



Sorting Out the Alphabet Soup of VPN Solutions

A practical approach to assessing WAN technologies that support your distributed organization's diverse needs

Executive Summary

Sorting Out the Alphabet Soup of VPN Solutions

Today's distributed organizations face the challenge of finding VPN WAN solutions that support the proliferation of branch offices and mobile workers, along with the successful deployment of demanding, critical, and converged applications—such as video, Voice over IP (VoIP), payment processing, storage, CRM, and ERP.

MPLS-based IP VPN technology has become the leading WAN solution for multi-site connectivity. Proven and hardened, MPLS IP VPNs take advantage of cloud-based, performance-enhancing, and cost-saving technologies that enable the consolidation of all enterprise applications onto a single private network with Class of Service (CoS) capabilities, built-in security, and a wide range of access options. This results in WANs with superior performance, enhanced flexibility, and significantly lower total cost of ownership (TCO) when compared with legacy alternatives.

IPSec VPNs securely connect remote sites onto a network with confidentiality, data integrity, and authentication for safe access to the enterprise network.

SSL VPNs provide secure and cost-effective mobile remote access; they do not require extra software to install and free organizations from the burden of buying and managing remote access systems.

MPLS VPN services are widely available and commonly used by enterprises of all sizes. Mid-tier businesses significantly benefit from the leading-edge enterprise-class VPN WAN services because of the minimal capex and pay-for-use pricing.

The details of MPLS VPN services can look like a cloudy alphabet soup of acronyms: IP. MPLS. CoS. QoS. FR and ATM. IPSec. SSL. VoMPLS. This white paper was written with business executives and IT decision makers in mind. It succinctly defines these essential terms, outlines the relevant issues when considering today's VPN options, and touches upon remote access, security, legacy VPN technologies, and secure Internet access.

The Challenge

Distributed organizations are faced with the challenge of managing the complexity and costs associated with multi-site wide area networks (WANs). VPN implementations must support growing networks of branch offices, business partners, and mobile employees with fast, reliable, secure, and cost-effective access to a company's real-time data and enterprise applications.

While constrained capex spending is today's reality, WANs still must support a new generation of bandwidth-intensive and critical applications across the distributed enterprise with reliable, high-quality services, including:

- Latency-sensitive applications — such as VoIP
- Business-critical applications — such as payment processing, CRM and ERP
- Bandwidth-intensive collaboration tools — such as video conferencing

For many companies, connectivity and bandwidth requirements change so fast that traditional network services—such as Frame Relay and ATM—can't meet requirements within capex and budgetary constraints.

Escalating customer expectations and growing international competition add to the challenge. Businesses require networks that are cost-effectively flexible and scalable in order to take advantage of growth opportunities.

Trends and Opportunity Drivers

MPLS VPN technology has become the leading WAN solution because of its technological maturity and mainstream adoption. It provides CoS capabilities and QoS guarantees that support the delivery of demanding and mission-critical applications—including VoIP, video, social networking, enterprise SaaS and other Web 2.0 applications—with lower capex and network TCO.

Network Security Continues To Be the #1 Overriding IT Concern

MPLS networks offer powerful and cost-effective cloud-based and managed security solutions at a time when more companies are implementing SaaS and managed solutions to address their overriding security concerns.

The Impact of Cloud Computing

Cloud computing has evolved to offer reliable and secure high-performance IT services with game-changing economics. Initial perceptions that ‘the cloud’ isn’t secure are giving way to the understanding that many cloud-based services offer significant security advantages—including the strength and quality of security services, cost-effectiveness, and ease of management.

Strong growth in managed and cloud-based IT solutions across small, medium, and large businesses is driven by:

- Lower capex and operating costs
- Cost management from predictable pricing
- Consistent reliability and quality of services
- Easing the challenge of multi-location complexity and new applications
- Availability of reliable, low-cost broadband access options

Convergence Realized

Converging all business traffic—including latency-sensitive applications, such as VoIP—onto one network reduces costs, simplifies operations, and meets the requirements of today’s applications.

MPLS VPNs Are Frequently Self-Funded

The savings recognized by leveraging a single access connection for all applications can fully fund the WAN. In addition, the use of VoIP over an MPLS VPN (VoMPLS) network can leverage voice savings that can often fully fund the data network.

