Why the Distributed Enterprise Should Consider Multi-circuit WAN VPN Solutions versus Traditional MPLS
Table of Contents

Introduction ................................................. 3
Cost .................................................................... 4
Network Availability ..................................... 4
Quality of Service ........................................... 6
Security .......................................................... 7
Real Life Scenario .......................................... 8
About the Author ............................................. 9
About iPpass MNS ........................................... 9
About iPpass ................................................... 9
The Next Generation Network
Why the Distributed Enterprise Should Consider Multi-circuit WAN VPN Solutions versus Traditional MPLS

Introduction
When considering a Next Generation Wide Area Network (WAN), enterprises have their own unique business challenges, evolving demands and specific requirements that combine to impact their decision. Distributed enterprises, those companies with several hundred or even several thousand branch offices, or retail/business locations, have larger network challenges to consider. In order to meet these challenges, today’s distributed enterprises find themselves with two primary WAN options for consideration: MPLS or an Internet IP VPN solution. While MPLS has been a popular solution for many companies in recent years, the tremendous growth in IP applications and evolving demands for Internet bandwidth is forcing distributed enterprises to look for alternative, scalable and more cost effective solutions. In a typical MPLS WAN, all traffic is passed between branch locations and the main headquarters location. This traffic includes data that is specific to the applications running at the corporate headquarters, but it also includes traffic destined for the Internet. Today, most distributed enterprises are experiencing a huge growth in Internet traffic. IDC forecasts that Internet-generated traffic on fixed networks will continue to grow, increasing approximately 50 percent year over year.

There are two primary drivers for this growth in Internet traffic. First, is the increasing usage of online cloud applications, such as customer relationship management, collaboration and information-sharing services. Second, is the increase in video traffic triggered by the growing amount of online video content available, and the growing number of connected devices such as surveillance cameras and webcams. According to Cisco, over 50 percent of the traffic over the Internet today is video, with the total Internet traffic expected to quadruple by 2014. This same report forecasts that in the next five years, IP traffic generated by Wi-Fi and mobile devices will increase from 45 to 61 percent, exceeding wired IP generated traffic.

Historically, a distributed enterprise needed just 300 to 500 kilobits per second to connect each branch location. For most distributed enterprises, MPLS service over a fractional T1 has been an affordable solution. Today, Internet traffic requires broadband connectivity of several megabits per second. If distributed enterprises want to increase their MPLS WAN bandwidth to support their growing Internet traffic, it would increase their monthly MPLS service fee by 300-400 percent. As a result, many businesses are rethinking their WAN solution and looking for an alternative to MPLS.

iPass MultiLink Connect is an alternative WAN solution to MPLS. MultiLink Connect provides improved availability, higher bandwidth, encrypted security, and more network flexibility at a fraction of the cost of MPLS. For many distributed organizations, moving to MultiLink Connect means that their bandwidth increases from hundreds of kilobits per second to between 5-20 megabits per second. In other words, these branch locations experience a 200-300 percent increase in bandwidth for a lower monthly fee. This bandwidth increase is generally sufficient to cater to the increased usage of cloud services, Wi-Fi growth and expanding video content.

This paper will discuss four major considerations when comparing MPLS and Multi-circuit WAN IP VPN solutions; cost, network availability, quality of service and security. Further, it will explain how a Multi-circuit WAN IP VPN solution is the most flexible, scalable, and highest value option to meet the growing bandwidth demands that will be required by next generation enterprise networks.

**Cost**

A distributed enterprise has several branch locations that connect to applications hosted at the central headquarters. For example, a company may have several thousand offices that need to access a centralized application to get quotes, submit orders or query payments. For many distributed organizations, the branch location may only have a few employees, but it is critical to their business that they can access corporate applications in real-time. When a business location is unable to process transactions because their WAN is down or suffering performance problems, this can have a direct and negative impact on their operations, productivity and revenue.

Dedicated point-to-point circuits provide both high reliability and guaranteed bandwidth, but they are prohibitively expensive. **MPLS, like the Internet, is a shared network** and is therefore less expensive than dedicated circuits. The cost for an MPLS connection is typically based on the bandwidth required, Quality of Service (QoS), guaranteed availability, and the length of the contract. There may also be additional cost items such as security services and IP multicast. In general, distributed enterprises pay $300-600 US dollars per megabit of data for an MPLS service.

When comparing the cost between MultiLink Connect and an MPLS service, consideration needs to be given to both the cost of deploying multiple broadband connections and the cost per megabit of the WAN service. iPass customers have found that they can get broadband Internet connections at a fraction of the cost per megabit of an MPLS connection. Figure 1 compares the cost of MPLS with the cost of Internet broadband delivered over cable and fiber connections.

