more time to clearly identify the nature of emerging problems. Over time, this extra time consumption will exert a costly overhead on network operations and impact customer service quality.
- Dramatically higher MTTR: Without a detailed troubleshooting history of TE tunnel changes over time, network engineers who receive trouble ticket escalations are left with very little to work with. The result is that it takes far longer to resolve problems, and many problems remain unsolved. Ultimately, the lack of timely problem resolution affects the customer quality of experience, leading to increased churn and reacquisition costs.
- Inaccurate planning, costly maintenance mistakes: Without a holistic and accurate view of complex and inter-working routing, TE tunnels and traffic flows, it is simply too easy to make costly mistakes both in longer-term capacity planning as in routine maintenance. Such inaccuracies reduce network engineering efficiency and productivity, increase service level agreement (SLA) payouts and lower service quality, leading to top and bottom-line impacts.
- Higher risk of service failures and impacts: Without monitoring of tunnel protection mechanisms such as secondary tunnels, FRRs and SRLG analysis of facility diversity, there is no way for network engineers to ensure that infrastructure failures won’t cause service traffic delivery failures or degradations.

Route Analytics and Traffic Engineering—the Perfect Match

Route analytics is a technology pioneered by Packet Design that provides real-time, network-wide insight into the Layer 3 dynamics of IP networks—routing, traffic flows and traffic engineering tunnels. The foundation of route analytics is a unique way of monitoring, recording, visualizing and analyzing IP routing protocols. A route analytics network appliance acts like a router, setting up passive routed peerings (OSPF, IS-IS, EIGRP and BGP) with selected routers in the network (one per area in the case of OSPF), records all routing updates and creates an always-updated, highly accurate IGP, BGP and MPLS VPN routing topology using the same algorithms used by routers to choose routes. Route analytics can also intelligently and efficiently integrate NetFlow data into the topology by collecting NetFlow records from routers at the edge of the network, then projecting the flows across their respective routed paths to their exit router. Since route analytics records all routing and NetFlow events, it can not only provide real-time monitoring, but also
Network-Wide Traffic Engineering Management

rewindable troubleshooting and analysis. Finally, since the entire model is generated using routing algorithms, it can also be used as the basis for accurate network modeling.

With its complete understanding of IP-layer routing and traffic, route analytics provides the perfect context for monitoring, analyzing, and modeling traffic engineering tunnels.

Network-Wide TE Tunnel Discovery with Real-Time Monitoring

Unlike traditional network management approaches, route analytics can achieve continuous, real-time visibility into dynamically changing traffic engineering tunnels by leveraging its understanding of IGP routing. Using the comprehensive routing protocol-generated topology map as a starting point, route analytics can perform exhaustive tunnel discovery that gathers both the configuration and current operational state of all tunnels including full path details. Once discovered, route analytics monitors real-time tunnel state changes caused by underlying network issues. For example, when the route analytics appliances receives an OSPF or IS-IS message informing it that a particular link is down, it can immediately calculate that all tunnels traversing that link are down and consider their secondary tunnels to be active instead. In cases where OSPF-TE or ISIS-TE extensions announce that bandwidth availability has changed for a link in question, route analytics can query the link and connected router nodes in question to discover any shift of tunnels that occurred as a result. Additionally, real-time processing of router event log messages and an optional and periodic lightweight tunnel change discovery process ensures that any tunnel changes occurring due to re-optimization or auto-bandwidth timers are also captured in the topology.

Powerful Traffic Engineering Analyses Speed Problem Resolution

Route analytics’ real-time understanding of traffic engineering enables a variety of powerful analysis capabilities that aid engineers in detecting and solving TE tunnel problems:

**Integrated Routing and Traffic Engineering Topology Visualization**

Route analytics provides analyzable topology visualizations that can be used as the basis for understanding tunnel paths in their end-to-end routing context, as seen in Figure 1.
Network-Wide Traffic Engineering Management

Figure 1: Route analytics provides an integrated view of routing and TE tunnels

This contextual visualization, along with extensive drill-down details, helps operators quickly assess network conditions holistically and more quickly determine the true nature of traffic engineering-related problems.

**Comprehensive TE Tunnel Monitoring Views:**

Route analytics provides monitoring views of all tunnels, FRRs, as well as all TE-related routers and links. Traffic engineering monitoring reports include real-time status, configuration details and change history, as seen in Figure 2.

Figure 2: Traffic Engineering reports provide comprehensive information on all traffic engineering topology elements, including tunnels, FRRs, routers and links

Since route analytics understands the precise path of all tunnels, any chosen tunnel’s path can be viewed graphically to speed problem analysis, as seen in Figures 3 and 4:

Figure 3 & 4: Engineers can see isolated or contextual visualization of individual tunnel paths
Traffic Engineering Tunnel Analysis Provide Insight into Potential Problems

Beyond monitoring views, route analytics allows provides engineers with useful comparative analyses and insights into anomalous TE tunnel conditions that may be the cause of current problems, or may precipitate service issues in the future if they are not dealt with in a timely fashion. This intelligence allows engineers to proactively intervene before services are impacted, saving time and assuring customer quality of experience. Some examples of TE tunnel analyses are:

