

TECHNOLOGY INSIGHT

A Toolkit Approach to Enabling Emerging VPN Services

Sponsored by: Juniper Networks

Eve Griliches

October 2008

IDC OPINION

Provider-provisioned virtual private networks (PPVPNs) now dominate the VPN services market, which historically started with deployment of CPE-based solutions. VPNs are currently used by over half of the multisite companies that have 50 or more employees. VPNs have exceeded frame relay and ATM as well as leased lines as a form of private network deployed on a shared infrastructure with multiple sites. With the maturing of these underlying technologies, the applicability of VPN services has widened beyond multinational companies to now include content-intensive providers, cable companies, and small and medium-sized businesses (SMBs).

Video and voice conferencing, broadcast-based transactions, and other sophisticated services for businesses are leveraging the VPN infrastructure to deliver new services over secure and highly resilient networks. IP VPNs provide the initial foundation for key new services to be offered, such as multicast VPNs (MVPNs) and advanced IPv6-based services, which constitute a new wave of service rollouts in leading-edge provider networks. VPLS services driven by the emergence of Ethernet are gaining momentum and requiring scalable solutions with the need to extend the service reach beyond the metropolitan (metro) network domain.

Network consolidation, inter-region (inter-autonomous systems [AS]) services, and wholesale business models are driving different traffic types such as unicast and multicast, IPv4/v6, and Layer 2 and Layer 3, all with the need for higher resilience over a converged infrastructure. The dimensions that evolve out of these traffic types require scalability for service instances, size of route tables deployed, and extended service reach, with the ability to morph these service offerings over time to the changing business environment (i.e., mergers and acquisitions as well as the combining of disparate and varied networks [and protocols!], all within the changing regulation and legislative landscape). For example, SMB deployments have lower bandwidth requirements but a proliferation of VPN sites, large automotive companies require secure extranets with B2B suppliers, and CAD/CAM design tools require secure and media-rich collaboration tools.

IDC believes that to meet the comprehensive list of requirements that these rollouts demand, vendors need to provide scalable and highly reliable platforms with a toolkit that supports scalable control and forwarding planes as well as feature richness. Items in the toolkit need to be standards based and must interwork with multiple providers to meet end-to-end SLA and resiliency requirements. A toolkit needs to have a set of common protocols as well as smart provisioning templates to simplify operations.

IN THIS TECHNOLOGY INSIGHT

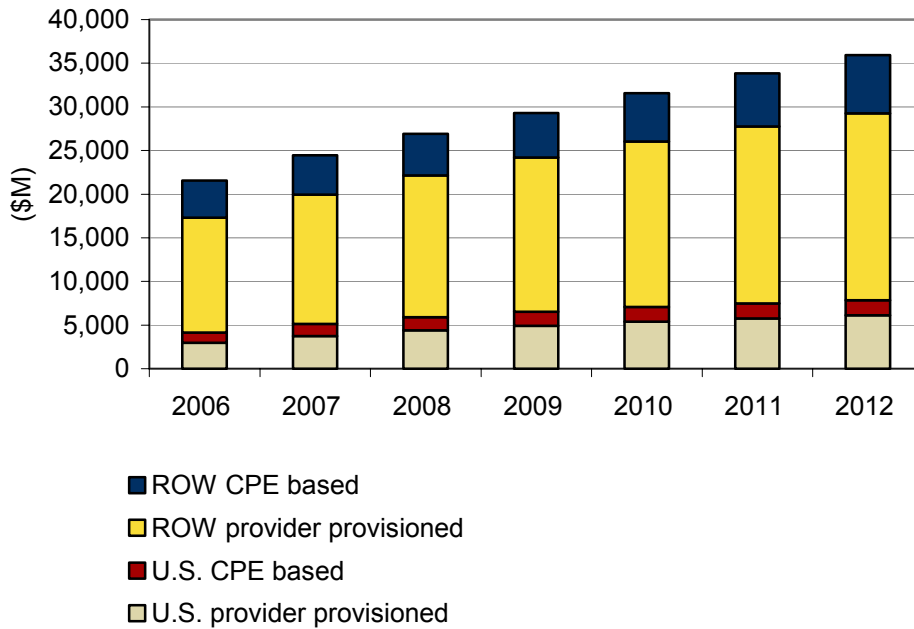
We discuss provider-provisioned VPNs as they relate to different applications and market segments as well as the toolkit and technical requirements to enable services across multiprovider networks.

