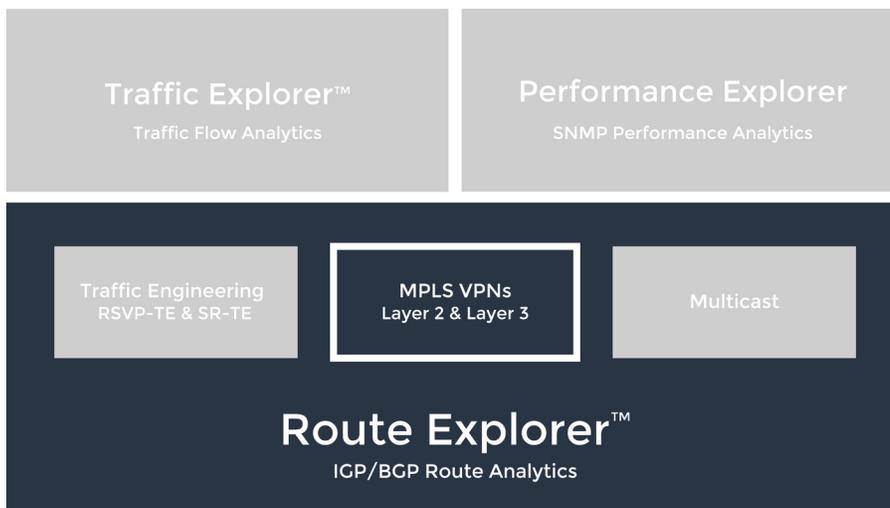


ROUTE EXPLORER™ FOR VPNS

The Route Explorer™ for VPNs module helps to overcome critical operational blind spots in MPLS VPN networks by providing Layer 2 Virtual Leased Line (VLL) and Layer 3 VPN routing analysis, network-wide.

Route Explorer delivers real-time knowledge about individual VPN routed topologies, VPN site-to-site reachability, and inter-VPN privacy. By passively monitoring, recording and analyzing the information contained in the MP-BGP and IGP routing protocols, Route Explorer computes and maintains in real time an accurate topology of each Layer 3 VPN. Using its always-current network model and key metric baselines, Route Explorer issues alerts whenever there are unexpected changes in the routed topology, whether they are in the core, access, wireless backhaul, or customer network. The same capabilities are available for Layer 2 VPNs, except the VLLs are collected from the routers using SNMP, NETCONF and CLI commands.

Powerful visualization, reporting, and diagnostic tools provide the current state of each VPN, as well as a complete audit trail of VPN routing events. Route Explorer's patented route processing algorithms and analytics features offer highly scalable and responsive operations, administration, and management capabilities for MPLS VPN services without the overhead or delays associated with traditional polling-based techniques. Route Explorer helps to reduce Mean Time to Repair (MTTR) and operational costs, while providing greater service assurance and customer satisfaction.



The VPNs module is an optional extension to the Route Explorer base product.

Route Explorer for VPNs Benefits

- Support both Layer 2 and Layer 3 VPN services without compromising service level management and reporting capabilities.
- Maintain visibility into VPN service levels and receive real-time alerts to threats for rapid response.
- Speed troubleshooting of Layer 2 VLL and Layer 3 VPN issues to improve customer satisfaction.
- Eliminate finger-pointing with powerful service forensics that isolate the source of routing and reachability issues to the provider or customer network.
- Avoid service interruptions following network maintenance by modeling planned changes to ensure proper operation.
- Know definitively which services will be impacted by maintenance windows so that affected customers can be notified beforehand.
- Maintain visibility into VLLs and pseudo-wires to ensure routing metrics are configured for optimum performance and redundancy.