![Figure 1: Comparison of MPLS and broadband Cost per Mbps](image)

**Network Availability**

There are several factors that go into network availability and much of that relies on core network characteristics and last mile network characteristics. **MPLS is a protocol and does not inherently support high availability.** Network availability over MPLS is provided through Service Level Agreements (SLA) with the network service provider based on underlying network technology type and core network, not the MPLS protocol itself. **These are most often the same as Internet Broadband SLA’s.** The SLA guarantees that a network technology has certain characteristics and that a technician will be on-site to resolve problems in a specified time period. Concerning the core network, the Internet is inherently reliable in the sense that if one connection fails, the IP packets are automatically routed in another direction. **When comparing an MPLS service with other broadband Internet technologies, both have similar availability statistics for the core network.**
The most common source of network outage in both an MPLS and a broadband Internet network is not the core network; it is problems with the last mile access link between the business location and the service provider’s core network. To be considered ‘highly available’ a network must achieve 99.99 percent availability.

MPLS service providers deliver MPLS over T1 or Dedicated Access Circuits along with Service Level Agreements (SLA). T1 technology is not inherently stronger than other internet technologies. In other words, the T1 connections used for MPLS have identical physical network characteristics to the T1 connections used for IP VPN, except that they are accompanied by a team of technicians that can be on site within hours of a problem being detected for resolution. This is the primary reason why MPLS networks are more expensive than other broadband connections. Today, there are alternative technologies and network designs that can deliver a lower cost and high performing network.

**MultiLink Connect is an IP VPN solution** that provides WAN connectivity between central and remote sites over the public Internet. It uses two or more connections between the branch and the public Internet. These connections are typically Business Cable, 3G/4G cellular, DSL, Fiber, Ethernet, or a traditional T1. The use of multiple access circuits is illustrated in Figure 2, where the corporate headquarters is connected to a typical branch office location. In this figure, the blue and red lines illustrate primary and secondary IP VPN tunnels.

![Figure 2: MultiLink Connect Solution](image)

MultiLink Connect achieves higher availability than typical MPLS networks by providing two or more access circuits along with automatic real-time failover specifically designed for the MultiLink solution. In other words, if the primary access link fails, traffic is automatically sent over the ‘always-on’ secondary link. **The MultiLink Connect solution delivers higher availability than an MPLS network.** In addition, the enterprise does not need to wait for the technician to arrive on site during failure. With two active circuits available in the MultiLink Connect architecture, bandwidth management and application traffic shaping can be supported over both high speed circuits vs. throttling network traffic over a single slow speed MPLS last mile circuit.

MultiLink Connect, by providing an automatic failover between multiple broadband connections, is able to leverage **higher bandwidth solutions at a fraction of the cost of an MPLS service while achieving the same or higher availability.**
Quality of Service

Every MPLS service provider has a different approach to packaging and selling MPLS services. MPLS adds labels to data packets to distinguish between different classes of traffic. This enables the MPLS service providers to offer different QoS levels. The higher class of MPLS service is typically more expensive. For example, a gold class for high priority and low latency traffic, a silver class for guaranteed delivery, and a bronze class for best effort Internet traffic.

Distributed organizations that use MPLS will map their applications to specific service classes. In an environment where the demand for bandwidth is growing, many businesses will reserve part of their MPLS bandwidth for critical legacy applications and voice connections. This puts strain and restrictions on the performance of newer online cloud services, which are often mapped to a lower service class.

Moving to a high bandwidth Internet solution removes the need to reserve bandwidth for specific legacy applications. Even though sending data over the public Internet on an IP VPN tunnel does not guarantee quality of service end-to-end, businesses are realizing that the increase in available bandwidth gives them a new advantage. This additional bandwidth reduces the network capacity constraints that previously required them to implement quality of service profiles. Internet bandwidth simply outpaces the need to prioritize and classify – there is more bandwidth than traffic available, so there is no need to throttle at the edge in the right MultiLink configuration.

MultiLink Connect does provide prioritization at the network edge. It provides a programmable QoS solution on the edge of the network and prioritizes the order that packets are sent out over the circuits between the branch and the Internet. In this way, critical application packets such as voice and legacy applications can be sent before anything else if there is packet contention at the site itself.

iPass provides the ability to monitor the performance and availability of the WAN using the iPass VantagePoint provisioning and management platform and portal. Figure 3 illustrates how MultiLink Connect works with iPass VantagePoint. iPass VantagePoint statistics show that a combination of prioritization at the network edge and broadband Internet access gives the same quality of service experience for headquarters applications as legacy MPLS networks. MultiLink Connect can also provide additional monitoring services targeted specifically to Voice over IP (VoIP), application flow monitoring, and web services for enhanced end-to-end network transparency and visibility.
Security

Security is always a key decision point for any network architecture. Enterprises need to ensure that their sensitive data remains private and secure. However, enterprises are starting to investigate intelligent architectures to offload internet traffic directly to the internet from the edge to save money, improve performance, and maintain a strong security posture to counter viruses, Trojans, and other malicious attacks.

