MPLS and IPSec
A Misunderstood Relationship

Jon Ranger, Riverstone Networks

ABSTRACT

A large quantity of misinformation and misunderstanding exists about the place in the Service Provider networks for these two technologies. This document seeks to dispel some of these issues and to show that far from being competing technologies, they are in fact both essential tools for the creation of profit making services. One provider may choose to deliver MPLS Services (or more accurately here MPLS VPN services) and another may choose to use IPSec. This should not be seen as one technology "winning" but as a service provider differentiating itself in a chosen customer base. In fact, many networks today choose to operate these technologies together. Again this decision is only made based on a business model that the provider is working toward. No service provider should make a technology decision without first considering if that technology fits with the overall business plan of the organization.
All service providers exist to make money.

THE MANY FACES OF MPLS

I have taken some time here to briefly explain the history and uses of MPLS today. Much more comprehensive reading material is available; this section seeks to give an overview of how MPLS is used in Service Provider networks.

Multi-Protocol Label Switching emerged from a set of competing, proprietary standards that existed in the early 1990s. The main purpose of MPLS was originally to remove the route look-up overhead required for each packet at each router in the data path. Frames enter an MPLS network, a look-up is performed at the edge of the network and a label is added to the frame as it is forwarded. All hop-by-hop decisions in the MPLS network are done by comparing the incoming label with a table that tells the router which port to send it out of and with which new label attached. The routers at the edge of an MPLS network (known as Label Edge Routers) are the only ones that perform an IP address look-up; all other routers (known as Label Switch Routers) just use the label-forwarding table. As interface speeds began to increase, the software-based routers of the time needed a way to reduce their processing overhead and MPLS was seen as a great way of doing this. However, routers have recently implemented hardware-based routing that allows for full IP address look-up per packet at wire speed. The future for MPLS was uncertain.

Vendors had realized that the uses for MPLS were far more extensive than just performance. The value of adding labels to an IP (or other protocol frame, this is multi-protocol after all) became apparent. The label could be used to differentiate one frame from another — this allows a number of possibilities. Also, advanced development was taking place to allow more than one label to be added to the frame. This led to some interesting new ideas. Some of the uses of these labels are:

- **Traffic Engineering**
- **Tunnelling**
- **VPN Technology**

Traffic Engineering was made possible by the ability to forward frames differently based upon the value of the label in the header. A service provider could use this to create premium, economy, restricted, and preferred routes through their network.

Tunnelling offers a provider the means to aggregate many labels that are being forwarded to the same destination by placing a common "tunnel label" into the frame. The datagram would now have 2 labels, but the Label Switch Routers (LSR) would only forward the frame based on the outer, tunnel label. Traffic engineering can cause an overhead in the network by having to signal each traffic engineered route. Tunnelling, among its other benefits, reduces the signalling and processing overhead of a traffic-engineered path by allowing one path to serve many customers.

VPN technology can be categorized into 2 groups:

- **Virtual Leased Lines**
- **Virtual Private Networks**

Virtual Leased Lines (VLL) are relatively self-explanatory. The concept of a leased line is well known and a large number of customers use Frame Relay, ATM, or PPP as a means of transporting data from one point to another between customer sites. A VLL is "virtual" only because it emulates the service delivered by the previously mentioned technologies. A Label Switched Path (LSP) through an MPLS network is analogous to an ATM PVC or Frame Relay DLCI. The header information marks the datagram as belonging to one or another leased line, whether this is an MPLS label, an ATM VPI/VCI, or a Frame Relay DLCI. So a leased line, whether logical or not, is a means by which traffic is separated by a unique header. Of course as described earlier, if more than one Virtual Leased Line exists between 2 points, tunnelling and traffic engineering can be used to improve CPU performance and to deliver differentiated services. Virtual Leased Lines are typically created today using the Internet draft known as "draft-Martini."