Certainly, a best-practice selection process for converged voice/data services includes ascertaining whether the service provider delivers network security and monitoring. Because SMB operations rely on the free flow of voice and data, these customers need assurance that their circuits are safeguarded from security threats—such as viruses and spam—and are protected from network outages. Therefore, the managed services provider should:

- **Proactively monitor the network**
The services provider should support and proactively monitor its data, voice, and security services on a 24 / 7 / 365 basis from multiple redundant network and security operations centers. Dedicated support and infrastructure ensures that the network services perform to their maximum potential, and customers receive the best technical support available.

- **Deliver network-based security**

The most advanced converged voice/data services are protected by managed security services that do not require customer premise equipment (CPE).

The managed security services should provide a multi-layer security approach that delivers holistic protection from individual and blended threats, as well as coordinated security alerting, logging, and reporting. Components—all of which are managed and maintained by the provider, in the network cloud—should include:

- Managed firewall
- Intrusion protection
- Anti-virus/anti-spyware protection
- Anti-spam protection
- Web filtering, including white list / black list and content filtering
- Personal protection suite

CoS = Class of Service is a network traffic management methodology that groups similar types of traffic (voice, video, etc.) together and treats each type as a class with its own level of service priority, but without a guaranteed level of service in terms of bandwidth, latency, and jitter.

QoS = Quality of Service leverages the CoS groupings to guarantee a level of service by reserving application specific bandwidth to meet the service guarantees by class in terms of bandwidth, latency, and jitter.

FR = Frame Relay is a legacy WAN technology that requires an expensive permanent virtual circuit (PVC) at each site and without QoS capabilities required for today's applications.

ATM = Asynchronous Transfer Mode is a legacy WAN technology that requires a permanent virtual circuit (PVC) at each site and without QoS capabilities.

PVC = Permanent Virtual Circuit is a software-defined logical connection typically found in a Frame Relay network and is used to privately connect locations within a network.

CIR = Committed Information Rate is the amount of bandwidth allocated to a logical connection in a permanent virtual circuit (PVC), essentially acting as the minimum guaranteed bandwidth of the connection.

IPSec = Internet Protocol Security is the most widely used data encapsulation technology for transmitting encrypted data across the Internet or any IP network. IPSec establishes mutual authentication, negotiates cryptographic keys, and secures IP communications by authenticating and encrypting each IP packet of data streams. IPSec VPNs provide confidentiality, data integrity, and authentication to securely connect remote sites onto the same network for safe access to enterprise data and applications.

SSL = Secure Sockets Layer is a standard cryptographic protocol built in to all of today's major Web browsers; it provides secure Internet-based communications. SSL VPNs provide a secure and cost-effective way of meeting the demand for mobile remote access, requires no client software to install, and doesn't require an organization to buy or manage a remote access system.

NNI = Network to Network Interconnection is an interface that specifies signaling and management functions between two networks. NNI can be used for the interconnection of either signaling, IP, or ATM networks.

SLA = Service Level Agreement is part of a service contract where the level of service is formally defined. It records a common understanding about services, priorities, responsibilities, guarantees, and warranties.

WAN VPN Solution Options

Alternatives for connecting multiple sites with WAN links fall into three categories: Traditional dedicated WAN VPNs (private line or FR/ATM), IPsec VPNs, and MPLS IP VPNs.

Traditional Dedicated WAN VPNs (Private Line or FR/ATM)

Traditional private line data services used to be the standard for most enterprise WANs, because they offered inherent security and dedicated site-to-site bandwidth. A point-to-point private line WAN epitomizes the concept of a private network by providing dedicated site-to-site circuits, so users have the entire capacity available whenever needed and no other clients sharing the circuit to present a potential security threat.

Existing layer 2 networks connected to a frame relay or ATM backbone to interconnect locations or create a VPN also provide dedicated bandwidth from site-to-site, but use Private Virtual Circuits (PVCs) instead of point-to-point dedicated circuits. Each PVC is allocated a certain amount of bandwidth—or Committed Information Rate (CIR)—that must be reserved on the local loop and on the provider's network.

A primary problem with legacy private line, frame relay, and ATM VPNs is they are not application or IP-aware, so they can't recognize or prioritize classes of network traffic. In addition, frame relay is bandwidth-constrained with services that do not typically exceed DS1 (also known as T1) capacity.

Built on the premise of consistent amounts of data traffic primarily flowing between HQ and branch offices, these networks no longer efficiently or economically support the site-to-site traffic patterns of today's distributed business networks.

