



Sorting Out the Alphabet Soup of VPN Solutions

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

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

Distributed organizations are facing 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 like video, 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) than 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 a secure and cost-effective method for mobile remote access with no client software to install and without the need for an organization to buy or manage a remote access system.

MPLS VPN services are now widely available and commonly used by enterprises of all sizes. They bring particular benefits to mid-tier businesses that can now reap the benefits of leading-edge enterprise class VPN WAN services with minimal capex and advantageous pay-for-use pricing.

The details can look like a cloudy alphabet soup of VPN acronyms: **IP. MPLS. CoS. QoS. FR and ATM. IPSec. SSL. VoMPLS.**

This white paper – written for business executives and IT decision makers – succinctly defines these essential terms and outlines the relevant issues when considering today's VPN options, with a focus on MPLS-based IP VPN services, and also touching 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 of 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 – with access and user experience just like at headquarters.

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 like VoIP
- Business-critical applications like payment processing, CRM and ERP
- Bandwidth-intensive collaboration tools like video conferencing

For many companies today, connectivity and bandwidth requirements change so fast that traditional network services like Frame Relay and ATM can't meet requirements within capex and budget constraints.

Escalating customer expectations and intensified international competition add to the challenge, and require networks that are flexible and scalable. Cost-effective scalability is an essential network requirement in order to facilitate a company's ability to take advantage of opportunities.



Trends and Opportunity Drivers

The trends driving the adoption and opportunities of MPLS IP VPNs include:

Technological maturity and mainstream adoption of MPLS IP VPNs

MPLS VPN technology has become the leading WAN solution, providing CoS capabilities and QoS guarantees to support reliable high-quality delivery of demanding and critical applications—including VoIP, video, social networking, enterprise SaaS and other Web 2.0 applications – with lower capex and lower 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 more companies are implementing SaaS and managed solutions to address their overriding security concerns.

VPN – a Virtual Private Network is a computer network that is layered on top of an underlying network. The private nature of a VPN means that the data travelling over the VPN is not generally visible to, or is encapsulated from, the underlying network traffic.

MPLS = Multi-Protocol Label Switching is a highly scalable, protocol agnostic, data-carrying mechanism. In an MPLS network, data packets are assigned labels. Packet-forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself.

IP = Internet Protocol is used for communicating data across a packet-switched internetwork and is the primary protocol of the Internet.

MPLS IP VPNs combine the flexible connectivity, scalability and low cost of IP-based services with the security, privacy and quality of ATM and Frame Relay.

VoMPLS – Voice over MPLS is VoIP on a QoS-enabled MPLS network which delivers end-to-end prioritization and quality assurance for critical VoIP traffic.

CoS = Class of Service is a methodology of managing traffic in a network by grouping similar types of traffic (voice, video, etc.) together and treating each type as a class with its own level of service priority 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 be able to meet the service guarantees by Class in terms of bandwidth, latency and jitter.

FR = Frame Relay is a legacy WAN technology requiring an expensive PVC at each site and without QoS capabilities required for today's applications.

ATM = Asynchronous Transfer Mode is a legacy WAN technology requiring a 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 that is utilized to privately connect to another location 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.

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, along with their cost-effectiveness and ease of management.

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

- Lower capex and lower operating costs
- Cost management from predictable pricing
- The consistent reliability and quality of services
- Easing the challenge of multi-location complexity and new apps
- The availability of reliable, low-cost broadband access options

Convergence realized

Converging all business traffic – including latency-sensitive applications like 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 amount to the WAN being fully funded. An example of this is the use of VoIP over an MPLS VPN Network (or, VoMPLS). With VoMPLS the voice savings recognized by convergence can often fully fund the data network.

Certainly, a best-practice selection process for converged voice/data services includes ascertaining that the service provider delivers network security and monitoring. Because SMB businesses' 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 protected from network outages. The managed services provider should therefore:

- **Proactively monitor the network:** The service provider should support and proactively monitor its data, voice and security services on a 24/7 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 possible 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 threats, blended threats and coordinated security alerting, logging and reporting. Components—all of which are managed and maintained by the provider, in the network cloud—should ideally include:

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

...

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.

1. 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 with no other clients sharing the circuit to present a security threat.

Existing layer 2 networks connected to a Frame Relay or ATM backbone to interconnect locations – or to create a VPN – also provide dedicated bandwidth from site-to-site, though they 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 different classes of network traffic. As well, Frame Relay is bandwidth-constrained with services that do not typically exceed DS1 (otherwise 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.

2. 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 over the public (Internet) network infrastructure from one site to another. A central site, generally a company's headquarters or primary location, acts as the hub in a classic hub-and-spoke topology. An IPSec

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 that provides for secure communications over the Internet.