SITUATION OVERVIEW

According to IDC, the worldwide VPN services market reached \$24.4 billion in 2007 and is expected to climb to almost \$36 billion in 2012. In the United States, the VPN market was \$5.1 billion in 2007 and is expected to increase at a five-year CAGR of 10.4% to reach \$7.8 billion in 2012 (see Figure 1). The VPN market in the rest of world (ROW), which consists of EMEA, APAC, and CALA, is also increasing at a very respectable five-year CAGR.

FIGURE 1

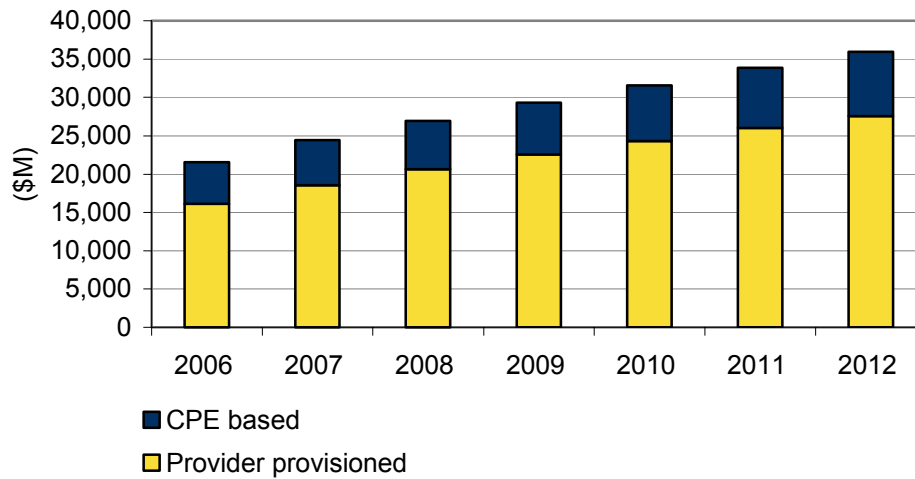
Worldwide VPN Services Market by Revenue Segment and Geography



Source: IDC, 2008

This document focuses on provider-provisioned VPNs as opposed to CPE or client-based VPNs.

Figure 2 shows the entire VPN services market for both CPE and provider-provisioned VPNs.

FIGURE 2**Worldwide VPN Services Market by Revenue Segment**

Source: IDC, 2008

It is also interesting to note that the largest worldwide growth will be in the company size range of 500–999 employees for provider-provisioned VPNs, and yet half of the market is in the under 500 employee size (see Table 1). Clearly, the highest potential growth in the United States is in the SMB market, the 1–99 employee size as noted in Table 1.

TABLE 1**Worldwide Provider-Provisioned VPN Forecast by Company Size (\$M)**

Company Size	2006	2007	2008	2009	2010	2011	2012	2007–2012	
								CAGR (%)	
1 to 99	1,648	1,901	2,117	2,307	2,460	2,579	2,731	7.5	
100 to 499	2,652	3,060	3,397	3,727	4,023	4,325	4,649	8.7	
500 to 999	1,904	2,267	2,600	2,941	3,278	3,635	3,998	12.0	
1,000 to 4,999	9,363	10,637	11,693	12,664	13,537	14,388	14,977	7.1	
U.S. Only									
1 to 99	39	50	59	67	74	79	85	11.2	
100 to 499	550	712	848	953	1,042	1,115	1,182	10.7	
500 to 999	280	357	424	476	522	561	599	10.9	
1,000 to 4,999	2,094	2,623	3,077	3,427	3,744	4,017	4,272	10.2	
U.S. total	2,963	3,743	4,408	4,922	5,382	5,774	6,138	10.4	
ROW Only									
1 to 99	1,609	1,851	2,058	2,240	2,386	2,499	2,646	7.4	
100 to 499	2,652	3,060	3,397	3,727	4,023	4,325	4,649	8.7	
500 to 999	1,624	1,909	2,176	2,465	2,756	3,073	3,400	12.2	
1,000 to 4,999	7,269	8,014	8,615	9,236	9,792	10,371	10,705	6.0	
ROW total	13,154	14,834	16,246	17,668	18,958	20,268	21,399	7.6	

