

# COMPREHENSIVE MPLS VPN SOLUTIONS

## Meeting the Needs of Emerging Services with Innovative Technology

### Challenge

Meeting the dynamic requirements of rapidly growing, worldwide VPN markets

### Solution

- Established service solutions: Next-generation multicast VPNs, VPLS, IPv6 VPNs
- Innovative technology solutions: P2MP LSP, LDP-BGP VPLS interworking

### Benefits

- Better operational efficiency
- Improved scalability
- Enhanced flexibility
- Extended service reach
- Minimized service disruption

The VPN market is growing at a record pace worldwide. IDC reports that provider-provisioned VPNs now dominate the VPN services market with VPNs deployed by over half of the multisite companies that have 50 or more employees. The worldwide VPN services market reached \$24.4 billion in 2007 and is expected to climb to almost \$36 billion in 2012. In the U.S. alone, it is estimated that the VPN market will have a 10.4 percent CAGR increase over the next five years.<sup>1</sup>

### The Challenge

The need to increase revenue while achieving operational efficiency is driving the need for increased multicast traffic, particularly for the growing deployment of voice, video, and collaboration-based applications. For instance, providers with an installed base of Layer 3 VPNs for unicast service are looking to upsell with new media-rich solutions. Numerous services, such as IPTV and financial applications, now demand scalable, reliable, and secure next-generation (NG) multicast VPN (MVPN) solutions. Service providers and cable operators are offering virtual private LAN service (VPLS) to small and medium businesses, as well as to large enterprises. Another growing revenue generator is IPv6 VPNs for new mobile applications. To address these divergent needs and in anticipation of changing environments, you would want to consider implementation flexibility, scalability of service instances, size of route tables deployed, and your ability to extend the service reach.

### Multi-Access, Multiprotocol, Multidomain MPLS VPN Solutions

Juniper Networks® supports a full breadth of technologies to deliver diverse services and meet these evolving needs (Figure 1). Juniper's comprehensive solution set enables service providers, large enterprises, telcos, cable companies, and information-intensive enterprises to cost-efficiently roll out networks that offer scalable control and forwarding planes, continuous service, and feature richness. VPN deployments using Juniper technology are standards-based and securely interwork amongst multiple providers, enabling you to exceed the most stringent service level agreements (SLAs) and resiliency requirements. Common protocols offer a consistent, streamlined operational model, thus reducing overall operating and troubleshooting costs.

<sup>1</sup> IDC, "A Toolkit Approach to Enabling VPN Services," October, 2008 Scalable control and forwarding planes.

VPNs provide numerous services within a variety of delivery models. This wide deployment of VPN services requires the availability of multiple access connectivity options, service reach across protocol and administrative domain boundaries, and support for multiple topologies and traffic profiles. Drivers include consolidations (mergers and acquisitions), interprovider partnerships, and changing end-user requirements based on available access connectivity and protocol options. To meet these dynamic needs, Juniper has created a comprehensive and flexible MPLS VPN toolkit that offers an array of options across multiple parameters.

- Flexible access connectivity options across multiple topologies, protocol and administrative boundaries (Table 1).
- Scalable control and forwarding planes.
- Maximized bandwidth and network efficiency for multicast with P2MP optimizations for VPLS and multicast VPN.
- Self-contained multihoming mechanisms for highly available edge service nodes.
- Consistent operational model for IPv4, IPv6, unicast, and multicast across L2 and L3 VPNs.
- Simplified operations with reduced template-based configuration, maintenance, and troubleshooting complexity.
- Cost-efficient rollouts with minimal network disruption.