Increase VPN Service Quality, Reduce MTTR

Service providers need every competitive advantage they can find to raise service quality and increase customer loyalty. They also need to continuously reduce operations costs through increased accuracy and efficiency of network management processes. Route Explorer offers unique visibility into MPLS VPNs that can dramatically reduce Mean Time to Repair (MTTR) while helping to deliver higher network and service quality. Route Explorer offers service providers not just Layer 3 VPN routing analytics, but also the properties and paths of transported Layer 2 VPN traffic (e.g. ATM, E-Line, Frame Relay, SONET/SDH, and TDM). Route Explorer provides visibility into virtual leased lines (VLL) to show how specific customer traffic is being routed, alerts on abnormal conditions, real-time operational views, an easy source and destination Attachment Circuit look up, and historical forensic analyses. Route Explorer helps operations and engineering teams to:

- Ensure dynamic VPN routing paths are always optimized to maintain service levels
- 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 VPNs
- Collect and analyze critical forensic data for fast troubleshooting and data continuity during problem escalation
- Easily model new VPN services and the impact of infrastructure changes, including end-to-end availability, delay and traffic loads of the VPN services

Operational Monitoring

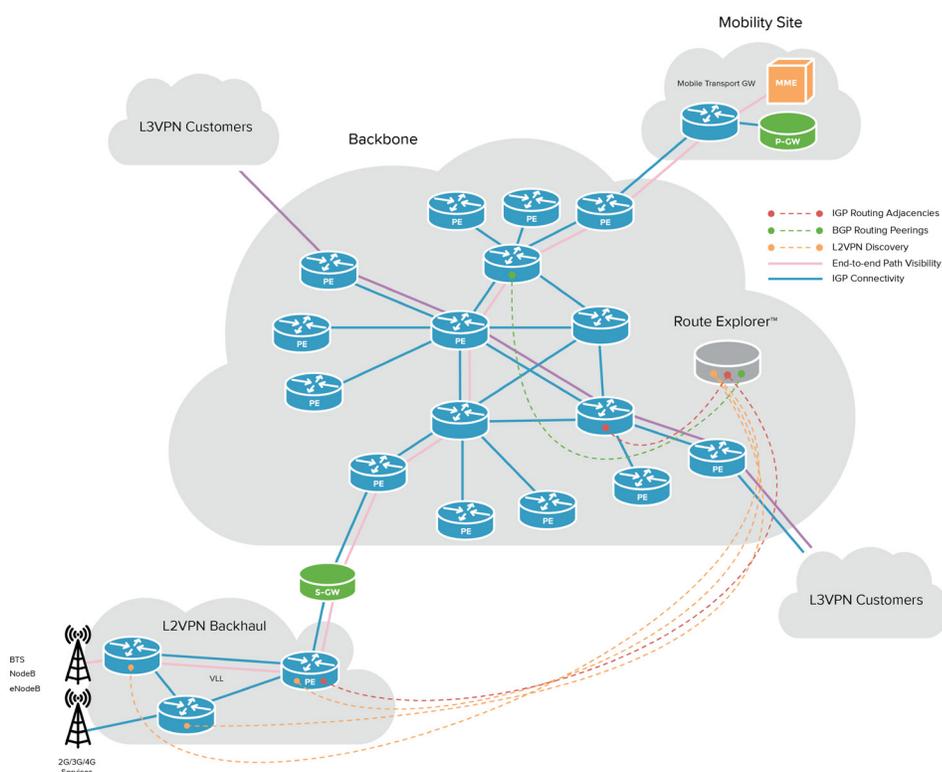
Route Explorer’s network topology views and summary dashboards provide at-a-glance visibility into the availability and performance of all VLLs and VPN services. This helps operators recognize possible performance issues and engage in proactive troubleshooting before customers complain. Operations teams can quickly check the current status of all the VPNs in the network, the status of VPNs per device, and corresponding VPN interface utilization. A single dashboard shows all the up, down, and new VPNs based on deviations from baseline. The user can drill down to a mini-map to see the path(s) for a specific VLL or VPN and for analytics pertaining to that customer or service, including the prefixes advertised and a complete list of all routing associated events. Being able to visualize just the links and routers that support a particular VPN is helpful when troubleshooting issues or planning network maintenance.

