White Paper:
Replacing Expensive MPLS

New business realities demand
NEW NETWORK THINKING.

If a company is operating an MPLS network between branch locations, it is likely paying too much. Equinox Secure provides the benefits of an MPLS network at a much lower cost with higher bandwidth, better redundancy, improved security, better reliability and superior application and service expansion. This whitepaper will attempt to clarify these issues by offering a comprehensive definition of MPLS and the business benefits an Equinox Secure solution can bring.

What is "MPLS"?

The evolution of enterprise networks over the last thirty years have followed a cycle of migration from varied technologies ranging from digital private lines and X.25 in the 1980s, to Frame Relay and some SMDS in the mid-1990s. In the late 1990s, ATM networks began to be adopted, but quickly began to be replaced by Internet VPNs and MPLS in the early 2000s. The underlying driver for these changes have largely been cost reduction, but not at the expense of compromising network security or reliability. In fact, each of these technology evolutions had one common element, they were all private networks that were either completely distinct from the public Internet or carved out a private network over the public Internet. Internet VPNs have proven to be complex and costly to maintain, so currently the preferred private network has become MPLS (Multi-Protocol Label Switching).

MPLS is attractive to many enterprises because it is much like a bridging service that uses short labels versus IP addressing, it is adaptable to a variety of network access services (private line, Frame Relay, ATM, IP and DSL), and extends its connection from LAN-to-LAN or private circuit to private circuit. MPLS operates much like an Internet VPN network without the public exposure and the complexities of deterministic IP addressing. MPLS offers the benefits of a private network with the additional benefits of enabling classes of service which allow for the integration of multiple traffic types onto a single physical network.

Strengths of MPLS

MPLS provides a private network architecture that keeps corporate traffic distinctly separate from the public Internet. MPLS network connections between offices act much like a LAN to LAN network, with the distinct exception of the connection speed between the locations. MPLS can utilize a variety of private access connections which makes its adaptability very strong, although the majority of connections are private T1 circuits which start at 1.544 Mbps, but can scale to faster connections through adding extra bonded T1 services. MPLS provides a network architecture that is relatively easy to maintain because of its abbreviated addressing methodology. And finally, MPLS

can integrate multiple traffic types by tagging packets with different cueing priorities. This allows for more sensitive traffic types such as VoIP to be integrated with less sensitive traffic types such as basic http Internet traffic. But, unless you are actually integrating multiple traffic types on a single connection, this may not be an advantage because it adds complexity.

Limitations of MPLS

MPLS requires expensive network routers in order to facilitate and administer the network. Typically Cisco 28xx and 29xx routers are used to facilitate MPLS networks, which are the most expensive routers in their class. As a result, the cost of each new site deployment is significant due to the equipment cost and its associated support contracts and software licenses. This does not even account for the costs of designing, configuring, implementing and operating your MPLS network.

MPLS requires significant complexity in configuration of the network as IT staff must maintain explicit configurations within every router. The larger the network scales the more exponential the complexity becomes because of the point-to-point star topology nature of the network. The complexity burden also carries with it the cost of hiring expensive technicians which commonly require Cisco certifications. Cisco certified technicians are very expensive, scarce, and difficult to retain without matching ever increasing competitive salaries. The more traffic types consolidated onto the MPLS network, the more advanced the technician base needs to be, the greater the complexity and the higher the overhead of operating the network becomes.

If Cisco equipment is used in a network, then one is probably paying significant license fees for support and network management applications. Cisco support programs are costly additions that tend to be overlooked in the total network cost evaluation. In addition, one needs to examine the costs of network management programs that allow administration and management of the network.

MPLS predominately uses expensive T1 circuits which are bandwidth limited. MPLS can use a variety of network access methodologies, but T1 comprises the largest percentage of all access circuits used. This is because Frame Relay and ATM services are being phased out by ILECs and priced to facilitate their retirement. ILEC and CLEC metro Ethernet services provide significant bandwidth benefits but are typically limited in availability to office parks and high density areas, therefore their ubiquity is limited, and they are still expensive and priced to compete against expensive T1 services. DSL access to MPLS is used in some cases, but the perception of DSL instability has limited its acceptance, and the special nature of layer two DSL services command a higher price. As a result, T1 has been the access method of choice, but it is very expensive, and is cost linear in its scalability.