Virtual Private Networks (VPNs) differ from VLLs by virtue of the fact that (in most cases) they are multipoint networks rather than point-to-point networks. The concept, however is the same. The traffic from one customer is separated from another using a unique label. The label is chosen based on the eventual destination of the datagram. As the network is multipoint, a number of destinations are available. The LER will decide, based on its VPN forwarding table, which is the appropriate destination, and therefore which is the appropriate label to add to the datagram. IP VPNs over MPLS are typically built to the RFC 2547-bis standard. RFC 2547 describes a Layer 3 VPN service that relies on the customer sending routing updates to the provider network. These routes create a Virtual Router Forwarding table (VRF). The VRF is shared with the other LERs that have a member of the same VPN attached. This converged forwarding table on the LER then makes the decision on which LSP to send an incoming traffic. Once again, tunnelling and Traffic Engineering are used to add value in the network.

An alternative to the RFC2547-bis standard as described above is coming into prominence. This new Internet draft (draft-lasserre-tls-mpls-00) is a multipoint service offering a Layer 2 VN service. This means that data is forwarded to the appropriate Label Switched Path using the Ethernet Layer 2 header information as discussed when using Virtual Leased Lines. Draft-lasserre again uses a mapping between the incoming Layer 2 header with an MPLS LSP. Each LER will look for members of the same VPN and signal the appropriate paths between the routers.

MPLS, as you can see, is a network technology that provides data separation in an IP topology. By creating paths or a collection of paths, traffic can be separated for the purposes of Virtual Leased Lines, Virtual Private Networks, or for classification into a Traffic Engineered path. These technologies can be combined to create even more service classes. Tunnelling can be added to provide aggregation and also to carry data across another provider's network.

HOW DOES THAT DIFFER FROM IPSEC?

IPSec is an abbreviation of IP Security. This should immediately alert the reader to the first and main difference. MPLS in all its standards does not provide any means to encrypt customer data as it passes through the provider network. This is the sole purpose of IPSec. It has to be said that IPSec is the only technology seen as a viable data encryption service today. None of the leased line services available today (Frame Relay, PPP, and ATM) offer any form of encryption. This fact alone should place in your mind where IPSec and MPLS VPN differ.

The 2 ends of an IPSec "VPN" are configured to exchange an encryption key with their peer "gateway." This is a key point to note — data that passes between gateways is encrypted, whereas data behind the gateway in the "trusted" network in unencrypted. It is the job of the gateway to ensure that the site with which it peers is the appropriate end point of the VPN and to encrypt/de-encrypt data that passes between these peers. It is possible that the gateway could be a PC, server, router, firewall, or dedicated IPSec security device. A PC can peer with a server to ensure that all traffic that passes between them is encrypted; a server can peer with a firewall to ensure that data from all "trusted" users behind that firewall is encrypted.

As the IPSec device can be one of a number of different types, it is feasible that the customer of the service provider will own and manage their own encryption across the links that exist between their sites. These links could be any form of IP data connection, a leased line, a fiber link, or an IP network such as the Internet. One of the main uses of IPSec is to ensure that remote workers can connect to their corporate network in a secure manner across the Internet.

The other option is for the ISP to own and operate a data encryption service. This could be a "network-based" service where the encrypting gateways are located in the provider network. Network-based solutions allow the provider to offer encryption services to multiple customers using a single gateway, but customers must feel confident that the link from the customer site to the provider network cannot be compromised. An alternative is to place smaller customer gateways at the customer premises thus ensuring that traffic is encrypted end to end. These 2 solutions both target a similar market, the small enterprise, and are only differentiated by the level of trust of the last mile network. Large enterprises typically (although not exclusively) do not want a third party to be responsible for the security of their data. The larger an organization becomes the more likely they are to have their own security expertise. These large enterprises still need to buy connectivity and capacity between sites from service providers.

SO WHAT DO I CHOOSE?

The conclusion here is that MPLS VPNs provide no encryption in the same way as traditional L2 service providers that offer Frame and ATM services. This means that there are actually 2 different decisions to make in respect to these technologies.