Source: IDC, 2008

The Business-Class VPN

The emergence of VPNs as a "managed service" is grounded in the fact that the enterprise can now offload the complexity of the routing and network configuration of a large-scale VPN to a service provider. The leading use of business-class VPNs is the company intranet so that internal organizations can connect to and access the appropriate servers. But increasingly, VPNs enable supply chains, which integrate remote employees (remote access), customers (B2C), vendors (B2B), wholesalers, and other partners.

Business-class VPNs also apply to SMBs, which may well be the largest opportunity market that service providers will address in the next few years. SMBs want integrated and complete packages since they tend to invest less in in-house telecom expertise; thus, simple packaging from the provider as well as ease of use are required. Looking at the high growth potential in this segment, telcos and cable companies such as Verizon and Comcast are now targeting their services to SMBs.

Layer 3 BGP VPNs have been the strongest solutions to date because they are scalable and easy to provision via proven and widely deployed BGP mechanisms. We discuss these technologies further, but it's important to note that BGP VPNs support Layer 2 and Layer 3 VPN service offerings, including IPv6 support and multicast enhancements, which are key for infrastructure deployments as well as provider-based managed enterprise services. This also facilitates a migration path to upsell the MPLS BGP VPN installed base to multicast and IPv6-enabled VPN services.

With the growth of Ethernet services in the metropolitan markets, Layer 2 VPNs and VPLS deployments are growing at a fast rate and seem to be the flavor of choice for new networks today. VPLS, a key enabler for delivering multipoint Ethernet services, is being used by providers to offer transparent LAN service to enterprise customers and is also being used as an infrastructure technology. VPLS appeals to enterprises since it allows them to extend their reach beyond their local areas with the same Layer 2 Ethernet connectivity paradigm. This significant interest from service providers is measured by real VPLS deployments including inter-provider offerings.

The Infrastructure VPN

Large global carriers as well as midsize national carriers have implemented MPLS backbones since MPLS offers scalability, traffic engineering, and bandwidth guarantees. MPLS provides the advantage of Layer 2 networking with the flexibility and diversity of Layer 3 technologies for business-class VPNs as well as infrastructure VPNs. When VPNs are used as infrastructure in a provider network, there are two options: to provide service as a wholesale solution to other providers that want to extend the reach of their own services and to backhaul customer traffic to a centralized service delivery edge over an access network.

The Wholesale Model

A single carrier will often partner with multiple carriers to provide end-to-end VPN services and is often called a "carrier of carriers." In this case, the single carrier will use its own VPN to distribute VPN traffic from other service providers. Telco providers as well as cable operators already use VPNs as infrastructure technology and as a transport mechanism. This requires standards-based deployments and is important to the largest service providers worldwide such as AT&T, France Telecom, Verizon Business, and Deutsche Telekom, which already deploy thousands of end-to-end VPN services.

The Backhaul Model

VPNs are often used in Carrier Ethernet networks to backhaul traffic from DSLAMs over the metro Ethernet network to the local point of presence (POP) where service is terminated. In many cases, a provider will not own the local metro network but will want to extend a VPN service into that metro area. This infrastructure backhaul model enables two providers to connect and enable seamless VPN communication across two disparate provider networks. As high-speed mobile services support applications such as music downloads, online multiplayer gaming (device to device), streaming TV, and mobile IM and data downloads, service providers hope this growth will turn into increasing profitability for their network.

Mobile backhaul requires reliable transport across carrier-grade platforms, as well as full MPLS feature sets and a network operation model that supports legacy as well as emerging technologies. Providers owning a metro network are partnering with mobile providers to backhaul the remote cell site traffic over the metro network. Examples of this model include wireless backhaul to central sites using VPN as a transport mechanism to support wholesale services. With Ethernet emerging at cell sites for low-cost transmission, 3G, 4G, or WiMAX may be transported over Ethernet as TDM circuits are replaced or moved.