The bandwidth limitations of T1 services diminish the value of MPLS's multi-service capabilities. T1 services provide 1.544 Mbps symmetrical (upstream and downstream) speeds, which is about one-fifth of the average downstream speed of a DSL circuit. Purchasing additional T1 circuits and bonding them together has a linear cost curve as discussed above, so many MPLS networks simply use a T1 connection at remote branches. This bandwidth limitation resulting from the ineffective cost model of MPLS T1 also limits the usefulness of the service to integrate multiple traffic types, because there is not enough bandwidth to support multiple applications effectively. Therefore, one of the primary benefits of MPLS, multi-service support, is diminished. This relegates MPLS to be a very expensive VPN network that is only slightly easier to maintain than Internet VPNs services, albeit more secure.

MPLS Displacement

MPLS is a technically attractive service with significant advantages over private lines, Frame Relay, ATM and Internet VPNs facilitated in many-to-one star topologies, or many-to-many mesh topologies. The fundamental issue with MPLS is it is based on an unsustainable cost structure when faced with the economic realities of a competitive marketplace.

MPLS is typically priced at $300 to $600 per Mbps per month for the copper connectivity typically deployed at all but the very largest enterprise locations, while the monthly price of broadband connectivity is now $1.50 to $15 per Mbps per month. Broadband Internet service costs roughly $50 to $200 per month, and the bandwidth available is in the range of 3 Mbps to 150 Mbps. Examples include FiOS 150 Mbps downstream for $199.99 a month from Verizon, or the more widely available XFINITY Internet at 105 Mbps downstream for $199.95 a month from Comcast.

Fiber MPLS connectivity at customer premises is typically in the $60 to $200 per-Mbps-per-month range, while fiber Internet connectivity at a customer location is typically half that, and high-bandwidth Internet connectivity at a collocation facility is typically down around $10 to $20 per Mbps per month, and you even see it advertised for under $2 Mbps per month in some cases.

The reality is that for most distributed enterprise, or branch-centric enterprises, copper is the predominately available alternative, and the difference in pricing between MPLS and public broadband is becoming increasingly hard to justify. The reasons that keep enterprises from adopting public broadband are several, but Equinox Secure has eliminated those barriers allowing for a dramatic cost reduction alternative.

The Client Approach

Our client faced this exact issue and had to determine the best approach to address how to reduce its cost structure for delivering services to its 300 plus branches. The client had hundreds of thousands of dollars invested in its MPLS network, and faced continued high costs when opening each new store. This was inhibiting the client's growth and lengthening the breakeven of each new store investment. It was also increasing corporate overhead through increasing network and IT staff costs, and it was seriously taxing profitability. The IT budget could not continue to grow at the same rate it had been growing for years, and adding more IT staff in order to administer the network was not an acceptable budget request. The client had to find a way to reduce the costs of its current IT services approach.

The client decided to go out to bid to see if other carriers could provide the same MPLS solution for a lower cost. It found only a handful of carriers could serve its entire nationwide footprint, as the balance of the providers could only serve specific geographic regions. Of the carriers that could meet its needs, the client found some to be more expensive, but some could reduce its costs by about 5

Payment Processor   Client Datacenter

Remote Cisco 2800
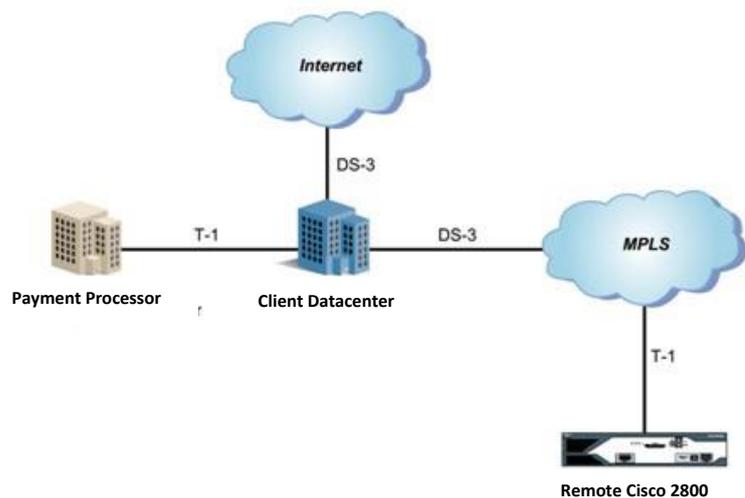
percent, including its incumbent carrier who just lowered its price to keep the business. This would not "move the needle" anywhere near where it needed to go. The client decided to issue a Request for Information (RFI) in order to get educated on alternative options.