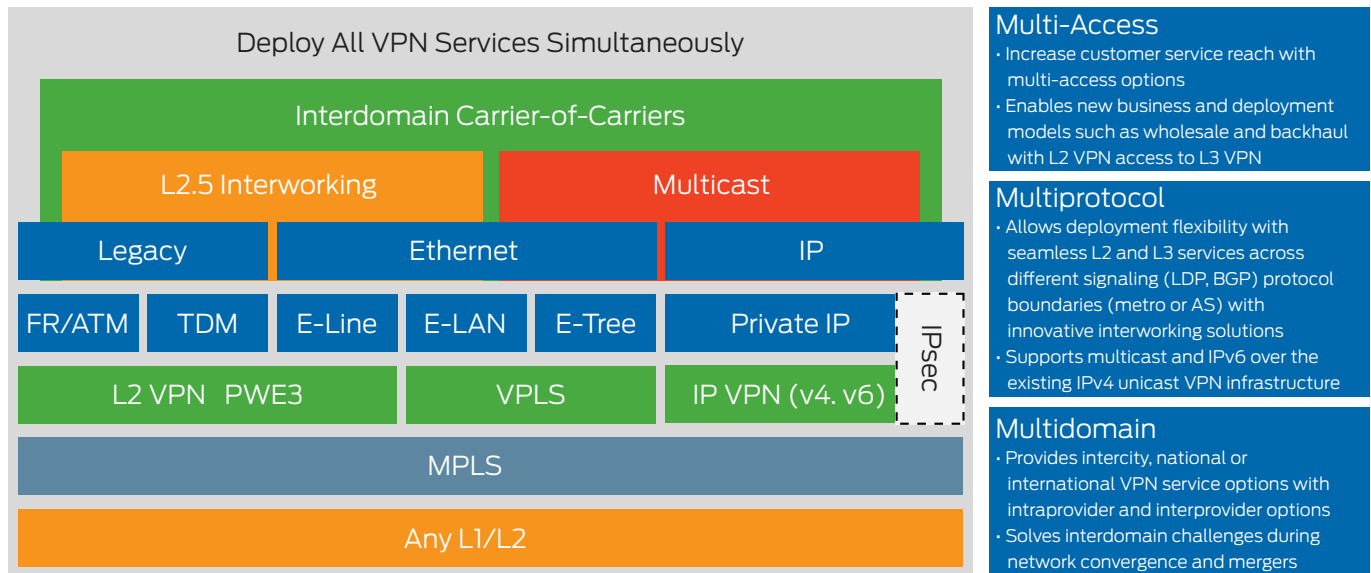


Figure 1: Multi-access, multiprotocol, multidomain MPLS VPN solutions

Table 1: Comprehensive and Flexible MPLS VPN Toolkit

PARAMETERS	OPTIONS	APPLICATIONS
<b>Signaling</b>		
VPN Reachability	<ul style="list-style-type: none"> <li>• T-LDP</li> <li>• MP-BGP</li> </ul>	<ul style="list-style-type: none"> <li>• Intrametro</li> <li>• Intermetro</li> <li>• Intra-AS</li> <li>• Inter-AS</li> </ul>
Transport	<ul style="list-style-type: none"> <li>• MPLS: LDP, RSVP-TE (P2P [point to point] or P2MP [point to multipoint]) LDP over RSVP, RSVP over RSVP</li> <li>• Non-MPLS: GRE, IPsec</li> </ul>	<ul style="list-style-type: none"> <li>• RSVP for traffic engineering</li> <li>• P2MP MPLS for multicast</li> <li>• GRE and IPsec for non-MPLS transit</li> </ul>
<b>Domain</b>		
Autonomous System (AS)	<ul style="list-style-type: none"> <li>• Intra-AS</li> <li>• Inter-AS</li> </ul>	<ul style="list-style-type: none"> <li>• Carrier-of-carrier services</li> <li>• Interprovider services</li> </ul>
Protocol Interworking	<ul style="list-style-type: none"> <li>• LDP to BGP</li> <li>• LDP to LDP</li> <li>• BGP to BGP</li> </ul>	<ul style="list-style-type: none"> <li>• Applies to both pseudowire and VPLS</li> <li>• Extends services beyond metro and AS domain</li> </ul>
<b>Access</b>		
End User	<ul style="list-style-type: none"> <li>• Ethernet</li> <li>• Bridged and routed ATM</li> <li>• Bridged and routed Frame Relay</li> <li>• Bridged and routed PPP</li> <li>• MLPPP</li> <li>• Pseudowire</li> </ul>	<ul style="list-style-type: none"> <li>• Multi-access (DSL, cable, Ethernet) for L2 and L3 VPN</li> <li>• Non-Ethernet access into VPLS</li> <li>• Single VLAN for simultaneous VPLS and IP VPN services</li> </ul>
Infrastructure	<ul style="list-style-type: none"> <li>• Pseudowire access into pseudowires, VPLS, or IP VPNs</li> <li>• VPLS access into IP VPNs</li> </ul>	<ul style="list-style-type: none"> <li>• Backhaul model</li> <li>• Wholesale model</li> <li>• Scaling within metro</li> </ul>