The Inter-Provider VPN

An inter-provider VPN offers the ability to extend the reach of VPNs across multiple providers. When two companies merge and have disparate offices across large geographic and administrative (AS) domains, inter-provider agreements and support are deployed in order for customers to receive full VPN connectivity as well as one complete bill for their network. Service continuity is key here, especially when mergers and acquisitions bring new demands to patch the services seamlessly across domains (administrative and protocol). Examples of this are enabled by supporting LDP-BGP VPLS interworking for fast and seamless integration across heterogeneous protocol environments.

Table 2 sums up the models we've discussed for VPNs as well as the toolkit solutions for each of these variants.

TABLE 2**VPN Models by Key Requirements and Toolkit Solutions**

VPN	Key Requirements	Tools/Solutions
Business class		
All business	Flexibility	IPv4, IPv6, dual stack v4/v6, unicast and multicast traffic, service customization, and third-party integration tools (SDK or APIs)
Large enterprise	High availability	Multihoming for provider redundancy, MPLS-based restoration (FRR)
	Extranets	L3 VPN extranets including for MVPN
SMB	Service instance scale	Scalable VPN instances for both unicast and multicast
Infrastructure VPN		
DSLAM aggregation or mobile backhaul	Transport options	Multiple types of pseudowires, L2 (VPLS, L2 VPNs) and L3 (unicast and multicast L3 VPN)
	High availability	Multihoming for PE redundancy, MPLS-based restoration (FRR)
	Administrative separation	Inter-AS, interdomain, carrier of carriers VPN
Financial infrastructure	Multicast delivery	Efficient multicast replication: P2MP MPLS, MVPN

Source: IDC, 2008

NEW TRENDS: EMERGING VPN APPLICATIONS

Now that VPNs are being used as a secure network service for all types of businesses as well as infrastructure transport for multiplay services, and as wireless backhaul, *the VPN as a platform* is being extended to enable additional features and applications that reflect the new market trends of video distribution and multiplay requirements. Thus VPN service technologies must now be optimized to carry different traffic types (voice, data, video, and mobile access) as well as support the new features discussed in the following sections.

MPLS Multicast

Emerging media-rich services are posing new technological challenges in terms of optimized content insertion, transformation, and distribution. Service providers, content providers, and cable operators are expanding their high-definition (HD) offerings to thousands of channels while simultaneously offering increasingly sophisticated media-rich collaboration tools. Traditionally, multicast technology options for content delivery were limited, and implementations were based on IP Protocol Independent Multicast (PIM) protocols in the infrastructure core. Early PIM-based multicast deployments posed a series of challenges for network operators.

IP multicast does not allow end-to-end traffic-engineered paths or QoS guarantees. With traditional IP multicast approaches, recovery from network failure is in multiseconds rather than milliseconds. Point-to-multipoint (P2MP) LSPs leverage the functionality inherent in MPLS such as fast reroute (FRR) and the QoS guarantees in RSVP. IP unicast, multicast, and Layer 2 traffic can all be mapped into P2MP LSPs, allowing providers to migrate their legacy traffic over time onto their core. It is important to note that P2MP LSPs increase service control without adding state management to the core network, thereby implicitly being more efficient. P2MP also provides an efficient underlying replication mechanism for VPLS, which was created for Layer 2 broadcast delivery.

IDC expects that content distribution will expand the use of P2MP LSPs. Large service providers are already deploying P2MP LSPs in their networks today, putting pressure on all vendors to support this efficient tool. In fact, over 10 major providers ranging from telcos to MSOs and enterprise organizations have deployed P2MP LSPs in their network, and IDC believes many other providers will follow.

Multicast VPNs

Service providers have been offering VPN services for many years now. The ease of migration from a current VPN service to offering a multicast VPN is often understated. Because the provider is already familiar with the protocols and provisioning, in terms of scope, economies of scale, and SLA familiarity, the migration is natural. The same is now true for next-generation multicast VPNs. Some of the key emerging multicast applications are as follows:

- ☒ Service providers are beginning to offer Layer 3 VPN multicast service to their enterprise customers.
- ☒ Video transport is beginning to be offered within a VPN for separation and virtualization between different customers. This is an example of IPTV being used as a wholesale model. Another example is where content providers that are interconnected within the same network require separation and virtualization for efficient video transport. Custom TV configurations can be created by the consumer within the broadcast networks so that MTV, HBO, or any specific channel can be virtualized for custom packaging. Multicast VPNs can be used in this example to broadcast separate content on an IPTV network.