- TE tunnels that diverge from IGP paths:

![Figure 5: A list of all tunnels that don’t follow the IGP path](image)

- Tunnels with Inactive Primaries:

![Figure 6: Listing of tunnels with inactive primaries](image)
Network-Wide Traffic Engineering Management

- Tunnels with no or only partial FRR protection:

![Figure 7: List of tunnels with no or partial FRR protection](image)

- Primary and Secondary Tunnels with links in the same Shared Risk Link Group (SRLG):

![Figure 8: Analysis of tunnels where one or more hops share the same SRLG](image)

**Il rcexp rcb LcrDQow Traffic Analysis**

Understanding routing and TE tunnel dynamics is valuable to operators and engineers, but route analytics goes beyond this by intelligently and efficiently integrating NetFlow traffic information across the entire topology. Engineers can see comprehensive traffic reports by:

- Links
- CoS
- MPLS VPNs
- TE tunnels
Network-Wide Traffic Engineering Management

Each traffic report provides for extensive drill-downs so that engineers can isolate the precise flows of traffic that is relevant to the issue at hand. For example, engineers can initiate a drill-down view to find out the status of traffic for a specific traffic CoS, going across specific TE tunnels, for a particular MPLS VPN customer

- Starting with a report showing all traffic (inclusive of IPv4 and MPLS VPN traffic) on all links
- Drill down to all MPLS VPN traffic on all links
- Drill down further to view one MPLS VPN customers’ traffic on all links
- Drill down to view the customer’s traffic on all TE tunnels
- Drill down to isolate the customer’s traffic on specific TE tunnel

The topology-aware nature of route analytics’ insight into traffic allows engineers to quickly pinpoint the part of the network, including TE tunnels, that is carrying the traffic for a service that is experiencing a problem, eliminating time-consuming guesswork and speeding problem resolution.

Rewindable History Speeds Troubleshooting

While real-time monitoring and analysis views are invaluable for detecting and troubleshooting currently occurring problems, many problems aren’t reported or worked on until they’ve already ceased. Unlike with traditional network management approaches, where “history” is limited to summary statistics, route analytics records every single change in routing and TE tunnels in a complete forensic history that can be rewound to a past point in time, as seen in Figure 9. When rewound, the recorded network topology can be analyzed as if the engineer had “travelled back in time”, with all topology views as well as routing, traffic, and TE tunnel reports and analyses synchronized to that moment in the past when the problem was occurring. This rewindable history helps engineers understand tunnel changes and stability problems that have occurred in the past and improves overall problem resolution rates, leading to higher engineering productivity, network quality and customer satisfaction.

Figure 9: Route analytics provides a rewindable troubleshooting history that allows engineers to perform problem analysis on the network’s state at the time of the problem
Engineers can analyze the details of historical routing events, TE tunnel changes (Figure 10) as well as traffic levels, to pinpoint root causes.

Figure 10: Route analytics provides engineers with full tunnel change event details to speed root cause analysis

Accurate Modeling & Capacity Planning Reduces Maintenance Errors, Optimizes CAPEX

In addition to its real-time monitoring, rewindable history and extensive analysis capabilities, route analytics also provides integrated modeling and capacity planning. Network changes such as adding, editing, moving and deleting network elements can be modeled based not on an artificial approximation or periodic snapshot of the network, but on the always up to date, operationally accurate routing, TE tunnel and traffic topology. The result of a modeled change is calculated on a network-wide basis using the same routing calculations (SPF and CSPF) as would be performed by the actual routers, making the simulated results highly reliable as a basis for analyzing planned changes. Some common uses of route analytics’ modeling include:

- Ensuring that adding a new customer or MPLS VPN to the network will not cause per-link or per-CoS congestion and impact delivery of existing services
- Validating that proposed network changes such as link capacity upgrades (and their related metric changes) will result in the desired network-wide traffic distribution
- Assuring engineers that new TE tunnel constraints will achieve the desired path results
- Preventing errors when performing routine maintenance
Route analytics’ complete history of all routing, TE tunnel and traffic changes over time can also be used as the baseline for easy to use traffic trending projections to future timeframes or utilization levels, allowing network planners an automated way to generate capacity planning reports to analyze and justify capital expenditures on network upgrades. When route analytics’ modeling and trending capabilities are used together, network planners can explore ways to optimize the utilization of existing assets before upgrading the infrastructure, leading to significant CAPEX savings.

Conclusion: Growing Network Complexity Demands More Intelligent Network Management

The disruptive convergence of all communications over IP/MPLS networks is not only continues to affect the overall economics of service delivery today, but is also severely impacting those whose job it is to ensure that traffic delivery happens with the highest level of reliability and predictability. In short, networks are growing bigger and more complex. Traffic engineering is yet another layer of network logic that must be understood in real-time, with full historical insight, and with the ability to predictively model and plan for service growth and evolution. Traditional approaches to network management are not sufficient on their own to deliver the intelligence and automation that network operations, engineering and planning departments need to deliver best in class services. Route analytics’ unique visibility and functionality is a needed component of the network management portfolio for complex, traffic-engineered IP/MPLS networks.

For more information on route analytics and Packet Design solutions, please visit our website at http://www.packetdesign.com.