PARAMETERS	OPTIONS	APPLICATIONS
<b>Traffic</b>	<ul style="list-style-type: none"> <li>• L2 and L3</li> <li>• IPv4 and IPv6</li> <li>• Unicast and multicast</li> </ul>	<ul style="list-style-type: none"> <li>• All traffic types</li> </ul>
<b>Topology</b>	<ul style="list-style-type: none"> <li>• Full mesh</li> <li>• Hub and spoke</li> <li>• Extranet</li> <li>• Application-based</li> <li>• P2P, P2MP, and MP2MP (multipoint to multipoint)</li> </ul>	<ul style="list-style-type: none"> <li>• Branch-to-headquarters communication</li> <li>• Business-to-business communication</li> <li>• Application VPN</li> <li>• MVPN</li> </ul>
<b>Service Related</b>		
QoS	<ul style="list-style-type: none"> <li>• Per-hop QoS enforcement</li> <li>• End-to-end QoS: Mapping across L2, L3, and MPLS domains</li> <li>• DiffServ-aware traffic engineering (single or multiclass LSP)</li> <li>• Call admission control using bandwidth constraints and LSP policing</li> </ul>	<ul style="list-style-type: none"> <li>• Provide service guarantees for bandwidth, rerouting, and route failure</li> </ul>
High Availability	<ul style="list-style-type: none"> <li>• BGP-based multihoming</li> <li>• Pseudowire redundancy</li> <li>• Fast reroute</li> <li>• Nonstop active routing</li> <li>• ISSU</li> </ul>	<ul style="list-style-type: none"> <li>• Seamless BGP-based multihoming between customer and provider domains or provider-to-provider domains</li> <li>• Recovery from link, node, and pseudowire failure</li> </ul>
OAM	<ul style="list-style-type: none"> <li>• Multilayer integrated OAM</li> <li>• Ethernet OAM: 802.1ag, 802.1ah</li> <li>• MPLS OAM: LSP level ping, traceroute, BFD, statistics</li> </ul>	<ul style="list-style-type: none"> <li>• Repair</li> <li>• Fault management</li> <li>• Performance monitoring</li> </ul>
Accounting	<ul style="list-style-type: none"> <li>• Destination- and source-based accounting per VPN instance</li> </ul>	<ul style="list-style-type: none"> <li>• Accounting and billing models based on source and destination traffic</li> </ul>
Security	<ul style="list-style-type: none"> <li>• Per VPN filters and policing</li> <li>• Dynamically propagated packet filters via BGP</li> <li>• IPsec or SSL VPN into L3 VPN</li> <li>• PE-PE IPsec</li> </ul>	<ul style="list-style-type: none"> <li>• Contain DDoS attacks</li> <li>• Secure remote access</li> <li>• Encrypted VPN traffic in provider cloud</li> </ul>

## Meeting the Needs of Emerging VPN Services

Leading-edge providers and enterprises are leveraging the VPN infrastructure to deliver sophisticated services, such as video and voice conferencing, over highly secure, resilient networks. NG MVPNs and IPv6 VPN constitute a new wave of service rollouts. VPLS is also gaining momentum with the need to extend service reach beyond the metro domain.