- ☒ Financial services are being distributed via multicast, especially when the VPN is already in place. A large financial services company may want to propagate a national or international broadcast to its employees or deliver stock ticker as well as televised financial services in real time to its clients. Scalable multicast VPNs, along with P2MP LSPs to enable MPLS multicast, are seen as key solutions for this application.
- ☒ Research and education establishments also are beginning to use multicast VPNs for distance learning and media collaboration tools, where online video conferencing is used to connect teachers, musicians, and even doctors for surgical administration or surgical video viewing and active participation.

Next-generation MVPN drafts introduced a BGP-based control plane modeled after its successful counterpart of the VPN unicast control plane. The BGP-based MVPN control plane supports flexible topologies, such as extranet and hub and spoke, and supports IPv6. Draft-Rosen, an earlier MVPN scheme, is not being pursued in the IETF L3 VPN Working group as a standalone draft anymore.

Table 3 compares Draft-Rosen with BGP MVPN.

TABLE 3		
Comparison of Draft-Rosen with the Emerging BGP MVPN Standard		
	Draft-Rosen	BGP MVPN
Transport	PIM-SM GRE	Different MVPNs could use different tunneling technologies (P2MP MPLS or PIM-SM GRE).
Signaling	PIM	BGP
PE-PE sessions		
Signaling	Each PE needs a separate PIM adjacency with each remote PE per VRF.	Each PE uses existing IBGP sessions, which may only be sessions with the route reflectors.
Provider Tunnel mesh	Required between PEs.	Not required. Provider can build MVPN services based on sites with either sources or receivers, or both, with different pricing options.
Inter-AS operations	Inter-AS/inter-provider operations option A or C requires PEs in different ASs to have (direct) PIM routing peering.	BGP MVPN works with all three options (A, B, and C as defined in RFC 4364) available for inter-AS unicast. It also has the concept of segmented inter-AS trees that allow each AS to independently run a different tunneling technology.

Source: IDC, 2008

IPv6 VPNs

There has been discussion for years that the IPv4 address space will run out. At the same time, the number of mobile devices is exploding; many of these devices may become IP aware, and thus each device would require an IP address. Government mandates are also driving IPv6 implementations. Many of the federal agencies use MPLS VPN services supplied by carriers, hence the need to support IPv6 over MPLS VPNs on those carriers' networks as well. These are strong drivers for IPv6 and IPv6 support within VPNs.

Japan, China, and Korea are well ahead on IPv6 implementation; the U.S. government has already mandated IPv6, and so have BT 21CN and various other top-tier providers. The existing IPv4 networks will not be able to handle the potential explosion of IP-enabled mobile devices and the overlap of public and/or private addresses. RFC 4659 "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN" or the use of IPv6 islands over an MPLS IPv4 core (known as "6PE," RFC 4798) are mature technologies and will need to be supported. IPv6 MPLS BGP VPNs leverage IPv4 VPN technology and use M-BGP to exchange labeled routes between PEs (the VPN label). Also leveraged are route distinguishers to disambiguate routes, extended community route targets to identify the VPN, and a label stack on the data plane so the "outer" label is used for the transport layer.

IPv4 and IPv6 can be used within the same VRF and may also use the same LSP and the same BGP sessions just as with IPv4 VPNs. Packet processing, filtering, and accounting are the same, as well as the options for inter-provider or carrier-to-carrier VPNs. In principle, the operation and configuration of an IPv6 VPN is very similar to that of an IPv4 VPN based on the common underlying MPLS BGP VPN framework.

Global Crossing is one service provider that has differentiated itself with these service offerings. AT&T and Global Crossing also have direct IPv6 peering agreements. Global Crossing has implemented IPv6 peering with more than 20 partners and has more than 40 customers operating over IPv6 networks.