Public Infrastructure Internet-based VPNs (IPsec VPN)

IPsec VPNs provide confidentiality, data integrity, and authentication to securely connect remote sites onto the same network for safe access to enterprise data and applications. A site-to-site IPsec VPN uses the IPsec capabilities of a CPE access router to encrypt traffic going from one site to another over the public (Internet) network infrastructure. A central site—generally a company's headquarters or primary location—acts as the hub in a classic hub-and-spoke topology. An IPsec tunnel is built from a central hub to each site, giving each location secure access to the entire network.

With IPsec VPNs, complexity lives at the customer premises with the CPE-based firewall. IPsec VPNs require configured client-side software for access; this provides strong security but also requires additional administrative and management costs. In addition, IPsec VPNs only provide 'best-effort' performance and may not support performance-sensitive applications.

A hybrid MPLS/IPsec VPN can be used to connect on-net sites directly to the MPLS network and off-net sites via the public Internet with IPsec encryption. This allows an organization to extend the reach of the MPLS VPN to any site on the public Internet. All of these approaches provide adequate data and source/destination information security and the tools to ensure proper authentication and access controls.

Dedicated Access MPLS (site-to-site) VPNs

MPLS

Widely considered today as the best available technology to augment, back up, or replace a legacy WAN VPN, MPLS blends the performance and privacy of legacy WAN technologies with the flexibility and cost advantages of IP-based networks. The affordability of MPLS VPNs now puts them in reach of small, growing organizations.

In 2010, MPLS technology became the leading WAN solution for multi-site connectivity. Providing CoS capabilities and QoS guarantees to support reliable, high-quality delivery of demanding, critical, and converged applications—including VoIP, video, social networking, enterprise SaaS, and other Web 2.0 applications—MPLS VPNs deliver on the long-awaited promise of convergence with proven lower capex and lower network TCO than legacy alternatives.

Well-suited for today's dynamic, challenging network environments

With dedicated access to a core MPLS infrastructure and network backbone, MPLS VPNs provide any-to-any connection between sites and powerful, cost-effective MPLS-enabled automatic disaster recovery options.

Smart traffic engineering prioritizes critical applications

MPLS VPNs provide IP-aware and application-aware enabled services—controlling network traffic at the packet level—with QoS across the network backbone for smart traffic engineering and traffic prioritization, thereby solving the problems of high-bandwidth applications over distributed networks.

QoS classifies and prioritizes network traffic into as many as 5 or 6 classes of service. A typical design may include separate classes for real-time applications—such as VoIP, mission and business-critical traffic—such as email applications, and data traffic for all other non-critical transactions.

Security

A primary advantage of MPLS VPNs is that the network complexity lives with the network provider, enabling managed cloud-based network security services at the core and edge of MPLS VPNs. Additional security is available from both site and host/client security layers.

MPLS VPNs Top 10 Benefits

1. Privacy comparable to FR and ATM, without costly PVCs
2. Secure direct site-to-site connectivity
 - FR/ATM equivalent without encryption
 - Protection from the open Internet
 - Full meshing without additional PVCs
3. Superior connectivity and network performance
 - Minimal delay and packet loss for demanding applications
 - Higher bandwidth connections
 - End-to-end control for maximized performance
4. QoS and CoS to prioritize mission-critical and real-time applications
5. Flexibility
 - Any-to-any communication
 - Easily add and remove sites and users
 - IP addressing freedom
 - Ready for future applications
6. Scalability
 - Low to very high speed access for sites and users
 - Use any access technology
 - Small to very large number of sites
7. Centralized policy control and management
 - Simplifies distributed network management
8. Increased productivity for the business organization
9. Cost-effective disaster recovery
10. Managed security service options