VPN Baseline and Health Monitoring

Route Explorer passively monitors and records the routing protocols in the service provider’s network to compute real-time and historical routed topologies for each VPN. Baselines are automatically generated across multiple data attributes, including:

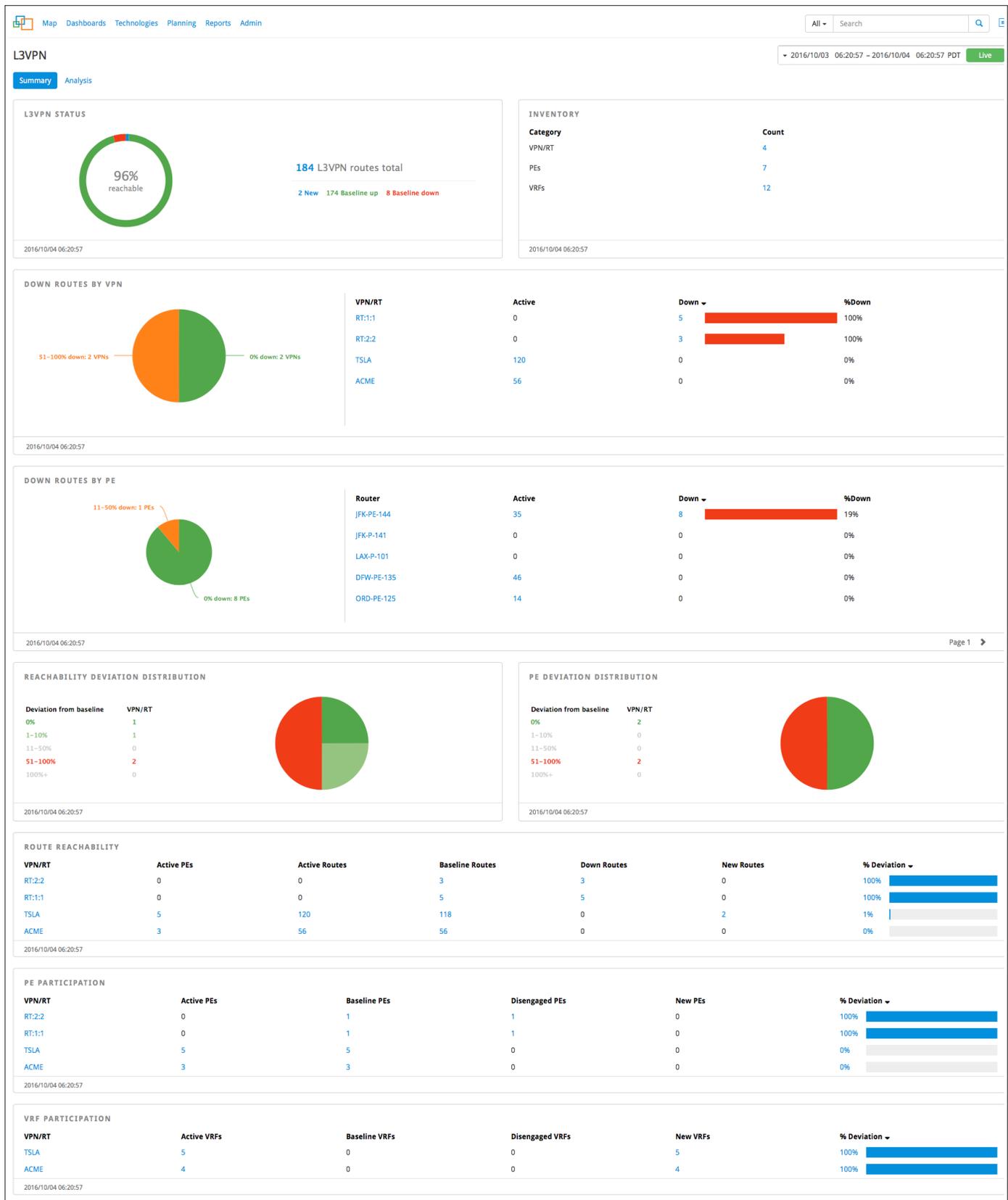
- PE routers participating in each VPN
- Network prefixes advertised by each VPN site
- Availability of each Layer 2 VPN’s VLLs

Using these baselines, Route Explorer provides network-wide and per-customer monitoring, reporting, and alerting on the most significant changes in VPN services. Instead of having to manually “hunt and peck” for this information by logging into



Route Explorer for VPNs provides visibility into both Layer 2 and Layer 3 VPN service delivery.

multiple routers, engineers can easily visualize the status of each customer's VPN network. From a network-wide topology view, a single mouse-click gives the user a mini-map view showing the health of an individual customer VPN, its site-to-site reachability and PE participation, as well as status indicators showing deviation from customer-specific baselines. Potential VPN problems are highlighted by an unusually high percentage rate of change in their status.