Table 4 captures some of these trends.

TABLE 4

Trends and Shifts in the Market

Trend	Current	Emerging
Services - L3	BGP MPLS IPv4	BGP MPLS IPv4 + IPv6
Services - L2	Pseudowires, VPLS-LDP in metro, BGP VPLS in WAN	Signaling-agnostic VPLS and LDP-BGP VPLS interworking
Reach	Intra-AS, single metro	Inter-AS, intermetro, carrier of carriers, transnational and wholesale model
Traffic/content delivery	Internet access, IPv4 unicast	Internet access, IPv4/v6 unicast and multicast
	MVPN with PIM overlay	BGP MVPN via P2MP LSP
TTM and service flexibility	12–18 months — basic connectivity	6–8 months with integrated offerings and best-of-breed third-party application integration

Source: IDC, 2008

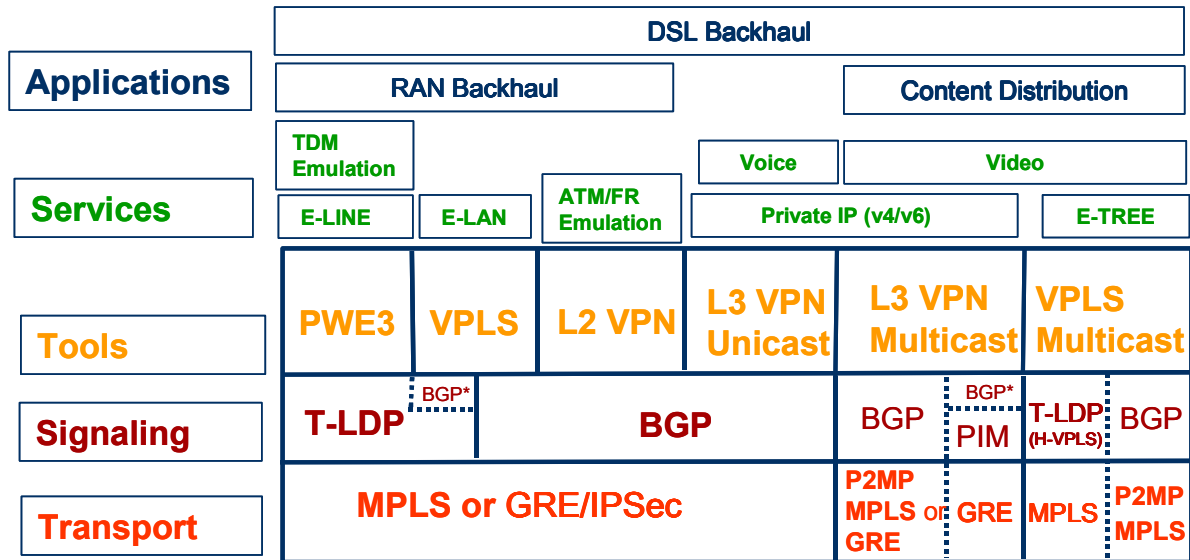
VENDOR TOOLKIT

As providers face the challenge of delivering existing services and enabling applications over their networks, there is an increasing desire to build a converged infrastructure. But this converged infrastructure will demand a high level of availability and resiliency as well as diverse methods of creating virtualization to offer the full spectrum of services. It is critical to choose the underlying technologies that can provide a common framework for transport as well as services to achieve economies of scale and simplified operations.

Figure 3 represents the different options being used today and highlights the common elements for consideration.

FIGURE 3

Multiservice Framework



BGP* - BGP used only for autodiscovery

PWE3 = Pseudowire

T-LDP = Targeted LDP

P2MP = Point to Multipoint

H-VPLS = Hierarchical VPLS

E-LAN, E-LINE, and E-TREE are service definitions as per MEF

Source: IDC, 2008

Vendors need to support the requirements discussed in the following sections to deliver next-generation multimedia VPN services.