### NG MVPNs

MVPN is a technology to deploy multicast service in an existing VPN or as part of a transport infrastructure. Multicast data is transmitted between private networks over a VPN infrastructure by encapsulating the original multicast packets.

NG MVPN is based on a BGP control plane with exceptional scaling properties that have been proven in L3 unicast VPNs on Juniper routing platforms for over seven years. Moreover, this BGP control plane lends itself naturally to supporting flexible topologies such as extranet, and hub and spoke. BGP-based NG MVPNs allow for an incremental approach to deploying multicast services so you can use the same technology as used for deploying Layer 3 VPN for unicast services. This approach reduces operational and deployment risks, in addition to qualification and operational costs,

resulting in a higher ROI. P2MP MPLS further extends the benefits of NG MPVN, allowing for a superior and efficient integration between the core and edge multicast domains.

The delivery of multicast traffic is particularly widespread in the deployment of video-based applications. As well, providers with an installed base of Layer 3 VPNs for unicast services are looking to upsell with new media-rich solutions.

### VPLS

VPLS is a Layer 2 multipoint VPN that emulates LAN service across a WAN. VPLS enables you to interconnect customer sites over a packet-switched network, effectively making all customer LAN segments behave as a single LAN.

Service providers are using VPLS to offer transparent LAN service to enterprise customers. With the emergence of metro Ethernet networks, VPLS is also being used as an infrastructure technology used for backhaul. Most major service providers already employ an IP/MPLS backbone and offer Layer 3 MPLS VPN services, and they are beginning to offer Layer 2 VPN services to both SMBs and large enterprises. VPLS appeals to enterprises, in particular, because it allows them to extend their reach beyond their LANs with the same Layer 2 Ethernet connectivity paradigm.

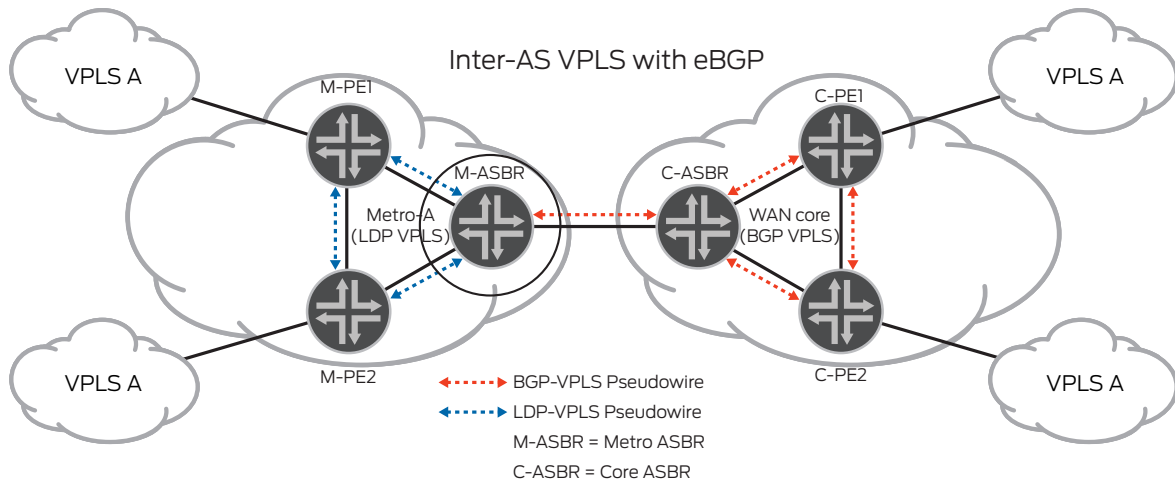


Figure 2: Interworking at Metro ASBR between LDP VPLS and BGP VPLS

Juniper leads the way in having been used in the first and largest VPLS service deployment in the U.S. Additionally, the first inter-AS between independent service providers was first deployed with Juniper Networks Junos® operating system, thus allowing the service providers to partner in providing intermetro VPLS services for global reach.