MultiLink Connect forms secure encrypted VPN tunnels between the branch and headquarters locations. Each multi-link connection encrypts the traffic using 256 bit AES encryption. Key distribution can be done using either preshared keys or a hosted PKI infrastructure.

Another advantage of MultiLink Connect is that it allows Internet traffic to be sent directly to the Internet, avoiding the need to route through the headquarters location. If all Internet traffic from the branch is sent through the headquarters location, it means that Enterprises need to be equipped to handle the decryption and routing of this growing traffic demand through their core security systems. It also creates general performance degradation at the edge. This requires a significant investment in ingress bandwidth and concentrator processing at the headquarters location. These costs can be avoided if Internet bound traffic is sent directly between the branch and the Internet.

Finally, to address the concerns regarding the branch being exposed to security vulnerabilities such as viruses when allowing direct internet access, MultiLink Connect can provide iPass Secure Extend, an integrated cloud-based Secure Web Gateway (SWG) platform. This is illustrated in figure 4.

Facts

MPLS does not inherently implement encryption
The SWG solution filters both incoming and outgoing traffic to ensure that it conforms to a company’s specific security policies set by the administrator through the cloud platform management console. The SWG also provides the ability to identify and actively remove potentially harmful traffic from entering the corporate network using a combination of real-time and signature-based methods. In addition, usage is fully logged and is available for real-time alarms and historical reports. The SWG allows the Enterprise to define and enforce their preferred traffic security policies for all branch locations. It also allows multiple policies per location to be applied.

**Real Life Scenario**

In 2010, a Fortune 500 company was evaluating their Next Generation WAN. As a distributed enterprise with several thousand branch offices across North America, they were receiving complaints from their field sales team about slow response times when entering orders and making online queries. The company was using a dedicated 256 kilobit per second private network solution between the branch locations and the central data center.

The IT department analyzed the problem and found large spikes in Internet traffic, particularly when video content was being downloaded. The IT department also observed that the sales teams were increasingly using their personal tablets and smart phones to access email and collaborative cloud applications. These usage changes were causing the network to be overloaded, and resulted in the sales team experiencing performance problems and delays when they connected to the headquarters systems to complete orders.

After analyzing the data, the IT department recommended implementing compression and video transrating techniques at the edge of the network. Even though compression reduced the traffic load, it was insufficient to address the bandwidth demands, and the sales team still experienced network delays and performance issues. The enterprise recognized that they needed to upgrade their WAN.

After an extensive trial of both MPLS and MultiLink Connect, the enterprise decided to deploy MultiLink Connect. Each branch deployed two broadband connections that depending on availability were cable, DSL, 3G, Fiber, or Internet T1. For example, most branches opted to deploy cable as their primary connection and DSL as the secondary connection. To keep costs to a minimum, they elected to deploy the primary connection at the desired higher data rates, and deploy a secondary failover connection at a lower data rate. They also took advantage of the iPass VantagePoint operational management and security architectures to safely route traffic from each branch office directly to the Internet.

The reason this Fortune 500 Company elected to deploy MultiLink Connect instead of MPLS was because it supported the current and projected growth in network traffic at a lower operational cost, while maintaining high availability and quality of service. The MultiLink Connect VPN solution delivered ten times more bandwidth and reduced annual network operational costs by more than 50 percent versus the proposed MPLS system. Their cost per megabit is literally a fraction of the cost of their legacy network.

The client’s system has been successfully running for since 2010. Network statistics show network availability and uptime is over 99.99 percent exceeding expectations. The desired quality of service levels have been achieved, performance is no longer a problem, and the sales teams’ satisfaction has greatly improved. The business benefits and long-term network scalability and flexibility of MultiLink Connect have made this distributed enterprise more effective, profitable, and successful in the market.
About the Author
Dr. Avril Salter is an award-winning IT and network researcher, consultant and instructor. She has over 20 years of experience working with major corporations and startups, and is a co-founder of Next Direction Technologies; a leading provider of network consulting and education solutions.

About iPass MNS
The Managed Network Services division of iPass delivers customized internet-based wide area and Wi-Fi networking solutions for the enterprise. iPass runs a state-of-the-art IP VPN Management Platform to remotely manage large enterprise-grade networks and deliver the security, availability and performance required today. iPass has relationships with over 200 internet broadband access providers, to provide a wide variety of high speed technologies delivering 100 percent coverage for its customers.

MultiLink Connect is available today. Additional information is available at http://www.ipass.com/mns
Contact us here or via telephone (866) 801-6930 or via email at mns@ipass.com

About iPass
iPass helps enterprises and telecom service providers ensure their employees and subscribers stay well connected. Founded in 1996, iPass delivers the world’s largest commercial-grade Wi-Fi network and trusted connectivity platform. With more than 780,000 Wi-Fi hotspots across 120 countries and territories, iPass gives its customers always-on, frictionless connectivity anywhere in the world – simply, securely and cost-effectively.

Additional information is available at www.iPass.com or on Smarter Connections, the iPass blog.