Through the RFI, the client learned about Equinox Secure, which took a completely different approach to solving the client's issues it had been asking for. Equinox Secure had already been adopted by many of the largest global retailers, so it offered a proven approach as opposed to a concept. Equinox Secure used a combination of a cloud based security model combined with a secure application appliance on the branch premise. Equinox Secure had a compelling architecture, and appeared through initial price requests to significantly "move the cost needle" in the right direction.
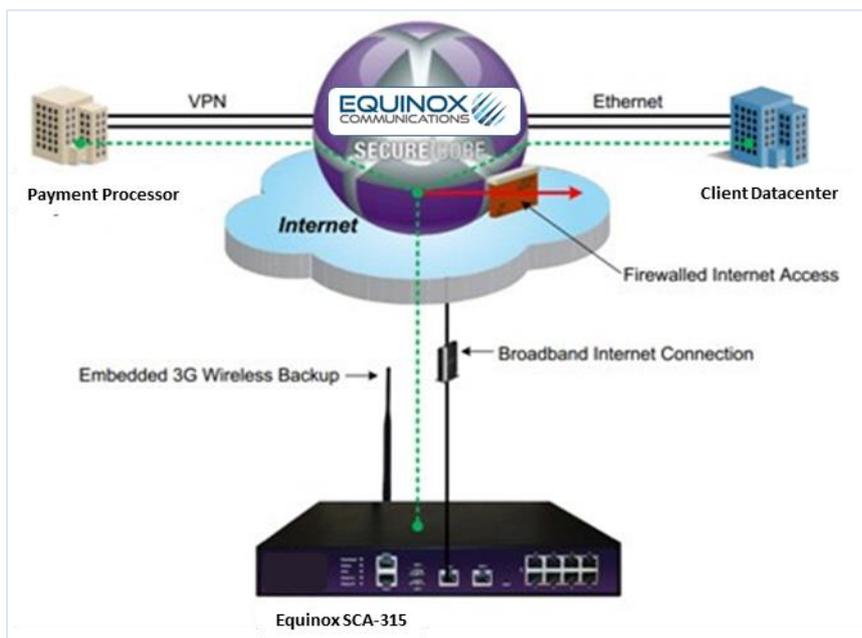
Several areas needed to be evaluated to validate the Equinox Secure approach, not the least of which the company would have to scrap its significant investment in Cisco routers and it did not want to accept a lower level of security. In addition, any new approach the client took needed to be able to facilitate new applications and services for its branches, which was the breaking point it faced on MPLS. The client knew that adding new T1s at each branch to address the current bandwidth limitations was not going to be acceptable. Thus, the client evaluated Equinox Secure on the following criteria:

- **Was Equinox Secure network security comparable to MPLS?** – Much like the MPLS network, Equinox Secure eliminated the need for public IP addressing at each site. It provided a completely secure overlay network, with MPLS at its core that kept the client's network invisible to hackers. Each branch is integrated into hosted VPN concentrators located in multiple data centers across the country with secure gateways to credit card processors, the client's corporate data center and even to POS equipment providers enabling secure remote support. Hosted firewall, intrusion detection, content filtering and complete network logging & retention applications provided an efficient and secure method of reducing the current network complexity. Equinox Secure provided equal security as MPLS, just without all the complexity.