Service dashboards give operations teams and managers at-a-glance visibility into the health of customer services.

VPN Alerts

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

Alerts

- Reachability Deviation by VPN
- Reachability Deviation by Specific Prefix(es)
- Reachability Deviation by Specific PE(s)
- PE Participation Deviation by VPN
- PE Participation Deviation by Specific PE(s)
- VLL State and Redundancy
- Service Availability Degradation

Detailed Analysis and Diagnosis of VPN Problems

When VPN service issues occur, Route Explorer not only detects them in real time, but helps operators diagnose complex Layer 2 and 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 help to identify the exact moment when these changes occurred. Operators can view a complete and accurate audit trail per VPN, including for specific source and destination prefixes, drill down to see relevant events, and use Route Explorer's powerful sorting and filtering functions to isolate the root cause. An easy source-destination lookup facility makes it easy for operations teams to diagnose Layer 2 and Layer 3 VPN reachability issues by entering known end-points and being able to view the VPN paths in both directions, including any TE tunnels.

Troubleshooting Transient Problems with a "Network DVR"

Route Explorer's unique rewind-and-replay capability makes it possible to go back in time to isolate and analyze the root cause of transient and intermittent problems. For example, if a problem does not persist long enough to be diagnosed when it happens, engineers can simply select the VPN in question from the summary overview and drill-in to view its mini-map. From there, they can enter the time period when the service delivery issue occurred to view the state of the network, and specifically the nodes and links comprising the VPN, during that time. Using the play, forward, and rewind buttons, they can view an animation of the network's behavior and observe the change(s) that caused the problem. Being able to solve intermittent issues this way instead of having to close trouble tickets without resolution can greatly improve operational efficiency and customer satisfaction.

Flexibility for Mobile Operators

Route Explorer provides mobile operators end-to-end management visibility regardless of the infrastructure components and topologies in their core and backhaul networks. As operators upgrade their infrastructure to support LTE services, either by extending MPLS Layer 3 VPNs from the core into the backhaul network or by deploying MPLS Layer 2 VPNs in the backhaul network (pseudo-wire emulation also provides backward compatibility with 2G and 3G services), they cannot afford to sacrifice manageability. Route Explorer gives them the same visibility into routing behavior that they had before the upgrade, helping them to meet stringent LTE performance requirements consistently. As demand for mobile services grows, Route Explorer's interactive, what-if modeling capabilities make it much easier to assess how changes, such as the addition of new base stations, will impact the backhaul network.

Change Modeling and Simulation on the As-Running Network

A large percentage of service-affecting problems are caused by misconfigurations. Route Explorer allows engineers to model network changes, failure scenarios, and new workloads interactively to see their effects. This goes a long way to preventing congestion, delays, and outages from simple misconfigurations, inadequate redundancy, and even 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.

