vmware®

VMware Smart Assurance Solutions Brief: MPLS Monitoring and Management

Providing service assurance on next-generation networks through business-focused management of MPLS VPNs

As service providers and enterprises continue to combine next-generation, packet-based services on a converged network, Multi-Protocol Label Switching (MPLS) is an integral part of the core network infrastructure. Business VPNs, IPTV, internal services for financial institutions and government entities, and media content are all examples of services that rely on MPLS infrastructures.

Managing this kind of advanced networking environment comes with challenges, including:

- The need to see and relate the MPLS infrastructure to the rest of the physical and virtual network environment
- Diagnosing the true cause of problems in such a dynamic control plane: Is the problem due to protocol errors, issues in the transport network, traffic engineering, or a combination thereof?

Managing the availability of critical MPLS-services requires a detailed end-to-end understanding of the infrastructure and its relationship to the services being delivered. Without it, service assurance can't be provided, and customer satisfaction and service-level agreements are at risk.

VMware Smart Assurance provides an industry leading MPLS management solution, offering mission-critical fault management of virtual private networks (VPNs) and the underlying Label Switched Paths (LSPs).

MPLS management maximizes the availability of IP VPNs based on MPLS and VPLS technology. Leveraging its advanced multi-dimensional deterministic model-based engine, Codebook, VMware Smart Assurance provides automated discovery and monitoring, root-cause and impact analysis, and network visualization. VMware Smart Assurance also supports MPLS traffic engineering discovery and analysis and multi-vendor network environments.

At-a-Glance

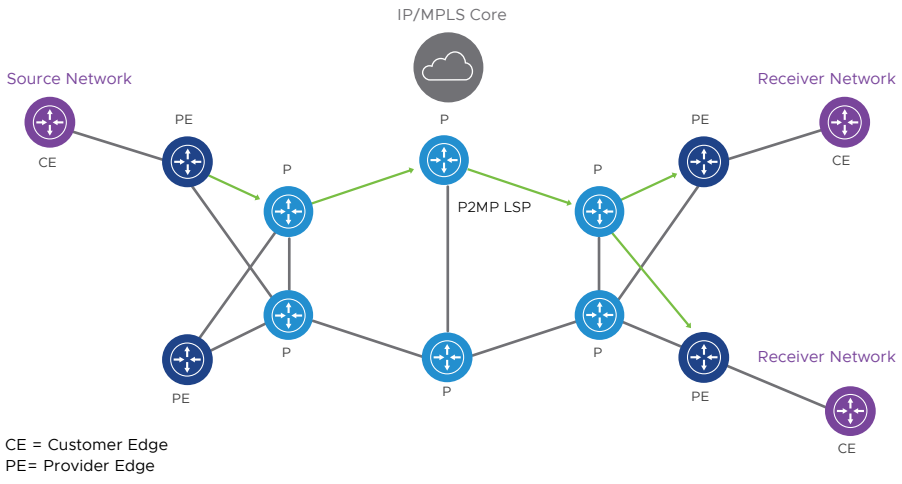
- Discovers, monitors, and analyzes Layer 2 and Layer 3 VPNs automatically—including multi-VRF CEs
- Correlates MPLS failures to services and business processes
- Supports networks with equipment from multiple vendors—such as Cisco Systems, Huawei, and Juniper Networks
- Offers LSP management capabilities—including enabling or disabling end-to-end path discovery, and discovering LSPs not associated with a VPN

Auto Discovery

Auto-discovery leverages topology information from SNMP management information bases (MIBs) and other sources to automatically discover logical and physical objects and relationships in MPLS, VPLS, and related domains. This includes LSPs, Layer 2 and Layer 3 VPNs, VPN routing/forwarding elements, LSP segments (hops), and traffic-engineering relationships. Discovery results also can be used to verify and reconcile VPN provisioning.

Root Cause and Impact Analysis

Root-cause and impact analysis automatically pinpoints the root cause of the problems that can affect services delivered by MPLS VPNs and calculates how underlying network problems impact MPLS VPNs and the customers using these services. VMware Smart Assurance can also determine root causes in the MPLS domain that are not caused by physical failures, such as a LSP signaling failure.



VMware Smart Assurance provides automated root-cause and impact analysis across the entire network, including support for next-generation multicast VPNs.

VMware Smart Assurance Supports:

- Routing protocols BGP, OSPF, IS-IS, and EIGRP
- MPLS L3VPN (including Multi-VRF CE)
- MPLS Point-to-Point L2VPN (VPWS)
- MPLS Multipoint L2VPN (VPLS)
- Load-balanced LSP
- NG-MVPN (Next-Generation Multicast VPN)
- Hub-and-Spoke VPLS
- Multi-tunnel MPLS
- Overlapping IP addresses
- Inter-AS LSP
- LSP ping and VRF ping tools
- Reconciliation of discovered and provisioned databases using an optional Cisco ISC adapter that associates VPNs with customers
- LDP and RSVP Protocol Diagnostics

Traffic Engineering

MPLS traffic engineering functionality analyzes MPLS network contingency paths that are used to re-route traffic in the event of a failure or problem in the primary path. By supporting and enabling MPLS traffic engineering, VMware Smart Assurance helps service providers ensure SLAs are met by analyzing protection mechanisms, as well as indicating single points of failure and true outages.

Network Visualization

This solution presents MPLS network topology in a variety of dynamically updated views that show the status of MPLS elements and their relationships within and across technology and service layers.

MPLS Management Benefits

- Easy understanding of network configurations using advanced visualization
- Automated root-cause and impact analysis reduces time and cost to repair
- Prioritization of events based on correlation of service impacts
- Improved customer satisfaction and SLA compliance by mapping infrastructure events to tenants and services
- Automatic repository updating following network reconfiguration reduces costs
- Carrier-grade scale for the most complex, multi-vendor environments

VMware Smart Assurance Supports Cont'd:

- Traffic Engineering (TE) Discovery
- Remote Ping/LSP Ping Functionality
- Cross-Domain Correlation of Layer 3 VPNs with BGP
- Discovery and monitoring of targeted LDP sessions
- Discovery of Layer 2 and Layer 3 VPN misconfigurations

Learn More

For additional information about VMware Smart Assurance:

1-877-VMWARE
(outside North America, dial +1-650-427-5000)

telco.vmware.com

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA | Tel 877-486-9273 | Fax 650-427-5001 | www.vmware.com