- **Would Equinox Secure provide affordable bandwidth expansion?** – Equinox Secure allowed the client to embrace local public broadband options without the security concerns of using public IP addressing. The Equinox Secure unique VPN architecture eliminated the local public

IP from the corporate network altogether. This technological advancement opened the door to adopting more affordable and higher bandwidth options. It eliminated the costly T1 costs and the associated backhaul costs the company incurred to many of its second and third tier markets. Our client could now increase its bandwidth at its branches from 1.5 Mbps to 7 Mbps up to 30 Mbps depending on the local service options.

- **Was Equinox Secure able to meet reliability requirements?** – Public broadband options certainly offered an attractive economic option, but the client was concerned about downtime associated with broadband. Downtime was very costly to sales and was not acceptable. But Equinox Secure provided an integrated 3G/4G failover function that included an "always-on" persistent VPN over the wireless backup connection. Therefore, if broadband failed, services would automatically failover to the wireless connection providing a level of diversity that the current MPLS network did not provide.

- **Could Equinox Secure improve Application & Service Expansion**? – Using a combination of hosted applications and premise server based applications allowed for the expansion of new services and applications in a flexible and cost effective manner. With Equinox Secure, the client would deploy a network appliance with an embedded Intel Linux server fully integrated into the same network security appliance. As a result, applications with smaller memory footprints could be deployed locally at the store location. Applications such as Payment, Loyalty and POS Support could be housed on a single device that was already secure. These applications could be deployed and maintained centrally, and future applications could be downloaded when needed. A secure WiFi hotspot capability was also integrated into the secure appliance so future WiFi enabled applications could be deployed at any time. The use of a single application and security appliance would place the client on solid footing to enable future services that would meet emerging business needs.

- **Does Equinox Secure maintain compliance requirements?** – If card transactions were to be placed on public broadband, the client had to be able to demonstrate compliance with all PCI security requirements. Transactions to be secured locally and in transit to the card processors, and all access to the POS system had to be logged and monitored. If the point-of-sale system provider needed to remotely log into the system to update software or fix a problem, the technician had to be authenticated and all of his actions logged. The penalty for falling out of compliance could cost the client thousands of dollars a day. To address this issue, the secure logging and data retention capabilities of Equinox Secure would be used to monitor all events on the network and maintain a database of network logs to demonstrate compliance if audited. This capability was integrated in the solution from the start.

- **Would Equinox Secure reduce the cost of new site deployment?** – This is where the client could not believe the differences in costs between its current MPLS model and Equinox Secure could be deployed for a fixed cost of $450 per site, versus the almost $6,000 fully loaded cost of an MPLS implementation. Equinox Secure could be installed by branch personnel easily, eliminating the costs of expensive technicians. The cost of the Equinox Secure SCA-315 was a fraction of the cost of the Cisco 28xx series routers currently being used, and only one device was required per site. All devices were pre-configured by Equinox and shipped to the site. Once installed, the store's SCA-315 device would pull down configurations from Equinox's secure cloud and be operational in less than 15 minutes. Not only did this completely collapse the current cost structure, it cost justified the replacement

of all the existing equipment which could then be resold.

- **Would Equinox Secure reduce monthly operating costs across all sites?** – Eliminating the expensive and bandwidth-limited T1 architecture supporting T1 MPLS and the costly extended backhaul to tier 3 and 4 towns provides significant monthly operating cost reductions. With the Equinox Secure security and redundancy architecture, the client could now embrace public bandwidth options, eliminating the mileage sensitive T1 services and expanding bandwidth. But savings are also found in the elimination of the expensive Cisco IOS and SmartNet services, as Equinox Secure provides a managed service with an operating system and many aspects of support included in the monthly price. Even further monthly operating costs reductions were achieved by a less intensive use of the 3G wireless services, as Equinox Secure does not force a protocol dependent fail-over requirement that drives up 3G bandwidth usages.

The MPLS versus Equinox Secure Business Case

The business case for comparing the alternatives of low bandwidth T1-based MPLS or Equinox Secure with a 7 Mbps DSL solution requires a comparison of both the monthly recurring costs and the initial one- time costs. Each solution is also equipped with a 3G wireless back-up solution for equivalent comparison of reliability.