L2VPN: BLDL
2016/09/16 04:05:54 - 2016/09/16 04:35:54 PDF Live

VLLs

VLLs Filter: vpn BLDL exact, any

Show neighbors
Map layout

2016/09/16 04:35:54 PDF
Play/skip by 1 minute

PE1	PE2	VC ID	Description	VPN	PE1 Interface	PE2 Interface	Payload	Status	Created Time
SEA-PE-113	DFW-PE-134	Multi Segment Wire	VLL-BLDR-401	BLDR	Gi0/4.401	Fa2/0.401	Ethernet VLAN	Down	2016-08-02 16:31:47
DFW-PE-134	ORD-PE-124	401 (Unprotected)	VLL-BLDR-100	BLDR	Gi0/3		Ethernet VLAN	Up	2016-08-02 16:31:47
DFW-PE-134	SEA-PE-113	100 (Unprotected)	VLL-BLDR-101	BLDR	Gi0/4.1		Ethernet VLAN	Up	2016-08-02 16:31:47
DFW-PE-134	SEA-PE-113	101 (Unprotected)	VLL-BLDR-102	BLDR	Gi0/4.2		Ethernet VLAN	Up	2016-08-02 16:31:47
DFW-PE-134	JFK-PE-143	102 (Unprotected)	VLL-BLDR-501	BLDR	Gi0/4.501	Gi0/3.2	Ethernet VLAN	Down	2016-08-02 16:31:47
DFW-PE-134	LAX-PE-104	501 (Unprotected)	VLL-BLDR-103	BLDR	Gi0/3.1	E16/0.501	Ethernet VLAN	Up	2016-08-02 16:31:47
JFK-PE-143	SEA-PE-113	103 (Unprotected)	VLL-BLDR-301	BLDR	E16/0.301	Fa2/0.301	Ethernet VLAN	Down	2016-08-03 13:19:50
LAX-PE-104	ORD-PE-124	301 (Unprotected)							

2016-09-16 04:05:54 - 2016-09-16 04:35:54 | 18 VLLs, 1 Multi-segment
First Previous 1 2 Next Last

VLL STATUS

53% up

- 10 VLLs up
- 8 VLLs down
- 0 VLLs standby
- 1 VLLs down with attachment circuit down

2016/09/16 04:35:54

INVENTORY

Type	Value
VLLs	19 (1 MultiSegment, 0 Protected, 0 Local)
PEs	6
Attachment Circuits	25

2016/09/16 04:35:54

DAILY AVAILABILITY FOR 30 DAYS FOR SERVICE BLDL

2016/08/17 04:35:54 - 2016/09/16 04:35:54

DEVICE AVAILABILITY

Device	Availability
ORD-P-122	100%
JFK-PE-143	100%
SEA-PE-115	100%
ORD-PE-125	100%
LAX-P-102	100%

2016/09/16 04:05:54 - 2016/09/16 04:35:54 Page 1

LINK AVAILABILITY

Link	Availability
SEA-P-112 → ORD-P-122	67%
10.68.18.0/24 → DFW-PE-133	100%
DFW-PE-134 → 10.68.18.0/24	100%
DFW-PE-133 → 10.68.18.0/24	100%
JFK-PE-143 → 10.68.23.0/24	100%

2016/09/16 04:05:54 - 2016/09/16 04:35:54 Page 1

AC INTERFACE UTILIZATION IN

Interface	PE	VPN	Utilization
E16/0.301	LAX-PE-104	BLDR	0%
Gi4	SEA-PE-113	BLDR	0%
Gi0/3	DFW-PE-134	BLDR	0%
Gi0/4.2	DFW-PE-134	BLDR	0%
Gi0/3.2	JFK-PE-143	BLDR	0%

2016/09/16 04:05:54 - 2016/09/16 04:35:54 Page 1

AC INTERFACE UTILIZATION OUT

Interface	PE	VPN	Utilization
Gi0/3	DFW-PE-134	BLDR	0%
Gi4	SEA-PE-113	BLDR	0%
Gi0/4.2	DFW-PE-134	BLDR	0%
Gi0/3.2	JFK-PE-143	BLDR	0%
Fa2/0.902	ORD-PE-124	BLDR	0%

2016/09/16 04:05:54 - 2016/09/16 04:35:54 Page 1

VPN-specific pages provide a mini-map of the VPN topology with contextual analytics, and the ability to rewind and replay routing behavior for troubleshooting transient issues.

VPN Reports

Customized 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, these reports reveal network problems and anomalies that can help operators avert service interruptions. 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. Customer-specific reports make SLA compliance management and reporting easy.

Reports

- Reachability by VPN
- PE Participation by VPN
- VRF Participation by VPN
- Prefixes by PE and VRF
- Prefix Reachability by VPN over Time
- PE Participation over Time
- VRF Participation over Time
- Event History by VPN
- VLLs by Router
- VLLs by VPN