Scale and Signaling-Agnostic Options

The support for different topologies and technologies is necessary since VPNs provide different services within different delivery models. In some cases, the drivers are consolidation (mergers and acquisitions), inter-provider partnerships, or simply the choice of end users — whether they are large enterprises or SMBs that want to outsource their network operations. Either way, a provider must support Layer 2 and Layer 3 VPNs as well as the ability to backhaul traffic to meet extended VPN site requirements, be they rural or remote.

Most vendors support Layer 2 and Layer 3 VPNs, but not all vendors support multiple signaling mechanisms. With the growth of Ethernet services, Layer 2 VPNs, including VPLS, are expected to have considerable uptake as well. VPLS uses either LDP or BGP as a signaling mechanism.

Table 5 captures the scaling characteristics of LDP-based VPLS and BGP-based VPLS.

TABLE 5		
Scaling Characteristics of LDP-Based VPLS and BGP-Based VPLS Networks		
	LDP VPLS	BGP VPLS
Pseudowire full-mesh requirement	Addressed by H-VPLS by creating hub and spoke hierarchy; introduces MAC address state scaling challenges in the hub	Addressed by BGP route reflectors already used in large IP networks
Provisioning	Manual or through provisioning or using separate BGP extensions	Automated by autodiscovery mechanism inherent to BGP
Multicast replication efficiency	Addressed partially by H-VPLS	Integrated with P2MP MPLS

Source: IDC, 2008

While LDP was the protocol deployed in early small-scale VPLS networks, now many BGP VPLS networks are being deployed, mainly because a BGP VPLS network provides scalability and seamless intermetro and inter-AS capabilities needed for large providers deploying it today. Over 10 major providers across telco and cable operators deploy BGP VPLS networks, and IDC expects these key carriers to provide the impetus for other providers to migrate in this direction. A proper toolkit should consist of LDP VPLS support since LDP has already been deployed in numerous metro areas.

BGP is a scalable protocol for emerging technologies such as next-generation multicast VPNs, multicast over VPLS using P2MP, and inter-AS operations. Providers may also want to interconnect existing LDP metro sites to a BGP core and may begin to deploy BGP at new metro sites to scale efficiently and seamlessly interwork with their core network. BGP VPLS allows the autodiscovery mechanism inherent in BGP to operate, making the network easier to provision and scale. BGP VPLS also leverages route reflectors used in BGP networks worldwide to alleviate the control plane scaling issues without affecting the forwarding plane.

Therefore, all vendors should seriously consider being signaling "agnostic" and support all signaling methods as well as interworking between these protocols, especially since new features such as multicast VPNs, IPv6 VPNs, and P2MP MPLS will need to be supported to deliver media-rich services on top of the VPNs already in place.

The various signaling-agnostic options are as follows:

- ☒ For VPN reachability, T-LDP or MP-BGP
- ☒ For tunneling, LDP or RSVP-TE or non-MPLS (GRE, IPsec)
- ☒ For interworking, T-LDP or MP-BGP VPLS interworking

Table 6 shows a comparison of the various protocols and signaling methods and their control and forwarding plane information.

TABLE 6						
Protocol Comparison for VPN Deployment						
	L3 VPN - Multicast	L3 VPN - Multicast	L2 VPN	VPLS	VPLS - Multicast	Pseudowires
Forwarding plane	MPLS (P2P RSVP or LDP), GRE, IPsec	MPLS (P2MP RSVP), GRE	MPLS (P2MP RSVP), GRE	P2P MPLS (RSVP or LDP), GRE	P2MP MPLS RSVP, P2P MPLS RSVP or LDP, GRE	MPLS (LDP)
Control plane	BGP	BGP, PIM	BGP	BGP, T-LDP	BGP, T-LDP	T-LDP

Source: IDC, 2008

Feature Richness

Deploying thousands of VPNs requires reliable fault detection and a standards-based approach. MPLS fast reroute is widely deployed and is beginning to replace SONET/SDH to enable SLAs. Additional support from BFD for fast failure detection and Ethernet OAM standards also provide additional resiliency and availability. Another critical feature for resiliency is multihoming. This is where a CE is multihomed to two PEs such that when one of the PEs or the PE-CE paths goes down, the other remote PEs in the network learn via BGP an alternate path to reach the CE via the redundant PE. This is key for VPN survivability and should be in any vendor toolkit.