### IPv6 VPNs

The explosive growth of mobile devices, along with government mandates, is accelerating the adoption of IPv6. With the widespread deployment of MPLS in today's networks, there is an increasing need to transport IPv6 over MPLS and offer IPv6 VPN services similar to IPv4 VPNs. Given both IPv6 and IPv4 are based on a common BGP MPLS VPN framework, they are similar in configuration and operation, using the same VRF and the same LSP and BGP sessions. Other similarities include packet processing, filtering, and accounting.

Large providers are now using IPv6 to differentiate themselves. In fact, one study indicates that 30 percent of US federal, state, and local government executives will be influenced by the transition to IPv6 in their IT purchasing decisions, which equates to \$39 billion in government IT spending.<sup>2</sup> Providers choosing to get ahead of the curve have already selected Juniper. For instance, one provider currently uses Junos OS solutions for IPv4 unicast and multicast, as well as IPv6 unicast delivery with up to 15 IPv6 peer/participant connections.

### Delivering Innovative Technology and Tools

This diversity and breadth of services pose a challenge when creating an infrastructure that supports Layer 2 VPNs, Layer 3 VPNs, IPv4, IPv6, unicast, and multicast traffic. The difficulty is particularly true for virtual services that require complex control and data plane operations. Another challenge is to support emerging multicast applications incrementally on top of existing Layer 3 VPN and VPLS infrastructures without adding operational complexity. To address these needs, Juniper Networks offers a variety of technologies and tools, such as LDP-BGP VPLS interworking, P2MP LSPs, MPLS Plug-and-Play, and a Partner Solution Development Platform (PSDP).

### LDP-BGP VPLS Interworking

Using LDP-BGP VPLS interworking, you can now offer regional or national VPLS in an economically scalable manner by traversing across different VPLS signaling boundaries that may exist between a metro and WAN (Figure 2) with little or no service disruption. For one, LDP-BGP VPLS interworking removes the need to make any changes on the LDP-VPLS provider-edge (PE) routers, thus minimizing configuration costs and downtime.

In this way, you can cost-efficiently cap and grow an existing LDP-VPLS deployment, using the more scalable BGP control plane to expand the VPLS.

<sup>2</sup>INPUT Federal IT Forecast and INPUT State and Local IT Forecast, FY2006-FY2011

Similarly, you can scale networks using LDP-BGP interworking to localize and extend the reach of VPLS beyond a single LDP-VPLS metro domain. One model is the use of BGP VPLS in the WAN to interconnect multiple LDP-VPLS metro domains. Using LDP-BGP VPLS interworking, there is no need to significantly change or upgrade the network. Nor is there a need to place additional burden on the control plane of the LDP-VPLS PE router in the metro network. Per IDC<sup>3</sup>, over 10 major providers across telco and cable operators have already deployed BGP-based VPLS and are expected to provide the impetus for other providers to migrate in this direction.

### P2MP LSPs

Juniper leads the industry in P2MP LSP technology with P2MP LSP solutions deployed worldwide since 2004. We are also leading efforts in standardizing the specifications of P2MP LSPs and services leveraging P2MP LSPs. Providers recognizing Juniper's leading-edge technology have specifically chosen to deploy Junos OS MPLS P2MP solutions to reduce overhead and to remove restrictions on the backbone, thus enabling them to cost-effectively grow their services offerings. Ovum<sup>4</sup> cites that large and small network operators, including a large cable/MSO operator, already have 10 deployments of P2MP technology across Europe, two in Asia, and one in North America.

P2MP LSPs provide efficient traffic replication in the network. MPLS-based P2MP LSPs optimize NG MVPNs with resource reservation, deterministic traffic engineering routing, and fast failover mechanisms that are not found in multicast protocols such as PIM. Using a common MPLS operational framework for unicast and multicast traffic, P2MP LSPs reduce configuration and maintenance complexity.