VPN Comparison Grid

How MegaPath MPLS VPNs compare to Frame Relay and IPsec VPNs

Features	DIY IPsec VPN	Frame Relay	Competitor's MPLS VPN	MegaPath MPLS VPN
Private circuits , not public Internet, for superior performance/reliability, easier troubleshooting and reduced risk of Internet-based attacks	X	✓	✓	✓
Connection-based versus packet-forward routing for faster data delivery and better network management capabilities	X	✓	✓	✓
Separate Classes-of-Service for Real-time (VoIP) and Business-Critical applications (ERP, Financial Transactions)	X	X	✓	✓
Fully Meshed versus Hub-and-Spoke network topology standard for lower latency	X	X	✓	✓
Scalable architecture and manageability to support growing businesses with dozens or even thousands of sites	X	X	✓	✓
Low Total Cost of Ownership due to low CapEx requirements and outsourced management and 24x7 monitoring and support	X	X	?	✓
Wide selection of access technologies offered nationwide (DSL, Cable, Wireless, Satellite or T1/T3)	X	X	?	✓
Built-in Security Gateways to provide Firewall, Intrusion Prevention, Anti-virus, Anti-Spam and Web Filtering	X	X	?	✓
Data encryption optional ; maximize security or increase throughput with low-cost CPE	X	X	?	✓
IPsec or SSL VPN Remote Access for mobile workers/partners with application and device specific access control policies	X	X	?	✓
Automatic Back-Up redundancy options featuring Dial, DSL, Cable, Wireless or Satellite access	X	X	?	✓
End-to-End SLAs (Availability, MTTR, Latency, Packet Loss, Installation Intervals, etc.) on T1/T3, DSL and Cable access	X	X	?	✓
4-hour Onsite CPE Maintenance with T1/T3, DSL, Cable and Satellite access	X	X	?	✓
Multi-cast to broadcast video and distribute large files more quickly and with less host bandwidth/CPE cost	X	X	?	✓
Multiple CPE options from Cisco, Adtran and Motorola to address feature/functionality and cost requirements	✓	X	?	✓
Flexibility to securely connect any site using its existing Internet access (Suppliers, Distributors, Customers, ASPs)	✓	X	?	✓

MegaPath VPN Solutions: A Distinct Difference

MegaPath is a leading provider of managed IP communication solutions. We reduce the cost and complexity of connecting geographically distributed enterprises while providing the high performance required for today's demanding business applications. MegaPath offers flexible, scalable, and cost-effective VPNs, as well as cloud-based managed voice and security solutions.

MegaPath has a strong track record of successful VPN installations, the broadest MPLS-based QoS-enabled voice network, and the largest broadband reach of any network in North America. MegaPath enables QoS not only at the circuit level, but also throughout the entire MegaPath MPLS network, preventing vital applications from failing due to network congestion or usage spikes.

MegaPath is one of only a handful of Cisco Managed Services Channel Partners to receive Cisco's Master Partner designation. To achieve this, Cisco made an extensive audit of MegaPath's NOC capabilities, reviewed our SLAs, and verified that MegaPath has both CCIE and ITIL certified team members.

MegaPath MPLS IP VPN Offerings

Providing cost savings and performance benefits, MegaPath VPN offerings cover the spectrum of managed WAN services, including:

- **MPLS site-to-site Managed VPN – Smart, superior performance for all of your applications**
Consolidates all of your business applications onto a single private network with up to five CoS, built-in security, and a wide selection of access technologies for maximum performance and flexibility.
- **IPSec Site-to-Site VPN – Secure connectivity for companies with 5 or fewer sites**
Securely connects all of your sites on the same network with IPSec, the standard Internet-encryption technology, so files, applications, and resources can be safely shared by multiple offices. Delivers the highest level of security protection using DES and 3DES encryptions to ensure data security. Offers the widest selection of access technologies.
- **Remote IPSec VPN – Secure client-based remote access**
Offered in conjunction with MegaPath's Site-to-Site MPLS VPN service and capable of seamless integration with MegaPath Security Services, a remote IPSec VPN uses a client on remote users' laptops and PCs to establish an encrypted tunnel to MegaPath's security gateways. This tunnel securely maps the traffic into your MPLS VPN.
- **Managed SSL VPN – Clientless, anywhere secure access for remote users**
A clientless, integrated SSL-based secure access solution that can be rolled out rapidly and managed with ease. Frees businesses from having to buy or manage a remote access system and install client software. A proven, cost-effective solution for secure mobile access.
- **Hybrid VPN solutions**
Ideal when on-net sites are connected directly to the MPLS network and off-net sites are connected via the public Internet using IPsec encryption. The latter allows businesses to extend the reach of the MPLS VPN to any site on the public Internet. All of these approaches provide adequate security of the data and source/destination information, as well as the tools to ensure proper authentication and access controls.

Next Steps

Go to <http://www.megapath.com/vpn-security/mpls-site-to-site-vpn/> to learn more about MegaPath MPLS network solutions.