Service providers today already offer class of service (CoS) to support mission-critical applications. The QoS mechanisms within the VPN meet this need by differentiating traffic types and assigning priority. QoS is used extensively in provider networks to ensure end-to-end SLA guarantees. Most providers today use at least three, and often four to five levels of QoS, ensuring that key applications reach the end user. When using RSVP-based bandwidth attributes for signaling, providers realize added benefits of Diffserv-aware traffic engineering since RSVP can be class aware when carried via IGP extensions, while an LDP approach tends to be more coarse.

Service Continuity and Reach

Most VPNs span not only multiple network elements but also multiple provider networks to facilitate service continuity across networks. Topologies may extend from metro and core networks across major and minor providers, local and national. A standards-based approach is one mechanism to interoperate network elements. MPLS BGP VPNs are already standard and span multiple network elements today. Nonstandard approaches might be advantageous in some ways; they are not universally applicable and therefore have limitations when it comes to interoperability and interworking. As providers partner more and more with local CLECs for metro access for VPNs to extend service reach, interworking across multiple provider networks is essential. We see this trend coming from many areas, from large financial firms and regional providers, both of which, through mergers and acquisitions, need to converge disparate networks. One example of this is where a metro Ethernet service based on LDP VPLS for VPNs is newly connected to a core MPLS BGP VPLS network. In this case, BGP to LDP VPLS interworking is needed. The wholesale model discussed earlier may cater to multiple metro providers for either Ethernet services or backhauling mobile connections. In this case, pseudowires need to be transported into the core MPLS network. Not all approaches today are standardized, as MPLS BGP VPLS is still an emerging market, but clearly VPN termination and transmission across these networks must be done as seamlessly as possible.

Streamlining Operations

While many protocols are deployed in carrier networks today, using the same protocol across domains and within the IGP network clearly will simplify the implementation of the VPN offering. A common BGP control plane and MPLS data plane ensure seamless integration and implementations. A single operating system that can span core, edge, and datacenter routers is also a key differentiator from an OSS perspective.

While it does seem that complexity continues to be added to network deployments of VPNs, new forms of assistance are emerging to simplify what has become complex. Configuration templates are now offered to help create standard and automated provisioning and network setup. Use of templates reduces human error (the largest configuration problem) and automates a significant portion of protocol work that added complexity. Common scripts that define specific customer rules on a per-provider basis are increasingly being used as well to ensure that the provider has checks and balances in the way each customer is provisioned.

Automation is another feature increasingly being used by providers to ease the use of protocol deployments. Autodiscovery of VPN endpoints as well as PE discovery lower the manual and static configuration, which only introduces human error potential. MPLS also inherently provides autoprotection of links and nodes, which comes with any MPLS fast reroute implementation.

FUTURE OUTLOOK

For VPN deployments, MPLS is a mature and well-tested protocol for transport. The multiservice capabilities of MPLS set a strong foundation for existing services as well as emerging services, such as multicast transport using P2MP LSPs. MPLS BGP VPNs have proven scalability, automation, and service expandability characteristics that can be leveraged for other VPN types such as Layer 2, VPLS, and multicast and IPv6 VPNs. Standard control and data plane deployments allow for clean migration to Ethernet services networks as well as the emerging mobile backhaul markets. The logical step then is applicable to provider-provisioned VPNs to underpin the transition for multiplay services and eventually IMS or fixed mobile convergence.

ESSENTIAL GUIDANCE

Vendors that provide a toolkit that consists of a standards-based approach and signaling-agnostic offerings and supports all protocol options will clearly be considered for wider deployments by providers as they expand their VPN networks.

The multidimensional scaling across control and forwarding plane techniques combined with the common protocol framework simplifies operations and improves ROI. The breadth of interdomain deployment options including protocol interworking allows service continuity and expanded service reach beyond traditional geographies and administrative and organizational domains. And unique tools such as third-party application development will help providers deliver new services quickly while offering true differentiation.

A toolkit of rich protocol support as well as media-rich feature sets offers flexibility and enables seamless migration to next-generation VPN technologies needed to support emerging Layer 2 and Layer 3 services.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2008 IDC. Reproduction without written permission is completely forbidden.