SSL VPNs provide a secure and cost-effective method to meet the demand for mobile remote access with no client software to install and without the need for an organization to buy or manage a remote access system.

NNI = Network to Network Interconnection is an interface which specifies signaling and management functions between two networks. Can be used for interconnection of either signalling, 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.

tunnel is built from that 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, providing strong security but along with additional administrative and management costs. As well, 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 using 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 security of the data and source/destination information and the tools to ensure proper authentication and access controls.

3. 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 (Quality of Service) across the network backbone for smart traffic engineering and traffic prioritization, thereby solving the problems of high-bandwidth applications over distributed networks

Quality of Service (QoS) classifies and prioritizes network traffic into as many as 5 or 6 classes of services. A typical design may include separate classes for real-time applications, such as Voice over IP (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 at 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 apps
 - Higher bandwidth connections
 - End-to-end control enables maximized performance
- 4. QoS and CoS to prioritize mission-critical and real-time apps**
- 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	?	✓

...

What to look for in an MPLS VPN Managed Solutions Provider

Your choice of a managed service provider for VPN services can make the difference between mediocre and exceptional network performance, so evaluate your options carefully. Look for a provider with its own enterprise-class infrastructure along with a strong extended network via partnerships with other carriers and access providers for a variety of access options from a single point of contact. Consider looking for a provider with a Cisco powered network, or perhaps even one who has been given Cisco's elite "Master Partner" designation.

Four primary criteria for evaluation include the service provider's network Service Level Agreements (SLAs), redundancy, coverage, and experience.

SLAs

Look for a single pre-negotiated SLA across multiple networks with metrics for Availability, Mean Time to Repair, Packet Delivery and Latency – with stringent requirements to meet your high-performance and resiliency needs.

Redundancy

Review network maps and, based on your locations, request specific routes for diversity if warranted.

Coverage

Carriers utilizing Network to Network Interconnections (NNIs) with numerous carriers provide greater coverage than those "going it alone" or just implementing their first NNI.

Experience and On-Staff Expertise

Delivering high-quality managed network services requires highly knowledgeable and skilled network professionals, as well as partnerships with leading equipment and network capacity vendors.



MegaPath VPN Solutions: A Distinct Difference

MegaPath is a leading provider of managed IP communication solutions that 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 along with cloud based managed voice and security solutions.

MegaPath has a strong track record of successful VPN installations along with the broadest MPLS-based QoS-enabled voice network and the largest broadband reach of any network in North America with DSL, Cable, Wireless, Satellite, T1, Ethernet (in many flavors), DS3, and Ocx. MegaPath enables QoS not only at the circuit level, but also throughout the entire MegaPath MPLS network, preventing vital applications from ever failing due to network congestion or utilization spikes.

MegaPath is one of only a handful of Cisco Managed Services Channel Partners to receive their "Master" designation. To achieve this, Cisco made an extensive audit of MegaPath's NOC capabilities, reviewed their 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:

1. MPLS site-to-site Managed VPN – *Smart, superior performance for all your apps*

Consolidates all of your business applications onto a single private network with up to five Classes of Services, built-in security and a wide selection of access technologies for maximum performance and flexibility.

2. IPSec Site-to-Site VPN – *Secure connectivity for companies with 5 or less sites*

Securely connects all 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 assure data security. Offers the widest selection of access technologies.

3. Remote IPSec VPN – *Secure client-based remote access*

Offered in conjunction with MegaPath's Site-to-Site MPLS VPN service and capable of seamlessly 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 which securely maps the traffic into your MPLS VPN.

4. 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 without the need to buy or manage a remote access system – and with no client software to install. A proven, cost-effective solution for secure mobile access.

5. Hybrid VPN solutions

One can use a hybrid MPLS/IPsec VPN in which 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 one 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 and the tools to ensure proper authentication and access controls.

• • •

Next steps

To learn more about MegaPath MPLS network solutions, go to:

<http://www.megapath.com/vpn-security/mpls-site-to-site-vpn/>

• • •

About MegaPath Inc.

MegaPath is the leading provider of managed IP communications services in North America. MegaPath leverages its wide selection of broadband connectivity, Virtual Private Networks (VPN), Voice over IP (VoIP) and security technologies to enable businesses to lower costs, increase security and enhance productivity. Organizations of all sizes can easily and securely communicate between their headquarters, branch offices, retail locations, mobile workers, and business partners.



1-877-MEGAPATH • www.megapath.com

555 Anton Boulevard, Suite 200 • Costa Mesa, CA 92626

© 2010 MegaPath Inc. Duet is a service mark of MegaPath Inc. All other trademarks are property of their respective owners. (04/2010)