1. Do we want to compete with the traditional providers of Frame and ATM services?
   Do we want to provide scalable carrier IP Transport services and virtual POP services?
   Do we want to be a high-capacity "large enterprise" carrier with 10mbps to >1Gbps capacity services?

If the answer to one or more of the questions listed is yes, then MPLS has the capability to provide these kinds of services and should be investigated.

2. Do we want to provide data security and encryption services for customers?
   Do we want to provide secure access to the corporate VPN across the public Internet?
   Is our target market the smaller enterprises?

If the answer to these questions is yes then IPSec is the only recognized means for delivering this.

Of course, the answer to both sets of questions could be yes. This, however, requires developing a broad range of services to attack such a large customer base. So the question of MPLS vs IPSec is really not appropriate. The questions that service providers should be asking themselves are "Who are my customers" and "What will they want to buy from me?" The answer may be that they want to buy both Virtual Leased Lines and data encryption, making both technologies appropriate. IPSec however does have a more restricted market, as it typically cannot be sold to large enterprises or other carriers, whereas MPLS services can. Just delivering IPSec across a pure IP network is limited in that it is only point-to-point but is very simple to implement. This simplicity, however, will only drive it quickly towards a point of commoditization.

Acronyms

ACL	*Access Control List*
ANSI	*American National Standards Institute*
ASIC	*Application-Specific Integrated Circuit*
ASP	*Application Service Provider*
ATM	*Asynchronous Transfer Mode*
CBR	*Constant Bit Rate*
CWDM	*Coarse Wave Division Multiplexing*
DS1/DS3	*Digital Signal, Level 1 (1.54 Mbps) or 3 (44.7 Mbps)*
DSL	*Digital Subscriber Line*
DWDM	*Dense Wave Division Multiplexing*
DVMRP	*Distance Vector Multicast Protocol*
E1/E2	*European Trunk 1/2 (2 Mbps/34.3 Mbps)*
ERP	*Enterprise Resource Planning*
HSSI	*High Speed Serial Interface*
ISP	*Internet Service Provider*
ITU	*International Telecommunications Union*
LAN	*Local Area Network*
LEC	*Local Exchange Carrier*
MAC	*Media Access Control*
MAN	*Metropolitan Area Network*
MDU	*Multiple Dwelling Unit*
MLPPP	*Multi Layer Point-to-Point Protocol*
MPLS	*Multiple Protocol Label Switching.* *See "MPLS in Metro IP Networks,"* *http://www.riverstonenet.com/technology/mpls.shtml*
MTU	*Multiple Tenant Unit*
OC-3/OC-12	*Optical Carrier 3/12 (155 Mbps/622 Mbps)*
PDH	*Plesiochronous Digital Hierarchy*
PIM	*Protocol Independent Multicast*
POS	*Packet over SONET*
PPP	*Point-to-Point Protocol*
PVC	*Private Virtual Circuit*
QoS	*Quality of Service*
RED	*Random Early Discard*
SONET	*Synchronous Optical NETwork* *See http://www.techguide.com/comm/sec_html/sonet.shtml*
SLA	*Service Level Agreement*
SPE	*Synchronous Payload Envelope*
SRP	*Spatial Reuse Protocol* *See RFC 2892*
T1	*Trunk 1 (1.544 Mbps)*
TCP/IP	*Transport Control Protocol/Internet Protocol*
TDM	*Time Division Multiplexing*
UBR	*Undefined Bit Rate*
VBR	*Variable Bit Rate*
VLAN	*Virtual LAN*
VoD	*Video on Demand*
WAN	*Wide Area Network*
WDM	*Wave Division Multiplexing*
WRED	*Weighted Random Early Discard*

Riverstone Networks, Inc.
5200 Great America Parkway, Santa Clara, CA 95054 USA

877 / 778-9595** or **408 / 878-6500** or **www.riverstonenet.com

Printed in the USA

v 1.1 10/01