Cost Element	MPLS Cost - T1 Plus 3G	Equinox Secure Cost - 7 Mbps DSL w/ 3G
Recurring Costs	$350.00	$59.95
Primary Circuit Extended Access Cost (Avg)	$225.00*	$00.00
Back-Up Circuit Cost	$10.00 - 3G	$10.00 - 3G
Back-Up Circuit Usage Cost	$135.00 (15 Gbps)**	$40.00 (1 Gbps)***
Basic Security Package Cost	Integrate Equipment Purchase	$24.95
POS Support App Cost	NA	$7.95
Loyalty App Cost	NA	$7.95
Total Recurring Costs	**$720.00**	**$110.80**

Cost Element	MPLS Cost - T1 Plus 3G	Equinox Secure Cost - 7 Mbps DSL
Non-Recurring Costs		w/ 3G
Equinox Secure Appliance	NA	$450.00
Cisco 28xx/29xx	$1,700.00	NA
Cisco 53xx Switch	$1,200.00	NA
Cisco 1131AG Access Point	$600.00	$600.00
3G Wireless Cradle Point	$149.99	NA
Cisco IOS	$250.00	NA
Cisco SmartNet	$175.00	NA
Installation	$1,500.00	NA
Total Non-Recurring Costs	**$5,574.99**	**$1,050.00**

* Average of extended access backhaul costs across all stores with some stores requiring no extended access and others requiring

significant extended access backhaul.

** 3G use as a primary back-up capability required the use of a load balancing protocol to run over the 3G connection at all times resulting in high extended usage of 3G service.

*** Equinox Secure 3G implementation requires limited usage of the circuit except in failover mode, reducing usage charges.

Savings Analysis

Equinox Secure Versus	Monthly Savings	% Savings	Upfront Savings	% Savings
T1 MPLS Plus 3G	($609)/Mo.	85%	($4,525)	81%

Monthly Savings

Equinox Secure was 85 percent less than the current costs of operating the limited bandwidth T1 MPLS connection offering only 1.544 Mbps in bandwidth. The monthly recurring savings alone provided enough justification to consider the existing Cisco investment as a sunk cost and opt to replace existing locations with Equinox Secure. Since the customer could leverage the existing Cisco Wireless Access point with the Equinox Secure solution, the only new capital costs required to achieve the savings was a fixed $450 per site. This made the decision to switch fairly easy because there was a payback in month one, and the savings after month one went straight to the bottom line.

New Site Deployment Savings

Equinox Secure reduced the costs of deploying a network site solution to a new store opening by over $4,500 per store providing a shorter investment recovery period to go along with the lower overhead recurring services. In addition, the simplicity of installation reduced the time requirements for configuration and installation on the IT department. These savings when applied across the entire client's footprint would **save an estimated $1.4 million a month** versus the current MPLS solution.

Equinox Secure Versus	Monthly Savings over 300 Stores	Upfront Savings over 300 Stores
T1 MPLS Plus 3G	($182,760)/Mo.	($1,357,797)

Summary

The economics of the Equinox Secure solution were both compelling and obvious. The adoption of Equinox Secure paid for itself through the savings achieved in monthly costs, plus the client would greatly expand its application and new service capabilities. The ability of the Equinox Secure solution to securely use public broadband allowed for the consolidation of all its critical applications onto a single broadband connection with higher bandwidth than MPLS T1. By moving applications that utilized analog lines (such as POS and POS Support), the client achieved even greater savings than depicted above. In addition, the ability to consolidate multiple devices in the stores to a single secure application appliance reduced ongoing support costs, which are also not reflected in the savings analysis. The existing investment in Cisco routers was easy to justify replacing because the savings achieved were so significant. The business case was very clear, and it resulted in a well-

established national restaurant chain to undertake a comprehensive network architecture change, and within an accelerated period of time. **Equinox Secure made the transition simple.**

About Equinox Communications

Equinox Communications delivers critical business and cloud communication solutions nationally through our network relations and own facilities with competitive SLAs, better pricing and award winning customer support. Ask us about our CLOUD and Managed Services and vertical strengths (retail, restaurant, hospitality, finance, medical, etc.). For more information, please visit http://www.EquinoxCommunications.com or call **1.877.344.2474**.