Reliable and Deterministic Transport for NG MVPNs—With P2MP LSPs deployed in the backbone, you can roll out NG MVPNs on the provider edge routers to seamlessly use the reliable P2MP MPLS transport, allowing for simpler configuration, management, and troubleshooting of devices. NG MVPNs offer the flexibility of using different tunneling mechanisms for MVPNs. So while existing MVPNs can continue to use the older GRE tunneling mechanism, newer MVPNs can take advantage of P2MP LSPs as the tunneling option.

Efficient Multicast Replication over VPLS—P2MP LSPs provide an efficient mechanism for transporting VPLS broadcast and multicast traffic. By default, VPLS implementations use ingress replication, which does not offer bandwidth efficiency. The use of P2MP LSPs with BGP VPLS, on the other hand, eliminates the ingress replication problem by efficiently replicating broadcast and multicast packets at the MPLS layer. These P2MP LSPs can be dynamically set up with BGP autodiscovery. Furthermore, to offer multicast virtualization services for Layer 3 VPN and VPLS, you have an option to use a common control plane (BGP) and data plane (MPLS) framework that leads to a consistent service model and simplified operations. This reduced operational overhead results in cost-effective service delivery and a faster time to market.

### MPLS Plug-and-Play

MPLS Plug-and-Play streamlines network operations using scripts to prevent procedural errors and simplify common configurations. MPLS Plug-and-Play also allows autodiscovery and adaptation to network changes, and automatic response to network conditions. Some of the features include autodiscovery of VPN endpoints, autodiscovery of multicast sources and receivers, automated link and node protection, enforcement of security policies, and bandwidth for RSVP-TE. You can use the template mechanism to configure only specific attributes and have all other common components automatically generated, which is particularly useful for VPN configurations.

### PSDP

PSDP provides a powerful set of tools and resources for developing and deploying applications that uniquely meet business needs. This solution includes a software development kit with intelligent and secure interfaces to Junos OS routing and services functions. PSDP enables you to tightly integrate applications with the network, thus enhancing service delivery with specific access and performance policies such as optimized routing, customized bandwidth management, advanced security, and extended operations toolsets. Juniper Networks provides access to the PSDP technology, as well as technical and business support to partners, through its Open IP Solution Development Program. To integrate new services with existing VPNs and offer true service differentiation, you can use PSDP for third-party application development. PSDP's open and flexible toolkit enables competitive time-to-market offerings by allowing third-party integration in a matter of only a few weeks to a few months.

<sup>3</sup> IDC, "A Toolkit Approach to Enabling VPN Services," October, 2008

<sup>4</sup> Ovum, "The Benefits of P2MP Label Switched Paths for MPLS Networks," November, 2008

## The Juniper Advantage

Juniper Networks has already been chosen by numerous providers based on its rich MPLS VPN toolkit that enables them to deliver diverse connectivity services more efficiently and cost effectively. Juniper's industry-leading approach to meeting changing and growing VPN service demands is standards-based and offers numerous access connectivity options, seamlessly supporting multiple protocols across different domains. Juniper's enabling technologies, such as LDP-BGP VPLS interworking, P2MP LSPs, NG MVPN, MPLS Plug-and-Play and PSDP, support rapid deployment of emerging services with complete continuity across multiple dimensions, from interdomain deployment to extensive reach beyond typical administrative domains.

## About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at [www.juniper.net](http://www.juniper.net).

---

### Corporate and Sales Headquarters

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
Phone: 888.JUNIPER (888.586.4737)  
or 408.745.2000  
Fax: 408.745.2100  
[www.juniper.net](http://www.juniper.net)

### APAC Headquarters

Juniper Networks (Hong Kong)  
26/F, Cityplaza One  
1111 King's Road  
Taikoo Shing, Hong Kong  
Phone: 852.2332.3636  
Fax: 852.2574.7803

### EMEA Headquarters

Juniper Networks Ireland  
Airside Business Park  
Swords, County Dublin, Ireland  
Phone: 35.31.8903.600  
EMEA Sales: 00800.4586.4737  
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.